Im heutigen gesellschaftlichen Umfeld gestiegener Sicherheitsbedürfnisse und postmoderner Rationalitäten werden staatliche Raumüberwachungs- und Informationsverarbeitungstätigkeiten zum Vorgehen gegen Kriminalität zunehmend diskutiert. So wird beispielsweise vorgeschlagen, Profile mutmasslich gefährlicher Personen zu erfassen oder Räume mittels automatisierter Systeme präventiv zu überwachen. Technologien, die derartige Vorgehensweisen ermöglichen sollen, bestehen bereits und werden in hohem Tempo weiterentwickelt. Ihr Einsatz birgt indes grosses Entgrenzungspotenzial, insbesondere auch, weil sich entsprechende gesetzliche Regelungen noch wenig ausgebildet haben.

Eine strafrechtstheoretische, kriminologische Auseinandersetzung mit dem staatlichen Einsatz derartiger Technologien ist daher angezeigt. In der vorliegenden Untersuchung arbeitet Jann Schaub die Materie aus verschiedenen Perspektiven auf, indem er sich an den Fragen orientiert, inwieweit der Einsatz dieser Technologien realisierbar, nützlich, rechtlich zulässig und gesellschaftlich wünschenswert ist.

ISBN 978-3-258-07932-5

Haupt

18

Schaub Postmoderne Kriminalitätsbekämpfungstechnologien

Haupt

Schweizerische kriminologische Untersuchungen 18

Jann Schaub

Postmoderne Kriminalitätsbekämpfungstechnologien

Informationsverarbeitung, Registrierung und Überwachung als Instrumente des Vorgehens gegen Kriminalität

Haupt

Schweizerische kriminologische Untersuchungen

Band 18

Herausgegeben von Prof. Dr. Karl-Ludwig Kunz, Prof. Dr. Dr. h.c. Hans Schultz †,
Prof. Dr. Martin Killias, Prof. Dr. Mark Pieth, Prof. Dr. M. A. Niggli,
Prof. Dr. Nicolas Queloz und Prof. Dr. Christian Schwarzenegger

Jann Schaub

Postmoderne Kriminalitätsbekämpfungstechnologien

Informationsverarbeitung, Registrierung und Überwachung als Instrumente des Vorgehens gegen Kriminalität

Haupt Verlag

Jann Schaub, Dr. iur., LL.M., studierte Rechtswissenschaften an der Universität Freiburg i. Üe. und absolvierte den Nachdiplomstudiengang Kriminologie (LL.M.) an der School of Criminology, International Criminal Law and Psychology of Law (SCIP) an der Universität Bern. Er ist als wissenschaftlicher Assistent an der Universität Bern tätig.

Inauguraldissertation zur Erlangung der Würde eines Doctor iuris der Rechtswissenschaftlichen Fakultät der Universität Bern.

Die Fakultät hat diese Arbeit am 19. Dezember 2013 auf Antrag der beiden Gutachter, Prof. Dr. Karl-Ludwig Kunz und Prof. Dr. Jonas Weber, als Dissertation angenommen.

Redaktion und Satzherstellung durch den Autor

1. Auflage: 2015

Bibliografische Information der *Deutschen Nationalbibliothek*

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-258-07932-5

Umschlaggestaltung: René Tschirren
Printed in Switzerland

www.haupt.ch

VORWORT

Aufrichtig danken möchte ich zunächst Prof. Dr. Karl-Ludwig Kunz, der mir viel Freiraum bei der Ausarbeitung und Fertigstellung des Projekts liess und mit wertvollen Anregungen zur Verbesserung der vorliegenden Arbeit beitrug, sowie Prof. Dr. Jonas Weber für seine spontane Bereitschaft, das Zweitgutachten zu erstellen. Lina von Siebenthal (MLaw), Philippe Stocker (MLaw) und Susanne Szarvas (MLaw) danke ich herzlich für die Durchsicht und Korrektur, Dr. phil. Sandra Matteotti für das kritische Lektorat der Arbeit. Ich möchte zudem allen Kolleginnen und Kollegen am Institut für Strafrecht und Kriminologie der Universität Bern sowie der Berner Graduiertenschule für Strafrechtswissenschaft (BGS) für die vielen interessanten Gespräche und hilfreichen Anregungen danken. Ein besonderer Dank gilt schliesslich meinem Bruder und meinen Eltern, die mir stets unterstützend zur Seite standen und ohne die dieses Projekt nicht möglich gewesen wäre.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

a. A.	anderer Ansicht
AB	Amtliches Bulletin der Bundesversammlung
Abs.	Absatz
ADABTS	Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces
AGVE	Aargauische Gerichts- und Verwaltungsentscheide
AJP	Aktuelle Juristische Praxis
Art.	Artikel
AS	Amtliche Sammlung
ASBO	Anti-social behavior order
Aufl.	Auflage
AwR	Anwaltsrevue: Publikationen des Schweizerischen Anwaltsverbandes
BAZ	Basler Zeitung
BBC	British Broadcasting Corporation
BBl.	Bundesblatt der Schweizerischen Eidgenossenschaft
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGH	Bundesgerichtshof (Deutschland)
BJ	Bundesamt für Justiz
BK	Beschwerdekammer
BKA	Bundeskriminalamt
BPI	Bundesgesetz über die polizeilichen Informationssysteme des Bundes vom 13. Juni 2008 (SR 361)
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (SR 780.1)

BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BVerfG	Bundesverfassungsgericht (Deutschland)
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVR	Bernische Verwaltungsrechtsprechung
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (SR 120)
ca.	circa
CaS	Causa Sport
CCC	Chaos Computer Club
CCTV	Closed Circuit Television
CILIP	Bürgerrechte & Polizei
CNBC	Consumer News and Business Channel
Co.	Compagnie
CODIS	Combined DNA Index System
CORDIS	Community Research and Development Information
CR	Computer und Recht
CROMATICA	Crowd Management with Telematic Imaging and Communication Assistance
CSS	Center for Security Studies der ETH Zürich
DAP	Dienst für Analyse und Prävention
DARPA	Defense Advanced Research Projects Agency (Behörde des Verteidigungsministeriums der Vereinigten Staaten)
ders.	derselbe
DETECTER	Detection Technologies, Counter-Terrorism Ethics, and Human Rights
dies.	dieselbe, dieselben
diesbzgl.	diesbezüglich

digma	digma. Zeitschrift für Datenrecht und Informationssicherheit
Diss.	Dissertation
DNA	Desoxyribonucleic acid (Desoxyribonukleinsäure)
DNA-Profil-Gesetz	Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen vom 20. Juni 2003 (SR 363)
DPI	Deep Packet Inspection
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
DSM-V	Diagnostic and Statistical Manual of Mental Disorders V
DuD	Datenschutz und Datensicherheit
E	Entwurf
E.	Erwägung
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (Europäische Menschenrechtskonvention; SR 0.101)
et al.	et alii
etc.	et cetera
ETH	Eidgenössische Technische Hochschule Zürich
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWHC	High Court of England and Wales
f./ff.	und folgende (Seite/Seiten)
FACTS	Factual Analysis Criminal Treat Solution
FBI	Federal Bureau of Investigation
FBO	Football Banning Order

fedpol	Bundesamt für Polizei
fMRT	funktionelle Magnetresonanz-Tomografie
Fn.	Fussnote(n)
FRGC	The facial recognition grand challenge
FRS	Facial Recognition System
FRVT	Face Recognition Vendor Test
GAMMA	GAMMA = polizeiliche Datenbank zu Sportveranstaltungen
gen.	genannt
gg.	gegen
gl.A.	gleicher Ansicht
gl.M.	gleiche Meinung
GPDel	Geschäftsprüfungsdelegation der Eidgenössischen Räte
GPS	Global Positioning System
GVP	St. Gallische Gerichts- und Verwaltungspraxis
HOOGAN	HOOGAN = Informationssystem des Bundesamtes für Polizei fedpol
HRRS	Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
HRW	Human Rights Watch
HUMABIO	Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis
IAO	Information Awareness Office
IEEE	Institute of Electrical and Electronics Engineers
INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment

INEX	Converging and conflicting ethical values in the internal/external security continuum in Europe
insb.	insbesondere
IP	Internet Protocol
IPbpR/CCPR	Internationaler Pakt über bürgerliche und politische Rechte vom 16. Dezember 1966 (SR 0.103.2) = International covenant on civil and political rights
i.S.	in Sachen
ISA	Schweizer Informationssystem Ausweisschriften
ISIS	ISIS; Staatsschutzinformationssystem
ISIS-V	Verordnung über das Staatsschutz-Informations-System vom 1. Januar 2002 (SR 120.3)
i.V.m.	in Verbindung mit
JANUS	JANUS; Informationssystem der kriminalpolizeilichen Zentralstellen des Bundes
JANUS-V	Verordnung über das Informationssystem der Bundeskriminalpolizei vom 15. Oktober 2008 (SR 360.2)
JZ	JuristenZeitung
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
LeGes	Mitteilungsblatt der Schweizerischen Gesellschaft für Gesetzgebung (SGG) und der Schweizerischen Evaluationsgesellschaft (SEVAL)
lit.	litera
LSE	London School of Economics
m.E.	meines Erachtens
MATRIX	Multi-State Anti Terrorism Information Exchange
MEP	Member(s) of the European Parliament
MisPel	Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendatei

MPI	Max-Planck-Institut
N.	Randnote(n)
NDG	Nachrichtendienstgesetz
N. J.	New Jersey
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NvWZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht (München – Frankfurt am Main)
NZZ	Neue Zürcher Zeitung
OGH	Oberster Gerichtshof (Österreich)
OPPAGA	Office of Program Policy Analysis & Government Accountability
P2P	peer-to-peer
PG Chur	Polizeigesetz der Stadt Chur vom 24. Februar 2008 (Churer Rechtsbuch 411)
PolG Bern	Polizeigesetz des Kantons Bern vom 8. Juni 1997 (Bernische Systematische Gesetzessammlung 551.1)
PolG Zürich	Polizeigesetz des Kantons Zürich vom 23. April 2007 (Loseblattsammlung 550.1)
QB	Queen's Bench Division (England and Wales High Court)
RAF	Rote Armee Fraktion
resp.	respektive
RK-NR	Rechtskommission Nationalrat
S.	Seite

SAMURAI	Suspicious and abnormal behaviour monitoring using a network of cameras and sensors for situation awareness enhancement
SIM	Subscriber Identity Module
SIPOL	Sicherheitspolitischer Bericht
SIS	Schengen Information System
SMS	Short Message Service
SNS	Social Network Services
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
StV	Strafverteidiger
SZIER	Schweizerische Zeitschrift für internationales und europäisches Recht
SZK	Zeitschrift für Kriminologie
TalibanV	Verordnung über Massnahmen gegenüber Personen und Organisationen mit Verbindungen zu Usama bin Laden, der Gruppierung „Al-Qaïda“ oder der Taliban vom 2. Oktober 2000 (SR 946.203)
TCP/IP	Transmission Control Protocol/Internet Protocol
TKÜ	Telekommunikationsüberwachung
TRECVID	Text Retrieval Conference – Video Retrieval Evaluation
UAV	Unmanned Aerial Vehicle
UNO	United Nations Organisation
USA	United States of America
usw.	und so weiter

VAwG	Verordnung über die Ausweise für Schweizer Staatsangehörige vom 20. September 2002 (SR 143.11)
VE	Vorentwurf
ViSOR	Violent and Sex Offender Register
VoIP	Voice-over-IP
VOSTRA	zentrales Strafregister Schweiz
VOSTRA-V	Verordnung über das automatisierte Strafregister vom 1. Dezember 1999 (AS 1999 3509)
VPB	Verwaltungspraxis der Bundesbehörden
vs.	versus
VVMH	Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und das Informationssystem HOOGAN vom 4. Dezember 2009 (SR 120.52)
WEF	World Economic Forum
WSIPP	Washington State Institute for Public Policy
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZRP	Zeitschrift für Rechtspolitik
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

EINLEITUNG

Die vorliegend thematisierten postmodernen Kriminalitätsbekämpfungstechnologien werden in einem Umfeld entwickelt und eingesetzt, das geprägt ist von gesellschaftlichen Unsicherheitsgefühlen und einem daraus resultierenden „heissen Klima“ in der Kriminalpolitik[1]. Die Thematik staatlicher Überwachungsmassnahmen, steigender Sicherheitbedürfnisse und der zunehmenden Erfassung von Profilen (mutmasslicher) Straftäter, Störer, Abweichler, Auffälliger und nicht zuletzt des Durchschnittsbürgers ist aktuell. Davon zeugt alleine schon die fast tägliche, breite Rezeption in den Medien. Die Problematik wurde auch im Fachdiskurs erkannt und teilweise intensiv besprochen. Eine sorgfältige Auseinandersetzung mit den Konsequenzen der postmodernen Sicherheitslogiken, Strategien und Technologien scheint unerlässlich. Oftmals läuft diese aber entweder in Expertenrunden oder in diesbezüglich vielfach polemisierenden und unkonstruktiven politischen Debatten ab. Erkenntnisse aus Ersteren dringen relativ spärlich an die Öffentlichkeit oder werden von dieser zuweilen ignoriert, insofern sie nicht spannend inszeniert oder intuitiv verständlich vermittelt werden. Letztere, politisierte Diskussionen über postmoderne Kriminalitätsbekämpfungstechnologien, drehen sich nicht selten um Mythen und Hoffnungen[2], um (scheinbar) drängende Bedürfnisse, technische Möglichkeiten und öffentliche Akzeptanz[3] oder um Effizienzabwägungen[4]. Die Technologien der Kriminalitätsbekämpfung werden begleitet von – sicherlich teilweise auch gut und ehrlich gemeinten – Versicherungen, diese würden (schon) nicht missbraucht werden oder sie fänden nur beschränkt auf bestimmte Bereiche erheblicher Bedrohungen und

---

1 LOADER/SPARKS, S. 2, 17 und 85.

2 „Aber meine Hoffnung gilt dem Computer als einem gesamtgesellschaftlichen Diagnoseinstrument. Das ist eine Prävention neuen Stils, die letztlich auch die Terrorursachen aufhebt, diesen Staat verrückt, ihn andersartig gestaltet, Gleichheit und Gleichrangigkeit im Prozess und in der Ökonomie schafft.“ (Horst Herold, ehemaliger Präsident des deutschen Bundeskriminalamts, im Interview bei COBLER, S. 40).

3 „Efforts to prevent governments from collecting such information are doomed to failure because modern threats increasingly require that governments collect it, governments are increasingly able to collect it, and citizens increasingly accept that they will collect it” (CHESTERMAN, S. 4).

4 „I’m not going to get more money. I’m not going to get more cops. I have to be better at using what I have, and that’s what predictive policing is about […]“ (Los Angeles Police Chief Charlie Beck auf <www.predpol.com>).

kriminelle Subjekte Anwendung – der Durchschnittsbürger jedenfalls habe von ihnen nichts zu befürchten. Oftmals halten sie ursprünglich kommunizierte Intentionen nicht ein, *können* sie nicht einhalten. In der heutigen Zeit, in welcher sich die Grenzen zwischen Wirtschaft, Politik, Medien und ihren Interessen mit dem Strafrechtskomplex im weiteren Sinn und *dessen* Interessen zusehends verwischen, entstehen derartige Versprechen aus einer teils naiven Hoffnung oder sind, problematischer, pures Blendwerk. Richtungsweisend scheinen Sicherheitslogiken, bezeichnend Kommunikationsmuster, die sich auf Sicherheitslogiken stützen, diese zugleich transportieren und festigen. Gesellschaftliche Sicherheitsbedürfnisse verursachen Handlungsdruck, möglichst jedes Mittel gegen Kriminalität einzusetzen. Freilich: Gestillt werden können sie nicht.[5]

Nicht alle postmodernen Kriminalitätsbekämpfungstechnologien vermögen Verbrechen zu verhindern, zumindest nicht immer effizienter und/oder effektiver als konventionelle Alternativen. Einige Einsatzvarianten können eventuell durchaus erfolgreich, das heisst hilfreich, nutzbringend, zweckmässig und relativ grundrechtsschonend angewendet werden. Andere hingegen versagen in mehreren Punkten, zeitigen nur symbolische und höchstens vage Effekte, höhlen Grundfreiheiten aus oder bringen schwerwiegende neue Probleme mit sich. Vielleicht können Mittelwege gesucht werden.[6] Zu beachten ist dabei aber, dass postmoderne Strategien nicht anstreben, Kriminalität zu beseitigen, denn dazu sind sie ohnehin nicht in der Lage, sondern sie zu regulieren, zu managen und nicht zuletzt die Gesellschaft zu lenken. Sie könnten zu einer Karikatur einer Gesellschaft führen. Eine Dystopie wie in GEORGE ORWELLS Erzählung „Nineteen eighty-four" ist aber nicht zu erwarten. Eine steigende Verüberwachlichung führt in der Realität subtiler[7], aber manchmal nicht minder problematisch, zum Beispiel zu Exklusionstendenzen.

Die vorhandenen technischen Möglichkeiten zum Vorgehen gegen Kriminalität sind bereits heute immens vielseitig und entwickeln sich in rasantem Tempo weiter. Zurzeit werden in diesem Gebiet mehrere Projekte und Studien in der EU durchgeführt. Ob indes in der Euphorie der „Goldgräberstimmung"[8] hinsichtlich

---

5 „Fighting terrorism is like being a goalkeeper. You can make a hundred brilliant saves but the only shot that people remember is the one that gets past you." (Paul Wilkinson zitiert in HOWELLS, S. 55).

6 Vgl. NOWAK, S. 43.

7 Vgl. KRASMANN, S. 334.

8 TINNEFELD/BUCHNER/PETRI, S. 51.

immer neuer und potenterer Technologien die für konventionelle Methoden des Vorgehens gegen Kriminalität vorgesehenen Schranken und Grundsätze fortwährend an die neu entwickelten Technologien angepasst und geachtet werden, ist zu bezweifeln. Es scheint wichtig, sowohl für Skeptiker und Kritiker als auch für die Befürworter dieser neuen Entwicklungen, sich fundierte Kenntnisse darüber anzueignen, um ihre Vorteile, drohende (versteckte) Gefahren, Probleme und (ungewollte) Konsequenzen zu erkennen und zu diskutieren. Eine gründliche Auseinandersetzung mit dieser Materie *vor* der Anwendung von neuen Kriminalitätsbekämpfungstechnologien ist damit nicht nur für die Experten, sondern auch für die Gesellschaft angezeigt.

Es gilt daher die Lage und auch kriminalpolitische Erwartungen zu reflektieren, um vorschnelles Handeln zu verhindern. Insbesondere ist nicht nur die Frage zu klären, *was* die Konsequenzen der postmodernen Kriminalitätsbekämpfungstechnologien sein könnten, sondern auch, ob die Gesellschaft mit diesen Konsequenzen *leben will* und *kann*.[9] Fraglich ist somit, inwieweit staatliche Tätigkeiten der Raumüberwachung, der Registrierung und der Informationsverarbeitung realisierbar, nützlich, rechtlich zulässig und wünschenswert sind.

I. Untersuchungsgegenstand

Die vorliegende Dissertation ist eine strafrechtstheoretisch-kriminologische. Ihr Ziel ist der Versuch, eine mehrschichtige Analyse des Komplexes postmoderner Technologien der Kriminalitätsbekämpfung vorzunehmen und deren Problematiken über verschiedene Zugänge darzustellen. Sie hat weder den Anspruch alle verfügbaren Technologien einzubeziehen, vielmehr soll die heutige Lage anhand von ausgewählten Instrumenten kritisch beschreibend und analysierend aufgezeigt werden, noch will sie Handlungsempfehlungen vorschlagen, wenn auch mögliche Alternativen und Lösungsansätze zur Sprache kommen werden.

---

[9] Gl. M. wie Sir Ken MacDonald bei VERKAIK in The Independent Online vom 21. Oktober 2008: „They [the powers of surveillance] will be with us forever. And they in turn will be built upon. We should imagine the world we are creating before we build it. We might end up living with something we can't bear." Ähnlich auch ROTHE, S. 73: „Jeder hat sich also zu fragen, was er, indem er auf diese oder jene Weise handelt, aus sich macht und ob er das zu sein wünscht, was er dadurch wird."

Im Verlauf der vorliegenden Arbeit wird eine mehrschichtige Analyse vorgenommen und Kritik aus verschiedenen Perspektiven zusammengetragen.[10] Dieser Vorgehensweise der mehrschichtigen Analyse mehrerer Technologien bleibt geschuldet, dass für die einzelnen Instrumente platzbedingt keine vertiefte und umfassende Beurteilung in Bezug auf grund- und datenschutzrechtliche Überlegungen angestellt werden kann.[11] Auch hinsichtlich der Technologien ist es nötig, den Untersuchungsgegenstand einzugrenzen: Thema der vorliegenden Arbeit sind postmoderne Technologien der Kriminalitätsbekämpfung.[12] Die Arbeit beschränkt sich dabei auf die Registrierung von Personen, Raumüberwachungs- und Informationsverarbeitungstechnologien.[13]

Der entscheidende Vorteil einer mehrschichtigen Auseinandersetzung mit verschiedenen Kriminalitätsbekämpfungstechnologien unter technischen, rechtlichen und kriminologischen Aspekten liegt darin, dass sie eine Gesamtübersicht ermöglicht. Eine rein juristische Betrachtung und Kritik einer einzelnen Technologie würde den gesellschaftlichen Aspekten des Gegenstandes nicht gerecht werden, da sie nur Teilbereiche erfassen könnte. Postmoderne Kriminalitätsbekämpfungstechnologien werden zunehmend entgrenzt eingesetzt, ohne klare Linien und in einem Umfeld, das zunehmend geprägt ist durch Präventions- sowie Sicherheitslogiken und durch eine Vermischung verschiedener Tätigkeitsberei-

---

10 Vgl. SINGELNSTEIN/STOLLE 2012, S. 153 ff.

11 Zwar werden insb. im Zweiten Teil auch grund- und datenschutzrechtliche Ausführungen angestellt, eine vertiefte Betrachtung der postmodernen Kriminalitätsbekämpfungstechnologien aus diesen Perspektiven wäre indes bei der jeweils angegebenen weiterführenden Literatur nachzulesen.

12 NOGALA 1989, S. 2 f., spricht von „avancierter Technik". M. E. schwingen beim Terminus „postmodern" treffendere Assoziationen mit als bei „avanciert", „aktuell" oder „neu". Wenn „modern" Vergangenheitsumsturz, Gegenwart und Trend bedeutet, steht „postmodern" für den Umsturz der Gegenwart, für die nahe Zukunft und das, was *nach* „modern" im Trend liegt. „Modern" heisst im heutigen Allgemeingebrauch auch ein technisch fortgeschrittenes („avanciertes") Gerät – „postmodern" wäre demnach die nächste Generation der Technologie. Nicht weniger wichtig gilt die Zeit, in der wir leben, als „die Postmoderne". „Postmodern" bedeutet also auch „typisch für unsere Zeit". In diesem Adjektiv sind somit viele Bedeutungsdimensionen, Gegenwart und Zukunft zusammengefasst und es vermittelt ein gutes intuitives Bild davon, welche Methoden die vorliegende Arbeit meint. Vgl. dazu SCHMIDT-SEMISCH, S. 209 f. Fn. 1. Zur Postmoderne, siehe etwa BAUMAN, S. 5 ff.

13 Dazu sind Verdachtsregister, anlassunabhängige Datenbanken (u. a. Vorratsdatenspeicherung), Videoüberwachung des öffentlichen Raums, virtuelle Raumüberwachung (insb. durch „Deep Packet Inspection" und „Government Ware"), Informationsverarbeitungstätigkeiten durch Rasterfahndung und rasterfahndungsähnliche Methoden zu zählen.

che und Rechtsgebiete. Das führt zu Situationen, die rechtlich nicht immer befriedigend zu lösen sind und in denen rechtsstaatliche Prinzipien zuweilen wenig bedeuten und oftmals nicht genügende Schranken zu setzen vermögen. Im Gegenteil können diese entgrenzende Positionen auch stützen, indem die mit ihnen geführte Kritik umgekehrt wird: Fehlt beispielsweise eine gesetzliche Grundlage für eine der Technologien, ist die Lösung, eine solche zu schaffen, naheliegend, womit in der Regel auch etwa dem Datenschutzrecht weitgehend entsprochen werden kann (zum Beispiel, indem Datenverknüpfungen in einer Ermächtigungsnorm erlaubt werden).[14] Wichtig ist doch aber nicht, *dass* die Ermächtigung gesetzlich geregelt ist, sondern die Frage, *weshalb* sie es sein soll oder eben nicht und *wie* die entsprechende Norm allenfalls auszugestalten wäre.

Im Fokus der vorliegenden Arbeit liegen Technologien, die darauf ausgerichtet sind, „der Kriminalität" als Ganzem kämpferisch entgegenzutreten, also Praktiken, die auf eine Verbesserung der Lage, der Situation oder der öffentlichen Räume hinsichtlich Kriminalitätsvorkommen zielen oder gefährliche Personengruppen zu klassifizieren, zu regulieren und zu demobilisieren. Technologien, die lediglich den Einzelnen oder ausschliesslich den privaten Raum[15] betreffen (zum Beispiel elektronische Fussfesseln oder die gezielte Überwachung eines Telefonanschlusses im Ermittlungsstadium eines Strafverfahrens) finden teils Erwähnung, insofern sie einen engen Bezug zum Untersuchungsgegenstand aufweisen, sie werden aber nicht näher thematisiert. Die wesentlichen Abgrenzungsmerkmale für die Auswahl der untersuchten Instrumente waren demnach, dass sie postmodernen Strategien der Kriminalitätsbekämpfung folgen, sie technisiert-automatisiert betrieben werden und darauf abzielen, das Gesamtbild der Sicherheitslage zu verbessern. Besonders untersuchungswürdig sind dabei Kombinationen postmoderner Kriminalitätsbekämpfungstechnologien und -strategien. Diese transformieren sich andauernd, sollen vielseitig mehrere Zwecke erfüllen

---

14 Siehe dazu SINGELNSTEIN/STOLLE 2012, S. 153 ff.; NOGALA 1998, S. 178.

15 Wobei in der vorliegenden Arbeit den Begriff des öffentlichen Raums sehr offen verstanden wird, siehe unten Erster Teil, Kapitel II.A. Auch sonst wird keine allzu geschliffen scharfe Typisierungen der einzelnen Instrumente vorgenommen. Die hier vertretene Meinung ist, dass die untersuchten Methoden zu vielseitig und ambivalent in ihren Funktionen und Zwecken sind, um sie sinnvoll klaren Kategorien zuzuordnen. Das stellt gerade das Hauptproblem ihrer rechtlichen Beurteilung dar. Auch unzureichend beschreibende Begriffe wie bspw. „Terrorist", „Verdächtiger" oder „Bedrohung" sind Teil der postmodernen Strategien, diese sind geprägt von unklaren Begrifflichkeiten. Diese Begriffe werden deswegen im Folgenden öfters bewusst vage verwendet, um die Problematik zu verdeutlichen.

und durch sie könnten weitläufige Kontrollapparate errichtet werden, mit denen es sich in Zukunft möglicherweise zu arrangieren gilt.

Beschäftigt man sich mit der zunehmenden Überwachung der Gesellschaft, sieht man sich einer kaum zu bewältigenden Flut an wissenschaftlicher Literatur gegenüber, vor allem aus Grossbritannien und den USA. Aufgrund der Aktualität fanden sich bis zur Fertigstellung der vorliegenden Arbeit zu jedem dieser Teilthemen immer wieder neue Literatur und Materialien, welche möglicherweise spannende Vertiefungsansätze dargeboten und allenfalls neue Perspektiven eröffnet hätten. Um den Rahmen der vorliegenden Arbeit nicht zu strapazieren, musste aber irgendwann eine Linie gezogen werden und es konnte nicht allen diesen Quellen nachgegangen werden. Der Thematik liegen zudem einerseits sehr aktuelle, flüchtige Fragestellungen und Ideen zugrunde, andererseits solche, die seit über 30 Jahren immer weiterentwickelt werden (zum Beispiel die Technisierung des Vorgehens gegen die Kriminalität[16]) oder aus vergangenen Tagen wiederbelebt wurden (zum Beispiel das anlagebetonte Kriminalitätsmodell CESARE LOMBROSOS). Insofern ist es auch durchaus möglich, dass sich die im Folgenden angesprochenen Problembereiche, beispielsweise durch technischen Fortschritt, in kürzester Zeit lösen – oder aber verdichten. Trotzdem oder gerade deswegen scheint eine grundsätzliche Diskussion postmoderner Kriminalitätsbekämpfungstechnologien und deren Einordnung in den gesellschaftlichen und kriminalpolitischen Kontext interessant. In den letzten Jahren hat sich in diesem Bereich viel getan. Viele neue Strömungen und Ansätze versuchen sich den folgenreichen Problemen der postmodernen Kriminalitätsbekämpfung anzunähern, sie zu kritisieren oder sie zu stärken. Die sich daraus ergebende Situation ist es wert, unter neuen Aspekten betrachtet zu werden. Zudem steht die heutige Gesellschaft anscheinend kurz davor, weitgehend automatisierte Überwachungstechnologien einzusetzen.

II. Untersuchungsaufbau

Neben der Einleitung und dem Schlusswort gliedert sich die vorliegende Arbeit in vier Hauptteile: Auf eine Darstellung des Stands der Technik, entsprechender rechtlicher Grundlagen und der nächsten Technologiegeneration (Erster Teil), folgen Gedanken aus rechtlicher Perspektive (Zweiter Teil) und kriminologische

16 Siehe etwa die von NOGALA 1989 aufgezeichneten Ansichten und Debatten aus dieser Zeit.

Überlegungen (Dritter Teil). Im letzten Teil sollen die Ergebnisse der vorangegangenen Teile zusammengeführt und weiterentwickelt werden (Vierter Teil).

Nach den einleitenden Bemerkungen zur Vorgehensweise werden in der Einleitung erste Abgrenzungsversuche vorgenommen, die eine Annäherung an den Untersuchungsgegenstand ermöglichen, im Laufe der Untersuchung indes einer vertieften Betrachtung bedürfen und zuweilen revidiert werden müssen. In einem ersten Schritt werden die vorliegend thematisierten postmodernen Kriminalitätsbekämpfungstechnologien in verschiedene Tätigkeitsbereiche eingeordnet. Danach wird ein allgemeiner, kurzer Überblick über einschlägige Grundrechte gegeben. Zudem werden einige grundlegende Begriffe aus dem Bereich virtueller Räume und des Datensammelns erklärt.

Der Erste Teil gibt einen Überblick über den Stand der Technik aktueller Verdachtsregister, Raumüberwachungs- und Massendatenverarbeitungstechnologien.[17] Aufgezeigt anhand eines aktuellen Beispiels aus der Praxis (Projekt INDECT), werden anschliessend zukünftig zu erwartende Entwicklungen dargestellt. Die Arbeit beschreibt in diesem Teil ausgewählte aktuelle und zukünftige Technologien. Die Erzeugnisse postmoderner Kriminalitätsbekämpfungstechnologien sind in der Öffentlichkeit zwar zunehmend häufiger wahrzunehmen – die Palette ihrer Möglichkeiten, aber auch ihre vielen Schwachstellen, und die technischen Abläufe der Systeme sind indes weniger bekannt. Vielfach operieren sie im Hintergrund, so dass ausserhalb von Entwicklerkreisen und anwendenden Behörden manchmal nur wenig zugängliche Informationen dazu vorliegen. Eine nutzbringende Diskussion über diese Technologien setzt aber zumindest Grund-

---

17 Der Meinung von FRANCO FRATTINI (ehemals EU-Kommissar für Justiz, Freiheit und Sicherheit) folgend, dass „[w]e need to listen to the technical experts to tell us what is technically feasible. Then we need to listen to experts on fundamental rights to see whether there are consequences of using these technologies […]" (FRATTINI, S. 5). Für den nachhaltigen Umgang mit der Einführung neuer Systeme angebracht wäre es an sich, zuerst den rechtlichen Rahmen zu bestimmen und als unveränderlich zu erklären und erst *danach* und darauf beruhend die rechtlich zugelassenen technischen Möglichkeiten ausfindig zu machen. SZUBA, S. 39 und SIMON D., S. 268, weisen m. E. zutreffend darauf hin, dass einmal ausserhalb eines jeden rechtlichen Rahmens, mit erheblichem Forschungsaufwand und finanziellen Mitteln entwickelte Technologien dazu verleiten, den rechtlichen Rahmen an die technisch vorgegebenen Fähigkeiten anzupassen. Ohne aber zu wissen, was heutige und kommende Technologien zu leisten vermögen, ist schwer zu beurteilen, wo und in welcher Weise angemessene gesetzliche Grundlagen neu zu schaffen sind und wo bereits ausreichende bestehen. Für einen übersichtlichen und nachvollziehbaren Aufbau der vorliegenden Arbeit ist das Vorgehen nach FRATTINI jedenfalls geeigneter.

kenntnisse ihrer Funktionsweise und die Kenntnis einiger Einsatzbeispiele voraus.[18] Auf dieser Basis werden danach, jeweils bezogen auf die ausgewählten Technologien, Bilanzen ihrer Wirksamkeit und Nützlichkeit Schlüsse gezogen und die Rechtslage in der Schweiz dargestellt. Es werden zum einen Vorteile, Nachteile, erfolgversprechende Funktionen und Schwachstellen der einzelnen Technologien angesprochen, zum anderen gesetzliche Grundlagen, auch de lege ferenda, diskutiert.

Die rechtlichen Ausführungen im Zweiten Teil konzentrieren sich auf das Schweizer Recht. Ein Rechtsvergleich mit anderen Staaten wird nicht vorgenommen. In einzelnen Fällen werden jedoch auch internationale Vergleiche heran gezogen. Insbesondere sollen die Erfahrungen, die Normen und die Rechtsprechung von in diesem Bereich weiter fortgeschrittenen Staaten beigezogen werden. Im Rechtsraum Schweiz sind die untersuchten postmodernen Kriminalitätsbekämpfungstechnologien in der Praxis der Kriminalprävention und Strafverfolgung verhältnismässig neu. Entsprechend ermächtigende Bestimmungen werden erst allmählich in rechtliche Erlasse aufgenommen. Einige postmoderne Kriminalitätsbekämpfungstechnologien wurden unlängst höchstrichterlich beurteilt. Anknüpfend an die Ausführungen zu den (teils fehlenden) gesetzlichen Grundlagen im Ersten Teil, werden deshalb im Zweiten Teil rechtliche Problemstellungen und allfällige Lösungsansätze herausgearbeitet. Der Fokus dieses Kapitels liegt darauf, rechtliche Problembereiche von Massendatenverarbeitungstechnologien, Registern, Video- und Online-Überwachungsmassnahmen anhand von ausgewählten Praxisbeispielen zu erörtern, die aktuelle Rechtsprechung darzustellen und erwägenswerte Leitsätze zu diskutieren.[19]

---

18 Die technischen Begriffe und die genaue Funktionsweise der Technologien werden lediglich soweit sie für die rechtlichen und kriminologischen Überlegungen relevant sind und möglichst kurz besprochen. Umfassende technische Ausführungen sind daher nicht zu erwarten. In aller Regel aber wird an den entsprechenden Orten jeweils auf weiterführende Literatur hingewiesen, in welcher der Leser bei Interesse einen guten Einstieg findet, sich in technische Themen zu vertiefen.

19 Zum Beispiel veranlasste das sich laufend an Möglichkeiten und Errungenschaften erweiternde Sortiment des Internets das schweizerische Bundesgericht, das deutsche Verfassungsgericht und den Europäischen Gerichtshof für Menschenrechte einige rechtliche Rahmenbedingungen für staatliche Massnahmen für den virtuellen Raum umzuinterpretieren oder neue Grundsätze zu bestimmen. Insbesondere anhand dieser aktuellen Rechtsprechung werden die ausgewählten Vorgehensweisen und Technologien dargestellt.

Im Dritten Teil werden zu den in den vorangegangenen Teilen bereits angedeuteten Logiken und Problemfeldern kriminologische Überlegungen angestellt. Zunächst wird der kriminalpolitische, gesellschaftliche Kontext skizziert. Anschliessend werden postmoderne Konzepte bezeichnet, welche deren Einsatz auslösen, begünstigen und/oder rechtfertigen. Es wird unter anderem der Zusammenhang zwischen den untersuchten Technologien und hohen Sicherheitsbedürfnissen der Gesellschaft, einfachen postmodernen Erklärungsmustern, Selbstaktivierungsprozessen sowie der Klassifizierung von Risiken diskutiert. In den einzelnen Kapiteln wird zudem immer auch berücksichtigt, ob die untersuchten Themen oder deren Aspekte Antworten auf die Frage nach den möglichen gesellschaftlichen Folgen geben können.

Im Vierten Teil werden die Erkenntnisse aus den anderen Teilen zusammengeführt, zum einen im Sinne einer etwas ausführlicheren Zusammenfassung, zum anderen im Sinne einer Weiterentwicklung der Ausgangsthesen und Gedankengänge. In einem ersten Schritt werden die Funktionen und Möglichkeiten der postmodernen Kriminalitätsbekämpfungstechnologien rekapituliert. Sodann werden weitere Perspektiven diskutiert. Es wird insbesondere auf die fortschreitende Technisierung der Kriminalitätskontrolle eingegangen, auf Logiken postmoderner Kriminalitätsbekämpfungstechnologien, auf mögliche (gesellschaftliche) Folgen, auf den verborgenen sowie verknüpften Einsatz dieser Technologien und auf die bedingte Wirksamkeit rechtlicher Schranken. Es wird erörtert, inwieweit technisierte Rationalitäten das Strafrechtssystem umformen und letztlich, anstatt nur die Kriminalität zu bekämpfen, soziale Kontrolle ausüben.[20] Sodann werden Möglichkeiten kriminologischer Antworten auf die aufgeheizte öffentliche Stimmung hinsichtlich „der Kriminalität“ dargestellt.

III. Erste Abgrenzungsversuche

Die Kompetenzzuweisung, die Zuordnung der technisierten Massnahmen zu einzelnen Rechtsgebieten, die Definitionen der Einsatzform und der Einsatzgebiete postmoderner Kriminalitätsbekämpfungstechnologien – um nur einige Punkte zu nennen – sind zuweilen schwer einzugrenzen.[21] Zunächst werden einleitend einige allgemeine Begrifflichkeiten, soweit möglich, geklärt und Problempunkte

---

20 Siehe SINGELNSTEIN/STOLLE 2012, S. 67; KUNZ 2011, S. 241 ff.

21 Siehe unten Zweiter Teil.

skizziert, die in den anschliessenden Kapiteln ausführlicher beschrieben und diskutiert werden. Um später Wiederholungen zu vermeiden, werden auch einige Bemerkungen zu den Grundrechtsgarantien der persönlichen Freiheit vorausgeschickt. Weitere potenziell betroffene Grundfreiheiten werden nur spezifisch hinsichtlich der jeweiligen Kriminalitätsbekämpfungsinstrumente zugezogen.

A. Einordnung der Kriminalitätsbekämpfungstechnologien

Die innere Sicherheit des Staats wird durch die im allgemeinen Sprachgebrauch als Polizei bezeichnete Institution gewährleistet.[22] Das Polizeiorgan wird untergliedert in die Sicherheitspolizei, welche den Polizeigüterschutz wahrnimmt, und die Gerichtspolizei, welche die Strafverfolgungs- beziehungsweise Justizbehörden unterstützt.[23] Die Aufgabe der Gerichtspolizei beginnt mit der Einleitung eines Strafverfahrens. Deren Tätigkeit unterliegt mithin grundsätzlich dem Strafprozessrecht. Der Aufgabenbereich der Sicherheitspolizei ist grundsätzlich dem Polizeirecht und somit vor allem dem Verwaltungsrecht zuzuordnen.[24] HÄFELIN/MÜLLER/UHLMANN definieren die polizeiliche Tätigkeit wie folgt: „Polizei ist diejenige staatliche Tätigkeit, welche die öffentliche Ruhe und Ordnung, die öffentliche Sicherheit, Gesundheit und Sittlichkeit sowie Treu und Glauben im Geschäftsverkehr durch die Abwehr von Störungen und Gefährdungen schützt."[25]

Die polizeiliche Tätigkeit kann präventiver (*Verhinderung* eines polizeiwidrigen Zustands) oder repressiver (*Behebung* eines polizeiwidrigen Zustands) Natur sein.[26] Polizeiliche Massnahmen unterliegen als eine Form staatlichen Handelns Art. 5 BV[27] (Grundsätze rechtsstaatlichen Handelns) und müssen den Anforderungen von Art. 36 BV genügen, sofern sie in Grundrechte eingreifen. Demzufolge bedürfen Eingriffe einer ausreichend bestimmten und voraussehbaren gesetzlichen Grundlage (Abs. 1), müssen durch ein öffentliches Interesse gerechtfertigt (Abs. 2) und verhältnismässig (Abs. 3) sein, sowie den Kerngehalt der

---

22 Siehe ausführlich zum Polizeirecht MOHLER 2012 und insb. zu den Begrifflichkeiten DERS. 2012, S. 17 ff.

23 ALBERTINI, S. 11 ff.; Bericht SIPOL, S. 67 f.

24 MOHLER 2012, S. 54. Vgl. BGE 136 I 87 E. 3.4. S. 93 f.

25 HÄFELIN/MÜLLER/UHLMANN, S. 558. Siehe aber zu Abgrenzungsproblemen MOHLER 2012, S. 35 ff.

26 HÄFELIN/MÜLLER/UHLMANN, S. 567 f.

27 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

Grundfreiheit unangetastet lassen (Abs. 4).[28] Die Handlungsbefugnisse für den Polizeigüterschutz lassen sich aus zwei Rechtsquellen ableiten: Zum einen aus einer spezifizierten, auf die jeweiligen Anforderungen der Situation abgestimmten, gesetzlichen Grundlage (zum Beispiel in einem kantonalen Polizeigesetz). Konnte eine Situation gesetzlich nicht vorhergesehen werden, erfordert aber trotzdem ein Eingreifen der Polizei, kann diese ihr Handeln zum anderen subsidiär und ausnahmsweise gestützt auf die polizeiliche Generalklausel vornehmen.[29]

Polizeiliche Massnahmen haben weiter das „Störerprinzip" zu beachten, wobei auch davon, um eine akute Gefahr zu beheben, ausnahmsweise abgewichen werden kann.[30] Das Störerprinzip besagt, dass sich eine Massnahme gegen den Verursacher einer Gefahr und in der Regel nicht gegen unbeteiligte Dritte (Ausnahme: Polizeinotstand) zu richten hat. Erfüllt eine Massnahme diese Bedingung nicht, ist sie (meist) ungeeignet, nicht erforderlich oder unzumutbar.[31] Der Europäische Gerichtshof für Menschenrechte (EGMR) hielt dahingehend in einem neueren Entscheid fest, dass polizeiliche Massnahmen, welche in Grundrechte eingreifen, lediglich zielgerichtet, also basierend auf dem Störerprinzip, angewendet werden dürften. Generelle Massnahmen („interdiction imposée de manière générale"), welche neben den potenziell Gefährlichen andere Ungefährliche betreffen, hält der EGMR für unvereinbar mit dem Störerprinzip.[32]

In den letzten Jahren liessen viele neu geschaffene Rechtsgrundlagen zum einen auf Kantons- und Bundesebene, zum anderen auf überkantonaler oder internationaler Ebene (Polizei-Konkordate, völkerrechtliche Abkommen etc.) eine schwer

---

28 MOHLER 2012, S. 55 und 110 ff. Siehe auch BGE 133 I 77 E. 4.1 S. 81; 136 I 87 E. 3.2 S. 91 ff.

29 Siehe dazu MOHLER 2012, S. 247 ff.; HÄFELIN/MÜLLER/UHLMANN, S. 565 ff. Die Anwendbarkeit der polizeilichen Generalklausel wurde jedoch mittlerweile stark eingeschränkt, siehe MOHLER 2012, S. 2 und 247 ff.; zur Kritik an der diesbzgl. bundesgerichtlichen Rechtsprechung, DERS. 2012, S. 249 ff. Vgl. MÜLLER L. 2011, S. 204 mit weiteren Hinweisen.

30 Siehe dazu HÄFELIN/MÜLLER/UHLMANN, S. 569 ff. und 537; MOHLER 2012, S. 232 ff.

31 LIENHARD/HÄSLER, S. 134. Ähnlich MOHLER 2012, S. 233.

32 Entscheid des EGMR Gsell gg. Schweiz vom 8. Oktober 2009, Nr. 12675/05, § 60: „Par ailleurs, selon la jurisprudence du Tribunal fédéral, pour être valables, les mesures limitant la liberté de réunion doivent être ciblées, c'est-à-dire être dirigées contre celui qui est à l'origine du trouble ou de la menace grave qui pèse sur l'ordre public (arrêt précité au paragraphe 31). Or, dans la présente affaire, les autorités cantonales ont omis de faire une distinction entre les personnes potentiellement violentes et les manifestants pacifiques." Vgl. MOHLER 2010, S. 3 f.

überschaubare und unklare Polizeirechtsmaterie entstehen, was unter anderem den Rechtsschutz verschlechterte und zu wenig bestimmt formulierten und schwer vorhersehbaren Eingriffsbefugnissen führte.[33]

Zudem beteiligen sich immer mehr Akteure an den Polizeiaufgaben, beispielsweise private Sicherheitsdienstleister oder das Militär im Rahmen von Assistenzdiensten. Deren Kompetenzen sind schwer zu durchblicken.[34] Abgesehen davon agieren postmoderne Kriminalitätsbekämpfungstechnologien regelmässig in Graubereichen oder Schnittmengen von verschiedenen Rechtsgebieten. Sie können mehreren Zwecken dienen und in mehreren Stadien, oft sowohl präventiv[35] als auch repressiv, eingesetzt werden. Grundsätzlich bestimmt der Verwendungszweck im Einzelfall, wo die Instrumente und die gestützt auf sie veranlassten Folgemassnahmen einzuordnen sind. So unterstehen (geheime) Überwachungsmassnahmen grundsätzlich dem anwendbaren Polizeirecht, wenn sie nicht der Strafverfolgung dienen.[36] Zuweilen greifen die verschiedenen Zwecke der Techniken aber derart stark ineinander, dass sie kaum sinnvoll nur *einem* Gebiet zugeordnet werden können. Ihnen kommt insofern eine Doppelfunktion zu, was insbesondere in der Praxis Abgrenzungsschwierigkeiten verursachen kann.[37] Diese stellen deshalb ein Problem dar, weil jedes der Rechtsgebiete auf unterschiedlichen rechtlichen Grundlagen beruht, welche den Anwendern jeweils unterschiedliche Befugnisse zugestehen und Pflichten beziehungsweise Schranken auferlegen.[38] Beispielsweise beansprucht das Datenschutzrecht zwar in der Regel Geltung für die Bereiche der Prävention und der verdachtsforschenden Datenbearbeitung (Aufdecken noch unbestimmter, geplanter Straftaten)[39], ansonsten gilt das Datenschutzrecht im Strafverfahren aber grundsätzlich nicht.[40] Im Strafver-

---

33 MOHLER 2012, S. 4 f., 56 ff. und 372.

34 MOHLER 2012, S. 57 f. und 85 f.

35 Zu verschiedenen Arten der Prävention, siehe GRAS, S. 16 ff.; NOGALA 1989, S. 27 f.; MÜLLER L. 2011, S. 27 f.; LINGG, S. 32 f.; ZEHNDER M., S. 25 jeweils mit weiteren Hinweisen.

36 RHYNER/STÜSSI, S. 464.

37 BÜLLESFELD 2002, S. 91 f.; MÜLLER L. 2011, S. 28 ff.; PETRI, G N. 525; RHYNER/STÜSSI, S. 465; ROGGAN 2009, S. 260; STEGMANN A., S. 202 und 206 f.; THIEL, S. 51; VOLKMANN, S. 218; ZSCHOCH, S. 15 f. Vgl. BGE 136 I 87 E. 3.4 S. 93 f.

38 Zu den unscharfen Grenzen und der immer stärkeren Verschränkung und Vermischung der Rechtsgebiete, siehe unten Zweiter Teil, Kapitel I.I.

39 Siehe TROCHSLER-HUGENTOBLER/LOBSIGER, S. 329 mit Hinweisen.

40 Art. 2 Abs. 2 lit. c des Bundesgesetzes vom 10. Juni 1992 über den Datenschutz (DSG; SR 2315.1). Das DSG des Bundes gilt grundsätzlich nur für Bund und Private, ansonsten kommen die kantonalen Datenschutzgesetze und allenfalls besondere Datenschutzbestimmun-

fahren wahren andere Prinzipien, unter anderem die Unschuldvermutung[41], die Grundrechte des Betroffenen.[42]

B. Persönliche Freiheit

In der neuen Bundesverfassung ist die persönliche Freiheit in verschiedenen Garantien normiert. Die Teilgehalte sind voneinander abzugrenzen, so schützt etwa Art. 10 Abs. 2 BV die persönliche Freiheit im engeren Sinn. Bis dahin beruhte die Garantie der persönlichen Freiheit auf der schöpferisch entwickelten Rechtsprechung des Bundesgerichts.[43] Die diesbezüglichen bundesgerichtlichen Feststellungen und Überlegungen können indes immer noch zur Auslegung beigezogen werden. Geschützt sind nach bundesgerichtlicher Rechtsprechung „nicht nur

gen in Abkommen etc. zur Anwendung, siehe dazu weiterführend MOHLER 2012, S. 371 ff. Siehe weiterführend zum Datenschutzrecht BELSER/EPINEY/WALDMANN; ausführlich zum Datenschutzrecht bzgl. Videoüberwachung MÜLLER L. 2011, S. 31-95. Für einen Überblick über die kantonalen Regelungen, siehe RUDIN, S. 283. Das Datenschutzrecht setzt für die Bearbeitung von Personendaten eine hinreichend bestimmte Grundlage (Bestimmtheitsgebot), eine Zweckbindung oder eine gesetzlich legitimierte Zweckänderung und die Verhältnismässigkeit der Massnahme voraus (siehe RUDIN, S. 277 f.; MOHLER 2012, S. 377 f.; PROBST, S. 39). Das DSG kennt zusätzlich zu den normalen Personendaten eine qualifizierte Kategorie „besonders schützenswerter Personendaten" (Art. 3 lit. c DSG; SCHWEIZER 2008, N. 42 zu Art. 13 BV mit Hinweisen auf das kantonale Datenschutzrecht) und den Begriff des Persönlichkeitsprofils, das nach Art. 3 lit d DSG „eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt", bezeichnet (siehe dazu BELSER, S. 1 f. N. 3; PROBST, S. 7; MÜLLER L. 2011, S. 56 f.; AL-FAROUQ ABO YOUSSEF, S. 98). Personendatenverknüpfungen führen zu einem Persönlichkeitsprofil, wenn durch sie mindestens ein „wesentliches Teilbild" der betroffenen Person entsteht (PROBST, S. 25 f. mit weiteren Hinweisen; vgl. auch BELSER, S. 1 f. N. 3).

41 Die Unschuldsvermutung gilt grundsätzlich nur im Strafverfahren. Der Grundsatz der Unschuldsvermutung fliesst aus Art. 14 Ziff. 2 des Internationalen Pakts über bürgerliche und politische Rechte vom 16. Dezember 1966 (IPbpR; SR 0.103.2), Art. 6 Ziff. 2 EMRK und Art. 32 Abs. 1 BV. Er besagt, dass jede Person bis zur rechtskräftigen Verurteilung als unschuldig gilt. Eine Verfügung kann die Unschuldsvermutung verletzen, wenn das Gericht oder die Behörde damit ausdrückt, die betroffene Person sei schuldig, obwohl die Schuld nicht gesetzlich bewiesen ist. Siehe dazu BGE 120 Ia 147 E. 3.b S. 155; HÄFELIN/HALLER/KELLER, N. 865 f. S. 275 f.; VEST, N. 5 zu Art. 32 BV und DERS. N. 13 zu Art. 32 BV: „Sie [die Unschuldsvermutung] verbietet es, einen Tatverdächtigen (öffentlich) als Schuldigen hinzustellen". Blosse Verdachtsäusserungen fallen nicht unter den Schutzbereich dieses Prinzips, siehe BGE 120 Ia 147 E. 3.a S. 155. Zur Unschuldsvermutung bzgl. Videoüberwachung, siehe ausführlich MÜLLER L. 2011, S. 157 ff.

42 TROCHSLER-HUGENTOBLER/LOBSIGER, S. 329.

43 Siehe HÄFELIN/HALLER/KELLER, N. 336 f. S. 113 f.; BGE 133 I 77 E. 3.2 S. 81.

die Bewegungsfreiheit und körperliche Integrität, sondern darüber hinaus alle Freiheiten, die elementare Erscheinungen der Persönlichkeitsentfaltung bilden". Dieser Schutzbereich umfasst den Anspruch auf persönliche Geheimsphäre.[44] Durch staatliches Handeln verursachte negative Auswirkungen auf die persönlichen Verhältnisse des Betroffenen vermögen grundsätzlich in den Schutzbereich einzugreifen. Insbesondere Tatumstände (Motive, der Hergang, die Begleitumstände, Intimitäten oder von der Norm abweichende Charaktereigenschaften), welche in spezifischer Weise die Persönlichkeitssphäre des Betroffenen berühren, können seinem Schutzinteresse ein gewisses Gewicht verleihen.[45] Die persönliche Freiheit kann hingegen nicht gegenüber jedem staatlichen Akt, welcher sich auf die persönliche Lebensgestaltung auswirkt, geltend gemacht werden. Der Schutzbereich ist mithin im Einzelfall, je nach Art und Intensität der Beeinträchtigung, auszulegen.[46] Schwerwiegende Einschränkungen der persönlichen Freiheit sind gemäss Bundesgericht lediglich zulässig, wenn sie sich auf eine „unzweideutige", formell-gesetzliche Grundlage stützen.[47]

1. Menschenwürde (Art. 7 BV, Art. 3 EMRK)

Das Grundrecht der Menschenwürde ist in Art. 7 BV geregelt. Nach bundesgerichtlicher Rechtsprechung hat sie allgemein die Bedeutung eines Leitgrundsatzes für jegliche Staatstätigkeit. Sie bildet als innersten Kern zugleich die Grundlage der Freiheitsrechte, dient deren Auslegung und Konkretisierung und ist Auffanggrundrecht.[48] Die Menschenwürde umfasst das Gebot, „den Menschen als vernunftbegabtes und freies Wesen zu achten, ihn stets als Subjekt des Rechts und nicht bloss als Objekt zu behandeln".[49] Die Einzig- und Andersartigkeit von Menschen ist folglich zu achten.[50]

---

44 BGE 119 Ia 99 E. 2.b S. 101.
45 BGE 119 Ia 99 E. 2.b S. 102 und E. 4.b S. 105.
46 BGE 120 Ia 147 E. 2.a S. 149.
47 BGE 124 I 34 E. 2.b S. 37.
48 BGE 132 I 49 E. 5.1 S. 54. Vgl. MASTRONARDI, N. 22 ff. und 38 ff. zu Art. 7 BV.
49 Häfelin/Haller/Keller, N. 335c S. 111.
50 BGE 132 I 49 E. 5.1 S. 54. Vgl. MASTRONARDI, N. 32 zu Art. 7 BV.

2. Geistige Unversehrtheit, Privatsphäre, informationelle Selbstbestimmung und Datenschutz (Art.10 Abs. 2 und Art. 13 BV, Art. 8 EMRK)

Der verfassungsrechtliche Persönlichkeitsschutz nach Art. 10 BV beinhaltet insbesondere das Recht auf Selbstbestimmung, individuelle Lebensgestaltung und den Schutz der elementaren Erscheinungen der Persönlichkeitsentfaltung.[51] Das Bundesgericht sieht darin eine subsidiäre Grundfreiheit, die zur Anwendung gelangt, wenn kein anderes Grundrecht greift. Art. 13 BV schützt die informationelle Selbstbestimmung, die Privatsphäre und den Datenschutz als selbstständige Garantien und geht Art. 10 Abs. 2 BV in der Regel vor.[52] Art. 13 BV enthält den Anspruch auf Schutz vor Missbrauch persönlicher Daten und auf selbstständige Entscheidung über die Offenlegung der eigenen persönlichen Lebenssachverhalte. Der Betroffene darf darauf gestützt zudem Auskunft und Einsicht in ihn persönlich betreffende Datenbestände verlangen.[53] Nach einem Teil der Lehre können sämtliche staatlichen, mit technischen Mitteln vorgenommenen Überwachungsmassnahmen, auch im öffentlichen Raum, Eingriffe in die informationelle Selbstbestimmung der Betroffenen bedeuten.[54] Jeder Umgang mit personenbezogenen Daten berührt den verfassungsrechtlichen Datenschutz. Dieser grenzt sog. „sensitive Personendaten" nicht wie das DSG von den übrigen Personendaten ab. Jedoch bedürfen Einschränkungen des informationellen Selbstbestimmungsrechts bei sensiblen Personendaten oder Persönlichkeitsprofilen einer besonderen Rechtfertigung im Sinne von Art. 36 BV, und deren Bearbeitung ist in der Verhältnismässigkeitsprüfung sorgfältig zu berücksichtigen.[55]

3. Bewegungsfreiheit (Art. 10 Abs. 2 BV)

Der Teilgehalt der Bewegungsfreiheit garantiert die Freiheit, zu kommen und zu gehen. Nicht nur physische, sondern auch psychische Mechanismen, welche die Bewegung hemmen, fallen unter diese Garantie.[56] Eine Auflage, ein zugewiese-

---

51 BGE 132 I 49 E. 5.2 S. 55 f.; SCHWEIZER 2008, N. 5, 25 und 27 zu Art. 10 BV jeweils mit Hinweisen.

52 BGE 133 I 110 E. 5.2 S. 119; BREITENMOSER, N. 4 und 33 zu Art. 13 BV; SCHWEIZER 2008, N. 39 zu Art. 13 BV mit Hinweisen auf die Rechtsprechung des Bundesgerichts.

53 HÄFELIN/HALLER/KELLER, N. 389 S. 129; SCHWEIZER 2008, N. 45 zu Art. 13 BV.

54 Siehe TROCHSLER-HUGENTOBLER/LOBSIGER, S. 334; BREITENMOSER, N. 13 zu Art. 13 BV.

55 SCHWEIZER 2008, N. 41 und 42 zu Art. 13 BV.

56 BGE 130 I 369 E. 2 S. 373 f.; FLÜCKIGER/AUER, S. 932; SCHWEIZER 2008, N. 23 zu Art. 10 BV („sich nach seinem Willen und ohne staatliche Eingriffe zu bewegen").

nes Gebiet nicht zu verlassen oder ein bestimmtes Gebiet nicht zu betreten, berührt die Bewegungsfreiheit. Wie Art. 13 BV gewährt Art. 10 Abs. 2 BV aber keine allgemeine Handlungsfreiheit.[57]

C. Das Internet und andere virtuelle Räume

Ein Rechner oder Computer ist eine „elektronisch arbeitende Einrichtung, die Probleme dadurch löst, dass sie Daten nach einem vorgegebenen Algorithmus beziehungsweise Programm verarbeitet."[58] Das Internet ist ein „elektronischer Verbund von Rechnernetzwerken."[59] Über das Internet stehen dem Anwender, der sich in der Regel über einen Internetdienstanbieter (Internet Service Provider, ISP) einwählt, verschiedene Dienste zur Verfügung (unter anderem World Wide Web, E-Mail, Diskussionsforen und Internet-Telefonie).[60] Dabei ist es für die folgenden Ausführungen wichtig, zu verstehen, dass Informationen im virtuellen Raum in Datenpaketen transportiert werden.[61]

Als virtuelle Räume sollen für diese Arbeit diejenigen „Räume" gelten, bei denen uns die technische Lösung in Verbindung mit einer angewendeten Überwachungsvariante einen real nicht existierenden Raum vorstellen lässt. Gemeint sind somit Räume, die wir physisch nicht betreten können, hingegen durch eine Übersetzung unserer (beispielsweise sprachlichen) Kommunikation in Datenpakete oder durch die Eingabe von Anweisungen an ein Datenverarbeitungssystem beeinflussen sowie metaphorisch erreichen und durchqueren können.[62]

An der Kommunikation über Kanäle des virtuellen Raums beteiligen sich Nutzer und Dienstleister (auch Anbieter oder Provider genannt). Neben der Abgrenzung

---

57 BGE 132 I 49 E. 5.2 S. 56; HÄFELIN/HALLER/KELLER, N. 353 f. S. 110.

58 Definition gemäss Brockhaus Online, siehe <http://www.brockhaus-enzyklopaedie.de/be21_article.php>. Als alternative Bezeichnungen sind auch „informationstechnisches System" oder „Datenverarbeitungssystem" gebräuchlich, siehe etwa BVerfGE 120, 274 (276); Botschaft BÜPF 2013, S. 2771.

59 BVerfGE 120, 274 (276). Vgl. KLESCZEWSKI, S. 738. Siehe ausführlich TANENBAUM/WETHERALL, S. 80 ff.; TESCHNER, S. 19 ff.; ZIMMER, S. 26 ff. jeweils mit weiteren Hinweisen.

60 Siehe dazu ausführlich: KLESCZEWSKI, S. 738 f.; PERREY, S. 7 ff.; TANENBAUM/WETHERALL, S. 88 ff.; ZIMMER, S. 25 ff.

61 KLESCZEWSKI, S. 738 und ausführlicher COOPER, S. 141-143; FREILING/HEINSON, S. 547-550; TANENBAUM/WETHERALL, S. 88-91; BUERMEYER, S. 155.

62 Diese Definition umfasst somit vor allem die von den diversen Internetdiensten geschaffenen „Räume", die über virtuelle Kanäle ausgetauschte Kommunikation und den Inhalt einzelner informationstechnischer Systeme.

nach Sparten – für die vorliegende Arbeit besonders interessant sind Mobilfunkanbieter und Internetdienstanbieter – lassen sich je nach angebotenem Netzwerk-Dienst Access-, Network-, Hosting- und Content-Provider unterscheiden. Ein Dienstleister kann einen, mehrere oder alle Dienste anbieten und abdecken und demnach einen, mehrere oder zugleich alle Providerrollen ausüben. So bieten Telekommunikationsdienstanbieter beziehungsweise Telekommunikationsnetzbetreiber häufig mehrere Mobilfunk-, E-Mail- und Internetdienste gleichzeitig an.[63] In der Sparte Internet halten, etwas vereinfacht zusammengefasst, die Network-Provider (Netzdienstleister) die Netze für den Datentransport aufrecht, wobei die Access-Provider (Zugangsdienstleister) Nutzern den Zugang ins Internet vermitteln. Content- und Hosting-Provider (Inhaltsanbieter und Hostingdienstleister) stellen selbst Inhalte (eigene oder Dritter) respektive ihren Kunden den Speicherplatz dafür bereit.[64]

D. Datenarten und Datenquellen

Informationstechnologien, worunter die postmodernen Kriminalitätsbekämpfungstechnologien zu zählen sind, gründen auf Informationen, diese wiederum auf Daten.[65] Dementsprechend intensiv wird versucht, durch sie Daten zu sammeln, zu verarbeiten und zu verknüpfen[66], um das kriminalpräventive oder ermittlungstechnische Ziel zu erreichen. Wird von Daten gesprochen, können denkbar viele Arten von Daten gemeint sein, wobei verschiedene Datenarten nicht immer klar voneinander abzugrenzen sind. Zunächst ist eine Unterscheidung zwischen tendenziell schützenswerteren und weniger schützenswerten Daten notwendig: Unter Erstere fallen biometrische und andere personenbezogene Daten, mit welchen beispielsweise bestimmte Spuren an einem Tatort einem Verdächtigen zugeordnet werden können. Unter Letztere fallen andere Daten, welche vorerst keine Rückschlüsse auf Personen, Verhaltensweisen oder Bedrohungen zulassen und möglicherweise erst in einem bestimmten Kontext oder in Verbindung mit Daten aus anderen Quellen ein Bild einer Person ergeben oder

---

63 Bericht EJPD 2003, S. 28 f. Eine Übersicht über verschiedene Netzwerkarten findet sich im Bericht EJPD 2003, S. 30 ff.

64 Bericht EJPD 2003, S. 28 f.; UECKER, S. 5 f. Ausführlich ZIMMER, S. 28 ff. Weitere, spezifischere Bezeichnungen kursieren für die Anbieter einzelner Dienste (Beispiel: Web-Mail-Provider).

65 Vgl. ZEHNDER C. A., S. 13 ff. und 18.

66 Vor allem im Bereich der Datenverknüpfung von frei verfügbaren Informationen im Internet liegt noch viel ungenutztes Potenzial, vgl. PROBST, S. 3.

auf (zukünftiges) problematisches Verhalten hinweisen.[67] Der weiter gefasste Begriff der „anderen personenbezogenen Daten" kann weitgehend der Definition der „Personendaten" des schweizerischen Datenschutzgesetzes entlehnt werden („alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen"). Darunter fallen neben physischen, insbesondere auch psychische Eigenschaften sowie die sozialen und wirtschaftlichen Verhältnisse oder politischen Anschauungen einer Person.[68]

Biometrische Daten sind Daten über all jene äusseren Merkmale, die eine Person als sie selbst kennzeichnen.[69] Allgemein bekannte Vertreter dieser Art von Daten sind beispielsweise die Fingerabdrücke einer Person. Weniger bekannt ist vielleicht, dass auch aufgrund der Gangart einer Person Rückschlüsse auf ihre Identität gezogen werden können. Auch diese personenbezogenen Merkmale sind den biometrischen Daten zuzuordnen.[70]

DUNSTONE/YAGER unterscheiden vier Arten der Speicherung von biometrischen Daten: Speichert das Sensorsystem die biometrische Information, ohne diese weiter zu bearbeiten, handelt es sich um Rohdaten („raw data", „biometric sample"). Werden die Rohdaten für eine bessere Weiterverwendung (zum Beispiel für den Abgleich mit einer Mustervorlage) aufgearbeitet, handelt es sich um markierte Daten („token data", „template interoperability"). Die dritte Gruppe der biometrischen Information bilden die Schablonen- oder Musterdaten („template data"). Sie dienen als Vergleichsmuster. Beispiele dafür sind das Foto und der Fingerabdruck, die für den biometrischen Schweizer Pass gespeichert werden. Sodann werden Zusatzinformationen, die etwa mit den biometrischen Daten intrinsisch verknüpft sind oder die beim Sammlungsprozess nebensächlich erhoben werden, als Metadaten („metadata") umschrieben. Wichtig ist diese Art von

---

67 Dazu mehr im Vierten Teil, Kapitel IV.D.

68 Art. 3 lit. a des Datenschutzgesetzes vom 19. Juni 1992 (DSG; SR 235.1); SCHWEIZER 2008, N. 41 zu Art 13 BV mit Hinweisen.

69 DUNSTONE/YAGER, S. 99, welche vier Bedingungen an die Beschaffenheit eines biometrischen Charakteristikums stellen: Jede Person muss dieses haben (Universalität), es muss bei jeder Person ausreichend unterschiedlich sein (Eindeutigkeit), über die Zeit konstant bleiben (Beständigkeit) und auch mengenmässig gemessen werden können (Erfassbarkeit). Vgl. auch TINNEFELD/BUCHNER/PETRI, S. 441. Die DNA fällt streng genommen nicht unter die biometrischen, sondern unter die sonstigen personenbezogenen Daten, da ihr das Element der äusseren Erkennbarkeit fehlt. Der Einfachheit halber kann sie in der vorliegenden Arbeit trotzdem als biometrische Information gelten. Siehe auch BARTSCH, S. 21 mit Hinweisen.

70 Ebenso können bspw. spezifische Wärmesignaturen der Gesichter von Personen als biometrische Identifikationsmerkmale dienen, siehe INTRONA/NISSENBAUM, S. 19 f.

Daten insbesondere, wenn Probleme beim Abgleich entstehen oder um Ergebnisse besser zu verstehen und zu deuten.[71]

Daten zu sammeln und zu archivieren ist in einer Zeit, in welcher Informationsströme vielfach ungehindert fliessen, auf nahezu unbegrenzt vielfältige Art und Weise möglich.[72] Als Datenquellen bieten sich namentlich die Aufnahmen von Videoüberwachungsanlagen, jede Art von elektronischer Kommunikation und verschiedene öffentliche und nicht-öffentliche Datenbanken an. Daneben sind viele andere Formen der Datenextraktion aus verschiedenen anderen Quellen denkbar.[73] Gemäss Art. 3 lit. g DSG erfüllt „jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind", die Voraussetzungen einer Datensammlung. Für die vorliegende Arbeit soll auch hier grundsätzlich ein weiteres Verständnis gelten, und es sollen somit nicht nur personenbezogene Datencontainer, sondern auch Sammlungen mit vorerst nicht zugeordneten Daten mit den Begriffen „Datensammlungen" oder „Datenquellen" gemeint sein.[74]

E. Data Mining und Algorithmen

Um die Masse an Daten aus diesen verschiedenen Quellen effizient nutzen zu können, müssen potenziell relevante von irrelevanten Daten getrennt werden. Was früher mühsam per Hand abgearbeitet werden musste, erledigen heute Computerprogramme in wenigen Augenblicken. Für diesen elektronisch automatisierten Aussiebprozess hat sich der Begriff „Data Mining" („Datenförderung"; „Bergbau von Daten") eingebürgert. DUNSTONE/YAGER beschreiben diesen Prozess als „[…] the process of searching through large volumes of data in an effort to discover patterns, trends, and relationships."[75] In erster Linie sorgen die Data-Mining-Programme für eine übersichtlichere Darstellung aller vorhandenen Daten und vereinfachen damit dem Benutzer die Analyse der Daten. Diese Daten

---

71 Zum Ganzen: DUNSTONE/YAGER, S. 13 ff.; SKILLICORN 2008b, S. 21 ff.; TINNEFELD/BUCHNER/PETRI, S. 440 ff.; STEINBOCK, S. 9 ff. Zur Datenentstehung im Internet: PERREY, S. 69 f. Vgl. ferner ROSSNAGEL/DESOI/HORNUNG 2011, S. 698; MÜLLER L. 2011, S. 18 f.

72 Vgl. SKILLICORN 2008b, S. 21. Zur (oftmals unscharfen) Abgrenzung von Rand-/Verbindungs- und Inhaltsdaten, siehe ALBRECHT H. J. ET AL., S. 13 ff.; BIENDL, S. 12 ff. und 50; LSE Briefing, S. 10; KURZ/RIEGER, S. 5; PERREY, S. 67 ff. Vgl. OBERHOLZER 2004, S. 59.

73 Bspw. Community-Plattformen im Internet oder Bonuskarten von Supermärkten.

74 Vgl. MOECKLI/THURMAN, S. 1 f.; PROBST, S. 21 f.; MÜLLER L. 2011, S. 58 f.

75 DUNSTONE/YAGER, S. 188. Ebenso MOECKLI/THURMAN, S. 1 f.

fördernden Programme basieren auf Algorithmen, also auf „mathematischen oder logischen Bedingungen für ein Set von Instruktionen".[76] Erst diese Sets von Instruktionen erlauben es einem Computer, übersetzt in Programmiersprache, die *Wahrscheinlichkeit* einer Übereinstimmung der gesammelten Daten mit einer Probe (etwa dem registrierten Fingerabdruck einer bereits einmal straffällig gewordenen Person) oder mit bestimmten Kriterien (etwa bezüglich auffälliger Verhaltensmuster) zu ermitteln.[77].

Computersysteme respektive Computerprogramme vermögen also gesammelte Daten einer mehr oder weniger oberflächlichen Analyse gemäss den vorgegebenen Instruktionen zu unterziehen. Es ist indes zu beachten, dass Programme insbesondere beim Abgleichen von biometrischen Daten nie eine hundertprozentige Sicherheit über die Übereinstimmung zweier Vergleichsproben liefern können.[78] Um eine einigermassen zuverlässige automatisierte Analyse zu ermöglichen, müssen die Vergleichsprobe einen gewissen Qualitätsstandard erfüllen – der Grund, weshalb die neuen biometrischen Schweizer Pässe hohe Anforderungen an die Qualität der Fotovorlage stellen[79] – und die eingegebenen Kriterien beispielsweise das gesuchte Objekt oder die gesuchte Person treffend beschreiben. Systemen, die beobachtete oder erwartete Delinquenz als solche erfassen können sollen, müssen Prädiktoren vorgegeben werden, die abweichendes Verhalten zutreffend beschreiben. Das in dieser Weise zu Kriminalitätsbekämpfungszwecken eingesetzte Data Mining bedarf mithin unter anderem tiefgreifender Forschung in der Erstellung von (möglichst fehlerfreien) Tat- und Täterprofilen, der Verhaltensanalyse und der Voraussage von Tathandlungen.[80] Zudem muss der Algorithmus, das heisst die Instruktion an das System, die vorgegebenen Kriterien korrekt definieren und nicht etwa zusätzlich unerwünschte Kriterien miterfassen. Die gesuchten Eigenschaften müssten also präzise in die Programmiersprache übersetzt werden (können).

---

76 INTRONA/WOOD, S. 180 f. und 185 f. Die detailliert-technische Funktionsweise dieser Programme und einige mathematische Lösungswege können bei Interesse bspw. bei SKILLICORN 2008b nachgelesen werden.

77 Für eine gut verständliche Einführung in die Funktionsweise von biometrischen Gesichtserkennungssystemen, siehe INTRONA/NISSENBAUM, S. 10-20.

78 Vgl. DUNSTONE/YAGER, S. 189.

79 Vgl. dazu das Merkblatt „Kriterien für die Annahme von Fotos für Pässe und Identitätskarten" des Bundesamtes für Polizei, <http://www.schweizerpass.admin.ch/content/dam/data/passkampagne/definitivefotomustertafel220906.pdf>; INTRONA/NISSENBAUM, S. 18 f.

80 Vgl. STEINBOCK, S. 4. Zum Begriff des Profiling, siehe etwa NOWAK, S. 31 f.

ERSTER TEIL:
STAND DER TECHNIK, GESETZLICHE GRUNDLAGEN UND DIE NÄCHSTE GENERATION DER TECHNIK

I. Die Registrierung gefährlicher Personen und die Verarbeitung von Informationen

Eine der ältesten Personenlisten stammt aus dem Jahr 1215. Sie führte alle diejenigen Personen auf, die mindestens einmal im Jahr die Beichte abgelegt hatten und schloss jene, die nicht darauf verzeichnet waren, teilweise vom Erhalt der Kommunion aus.[81] Für den Untersuchungsgegenstand sind an dieser Beichtliste zwei Aspekte interessant: Sie diente der Sozialkontrolle und sie bewirkte, durch die Registrierung der konformen Masse, eine Stigmatisierung und Exklusion der Abweichler aus einem für die Menschen dieser Zeit bedeutenden gesellschaftlichen Kreis. Im Wesentlichen funktionieren die heutigen Verdachtsregister[82] nicht anders, mit dem Unterschied, dass sie umgekehrt Abweichler anstatt konforme Bürger auflisten. Bereits wenig später im 13. Jahrhundert folgten geheime oder auch öffentlich bekannt gemachte juristische Listen diesem heutigen Prinzip, indem (flüchtige) Straftäter registriert wurden, um diese besser fassen zu können und öffentlich zu ächten.[83] Seit dem 18. Jahrhundert wurden sodann in der Schweiz und in Deutschland überraschend umfangreiche Listen von gefährlichen Personen geführt.[84] Schon damals hat man versucht, die Eingetragenen mit quasi-biometrischen Merkmalen zu beschreiben und ihre Verfehlungen möglichst lückenlos aufzuführen.[85] Neu ist indes das Ausmass der Verbreitung und Funktionalität der heute bestehenden und vor allem der in der Entwicklung befindlichen Registersysteme. Diese Neuerungen ergeben sich aus der Digitalisie-

---

81 GROEBNER, S. 51.

82 Siehe dazu gleich mehr.

83 GROEBNER, S. 51 ff.

84 BLAUERT/WIEBEL, S. 38 ff. und insb. 43; GROEBNER, S. 161. Interessanterweise beschrieben einige dieser Listen die Umstände der Straftaten der Eingetragenen wesentlich nachvollziehbarer als viele der heutigen Verdachtsregister (vgl. etwa die „Sulzer Jauner- und Diebesliste von 1784" bei BLAUER/WIEBEL, S. 179 ff.).

85 Siehe BLAUERT/WIEBEL, S. 44; GROEBNER, S. 60 und 172 f. Eine grosse Auswahl an Beispielen findet sich bei BLAUERT/WIEBEL, S. 116 ff.

rung der zugehörigen Daten und der Zugänglichkeit neuer Kommunikations- und Speichermedien. Eine schriftliche Liste war damals nur mühsam zu vervielfältigen und viele Leute konnten sie, mangels Lesefähigkeit, ohnehin nicht benutzen. Die Errungenschaft technisierter Listen und deren digitale Vernetzung scheint somit ein wesentlich effizienteres Instrument zu erschaffen, von dem neben den zuständigen staatlichen Behörden auch die breite Öffentlichkeit profitieren und an deren Durchsetzung sie teilhaben soll.

A. Strafregister

Traditionelle Strafregister und Register, die nachfolgend „Verdachtsregister" genannt werden, sind abzugrenzen: Unterschiede zeigen sich insbesondere in ihren abweichenden Zwecken und Konsequenzen. Bereits die Verwendung von Strafregistern kann problematisch sein.[86] Die Verwendung von Verdachtsregistern kann für Betroffene ungleich stärker einschneidende Folgen haben und scheint wesentlich grössere, nicht immer auf den ersten Blick erkennbare Auswirkungen auf die Gesellschaft in sich zu bergen.

Das Strafregister ist ein Institut, welches mittlerweile überall auf der Welt in sehr ähnlicher Ausprägung vorzufinden ist. Im hiesigen zentralen Strafregister VOSTRA werden auf dem Staatsgebiet verurteilte Personen und im Ausland verurteilte Schweizer aufgeführt (Art. 366 Abs. 1 StGB). Das Bundesamt für Justiz ist zuständig, das elektronische Informationssystem, unter Mitwirkung anderer Bundesbehörden und der Kantone, zu führen (Art. 365 StGB).[87] Aufgenommen werden die Taten der Verurteilten, sofern jene ein Verbrechen oder Vergehen darstellen und eine Massnahme oder Strafe dafür ausgesprochen wurde (Abs. 2 lit. a), oder es sich bei ihnen um eine von einer Verordnung des Bundesrats zu bezeichnende Übertretung handelt (Abs. 2 lit. b). Zusätzlich werden hängige Strafverfahren automatisch erfasst, sobald eine berechtigte Behörde die eingetragenen Straftaten einer Person abfragt und das Anlassverfahren ein Ver-

---

86 Sie sind auch vor einem (geringfügigen) Wandel in Richtung Verdachtsregister nicht gefeit. Vgl. für einen problematischen Punkt GRUBER, N. 8 ff. zu Art. 371 StGB: Privatauszüge sind nicht unbedenklich. Insbesondere die immer weiter verbreitete „freiwillige Pflicht" des Vorzeigens eines Strafregisterauszugs im Rahmen von Art. 371 StGB etwa bei der Bewerbung um eine zivile Arbeitsstelle kann heikel sein, systematisch diskriminierend und eine die Wiedereingliederung erschwerende Brandmarkung für den Eingetragenen bedeuten.

87 GRUBER, N. 1 und 5 zu Art. 365 StGB.

gehen oder Verbrechen betrifft.[88] Die bearbeiteten Daten werden ausdrücklich als besonders schützenswerte Daten im Sinne von Art. 3 lit. c DSG qualifiziert.[89] Die Hauptaufgabe des traditionellen Strafregisters ist es, der Justiz, etwa dem Strafrichter oder der Vollzugsbehörde, einen Ausgangspunkt oder einen Hinweis von vielen für die Beurteilung des (zukünftigen) Verhaltens des Registrierten bereitzustellen (Art. 365 Abs. 2 lit. a-c, e und k StGB). Daneben dient es insbesondere als Grundlage für verschiedene Tätigkeiten oder Bewilligungen, welche einen guten Leumund des Prüflings erfordern (Art. 365 Abs. 2. lit. d und f-i), und erlaubt eine statistische Erfassung der Verurteilungen (Art. 365 Abs. 2. lit. j StGB).

Im Gegensatz dazu fokussieren Verdachtsregister auf die Zielpersonen selbst. Eingetragen wird, wer – aus welchem Grund auch immer – für gefährlich gehalten wird. Zum einen kann dies ein potenzieller oder gar hypothetischer Störer oder Täter sein, also einer, der durch sein (vermeintlich) auffälliges Verhalten zum (mehr oder weniger dringend) Verdächtigen wird[90], zum anderen jemand, der eine Katalogstraftat begangen hat oder anderweitig, etwa durch mehrfaches Begehen von Straftaten, für die Gesellschaft eine Gefahr darstellt oder darstellen könnte.[91] Die eingetragenen Personen sind mithin nicht in jedem Fall effektiv straffällig geworden, sondern stellen eine hypothetische Bedrohung für die Gesellschaft oder den Staat dar. Eine effektive Verurteilung spielt für viele dieser Register höchstens eine untergeordnete Rolle.Von aktuellen Straftätern im engeren Sinne über (mutmasslich) Tatwillige bis hin zu sehr abstrakt verdächtigen Personen (beispielsweise wegen Kontakten zu anderen eingetragenen Personen) können in derartigen Registern somit unterschiedlich typisierte Personenkategorien (nebeneinander) vertreten sein.

Das traditionelle Strafregister unterscheidet sich somit in einem zentralen Punkt von Verdachtsregistern: Es listet Verurteilungen unter dem Namen eines aktuellen Straftäters auf und vermerkt seine Personalien sowie andere ergänzende Informationen in diesem Eintrag. Das Strafregister interpretiert diese Daten jedoch

---

88 Art. 9 lit. h der Verordnung über das automatisierte Strafregister vom 1. Dezember 1999 (VOSTRA-Verordnung; AS 1999 3509); GRUBER, N. 2 zu Art. 365 StGB.

89 Art. 365 Abs. 1 StGB; GRUBER, N. 4 zu Art. 365 StGB.

90 Paradebeispiele: „Hooligans“ und „Terroristen“, welche sich *noch* nichts zu Schulden haben kommen lassen, denen es die beurteilende Stelle aber *zutraut*, sich etwas zu Schulden kommen zu lassen.

91 Anstatt von „Verdachtsregistern“ könnte daher auch von „Registern gefährlich Eingestufter“ gesprochen werden.

nicht. Es ordnet Verurteilte keiner Kategorie, sondern umgekehrt die Verurteilungen einer Person zu. Schwerwiegendere Taten werden nicht hervorgehoben, indem diese zum Beispiel in einem Sonderregister aufgeführt werden. Die beiden Arten von Registern stellen mithin unterschiedliche Informationen bereit. Wie erwähnt, hält das traditionelle Strafregister die Straftaten eines Verurteilten fest, das Verdachtsregister hingegen die Person als solche. Dahinter liegt ein konzeptuell grundlegend unterschiedlicher Zugang, der zur Folge hat, dass die beiden Registrierungsmethoden in ihrer Ausgestaltung stark voneinander abweichen: Ein Register, das Straftaten eines Verurteilten festhält, stellt Informationen zur Verfügung, aus denen allenfalls Schlüsse gezogen werden können. Im Gegensatz dazu präsentieren die Verdachtsregister das Schlussergebnis einer Analyse oder Prognose. Es macht die eingetragenen Personen zu „Figuren der Delinquenz“[92], zu präsentier-, kommunizier- und kontrollierbaren Abstraktionen personifizierter Kriminalität. Es drückt dem Fehlbaren ein stigmatisierendes Label auf und sagt damit etwas darüber aus, was der Täter *ist* (beziehungsweise als was er zu gelten hat[93]) – Rückschlüsse über den Ursprung und die Genese dieser Schlussfolgerung liefert der Registereintrag in der Regel nicht oder lediglich in stark zusammengefasster Form.

Eine weitere Unterscheidung der Register kann bezüglich ihrer Öffentlichkeit respektive ihrer Zugangsregelungen und der verfügbaren Zusatzinformationen getroffen werden: In puncto Abrufbarkeitsschranken sind die verschiedenen Register sehr unterschiedlich gestaltet. Es stehen verschiedene Möglichkeiten zur Verfügung, um die Daten im jeweils vorgegebenen Rahmen zu verbreiten beziehungsweise für die jeweils vorgegebene Zielgruppe abrufbar zu machen.[94] Äusserst problematisch scheinen diejenigen Register, welche öffentlich einsehbar geführt werden.[95] Diese können unter anderem im Internet offen zugänglich von jedermann eingesehen werden und beinhalten neben Rückschlüssen auf die ein-

---

92 KRASMANN, S. 12 und 33. Bsp.: Das traditionelle Strafregister vermerkt die Person X, welche für Exhibitionismus, die Mithilfe bei einem Bombenattentat oder für eine Körperverletzung (z. B. in der Nähe eines Fussballstadions nach einem Spiel) verurteilt wurde. Das Verdachtsregister hingegen präsentiert den Sexualstraftäter X, den Terroristen Y oder den Hooligan Z.

93 Vgl. GROEBNER, S. 66 f.

94 Die Bandbreite reicht von geheimen Registern, welche nur behördenintern bekannt und verfügbar sind, bis zu interaktiven Registern, die von jedem über das Internet eingesehen werden können.

95 Siehe dazu unten Zweiter Teil, Kapitel I.B., I.G. und II.A.

getragene Person vielfach den Wohnort, den Bewegungsbereich, deren übliche Aufenthaltsorte und ähnliche personenbezogene Informationen. Sexualstraftäterregister in den USA unterstützen zudem oftmals Applikationen, die den Wohnort gelisteter Personen unkompliziert auf interaktiven Google-Landkarten geografisch nachvollziehen lassen. Das Strafregister hingegen enthält insbesondere keine Angaben zum Wohn- und Arbeitsort sowie Aussehen des Täters.[96]

Zusammenfassend werden die Verdachtsregister demnach im Gegensatz zum Strafregister primär und rege als Kriminalitätsbekämpfungsinstrument (sowohl präventiv als auch für Ermittlungen) benutzt und sind, wenn nicht öffentlich, so zumindest seitens verschiedener Behörden, erleichtert einsehbar.

B. Verdachtsregister

Die bekanntesten Formen von öffentlichen Verdachtsregistern sind wohl die „Schwarze Liste" der Vereinten Nationen (fortan: UN-Terrorliste) und die „Sexual Offender Register" der USA. Die Schweiz unterhält kein öffentliches Verdachtsregister. Für die Schweiz als Mitgliedstaat der Vereinten Nationen ist indes das Sanktionsregime der Terrorliste des Sicherheitsrats verbindlich. Zudem zeigen sich auch im europäischen und schweizerischen Rechtsraum auf politischer Ebene zunehmend Bestrebungen, Sexualstraftäterregister zu schaffen. In voller Ausprägung werden Letztere heute lediglich in den Vereinigten Staaten geführt.[97] So sind zurzeit in den komfortabel über das Internet öffentlich zugänglichen Registern insgesamt über 700'000 Eingetragene verzeichnet. Mithilfe von einfach zu bedienenden Suchprogrammen kann dort jedermann Informationen über bestimmte Sexualstraftäter in Erfahrung bringen oder umgekehrt alle Sexualstraftäter, welche an einem bestimmten Ort wohnen, vielfach auf einem übersichtlichen google-basierenden Stadtplan oder einer Landkarte, anzeigen lassen.[98] Sicherlich handelt es sich bei der amerikanischen Lösung um eine Ext-

---

96 Vgl. Stellungnahme des Bundesrats vom 7. Mai 2008 i. S. Natalie Simone Rickli.

97 Für eine Übersicht über die Situation in anderen Ländern, siehe Bericht HRW, S. 118; zum finanziellen Aufwand in den USA, bspw. in New Jersey, siehe ZGOBA ET AL., S. 35 f.

98 Gemäss Erhebungen mit Stand 8. Dezember 2009 waren 704'777 in den USA registriert, siehe <http://www.missingkids.com/en_US/documents/sex-offender-map.pdf>. Die National Sex Offender Website <www.nsopw.gov> wartet neben der Suche nach einem bestimmten Namen mit einer Liste mit Links zu den einzelnen gliedstaatlichen Registern auf, die Website <http://www.prevent-abuse-now.com/register.htm> zusätzlich auch Links zu den

remvariante eines Sexualstraftäterregisters. Verglichen mit ähnlichen Ansätzen und laufenden Projekten zu Sexualstraftäterdatenbanken in anderen Ländern (zum Beispiel in Grossbritannien), befindet es sich in seiner elektronischen Erfassung und breiten Veröffentlichung von Daten zu registrierungspflichtigen Sexualstraftätern in einem weit fortgeschrittenen Stadium. Für die jüngst, und insbesondere im europäischen Raum, entfachten hitzigen Diskussionen über den Bedarf derartiger Verdachtsregister, eignen sich die aus den gesammelten Erfahrungen mit Registersystemen der USA gewonnenen Erkenntnisse und Lehren indes vortrefflich als Anschauungsmaterial. Neben Sexualstraftäterregistern sollen insbesondere Terrorlisten und „Hooligenregister" beispielhaft diskutiert werden. Andere Register können in dieser Arbeit grösstenteils nur kurz angesprochen werden. Da die ihnen innewohnenden Konzepte stets die gleichen sind, erübrigt es sich, eine ohnehin niemals annähernd komplette Liste von Registern zu präsentieren.

1. Sexualstraftäterregister

Sexualstraftäterregister haben in den USA eine lange Tradition. Bereits in den Vierzigerjahren des letzten Jahrhunderts schufen einige Bundesstaaten erste (rudimentäre) Sonderregister für Sexualstraftäter. Während der nachfolgenden Jahre führten immer mehr Bundesstaaten Register ein, wobei insbesondere in den Neunzigerjahren ein regelrechter Boom herrschte, öffentliche Sexualstraftäterregister einzuführen. Mittlerweile verlangt das US-Bundesrecht, derartige Register in jedem Bundesstaat zu schaffen und aufrechtzuerhalten, und regelt zudem, im Sinne einer Harmonisierung der sehr unterschiedlichen rechtlichen Grundlagen, in bestimmten Teilbereichen deren Ausgestaltung.[99]

entsprechenden rechtlichen Grundlagen. Ein gutes Beispiel ist das Register von Florida, siehe <http://offender.fdle.state.fl.us/offender/homepage.do>.

99 Zur Chronologie der Rechtslage in den USA, siehe LOGAN, S. 598 ff. Für die bundesweite Vereinheitlichung waren insb. der „Jacob Wetterling Act" (1994), das „Megan's Law" (1996) und der „Adam Walsh Act" (2006) wegweisend, siehe dazu den Bericht HRW, S. 35 ff. und 48 ff.; ZGOBA ET AL., S. 3 f. Harmonisiert wurden bspw. die Registrierungsvoraussetzungen und die Zeitspanne der regelmässigen Meldepflichten der Eingetragenen bei den zuständigen Behörden. Den Bundesstaaten steht ein gewisser Spielraum offen, den zum Beispiel Florida zum Erlass des verschärfenden „Jessica Lunsford Act" (2005) nutzte.

Die Sexualstraftäterregister in den USA basieren im Wesentlichen auf drei Säulen[100]:

- Der Polizei soll ein Instrument in die Hand gegeben werden, das die Strafverfolgung erleichtert. Die Idee ist, mit geringem Aufnwand eine Liste möglicher Verdächtiger zu erstellen, wenn in der näheren Umgebung des Tatorts einer Sexualstraftat Aufenthaltsorte von Eingetragenen verzeichnet sind. Bekräftigend werden dahingehend Studien angeführt, die empirisch nachweisen würden, nur wenige Delinquenten seien für viele Sexualstraftaten verantwortlich und die Rückfallrate sei bei einmal straffällig gewordenen Sexualstraftätern sehr hoch. Es sei demgemäss sehr wahrscheinlich, dass der effektive Täter unter den registrierten Sexualstraftätern in einer bestimmten Region um den Tatort zu finden sein werde.[101]
- Über das Register sollen die Anwohner darüber informiert werden, welche Regionen, zum Beispiel wegen ihrer erhöhten Dichte an ansässigen oder besonders gefährlichen Registrierten, zusätzlich Wachsamkeit gebieten. Die Warnung soll beispielsweise in der Nachbarschaft wohnhaften Eltern helfen, risikobehaftete Orte zu identifizieren, um ihre Kinder anzuweisen, diese Orte zu meiden und den dort drohenden Gefahren auszuweichen. Mit der Kenntnis der Aufenthaltsorte von Sexualstraftätern können somit, so meinen Befürworter öffentlicher Verdachtsregister, sichere Schulwege geplant oder Kinder vor dem Kontakt mit bestimmten Personen gewarnt werden.[102]
- Die eingetragenen Sexualstraftäter sollen von delinquenten Handlungen abgehalten werden, indem ihnen verboten wird, sich in bestimmte Areale zu begeben, zum Beispiel in die Nähe eines Kindergartens oder eines Spielplatzes. Der angestrebte Zweck dieser Auflage ist eine Reduzierung der – bestenfalls die restlose Beseitigung jeglicher – Tatgelegenheiten für den Registrierten. Mithilfe des Registers kann (und soll) von jedermann überprüft werden, ob die Auflage eingehalten wird, und eine allfällige Zuwiderhandlung sogleich an die entsprechende Dienststelle gemeldet werden. Neben dem eigentlichen Eintrag unterstehen Registrierte zudem unter anderem einer Meldepflicht hinsichtlich ihres Aufenthaltsorts bei längeren Aufenthalten ausserhalb des ge-

---

100 Vgl. Bericht HRW, S. 4.

101 Dieser Ansatz, welcher auch für die Kombination von Registrierung und Überwachung interessant sein dürfte, wird noch zu diskutieren sein.

102 Siehe aber unten Erster Teil, Kapitel IV.A.

meldeten Gebiets oder bei Umzug. Die zuständige Behörde informiert die Anwohner anschliessend über den Aufenthaltsortswechsel. Dazu benutzt sie eine Vielzahl an Kanälen, beispielsweise E-Mails, Newsletter, Ankündigungen in den lokalen Medien, Flugblätter oder persönliche Besuche. Einige kommunale Behörden führen die auf dem Gemeindegebiet lebenden Registrierten auch zusätzlich mit periodisch aktualisierten Fotos und Adressen auf ihren Websites auf.[103]

2. Terrorlisten

Die UN-Terrorliste wurde vom Sicherheitsrat als Antwort auf die Angriffe der Al-Qaïda auf die amerikanischen Botschaften in Kenya und Tansania im Jahr 1998 per Resolution 1267 (1999) vom 15. Oktober 1999 in Kraft gesetzt.[104] Aufbauend auf Informationen aus den Mitgliedstaaten und von regionalen Organisationen, wurde ein aktuelles Register terrorverdächtiger Personen und Einrichtungen geschaffen.[105] Der Fokus des Sanktionsregimes liegt in erster Linie darauf, Terroristen und terroristischen Vereinigungen die finanziellen Mittel zu entziehen, damit diesen die Ressourcen für Terrorakte, Ausbildung und Propaganda fehlen.[106] Dementsprechend listet es mehrheitlich mutmassliche Financiers und Begünstigende des Terrors und nicht etwa „Frontagenten" der terroristischen Organisationen auf.[107] Das Sanktionsregime sieht Individualsanktionen vor, sog. „Smart Sanctions", die sich direkt gegen Personen oder Institutionen richten. Zu diesen Individualsanktionen, welche die Mitgliedstaaten zu vollziehen haben, gehört, die finanziellen Mittel der Registrierten umgehend einzufrieren, den Registrierten die Ein- oder Durchreise zu verwehren und jegliche finanzielle Unterstützung der Registrierten zu unterbinden.[108] Während der ersten Jahren nach den

---

103 Siehe zum Ganzen OPPAGA 2008, S. 2 und 4; Bericht HRW, S. 49 ff. und 100 ff. Zur ähnlichen Massnahme der Meldeauflage gemäss schweizerischem Hooligan-Konkordat, siehe etwa MÜLLER J. O., S. 117 f.; Bericht KKJPD, S. 21 f.

104 SULLIVAN/HAYES, S. 12. Zu den gesetzlichen Grundlagen, siehe unten Erster Teil, Kapitel I.G.2. Einen ausführlichen Überblick über Terrorlisten bieten KOCHER und SULLIVAN/HAYES. Zur auf der S/RES/1373 (2001) vom 28. September 2001 basierenden Terrorliste der EU (fortan: EU-Terrorliste), siehe SCHULTE, S. 93 ff. und 137; BARTMANN, S. 25 f., 33 ff.; MEYER/MACKE, S. 446. Ferner DIGGELMANN, S. 308 f.

105 Siehe dazu ausführlich KOCHER, S. 39 ff.

106 BARTMANN, S. 24.

107 So Richard Barrett, Koordinator des UNO-Monitoring Committee, in KOCHER, S. 149 f.

108 BARTMANN, S. 24 f. und 59; DIGGELMANN, S. 309; SULLIVAN/HAYES, S. 11; MEYER/MACKE, S. 446 f. MEYER, S. 74 hält die Bezeichnung „Smart Sanctions" angesichts der Ein-

Anschlägen im September 2001 kamen viele Namen auf die damals noch wenig durchdachte Terrorliste, was vor allem deshalb äusserst problematisch war, weil keine Überprüfungsmechanismen zur Verfügung standen: Wer einmal auf der Liste stand, war dem Sanktionsregime hilflos ausgeliefert.[109] Im Jahr 2010 befanden sich nach einer Totalbereinigung noch 433 Namen im Register. Im Rahmen dieser Überprüfung wurden 45 Einträge gestrichen; dass aber nach wie vor einige Dutzend tote Personen oder aufgelöste Organisationen gelistet sind, spricht nicht gerade für die Verlässlichkeit des Registers oder dafür, dass es einfach wäre, sich von der Liste streichen zu lassen.[110] Der Fall des auf der UN-Terrorliste platzierten mutmasslich den Terror Begünstigenden Youssef Mustapha Nada, der verschiedene schweizerische Behörden über mehrere Jahre beschäftigte, ist ein gutes Beispiel für das damals entmutigend unzugängliche Entlistungsprozedere.[111]

3. Andere Verdachtsregister

Die Liste der heute betriebenen und für die nahe Zukunft geplanten Verdachtsregister ist schier endlos. Neben der komplett öffentlichen UN-Terrorliste betreiben unzählige andere Organisationen, Bündnisse, Staaten, staatliche Behörden oder auch private bzw. privatisierte Anbieter ähnliche, grösstenteils nicht- oder halböffentliche Register etwa mit Terrorverdächtigen, gewaltbereiten Störern, mutmasslichen Exponenten aus der organisierten Kriminalität und dem Drogen-

griffstiefe der Sanktionen für „euphemistisch". Siehe auch THORNE, S. 5 ff. zu den (praktisch identischen) Sanktionen staatlicher Terrorlisten.

109 Vgl. MEYER/MACKE, S. 445 und MEYER, S. 77. Gemäss der späteren Überprüfung des im Jahr 2008 eingesetzten Monitoring Teams stammten über 300 Einträge aus dem Jahr 2002. Siehe dazu KOCHER, S. 43 und 48.

110 Siehe dazu SCHULTE, S. 63; KOCHER, S. 163 ff.; BARTMANN, S. 276. Momentan umfasst die Liste 225 Personen und 64 Organisationen (Stand: 1. Juli 2013), siehe <http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml>. Zu den Verbesserungen des Entlistungsverfahrens über die vergangenen Jahre, siehe unten Erster Teil, Kapitel I.G.2. und Zweiter Teil, Kapitel I.F.

111 Der Bezug zur Schweiz ergab sich daraus, dass Nada in seinem Haus in der ausschliesslich über Schweizer Gebiet zugänglichen italienischen Enklave Campione festsass, nachdem der schweizerische Zoll ihn wegen des Registereintrags nicht mehr in die Schweiz einreisen hatte lassen. Die weiteren Hintergründe des Falls können bei KOCHER, S. 27 ff., in den in dieser Sache ergangenen Entscheiden BGE 133 II 450 und EGMR Nada gg. Schweiz vom 12. September 2012, Nr. 10593/08 nachgelesen werden.

milieu.[112] Beispielsweise unterstehen in Grossbritannien Sexualstraftäter einer Registrierungs- und alljährlichen Meldepflicht. Die entsprechende Datenbank beruht auf dem „Sexual Offences Act 2003".[113] Darauf gestützt sind die gesammelten Daten, im Gegensatz zum amerikanischen Register, jedoch nicht öffentlich, sondern über eine speziell dafür entwickelte elektronische Plattform, dem ViSOR (Violent and Sex Offender Register), lediglich von einigen ausgewählten Behörden und, falls nötig, von bestimmten Arbeitgebern (Arbeitsstelle mit Kontakt zu Kindern) einsehbar.[114]

Verdachtsregister, welche (mutmassliche) Terroristen, gewaltbereite Störer an Sportveranstaltungen oder andere (mutmassliche) Hochrisikopersonen auflisten, sind in der Regel nicht-öffentlich konzipiert. Sie versuchen Gefahren zu verhindern, welche sich, so der Anspruch, wegen ihrer potenziell immensen Bedrohung für die Polizeigüter, nicht verwirklichen dürfen. Dementsprechend konzentrieren sich derartige Register stark darauf, bedrohlich wirkende Personen, welche nicht zwingend Gegenstand eines konkreten Ermittlungsverfahrens sein müssen, so früh wie möglich zu identifizieren und unter ständiger Kontrolle zu halten. Um das Aktiv-Werden im Vorfeld einer potenziellen Straftat, also in der Vorbereitungsphase oder sogar noch früher, zu ermöglichen, berücksichtigen diese Datenbanken bereits „auffälliges" oder „unerwünschtes" Verhalten, sofern es Bezugspunkte zum zu verhindernden Risiko aufweist. Die Eintragsvoraussetzungen der inkriminierten oder bedrohlichen Handlungen oder Verhaltensweisen sind häufig bewusst vage umschrieben oder politisch motiviert.[115] Diese Datenbanken erfassen daher über die unmittelbaren Informationen über den potenziellen Täters hinaus vielfach zusätzlich Daten zu seinen sozialen Kontakten, seinem Umfeld, seinen Verbindungen zu Organisationen usw. Einträge in derartigen Verdachtsregistern beschäftigen sich also oftmals nicht nur mit der eigentlichen Risikoperson selbst, sondern verweisen zugleich auf Personen aus dem weiteren

---

112 Siehe dazu SULLIVAN/HAYES, S. 94 ff. und KOCHER, S. 22 f. und 102 ff. mit zahlreichen Beispielen und Hinweisen sowie THORNE, S. 2 ff. und DUDOUET, S. 3 f.

113 Sexual Offences Act 2003, abrufbar unter: <http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1>.

114 Insofern normiert Grossbritannien die bereits angesprochene „freiwillige Pflicht" des Vorzeigens eines Strafregisterauszugs bei der Bewerbung um eine Arbeitsstelle in bestimmten, besonders kritischen Bereichen. Der Unterschied der beiden Ansätze scheint in dieser Hinsicht nicht sehr gross. Zu ViSOR und anderen (geplanten) Datenbanken in Grossbritannien, siehe etwa NORRIS, S. 143 ff.

115 Vgl. CHESTERMAN, S. 186; SINGELNSTEIN/STOLLE 2012, S. 79.

Bekanntenkreis, die wiederum als potenzielle Gefahrenquellen Interesse wecken. Durch solchermassen verknüpfte Informationsbestände ergeben sich, bei einer genügend grossen Anzahl an Daten, ganze Netzwerke von Risikopersonen und -gruppen. Da nicht nur der mutmassliche Delinquent selbst in den Fokus der registrierenden Behörde gerät, drehen sich viele Registereinträge um Personen, die nur am Rande verdächtig sind.[116] Die beständige Ausweitung der erfassten Netzwerke führt dazu, dass der Daten- und Personenbestand dieser Register systembedingt von selbst anwächst. Hierin wird ersichtlich, dass der Erfassung von Personen grundsätzlich kaum Grenzen gesetzt sind, wenn die Verdachtsschwelle tief angesetzt wird und insofern nahezu unkontrollierbare Ausweitungen, im Sinne einer umfassenden Berücksichtigung von geringen Risikowahrscheinlichkeiten, die Regel sind.

Einige geplante Register scheiterten hingegen bereits vor ihrer Einführung. In Deutschland stand beispielsweise ein nationales Antikorruptionsregister, in welchem unzuverlässige Unternehmen aufgelistet worden wären, zur Diskussion.[117] Dieses Register hätte bei der öffentlichen Vergabe von Aufträgen beigezogen werden müssen und somit dafür sorgen sollen, dass von staatlicher Stelle keine zwielichtigen Unternehmen bei der öffentlichen Auftragsvergabe berücksichtigt werden. Das vorgeschlagene Gesetz wurde im Bundestag abgelehnt.[118]

In den USA wurden zudem Stimmen laut, ein öffentliches nationales Terroristenregister zu schaffen. Darin würden unter anderem die aus Guantanamo Entlassenen aufgelistet werden. Begründet wird diese Absicht mit einem Bericht des Pentagon, der festhielt, dass einige dieser ehemaligen Insassen rückfällig geworden seien und sich direkt nach der Entlassung wieder in „terroristischen Kreisen" bewegt hätten.[119]

---

116 Siehe unten Erster Teil, Kapitel I.F.1. und IV.A.2.

117 Siehe den Gesetzesentwurf zur Einrichtung eines Registers über unzuverlässige Unternehmen (Korruptionsregister-Gesetz) vom 25. Juni 2008. Vgl. den Artikel „Register der Schuldigen" in Die Zeit 13/2002 vom 21. März 2002.

118 Siehe das Plenarprotokoll des Deutschen Bundestags 16/212 vom 20. März 2009, S. 23032.

119 Vgl. MCGOUGH in Radioviceonline vom 13. Januar 2009. Erstaunlich ist die Rückfallrate, auf welcher diese Forderung basiert. 11% aller Entlassenen seien „rückfällig" geworden. Nach einer Behandlung wie derjenigen in Guantanamo, würde man eine deutlich höhere „Rückfallrate" (zutreffender wohl „Entsozialisierungsrate" oder „Radikalisierungsrate") erwarten, vgl. Jean-Cosme Delaloye (Dokumentarfilmer) im Artikel „Kein Ende in Sicht" in der NZZ am Sonntag vom 5. Mai 2012.

C. Vorratsdaten und verdachtsunabhängige Datenbanken

Das (beiläufige) Datensammeln auf Vorrat ist ein weiteres zentrales Element postmoderner Technologien. Unter „Vorratsdatenspeicherung", die jüngst vor allem in Deutschland intensiv diskutiert wurde, wird das anlasslose Aufbewahren sämtlicher Telekommunikationsverbindungsdaten bei den Anbietern der entsprechenden Dienstleistungen (Telefonie, SMS, Internet) über einen gesetzlich bestimmten Zeitraum zum Zweck des Abrufs dieser Informationen durch staatliche Ermittlungsbehörden verstanden.[120] Freilich können aber auch Daten ohne Bezug zur Telekommunikation, Daten anderer Art und aus anderen Quellen auf Vorrat gespeichert werden, um sie eventuell zu einem späteren Zeitpunkt oder mit anderen Informationsverarbeitungsmethoden verwerten zu können. Allgemeiner bedeutet diese Methode also die Speicherung von potenziell nützlichen Daten über längere Zeit, unabhängig von einem Verdacht oder einer Bedrohungslage. Dazu gehören insbesondere Datenbanken mit ausserhalb eines Strafverfahrens oder über ein Strafverfahren hinaus erkennungsdienstlich gespeicherten Daten und allgemein Datenbanken mit (nahezu) verdachtsunabhängig archivierten oder auch nicht direkt personenbezogenen Daten und Informationen.[121] Letztere halten nicht primär Störer, Täter oder Straftaten fest, sondern archivieren Daten, beispielsweise biometrische Daten, aller Personen (etwa aus einem bestimmten Bereich oder Gebiet).[122] Beinahe verdachtsunabhängige Register personenbezogener Daten können theoretisch gute Dienste als äusserst ergiebige Quelle von Vergleichsmustern für Ermittlungen und präventive Massendatenverarbeitungen leisten.[123] In erster Linie dienen sie der Erleichterung der Ermitt-

---

120 Anstatt vieler: WEBER/WOLF/HEINRICH, N. 4; GLESS 2012, S. 13 f.; SZUBA, S. 47; ZIMMER, S. 109 ff. Ein interessantes Detail: Im Gegensatz zur Praxis in der Schweiz machen in Deutschland rückwirkende Randdatenerhebungen im Bereich des Internets einen überwältigenden Teil aus, wohingegen in der Schweizer Praxis vor allem rückwirkende Telefonie- und nur selten Internet-Randdaten abgefragt werden. In Deutschland betreffen rund 90% aller Auskunftsbegehren die Erhebung von Bestandsdaten bzw. Kundendaten hinter einer IP-Adresse. Siehe dazu die Statistiken unter <https://www.li.admin.ch/de/themes/stats.html> und Bericht BKA Mindestspeicherfristen, S. 5. Siehe zudem LSE Briefing, S. 17, 21, 22 f. und 37 zu praktischen Problemen der Koordination und der unterschiedlichen Regelungen in verschiedenen Staaten.

121 Bsp. „Biodatenbanken", siehe etwa WEBER-HASSEMER.

122 Zur wesentlich stärkeren Verbreitung und problematischeren Ausgestaltung derartiger Datenbanken in den USA und und in Grossbritannien, siehe etwa BARTSCH, S. 49; WOOD.

123 Vgl. etwa SCHWEIZER 2008, N. 51 zu Art. 13 BV und den Artikel „Effizienz contra Datenschutz" in NZZ Online vom 20. Juni 2006.

lungstätigkeit, indem Tatortspuren mit den auf Vorrat gesammelten Daten im Register abgeglichen werden können, sobald ein Verbrechen geschieht. Sie könnten indes auch dazu gebraucht werden, Bedrohungen zu lokalisieren und Risikopersonen zu identifizieren. Mit dieser Art von Register wird (relativ) generell – ohne Anspruch, tatsächliche oder prognostisch wahrscheinliche Störer oder Täter spezifisch zu erfassen – eine grosse Zahl an Personen („virtuelle Störer oder Täter") verdächtigt.[124] Sie sind somit grundsätzlich verdachtsunabhängig, Anknüpfungspunkt ist aber häufig eine (schwache) Hypothese.

D. Privat verwaltete Register

Neben den staatlichen Registern existieren unzählige private Register, welche meist einem kommerziellen Nutzen dienen. Sie archivieren etwa das Konsumverhalten oder führen säumige Schuldner auf. Sie werden hier erwähnt, weil sie einerseits auf ähnlichen Modellen wie die Verdachtsregister beruhen. So dient ein Register von wiederholt zahlungsunwilligen oder zahlungsunfähigen Kreditkartenbenutzern demselben Zweck wie ein staatliches Verdachtsregister: Es soll potenzielle Gläubiger vor „schlechten" Schuldnern warnen und Personen abschrecken, die in Betracht ziehen, ihre Kreditkarte missbräuchlich zu verwenden.

Andererseits werden sie erwähnt, weil der Zugriff auf sie eine ausgezeichnete Datenressource für Analysetätigkeiten der Informationsverarbeitungssysteme von staatlichen Ermittlungsbehörden darstellen würde. Insbesondere auch deshalb, weil diese Datenbanken meist nur rudimentär oder gar nicht vor externem Zugriff geschützt sind, jedoch Daten enthalten können, welche innerhalb des Schutzbereichs der Geheim- und Privatsphäre im weiteren Sinn liegen.[125] Die Verfechter der neuen Generation der Data-Mining-Technologien versprechen mithilfe dieser könnten, im Gegensatz zur älteren Generation, mit der Fülle an derart wertvollen (Profil-)Daten effizient umgegangen, private Datenbanken mit anderen (staatlichen) Datenbanken verknüpft und darauf aufbauend umfassende Personenprofile und Bedrohungsszenarien erstellt werden.[126]

---

124 Vgl. OBERHOLZER 2003, S. 331.

125 Siehe FIENBERG, S. 204. Über <http://www.searchsystems.net> können heute über 50'000 öffentlich zugängliche Register in den USA (es sind auch staatliche darunter) durchsucht werden. Eine wahre Goldgrube für Profilersteller.

126 Vgl. SKILLICORN 2008b, S. 11. Siehe unten Erster Teil, Kapitel III.

E. Rasterfahndung und Massendatenverarbeitung

Eine weitere zunächst vielversprechende Anwendungsmöglichkeit neuer Technologien könnten neuere Varianten der Rasterfahndung sein. Die Rasterfahndung ist eine neuere Fahndungsmethode. Stark vereinfacht ausgedrückt, ist sie ein Datenabgleich von grossen Datenmengen anhand vorgegebener Eigenschaften. Die Rasterfahndung wurde zuerst vor ca. 50 Jahren durchgeführt. Insbesondere in Deutschland wurde sie ausführlich diskutiert.[127] Eingebettet in den Komplex postmoderner Technologien kann sie heute aber kaum noch isoliert betrachtet werden. Rasterfahndungsähnliche Methoden begleiten die postmodernen Technologien und Automatismen bei ihrem Einzug in verschiedene Bereiche der Kriminalitätsbekämpfung, vielfach ohne dass sie rechtlich klar abzugrenzen und einzuordnen sind. Das gilt insbesondere für die Schweiz, in welcher die Rasterfahndung nie ein grosses Thema zu sein schien, jedoch mit der Technifizierung der staatlichen Behörden Formen davon in den praktischen Alltag übernommen wurden. Erleichtert wird die Informationsverarbeitungstätigkeit durch viele verschiedene Datenanalyse- und Datenvisualisierungprogramme, welche Daten verknüpfen und analysieren sowie Zusammenhänge visualisieren.[128] Deren Ergebnisse können viel Aussagekraft besitzen.[129] Die extensiver begriffene Form der Rasterfahndung, für welche die Bezeichnung „Rasterfahndung im weiteren Sinn“ grundsätzlich passt, aber verwirrend sein kann[130], soll im Folgenden *Massendatenverarbeitung*[131] genannt werden und schliesst neuere Techniken wie die Algorithmic Knowledge Discovery oder das intelligente Data Mining mit ein.[132]

Um die Funktionsweise weiterentwickelter, rasterfahndungsähnlicher Varianten greifbarer zu machen und Problemstellen verdeutlichen zu können, sollen die essentiellen Prozesse der Rasterfahndung zunächst kurz zusammengefasst werden: Die Rasterfahndung nach klassischer Definition versucht, verdächtige Personen mithilfe eines maschinell-automatischen Abgleichs bestimmter Suchkriterien (Rasterkriterien) innerhalb personenbezogener Massendaten zu identifizie-

---

127 Einen guten Überblick bieten: KUBE; PEHL; PETRI, G N. 528 ff.; ROGALL; RUDIN; THIEL, S. 241 ff.; ZSCHOCH; das Urteil des BVerfG zur präventiv-polizeilichen Rasterfahndung, BVerfGE 115, 320 („Rasterfahndung II“).

128 Zwei Beispiele mit Abbildungen für derartige Software finden sich bei KURZ/RIEGER, S. 5 f.

129 KURZ/RIEGER, S. 7.

130 Vgl. etwa ROGALL, S. 624 Fn. 85.

131 Vgl. etwa PETRI, G N. 528.

132 Siehe dazu unten Erster Teil, Kapitel III.

ren. Sie kann sowohl sicherheitspolizeilichen Zwecken dienen, als auch die Strafverfolgung unterstützen. Ihr Ziel ist, aus einer grossen Anzahl an sich unverdächtiger Personen durch Filterung nach bestimmten Kriterien eine möglichst geringe Zahl potenziell Verdächtiger zu ermitteln, die einem bestimmten Profil oder einer aufgestellten Hypothese entsprechen.[133] KLAUS ROGALL merkt dahingehend zwar an, dass „die Fahndung mittels Rasterung keineswegs an die Verwendung eines automatisierten Verfahrens gebunden ist, sondern eine gedankliche kombinatorische Leistung mit Alltäglichkeitscharakter" darstelle.[134] Grundsätzlich ist ihm zuzustimmen. Die alltägliche kombinatorische Leistung und die automatisierte, computergestützte Fahndungsmethode stehen aber auf sehr unterschiedlichen Ebenen: Das „Wahrnehmungsvermögen" der einsetzenden Person erweitert sich durch die Verwendung von (automatisierter) Technik beträchtlich.[135] Für die vorliegende Arbeit soll der Begriff Rasterfahndung somit in aller Regel eine maschinell-automatisierte (Teil-)Leistung umfassen.

Die Rasterfahndung ist zwar keine neue Idee, sie wird beispielsweise in Deutschland bereits seit den 1970er Jahren praktiziert, erhält aber mit der Weiterentwicklung in der automatisierten Analyse von Massendaten eine neue Grössenordnung. Bisher konnte sie zumeist nur wenig erfolgreich durchgeführt werden.[136] Die Rasterfahndung ist primär eine Methode, Hypothesen zu überprüfen und zu festigen oder Verdachtsmomente zu erhärten. Bei einer Rasterfahndung werden bestehende Datenbestände durchsucht, welche nicht in direktem Zusammenhang mit der Tat stehen. Zielpersonen der Rasterfahndung sind oft auch diejenigen Tatwilligen, Störer und Täter, welche sich durch „gesetzeskonformes und möglichst unauffälliges Verhalten" der Verdächtigung durch die staatlichen Behörden und ihren Ermittlungen entziehen wollen.[137]

---

133 KUBE, S. 50; WALDER/HANSJAKOB, S. 279 f.; ROGALL, S. 616 f.; RUDIN, S. 276; PETRI, G N. 528 und 530; BVerfGE 115, 320 (321). Vgl. die Stellungnahme des Bundesrats vom 7. Dezember 2001 i. S. Theophil Pfister.

134 ROGALL, S. 616. Ähnlich PEHL, S. 11; ROOS/JEKER, S. 176.

135 Gl. A. wie PETRI, G N. 48. Ähnlich BVerfGE 115, 320 (356 f.). Vgl. auch ROGALL, S. 617. Ähnliches gilt hinsichtlich der Videoüberwachung für die Kapazität der automatisierten, „intelligenten" Varianten verglichen mit der Beobachtungskapazität eines Menschen, siehe HORNUNG/DESOI, S. 155.

136 KUBE, S. 50 f.; siehe dazu bspw. die misslungene Rasterfahndung nach „Schläfern" in Deutschland nach dem 11. September 2001 bei PEHL, S. 233 ff.; RUDIN, S. 275 f.; BVerfGE 115, 320 (323 f.).

137 RUDIN, S. 276 und KUBE, S. 65 f. mit Hinweisen, beide dazu grundsätzlich kritisch. Dahingehend optimistischer ZSCHOCH, S. 107 f.

Die Rasterfahndung ist vom simplen Datenabgleich abzugrenzen. Ein solcher liegt vor, wenn das Ergebnis eines Datenabgleichs eindeutig ist oder voraussichtlich erwartungsgemäss eintreffen wird und lediglich behördeneigene Datenbanken herangezogen werden. Die Rasterfahndung hingegen basiert auf bestimmten Annahmen, auf Hypothesen und mindestens zum Teil auf behördenfremden Datenbeständen. Ihr Ausgang ist zunächst relativ ungewiss.[138] Mittels simplen Datenabgleichs sollen konkrete Fragestellungen geklärt werden (Bsp.: „Hat der Verdächtige X in der Nähe des Tatorts mit seiner Kreditkarte bezahlt? Hat er zum Tatzeitpunkt einen Anruf auf sein Mobiltelefon erhalten?"), mittels Rasterfahndung Hypothesen überprüft werden (Bsp.: „Alle diejenigen Personen, die zu einer bestimmten Zeit in der Nähe des Tatorts mit Kreditkarte bezahlt und einen Anruf aufs Mobiltelefon erhalten haben, sind verdächtig."). Im ersten Fall führt der Abgleich zu einem voraussehbaren und klaren Resultat. Hat der Verdächtige in der Nähe des Tatorts zum Tatzeitpunkt mit Kreditkarte bezahlt, dann macht ihn dieses Indiz noch verdächtiger oder auch unverdächtiger, wenn es ein Alibi bedeutet. Im zweiten Fall ergibt der Abgleich eine mehr oder weniger grosse Liste von Personen. Je unspezifischer die Suchkriterien sind, desto mehr Personen auf der Liste werden unverdächtig sein[139] – ein wesentliches Element von Rasterfahndungen ist die im Voraus schwer abschätzbare Grösse der verbleibenden Schnittmenge nach dem Merkmalsabgleich. Die Schnittmenge muss im nächsten Schritt auf näher umrissene Verdachtsmomente oder weitere Eigenschaften überprüft werden. Mittels Rasterfahndung können somit bestenfalls Personen eruiert werden, die als Gesuchte jedenfalls nicht ausgeschlossen werden können. Dieser Personenpool bildet sodann den Ausgangspunkt für weitere Ermittlungstätigkeiten.[140]

Neben der Abgrenzung nach rechtlichen Einsatzgebieten sind zwei Arten der Rasterfahndung zu unterscheiden – die positive und die negative. Erstere gleicht metaphorisch einer Schablone: Alle in ausgewählten Datenbeständen verzeichneten Personen, auf welche bestimmte Eigenschaften zutreffen, werden vorgemerkt. Letztere erinnert an eine Goldwaschpfanne: Wiederholt werden Datencluster aus grossen Datenmengen „ausgespült" und auf einen verbleibenden „Bodensatz" verkleinert.[141] Die positive Methode „dient der Feststellung weite-

---

138 RUDIN, S. 276; MIDDEL, S. 100 f.; PETRI, G N. 520 und 528. Vgl. WALDER/HANSJAKOB, S. 279 f. Zur Vorgehensweise, siehe ROGALL, S. 619.

139 Vgl. etwa BVerfGE 115, 320 (355 ff.).

140 ROGALL, S. 617 f.; PETRI, G N. 528; ZSCHOCH, S. 51.

141 PEHL, S. 13 f.; ROGALL, S. 620 ff.; RUDIN, S. 276 f.

rer für die Ermittlung bedeutsamer Prüfungsmerkmale", die negative bewertet Daten und sortiert sie nach ihrer Relevanz bezüglich der vorgegebenen Kriterien.[142] Die negative Rasterung schliesst mithin nicht zwingend irrelevante Daten aus, sondern verkleinert und ordnet einen unüberschaubaren Datensatz.[143] Die abgrenzende Definition der positiven und negativen Rasterfahndung veranschaulicht deren unterschiedliche Zugänge. Sie ist in der Praxis und aus rechtlicher Sicht aber unerheblich.[144] Die Qualität der Muster- oder Aussiebkriterien bestimmt, wie nützlich die verbliebenen Daten sind. Sind die täterspezifischen Merkmale zu ungenau oder teilweise sogar unzutreffend vorgegeben (eine mögliche Folge eines zu detailreichen oder fehlerhaften Eingabeprofils der gesuchten Person oder Personenkategorie), befinden sich im Endprodukt der Rasterfahndung neben Richtig-Positiven einige grundsätzlich verdächtige Falsch-Positive, welche die Behörde auf eine falsche Spur führen können. Sind die Kriterien zu weit gefasst, können die Daten nicht genügend stark eingegrenzt werden, um eine sinnvolle Verwertung zu gewährleisten. Diese Schwachpunkte der Rasterfahndung verhinderten grössere Erfolge.[145]

Im Unterschied zu spezielleren postmodernen Massendatenverarbeitungstechnologien geht die traditionell-konventionelle, manuelle Datenverarbeitung von konkreten Indizien aus und weitet das Spektrum schrittweise auf zusätzliche Hinweise und allenfalls mehrere Personen aus. Über Massendatenverarbeitungstechnologien hingegen werden zumeist viele Personen erfasst und die grosse Anzahl in den nächsten Schritten immer weiter reduziert. Der Nachteil der ersten Variante ist, dass es möglicherweise bei den Anfangsindizien, beim Kleinen bleibt. Der Nachteil der zweiten Variante liegt darin, dass, obwohl viele Personen erfasst werden, letztlich keine Garantie besteht, dass sich der gesuchte Störer oder Täter darunter befindet oder dass man diesen aus dem Gesamtpool heraus-

---

142 KUBE, S. 51, ZSCHOCH, S. 4 und ausführlich MIDDEL, S. 119 ff.

143 ROGALL, S. 620 f. Möglichst unter 1 % des Ausgangsdatenbestands, siehe ROGALL, S. 617.

144 Unter anderem da bspw. die dafür eingesetzten Suchprogramme die Anfrage bei der Übersetzung in die Maschinensprache ohnehin standardisiert und beide Formen rechtlich gleich zu behandeln sind, siehe PEHL, S. 15 und 293; PETRI, G N. 530; ROGALL, S. 620; ZSCHOCH, S. 47 f. jeweils mit weiteren Hinweisen.

145 Siehe MIDDEL, S. 104 ff.; KUBE, S. 52 ff. In den Siebzigerjahren gelang Deutschland gleich beim ersten grossen Einsatz der Rasterfahndung ein Achtungserfolg: Aus insgesamt 18'000 Ausgangsnamen konnten mit ihrer Hilfe zwei Namen eruiert werden, von denen einer zu einem gesuchten RAF-Terroristen gehörte. An diesen Erfolg anknüpfen konnte die Rasterfahndung ausschliesslich im Bereich der Vorbereitung von DNA-Reihenuntersuchungen, siehe PEHL, S. 266 f. und 293; HOPPMANN.

filtern kann. Insofern besteht die Gefahr, nicht über die Ebene der (ungerechtfertigten) Verdächtigungen von Personenkategorien hinaus zu kommen und Abstriche bei der vorausgesetzten Stärke des Anlassverdachts oder Anlassgrunds in Kauf nehmen zu müssen.

Die Massendatenverarbeitung funktioniert nach dem gleichen Prinzip wie die Rasterfahndung: Sie generiert die durchsuchten Datensammlungen hingegen unter anderem selbst in grossem Stil, anstatt sich auf fremde, bestehende Datenbestände zu verlassen.[146] Die herkömmliche Rasterfahndung kann nur dort angesetzt werden, wo überhaupt eine den vorgegebenen Merkmalen entsprechende Datensammlung existiert.[147] Zudem kann der Fahnder oder das Fahndungssystem bei der Methode der Massendatenverarbeitung über die Quellen und Eckpunkte der relevanten Informationen bestimmen und diese ausserdem selbst erheben. Der Fahnder muss sich nicht mit Vorgaben fremder Datenbestände abgeben, sondern kann die Informationen in beliebiger Art und Weise erheben. Die Information ist somit von Anfang an exakt auf den Fall zugeschnitten und muss nicht in einem ersten Schritt auf die Weiterverarbeitung vorbereitet werden. Nicht tatbezogene Daten können so am effizientesten mit tatbezogenen Daten abgeglichen und analysiert werden.[148]

F. Bilanz: Ambitionen und praktische Erfahrungen

1. Verdachtsregister und andere Datenbanken

Der Idee öffentlicher Verdachtsregister liegen zusammengefasst vor allem zwei Komponenten zugrunde: Zum einen die Erleichterung einer effizienten und effektiven Strafverfolgung und damit einhergehend die negative Spezialprävention kriminellen Verhaltens durch Abschreckung des (rückfälligen) Täters. Zum anderen unerwünschte Handlungen mittels Monitoring durch die Behörden, durch die ständige Überwachung und Isolierung des Registrierten durch sein Umfeld

146 Siehe WALDER/HANSJAKOB, S. 278 f. Bsp.: Die Aktion „Gitternetz“, siehe dazu den Artikel „Big Brother kennt 23 Millionen Bürger“ in Spiegel 46/1986 vom 10. November 1986.

147 Bsp.: Ist keine Liste aller Kennzeichen oder Farben der Fahrzeuge vorhanden, die die Grenze zum Zeitpunkt Y überquert haben, kann die Rasterfahndung nach einem roten BMW mit der Nummer „12“ im Kennzeichnen nicht durchgeführt werden. Vgl. KUBE, S. 53.

148 Daten auf ein einheitliches Format zu bringen verursacht bei der herkömmlichen Rasterfahndung nicht unerhebliche Schwierigkeiten, siehe PEHL, S. 293.

(die Nachbarschaft, die Arbeitskollegen etc.)[149] oder durch einschränkende Massnahmen zu erschweren oder verunmöglichen.[150]

Der Gesetzgeber des Bundesstaates Washington in den USA beauftragte das „Washington State Institute for Public Policy" (WSIPP), eine Analyse der Auswirkungen und der Effizienz des gliedstaatlichen Vorgehens gegen Sexualstraftäter vorzunehmen. Die in der Folge erarbeiteten Berichte des WSIPP stellen den in Washington gebräuchlichen Methoden gemischte Noten aus. Für die vorliegende Arbeit interessieren insbesondere zwei Aspekte der Berichte. Erstens, inwieweit die Einführung der Registrierungs- und Mitteilungspflicht für Sexualstraftäter die Rückfallrate beeinflusste, und zweitens, wie präzise das Washingtoner Instrument zur Rückfallbeurteilung die Gefährlichkeit eines Straffälligen vorauszusagen vermag. Das WSIPP untersuchte die Rückfallraten vor (1986-1989) und nach (1990-1996) Einführung der gliedstaatlichen Registrierungspflicht im Jahr 1990 sowie nach (1997-1999) der Angleichung der Vorschriften im Jahr 1997 an die bundesstaatlichen Direktiven. Die Studie entdeckte tatsächlich signifikant absteigende Rückfallraten (die Rückfallraten fielen von 7% in der ersten, auf 4% in der zweiten und 2% in der dritten untersuchten Zeitspanne). Diese Erkenntnis ist aber mit Vorsicht zu geniessen, zumal es sich bei den entsprechenden Prozentsätzen um tiefe Zahlen handelt, bei deren statistischer Analyse grundsätzlich gewisse Vorbehalte angebracht sind und die nichts darüber aussagt, welche Art von Sexualdelinquenten (leichte oder schwere etc.) weniger rückfällig wurden. Zudem sanken die Kriminalitätsraten in der untersuchten Periode insgesamt, wohingegen die Anzahl Weggesperrter in den USA zunahm.[151] Der Bericht hält deshalb auch ausdrücklich fest, dass eine Kausalität zwischen Einführung der Registrierung und Rückfallraten nicht nachgewiesen werden konnte und ebenso gut andere Faktoren (etwa die sinkende Kriminalitätsrate) für den Rückgang verantwortlich sein könnten.[152]

Das Ergebnis der Studie zur Genauigkeit der für die Gefährlichkeitsprognose gebräuchlichen Instrumente war eindeutiger: Die Voraussagen sowie die darauf

---

149 In diesem Sinne wird also etwas angestrebt, das man mit dem Begriff „künstliche Sozialkontrolle" umschreiben könnte.

150 Diese Massnahmen können bspw. wie bei der „Schwarzen Liste" der UNO darin bestehen, dem Gelisteten alle finanziellen Mittel zu entziehen.

151 Naturgemäss sind Rückfälle während des Gefängnisaufenthalts in der Regel ausgeschlossen. Siehe ZIMRING, S. 164 ff. zur wenig plausiblen Korrelation zwischen Anzahl Gefängnisinsassen und Kriminalitätsrate.

152 Siehe den Bericht WSIPP Nr. 05-12-1202, insb. S. 3.

gestützte Einstufung des Täters vermochten in keiner der Zeitspannen nach Einführung der neuen gesetzlichen Grundlagen zu überzeugen. Je nach Delikt waren sie entweder nicht oder nur wenig zutreffend.[153] Zumindest eines kann wohl aus diesen beiden Berichten des WSIPP gefolgert werden: Wenn sich die Rückfallraten tatsächlich aufgrund der neuen Registrierungs- und Mitteilungsgesetzgebung um bis zu 5% vermindert haben (was einer Verbesserung von 70% entspräche), was stark zu bezweifeln ist, so wurde diese nicht sehr beeindruckende Errungenschaft (diese Rate klingt, aufgrund der genannten verfälschenden Faktoren, besser als sie ist) mit dem hohen Preis vieler „Falsch-Positiver" erkauft.

ZGOBA ET AL. kamen in ihrer Studie über die Wirkung von Megan's Law[154] durchgeführt im Bundesstaat New Jersey zu ähnlichen Ergebnissen. Die Autoren zogen aus ihren Erhebungen zwischen 1985 und 2005 den Schluss, die Umsetzung von Megan's Law – in New Jersey praktisch gleichbedeutend mit der Einführung der Registrierungs- und Mitteilungspflicht[155] – habe weder einen nachweisbaren Effekt auf die Rate der Sexualstraftaten oder auf die Zahl der Opfer noch auf die Zusammensetzung des Pools an Straftaten bewirkt.[156]

Die nicht geringe Anzahl an kritischen Urteilen nationaler und supranationaler Gerichte in Einzelfällen gibt zudem erste Hinweise auf die Bilanz der UN-Terrorliste.[157] Daneben können auch die sichergestellten finanziellen Mittel als Indizien beigezogen werden. Die dazu verfügbaren Informationen ergeben aber kein klares Bild: Gemäss einem Bericht der Regierung der Vereinigten Staaten haben in den ersten zwei Jahren des Sanktionsregimes weltweit fast 200 Millionen US-Dollar an Finanzmitteln eingefroren oder eingezogen werden können.[158] Im Übrigen ist die Effizienz und Wirksamkeit der Terrorlisten schwer einzuschätzen, unter anderem, weil keine (öffentlich zugänglichen) Evaluierungen vorliegen.[159] Die Schwachstellen des Sanktionsregimes liegen insbesondere in der gewaltigen Aufgabe, die finanziellen Mittel von Terroristen oder Terrorvereinigungen aufzuspüren und festzusetzen. Häufig sind diese dezentral organisiert

153 Siehe die Berichte WSIPP Nr. 06-01-1204 und Nr. 05-12-1203, insb. S. 4 Exhibit 5.
154 Siehe oben Fn. 99.
155 ZGOBA ET AL., S. 3.
156 ZGOBA ET AL., S. 1 f., 37 ff. und 41.
157 Siehe dazu unten Erster Teil, Kapitel I.G.2.
158 Siehe dazu Bericht S/2008/324, BARTMANN, S. 276 f. und SCHULTE, S. 71 jeweils mit weiteren Hinweisen.
159 BARTMANN, S. 275 f. mit weiteren Hinweisen; THORNE, S. 9 f. Vgl. Entschluss des Europäischen Parlaments zur Evaluierung der EU-Sanktionen (2009/C 925 E/49), S. 54.

und versuchen finanzielle Transaktionen mit verschiedenen Methoden zu verschleiern. Ferner ist zu bezweifeln, dass alle UN-Mitgliedstaaten das Sanktionsregime gleichermassen sorgsam umsetzen und es ist zu bedenken, dass terroristische Anschläge nicht zwingend grosse Geldsummen erfordern, um trotzdem erheblichen Schaden anzurichten.[160] Weiter belasten viele praktische Probleme die Sanktion des Reiseverbots. So führen unter anderem bereits Tipp- oder Übersetzungsfehler, gleich oder ähnlich lautende Namen von ungelisteten Personen und Umgehungstaktiken der Gelisteten (gefälschte Reisepässe, Meiden der offiziellen Grenzübergänge etc.) zu in der Praxis schwer lösbaren Problemen.[161]

Zu nicht-öffentlichen Verdachtsregistern finden sich wenig aussagekräftige Zahlen oder Studien. Mehr als die Anzahl Registrierter ist hierzu jeweils kaum verfügbar. Die Massnahmen gegen Gewalt an Sportveranstaltungen werden aber vor allem von Seiten der Polizeibehörden insgesamt als wirkungsvolle und notwendige Instrumente eingeschätzt.[162] Die teils angeführten positiven Erfahrungen mit diesen Instrumenten im Ausland sind zwar im gesamten Kontext aller Anstrengungen zu sehen, die Gewalt an Sportveranstaltungen zu vermindern, deuten aber durchaus darauf hin, dass auch die Register mit ihren Folgemassnahmen dazu beitragen.[163] Sehr viel weniger positiv beurteilte die Geschäftsprüfungsdelegation der Eidgenössischen Räte im Jahr 2010 das Staatsschutzinformationssystem ISIS des damaligen Diensts für Analyse und Prävention (DAP), in welchem zu diesem Zeitpunkt rund 200'000 Ziel- und Drittpersonen registriert waren: Die Erfassungsrichtlinien hätten „systematisch zur Ablage von falschen Informationen" geführt, die Qualitätskontrolle sei vernachlässigt worden und dementsprechend die Richtigkeit und Erheblichkeit vieler Informationen anzuzweifeln. Die Mehrheit der Einträge zu Drittpersonen habe den rechtlichen Vorgaben nicht zu entsprechen vermocht. Es seien falsche und unnötige Daten be-

---

160 BARTMANN, S. 277 f. und SCHULTE, S. 69 ff. jeweils mit weiterführenden Hinweisen; Bericht S/2012/968, N. 27 ff. und 45 ff.

161 SCHULTE, S. 74 ff. mit zahlreichen Hinweisen und Beispielen; Bericht S/2012/968, N. 30 und 67 ff.

162 So SOÒS/VÖGELI, S. 158 und 160 f.; HENSLER, S. 41 ff.; DAENIKEN, S. 54 und 57; NUSSBAUMER, S. 149; TRUNZ/WOHLERS, S. 194; Bericht KKJPD, S. 5 ff.; Botschaft BWIS 2005, S. 5632. Beanstandet werden aber insbesondere zu lange Verwaltungsverfahren und Beweisschwierigkeiten.

163 Siehe dazu etwa den Bericht KKJPD, S. 8; den Länderbericht KKJPD. Zur Football Banning Order (FBO) in Grossbritannien im Speziellen: TRUNZ/WOHLERS, S. 199 ff. mit weiteren Hinweisen und <https://www.gov.uk/government/publications/statistics-on-football-related-arrests-and-banning-orders> (Statistiken). Kritisch aber bspw. WEICHERT, S. 73.

schafft, bearbeitet und aufbewahrt worden, was zulasten der Aufgabe gegangen sei, die innere Sicherheit des Landes zu gewährleisten.[164]

2. Informationsverarbeitung

Die Massendatenverarbeitung, wie grundsätzlich auch die Rasterfahndung, kann sowohl im virtuellen als auch realen Raum betrieben werden.[165] Die Massendatenverarbeitung teilt indes den Nachteil der Rasterfahndung: Mit den bisher zur Verfügung stehenden Mitteln ist sie sehr aufwendig und muss mit grossem Vorlauf geplant werden.[166] Als Instrument für eine zeitnahe und flexible Intervention ist sie wenig tauglich. Hinzu kommt, dass die Kriterien, die in das Analysesystem eingegeben werden, sehr spezifisch auf das gewünschte Endprodukt abgestimmt sein müssen, um nicht beliebige, das heisst nutzlose, oder nicht zu bewältigend viele Ergebnisse auszugeben.[167] Dafür ist die Technik des Profiling und der automatischen Datenanalyse heute noch zu wenig weit entwickelt. Die Evaluationsstudie von PEHL zur Effizienz verschiedener Verfahrensformen der Rasterfahndung in Deutschland zeigte dementsprechend wenig aussichtsreiche Ergebnisse. Allenfalls hätten durch die Rasterfahndung neue Ermittlungsansätze gewonnen werden können, von denen jedoch letztlich nur wenige dazu beigetragen hätten, Taten aufzuklären.[168] Die fortgeschrittene Technologie könnte die noch geringe Ausbeute der beiden Methoden jedoch ändern.[169] Einer der Kernzwecke neuer Systeme und der Varianten des Data Mining ist namentlich der effizientere, automatisierte Datenabgleich basierend auf bestimmten Merkmalen.

Auch die Ansprüche an das Leistungsvermögen der Vorratsdatenspeicherung sind hoch.[170] Der Bericht zu Mindestspeicherfristen des deutschen Bundeskrimi-

---

164 Bericht GPDel, S. 7666 f. und 7719 ff. Siehe auch die eher verhaltene Einschätzung der von der GPDel besuchten kantonalen Staatsschutzstellen im Bericht GPDel, S. 7704 ff. Vgl. BELSER, S. 9 N. 18 f. und ferner die Stellungnahme des Bundesrats i. S. Bericht GPDel.

165 Zur Rasterfahndung im virtuellen Raum: PERREY, S. 79.

166 KUBE, S. 58; PEHL, S. 256 ff. und 293. Siehe auch ausführlich ZSCHOCH, S. 105 ff. mit weiteren Hinweisen und Beispielen.

167 Vgl. ROOS/JEKER, S. 176, ROGALL, S. 618, PEHL, S. 15 mit Hinweis und das Bsp. bei KUBE, S. 59 f. Ebenso ernüchtert FIENBERG, S. 211.

168 PEHL, S. 235 ff. und 257 ff. Ähnlich ZSCHOCH, S. 107. Skeptisch zu deren Nutzen auch KUBE, S. 50 f.; RUDIN, S. 275 f.; ROGGAN 2009, S. 262. Siehe auch die ambivalenten Erfahrungen von Praktikern bei PEHL, S. 264 f. Optimistischer ist ROGALL, S. 642 ff.

169 Vgl. ROGALL, S. 618 (insb. Fn. 40) mit weiteren Hinweisen.

170 Siehe dazu ALBRECHT H. J. ET AL., S. 73 ff.; den Artikel „Vorratsdatenspeicherung unverzichtbar – oft einziger Ermittlungsansatz“ in Polizeispiegel vom 3. März 2012, S. 10; Eva-

nalamts hält die Vorratsdatenspeicherung dementsprechend für ein unerlässliches Instrument: Telekommunikationsanbieter hätten 4292 (84.45%) von für 5082 Anschlüsse gestellten Auskunftsersuchen nicht entsprochen.[171] Dadurch hätten im Bereich der Strafverfolgung von 4256 Fällen über 82% nicht und über 12% nur unvollständig aufgeklärt werden können. Lediglich 5% der Fälle hätten zu einem späteren Zeitpunkt beziehungsweise wesentlich erschwert aufgeklärt werden können. Bezüglich der Gefahrenabwehr (36 Fälle) hätten in 25% der Fälle die Gefahren nicht und in 75% der Fälle erst zu einem späteren Zeitpunkt beseitigt beziehungsweise ausgeräumt werden können. Weiter sei die ersuchte Massnahme in rund 45% der negativ beschiedenen Auskunftsersuche der einzige Ermittlungsansatz gewesen. In den restlichen rund 55% der Fälle habe jene zu rund 93% einen wichtigen von mehreren Ermittlungsansätzen dargestellt. Der Bericht des BKA folgert, dieses Ergebnis zeige, „dass Verkehrsdaten in einer Vielzahl der Fälle […] den ersten, sichersten und zugleich effizientesten Ermittlungsansatz" darstellten. Die negativen Bescheide hätten insbesondere in den „Phänomenbereichen" (Computer-)Betrug und Kinderpornografie zu einem Ermittlungsdefizit geführt.[172] Der Evaluationsbericht der Europäischen Kommission beurteilte die Vorratsdatenspeicherung sehr ähnlich wie der Bericht des BKA zu den Mindestspeicherfristen.[173]

Nach Ansicht des Max-Planck-Instituts für ausländisches und internationales Strafrecht (MPICC) ist dieser Evaluationsbericht indes haltlos.[174] Das MPI führte zum Nutzen der Vorratsdatenspeicherung in den Jahren 2010 und 2011 eine umfangreiche Studie durch. Es analysierte darin, ob durch den Wegfall der Vorratsdatenspeicherung praktische Probleme in der Gefahrenabwehr und Strafverfol-

luationsbericht der Europäischen Kommission, S. 31; Bericht BKA Mindestspeicherfristen; Botschaft BÜPF 2013, S. 2731. Vgl. WEBER/WOLF/HEINRICH, N. 6; SIMON D., S. 242.

171 Dabei sollten ca. 99% der Gesuche der Strafverfolgung dienen, lediglich ca. 1% der Gefahrenabwehr. Knapp 98% der Fälle betraf den Bereich des Internets, der Rest fiel auf den Bereich der Festnetz- und Mobilfunktelefonie.

172 Bericht BKA Mindestspeicherfristen, S. 12 und 16. Aus den dort erwähnten Statistiken einen unverzichtbaren Beitrag dieser Massnahme in der Strafverfolgung und Gefahrenabwehr abzuleiten, auch nur bezogen auf die Deliktsbereiche (Computer-)Betrug und Kinderpornografie, scheint indes einem Aussenstehenden und ohne weiteres Datenmaterial zur Verfügung zu haben nicht möglich. Was unter anderem fehlt ist eine (hypothetische) Statistik dazu, wie viele der Fälle aufgeklärt hätten werden können, wäre den Auskunftsersuchen entsprochen worden und dahingehende Vergleichszahlen.

173 Siehe den Evaluationsbericht der Europäischen Kommission, insb. S. 30 ff.

174 ALBRECHT H. J. ET AL., S. 132 f.

gung entstehen.[175] Das Gutachten des MPI nennt vier Konstellationen, in denen dieser Ermittlungsansatz theoretisch hilfreich sein könnte[176]:

1. Die Nutzung von Verkehrsdaten in der Feststellung von Kontakten beziehungsweise der Nähe zu einem Tatort oder Opfer.
2. Die Nutzung von Verkehrsdaten zur retrospektiven Identifizierung von Tatzusammenhängen bei Serientaten (durch Bewegungsprofile etc.).
3. Die Nutzung von gespeicherten Verkehrsdaten zur Feststellung von Zusammenhängen zwischen Tätern oder bei auf Dauer angelegter Tatbegehung in Gruppen oder durch Transaktionen.
4. Die Nutzung von gespeicherten Verkehrsdaten in Verbindung mit Bestandsdaten zur möglichst vollständigen Ermittlung in Volumenverfahren.

Das MPI zog aus seinen Untersuchungen im Gegensatz zum Evaluationsbericht der Europäischen Kommission und dem Bericht des BKA zu Mindestspeicherfristen wenig positive und teilweise sehr gegenteilige Schlüsse:

- So sei erstens bislang keine aussagekräftige Datenlage vorhanden.[177]
- Zweitens kam die Untersuchung des MPI hinsichtlich Aufklärungsquote zum Urteil, es habe sich aus dem Vergleich zwischen der Rechtslage in Deutschland, Österreich und der Schweiz *nicht* ergeben, „dass die systematische Sammlung und Speicherung von Verkehrsdaten beziehungsweise deren Fehlen mit sichtbaren Unterschieden in der Sicherheitslage verbunden wären", auch nicht unter Beiziehung anderer Informationsquellen. Relativierend fügen die Autoren hinzu, es sei sicher nicht auszuschliessen, „dass in komplexen Verfahren und bei Kapitaldelikten Verkehrsdaten wichtige Indizien repräsentieren oder zusätzliche Ermittlungsansätze schaffen", was sich aber auf die Gesamttrends nicht auswirke.[178]
- Drittens hielt es bezüglich der Ermittlungsmethoden, der Ermittlungseffizienz und der Aufklärungsquote fest, „die Fokussierung einer einzelnen Ermittlungsmassnahme […] auf der Grundlage empirischer Untersuchungen zu Er-

---

175 Zur Kritik des BKA an dieser Studie des MPI, siehe <http://www.bka.de/nn_233982/DE/ThemenABisZ/Mindestspeicherfristen/MPI-Studie/mpiStudie__node.html?__nnn=true>.

176 ALBRECHT H. J. ET AL., S. 221 f.

177 ALBRECHT H. J. ET AL., S. 221 f.

178 ALBRECHT H. J. ET AL., S. 219 ff.

mittlungen und Strafverfahren im Bereich komplexer Kriminalität (vor allem organisierter Kriminalität)" erscheine „nicht plausibel". Verkehrsdaten spielten in der Regel nur in Kombination mit anderen Ermittlungsmassnahmen eine Rolle. Es lägen aber bislang erst wenige systematische Untersuchungen zur Effizienz von Ermittlungsmassnahmen in der Aufklärung von Straftaten vor.[179]

G. Gesetzliche Grundlagen in der Schweiz

1. Nicht-öffentliche Verdachtsregister

In der Schweiz werden mehrere nicht-öffentliche Register und Datenbanken mit Profilen verdächtiger oder auffälliger Personen geführt. Neben anderen verdachtsbasierenden Informationssystemen, beispielsweise des allgemeinen Staatsschutzes wie „ISIS", der Bundeskriminalpolizei wie „JANUS" oder grenzübergreifenden Informationssystemen wie das Schengen-Informationssystem („SIS"), die platzbedingt lediglich exemplarisch in die folgenden Ausführungen mit einfliessen, können insbesondere Register zur präventiven Bekämpfung der Gewalt an Sportveranstaltungen als anschauliches Beispiel dienen.[180] So führten Basel und Zürich gestützt auf die polizeiliche Generalklausel bereits seit einiger Zeit Fichen über auffällige Fussballfans.[181] Um eine stabilere rechtliche Grundlage für diese Datenbanken zu schaffen, strebten Kantone und Gemeinden an, eigens für Hooligan-Register geschaffene Vorschriften zu verabschieden. Bei-

---

179 ALBRECHT H. J. ET AL., S. 221.

180 Siehe Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (BWIS; SR 120); Verordnung über das Staatsschutz-Informations-System vom 1. Januar 2002 (ISIS-Verordnung; SR 120.3); Bundesgesetz über die polizeilichen Informationssysteme des Bundes vom 13. Juni 2008 (BPI; SR 361); Verordnung über das Informationssystem der Bundeskriminalpolizei vom 15. Oktober 2008 (JANUS-Verordnung; SR 360.2). Siehe dazu und zu weiteren Beispielen etwa SCHWEIZER 2008, N. 53 zu Art. 13 BV; KOCHER, S. 103; SULLIVAN/HAYES, S. 95. Ausführlich zu JANUS: STEGMANN A., S. 167 ff.

181 Vgl. bspw. EUGSTER in BaZ vom 19. September 2009. Die Varietäten der Gewalt und Gewalttäter im Zusammenhang mit Sportveranstaltungen mit „Hooliganismus/Hooligan" zu bezeichnen, greift zu kurz (Ultras oder gewaltbereite Personen ohne Zugehörigkeit zur Hooligan- oder Ultra-Szene werden von diesen Begriffen an sich nicht erfasst), siehe etwa HENSLER, S. 39 mit weiteren Hinweisen und SOÒS/VÖGELI, S. 157. Da diese Begriffe in den Medien, der Politik und auch vom Gesetzgeber öfters verwendet werden, werden sie im Folgenden trotzdem stellenweise benutzt, vorzugsweise aber die allgemeinere Bezeichnung „gewaltbereite Störer".

spielsweise stimmte die Stadt Zürich am 27. September 2009 über die Verordnung zur Schaffung einer „Polizeilichen Datenbank zu Sportveranstaltungen in der Stadt Zürich (GAMMA; AS Stadt Zürich 551.190)“ ab. GAMMA wurde vom Stimmvolk mit einer deutlichen Mehrheit von 72.6% angenommen, ihr Betrieb aber nach ungefähr acht bis neun Monaten Laufzeit nicht verlängert.[182]

Gesamtschweizerisch besteht seit dem 1. Januar 2007 das vom Bundesamt für Polizei (fedpol) betriebene Informationssystem „HOOGAN“[183], in welchem Personen registriert werden können, die sich im In- oder Ausland an Sportveranstaltungen gewalttätig verhalten haben. Die gesetzliche Grundlage dafür findet sich in Abschnitt 5a des BWIS und in der Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und das Informationssystem HOOGAN vom 4. Dezember 2009 (VVMH; SR 120.52).[184] Seit 1. Januar 2010 bietet das BWIS nurmehr für die Aufnahme in das Informationssystem und die Massnahme der Ausreisebeschränkung eine rechtliche Grundlage. Die Ermächtigung, Rayonverbote, Meldeauflagen und Polizeigewahrsam auf der Grundlage des BWIS anzuordnen, war, vornehmlich aus kompetenzrechtlichen Gründen, auf Ende 2009 beschränkt und wurde anschliessend in das Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen vom 15. November 2007 (Hooligankonkordat) der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) fast unverändert übernommen. Diesem Konkordat sind alle und der revidierten Fassung des Konkordats vom 2. Februar 2012 (mit erweiterten und verschärften Massnahmen) inzwischen ungefähr ein Drittel der Kantone beigetreten.[185] Für den Eintrag einer Person in das Informati-

---

182 Siehe Abstimmungszeitung Stadt Zürich, S. 5 und <http://www.gemeinderat-zuerich.ch/geschaeft_details.aspx?ID=69d03c29-e869-400d-a023-27a8ea19921a>. Die GAMMA-Verordnung trat am 31. Dezember 2010 ausser Kraft (siehe <http://www.stadt-zuerich.ch/internet/as/home/inhaltsverzeichnis/5/551/551_190.html>).

183 Mit Stand Ende Januar 2013 belief sich die Anzahl in HOOGAN registrierter Personen auf 1’294 (siehe Medienmitteilung fedpol vom 31. Januar 2013). Vgl. die deutsche Verbunddatei „Gewalttäter Sport“ mit 13’032 erfassten Personen (Stand: 9. März 2012; siehe dazu Drucksache 17/9003 vom 16. März 2012 und PETRI, G N. 92).

184 Siehe die Änderungen BWIS 2006 vom 24. März 2006. Dieses Register zur Bekämpfung der Gewalt an Sportveranstaltungen wurde vor allem hinsichtlich der Fussballeuropameisterschaft 2008, der Eishockeyweltmeisterschaft 2009 und des Europäischen Übereinkommens über Gewalttätigkeiten und Ausschreitungen von Zuschauern bei Sportanlässen, insbesondere Fussballspielen, vom 19. August 1985 (SR 0.415.3; ratifiziert am 24. September 1990) geschaffen, siehe Botschaft BWIS 2005, S. 5614. Vgl. etwa HENSLER, S. 38 f.

185 Siehe zum Ganzen: MÜLLER J. O., S. 110 f. und 116 ff.; MOECKLI/KELLER, S. 236 f.; MOHLER 2012, S. 99 und 101; TRUNZ/WOHLERS, S. 179 und 192 ff.; ENGLER, S. 162 und 165;

onssystem HOOGAN wird alternativ vorausgesetzt, dass gegen diese eine Massnahme von einer richterlichen Behörde ausgesprochen oder bestätigt worden ist, die Massnahme aufgrund einer strafbaren Handlung ausgesprochen worden ist, die zur Anzeige an die zuständigen Behörden gebracht wurde oder die Massnahme für die Wahrung der Sicherheit von Personen oder der Sportveranstaltung notwendig ist und glaubhaft gemacht werden kann, dass die Massnahme begründet ist.[186]

Das Pendent auf dem Gebiet der Terrorismusbekämpfung sind die zahlreichen nicht-öffentlichen bzw. halb-öffentlichen Terrorlisten (von staatlichen Behörden intern geführte Listen, staatliche oder private „Schwarze Listen" etc.), welche teilweise trotz an sich fehlender überstaatlicher Gesetzgebungskompetenz internationale Auswirkungen entfalten und deshalb (mittelbar) auch Personen in der Schweiz betreffen können. Interessant sind unter anderem die sog. „No-fly-" und „No-Buy-Lists", geführt beispielsweise vom Office of Foreign Assets Control (OFAC) in den USA. Diese halböffentlichen Terroristenregister können ähnliche Sanktionsmassnahmen vorsehen wie die UN-Terrorliste. Die Listen werden in den USA an private Unternehmen aller Sparten weitergegeben. Die Unternehmen sind unter strafrechtlicher Folge verpflichtet, jeden Kunden anhand der Liste zu überprüfen. Mit den gelisteten Namen dürfen die Unternehmen keine oder nur eingeschränkt Geschäfte tätigen.[187]

2. Die UN-Terrorliste

Der Sicherheitsrat der Vereinten Nationen rief, gestützt auf Kapitel VII der UN-Charta, mit Resolution 1267 (1999) gegenüber den Taliban vom 15. Oktober 1999 die UN-Terrorliste ins Leben und dehnte sie am 19. Dezember 2000 mit Resolution 1333 (2000) auf Usama bin Laden und die Gruppierung „Al-Qaïda"

HENSLER, S. 39; Bericht KKJPD, S. 4 f.; Urteil des Bundesgerichts 1C.278/2009 vom 16. November 2010; Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 4.1 f. Vgl. zu den Änderungen die Botschaft BWIS II 2007b, S. 6475 und den Versionsvergleich Hooligan-Konkordat KKJPD; zu anhängigen Beschwerden vor dem Bundesgericht den Artikel „Hooligan-Konkordat im Gegenwind" in NZZ Online vom 16. Februar 2013; zum aktuellen Ratifikationsstand: <http://www.kkjpd.ch/frameset.asp?sprache=d>; zur Debatte, ob dem Bund die Kompetenz in dieser Sache zustand, siehe Botschaft BWIS 2005, S. 5639; SCHEFER, S. 61; STUDER, S: 66; MÜLLER J. O., S. 110; MOHLER 2008, S. 90; MOHLER/SCHWEIZER, S. 8; MOECKLI/KELLER, S. 236; ENGLER, S. 165 f.

186 Art. 24a Abs. 2 BWIS.

187 Siehe dazu KOCHER, S. 22 f. und 104 f.; SULLIVAN/HAYES, S. 96.

aus. Mittels Resolution 1390 (2002) vom 16. Januar 2002 löste der Sicherheitsrat das Sanktionsregime von der vorher vorausgesetzten Verbindung der Person oder Organisation zu einem Staat oder Territorium.[188] Der Schweizer Bundesrat setzte die Resolution 1267 (1999) am 2. Oktober 2000 mittels Verordnung über Massnahmen gegenüber Personen und Organisationen mit Verbindungen zu Usama bin Laden, der Gruppierung „Al-Qaïda" oder den Taliban (TalibanV, SR 946.203) ins nationale Recht um.[189] Der Bundesrat schuf damit eine spezifisch auf die UNO-Terrorliste ausgerichtete rechtliche Grundlage.[190]

Das Listungsverfahren kann durch Mitgliedstaaten und internationale Organisationen angestossen werden.[191] Der aus den Sicherheitsratsmitgliedern bestehende Sanktionsausschuss („Sanctions Committee"), der ein Unterorgan des Sicherheitsrats im Sinne von Art. 29 UN Charta ist, befindet in der Folge über den Antrag. Der einstimmige Listungsentscheid und die sich daraus ergebenden Rechtsfolgen werden sodann dem Betroffenen über seinen Heimatstaat mitgeteilt. Eine Anhörung des Betroffenen findet nicht statt. Auch begründet der Sanktionsausschuss seinen Entscheid nicht.[192] Dieses Vorgehen wurde seitens verschiedener Gerichte und Mitgliedstaaten vehement kritisiert.[193] Nicht zuletzt erzeugten einige Aufsehen erregende Fälle einen gewissen Handlungsdruck.[194] Mit einem der-

---

188 Siehe ausführlich BARTMANN, S. 61 ff.; SCHULTE, S. 43; SULLIVAN/HAYES, S. 11 ff. Weiterführend zu Terrorlisten aus rechtlicher (insb. auch aus völker- und europarechtlicher) Perspektive, siehe etwa BARTMANN; SCHULTE.

189 Der Vollzug der Resolution erfolgte damals noch autonom gestützt auf Art. 184 Abs. 3 BV, da die Schweiz erst am 10. September 2002 Mitglied der Vereinten Nationen wurde, siehe BGE 133 II 450 E. 4 S. 456.

190 BGE 133 II 450 S. 451 f. Die Gelder und wirtschaftlichen Ressourcen der in Anhang 2 der TalibanV aufgeführten natürlichen und juristischen Personen, Gruppen und Organisationen sind gesperrt (Art. 3 Abs. 1). Es ist verboten, ihnen Gelder oder wirtschaftliche Ressourcen zur Verfügung zu stellen (Abs. 2). Den aufgeführten natürlichen Personen ist zudem die Ein- und Durchreise verboten (Art. 4a Abs. 1).

191 Die Resolutionen verpflichten die Mitgliedstaaten nicht, dem Sanktionsausschuss Namen zur Listung zu übermitteln. Die Schweiz bspw. scheint grundsätzlich nicht gewillt zu sein, Listungsanträge zu stellen. Siehe dazu die Antwort des Bundesrats vom 13. Februar 2008 i. S. Daniel Vischer.

192 MEYER 2010, S. 75; BARTMANN, S. 92 f.

193 Siehe dazu anstatt vieler EMMERSON, N. 12, 14 und 20 f. sowie BARTMANN, S. 257, mit jeweils weiterführenden Hinweisen.

194 Siehe beispielsweise die Entscheide des EuGH Yassin Abdullah Kadi und Al Barakaat International Foundation vom 3. September 2008, verbundene Rechtssachen C-402/05 P und C-415/05 P; Französische Republik gegen People's Mojahedin Organization of Iran vom 21. Dezember 2011, Rechtssache C-27/09 P; CCPR Sayadi und Vinck vom 22. Oktober

artigen Fall hatte sich auch das schweizerische Bundesgericht in BGE 133 II 450 zu befassen. Es entschied zwar zuungunsten des beschwerdeführenden Betroffenen, Youssef Nada, kritisierte den Rechtsschutz des Sanktionsregimes aber.[195] Einige (schweizerische) Behörden setzten sich daraufhin für die Tilgung des Eintrags von Youssef Nada ein. Das UNO-Sanktionskomitee strich den Eintrag im März 2010 ohne weitere Erklärung von der UN-Terrorliste. Das schweizerische Parlament entschied sich zudem dafür, dem Sicherheitsrat mitzuteilen, die Schweiz werde Sanktionen der UN-Terrorliste gegen natürliche Personen nicht mehr umsetzen, insoweit die betroffene Person seit mehr als drei Jahren auf der Liste erscheint und nicht die Möglichkeit hatte, bei einer unabhängigen Instanz zu rekurrieren und noch nicht vor ein Gericht gestellt, in ihrer Sache von keiner Justizbehörde Anklage erhoben und seit der Aufnahme in die Liste kein neues belastendes Element gegen sie vorgebracht worden sei.[196] Youssef Nada führte gegen das Urteil des Bundesgerichts an den EGMR Beschwerde. Der EGMR erkannte, dass Art. 8 und 13 EMRK verletzt worden seien und dass die Mitgliedstaaten der EMRK den Zugang zu einem effektiven nationalen Rechtsmittel vorsehen müssten, da ein solches auf Ebene des UN-Sanktionsregimes nicht bestehe.[197]

Auf Drängen von vielen Seiten etablierte der Sicherheitsrat in den darauffolgenden Jahren mit weiteren Resolutionen Schritt für Schritt gewisse Kontrollmechanismen.[198] Namentlich schuf der Sicherheitsrat 2005 eine Koordinationsstelle für Entlistungsanträge („Focal Point") und entwickelte diese 2009 zur Abteilung der Ombudsperson („Ombudsperson's Office") weiter. Zudem verbesserte er 2006 die Mitwirkungsmöglichkeiten der Eingetragenen und der diese unterstützenden Staaten im Entlistungsprozess. Davor hat das Sanktionsregime über keine An-

2008, Nr. 1472/2006; des United Kingdom Supreme Court Ahmed and others v. HM Treasury vom 27. Januar 2010; des kanadischen Federal Court 2009 FC 580 vom 4. Juni 2009 (Abousfian Abdelrazik); den Bericht i. S. Maher Arar. Siehe auch EMMERSON, Fn. 24. Hintergrundinformationen zu den Fällen und den Registern finden sich etwa bei SULLIVAN/HAYES, S. 41 ff; KOCHER; BIGNAMI.

195 BGE 133 II 450 E. 7.4 S. 462 f. und E. 8.3 S. 464 f.

196 Siehe zum Ablauf des Falls Nada KOCHER, S. 27-38. Siehe zur Mitteilung an den Sicherheitsrat: Motion Dick Marty vom 12. Juni 2009; AB 2009 S 819 ff.; AB 2010 N 154 ff.; Kommissionsbericht Aussenpolitische Kommission des Nationalrates vom 1. März 2010.

197 Entscheid des EGMR Nada gg. Schweiz vom 12. September 2012, Nr. 10693/08. Ähnlich bereits der EuGH in seinem Entscheid Yassin Abdullah Kadi und Al Barakaat International Foundation vom 3. September 2008, verbundene Rechtssachen C-402/05 P und C-415/05 P.

198 BARTMANN, S. 94.

laufstelle verfügt und jegliche andere mögliche Überprüfungsinstanz abgelehnt. Weiter verlangt der Sicherheitsrat von den beantragenden Staaten seit 2005 ein Statement zum Fall („Statement of Case") und seit 2008 eine kurze Zusammenstellung zu den Hintergründen des Listungsantrags („Narrative Summaries")[199]. Mit Resolutionen 1988 (2011) sowie 1989 (2011) vom 17. Juni 2011 begrenzte der Sicherheitsrat die UN-Liste auf Al-Qaïda und deren Assoziierte und weitete mit Resolution 2083 (2012) vom 17. Dezember 2012 das Mandat der Ombudsperson aus, um das Entlistungsverfahren fairer und transparenter zu gestalten.[200]

3. Sexualstraftäterregister

In Kontinentaleuropa befasst sich momentan vor allem die Politik mit dem Thema Sexualstraftäterregister.[201] In der Schweiz lancierte die Nationalrätin Natalie Simone Rickli drei Vorstösse im Nationalrat: Die am 5. März 2008 eingereichte Motion „Schaffung eines nationalen Registers für vorbestrafte Pädophile" (08.2033) nahm der Nationalrat trotz des ablehnenden Antrags des Bundesrats vom 7. Mai 2009 am 3. Juni 2009 mit knappen 88 zu 87 Stimmen an.[202] Hinsichtlich der am 20. März 2009 eingereichten parlamentarischen Initiative „Register für Pädophile, Sexual- und schwere Gewaltstraftäter" (09.423), die weni-

---

199 Die Narrative Summaries sind abrufbar unter: <http://www.un.org/sc/committees/1267/individuals_associated_with_Al-Qaida.shtml> und <http://www.un.org/sc/committees/1267/entities_other_groups_undertakings_associated_with_Al-Qaida.shtml>.

200 S/RES/1617 (2005) vom 29. Juli 2005 (Statement of Case); S/RES/1730 (2006) vom 19. Dezember 2006 (Focal Point); S/RES/1735 (2006) vom 22. Dezember 2006 (Partizipationsmöglichkeiten); S/RES/1822 (2008) vom 30. Juni 2008 (Narrative Summaries); S/RES/1904 (2009) vom 17. Dezember 2009 (Ombudsperson); S/RES/1989 (2011) vom 17. Juni 2011; S/RES/2083 (2012) vom 17. Dezember 2012 (Begrenzung der UN-Liste und Ausweitungen des Mandats der Ombudsperson). Siehe zum Ganzen: SULLIVAN/HAYES, S. 14 ff.; KOCHER, S. 47, 49 und 57 f.; BARTMANN, S. 31 ff. und 94 ff.; SCHULTE, S. 39 ff.; die Committee Guidelines vom 15. April 2013; Bericht S/2012/305, N. 28 ff.; Bericht S/2012/968, Annex III.

201 Vgl. etwa für die Debatte in Deutschland MEIRITZ in Spiegel Online vom 7. März 2007. Im Europäischen Parlament scheint das Konzept einer Täterdatenbank, in der Art, wie sie in Grossbritannien praktiziert wird, Anklang zu finden. Der Schaffung eines europäischen (nicht-öffentlichen) Sexualstraftäterregisters steht wohl mehr die Bürokratie im Weg als wirkliche Bedenken gegenüber der Konzeption selbst. Siehe den Artikel „MEPs want EU sex offender list" in BBC vom 22. August 2007: Immerhin 84% der Mitglieder des Europäischen Parlaments hielten in der Befragung ein derartiges Register für sinnvoll.

202 Siehe AB 2009 N 1007. Vgl. zu dieser Forderung nach Verdachtsregistern RICKLI in Der Zürcher Bote vom 8. Mai 2009, S. 5.

ger ambitioniert ein halb-öffentliches Register, ungefähr in der Art, wie es in Grossbritannien praktiziert wird, anstrebte, beantragte die behandelnde Kommission für Rechtsfragen Nationalrat am 29. April 2010 die Ablehnung.[203] Die anschliessende Abstimmung im Plenum fiel zugunsten der Initiative aus.[204] Der Ständerat hingegen stimmte am 29. November 2010 ab, beiden Vorstössen nicht Folge zu geben.[205] Daraufhin reichte Natalie Simone Rickli am 20. März 2013 die Motion „Einführung eines Registers für Sexual- und Gewaltstraftäter" (13.3127) ein, die sich an der bereits am 20. März 2009 eingereichten parlamentarischen Initiative orientiert. Der Bundesrat nahm zu dieser Motion am 15. Mai 2013 ablehnend Stellung.[206]

Insgesamt scheinen somit die Schweizer Parlamentarier der Idee eines Sexualstraftäterregisters einerseits noch mehrheitlich skeptisch gegenüberzustehen.[207] Andererseits scheinen die Befürworter diese Idee nicht fallen lassen zu wollen. Druck aus der Bevölkerung könnte bei einem derart emotionsgeladenen Thema, entgegen rationaler Argumente, durchaus den Ausschlag dafür geben, ein Register im Sinne dieser Vorstösse zu schaffen.

4. Informationsverarbeitung

Materiell-rechtliche Grundlagen für die polizeiliche Datenbearbeitung finden sich in bereichsspezifischen Gesetzen, interkantonalen und internationalen Verträgen.[208] Die schweizerische Rechtslage ist bezüglich der Zulässigkeit von Rasterfahndungen nicht eindeutig. In der schweizerischen Rechtsordnung findet sich heute keine ausdrückliche Grundlage für (systematische) Rasterfahndungen.[209]

---

203 Die Initiative wurde mit nur 12 zu 11 Stimmen bei zwei Enthaltungen abgelehnt, siehe den Bericht RK-NR vom 29. April 2010.

204 Siehe AB 2010 N 1233 (mit 89 zu 80 Stimmen gab der Nationalrat der Initiative Folge).

205 Siehe AB 2010 S 1025.

206 Siehe Stellungnahme des Bundesrats vom 15. Mai 2013 i. S. Natalie Simone Rickli.

207 Vgl. etwa die Voten in der Beratung des Ständerats, AB 2010 S 1022 ff.

208 MOHLER 2012, S. 372; SCHWEIZER 2008, N. 50 und 53 zu Art. 13 BV. Bspw. Art. 14 Abs. 1 BWIS: „Die Sicherheitsorgane des Bundes und der Kantone beschaffen die Informationen, welche zur Erfüllung der Aufgaben nach diesem Gesetz notwendig sind. Sie können diese Daten beschaffen, selbst wenn dies für die betroffenen Personen nicht erkennbar ist."

209 Gl. A. wie RUDIN, S. 277; WALDER/HANSJAKOB, S. 280. Dies scheint einige Behörden aber nicht zu hindern, trotzdem derartige Techniken anzuwenden, siehe bspw. HEINE, S. 36; WALDER/HANSJAKOB, S. 280 (Bsp.: die Nachfrage bei Elektrizitätswerken nach Kleinverbrauchern, die einen sprunghaften Anstieg des Stromverbrauchs unkommentiert bezahlen, was auf Kleinproduzenten von Indoor-Hanf schliessen lasse).

Ausgeschlossen werden Rasterfahndung und Massendatenverarbeitung allerdings auch nicht.[210] Der Bundesrat antwortete kurz nach den Anschlägen vom 11. September 2001 auf eine Anfrage von Nationalrat Theophil Pfister ein wenig nebulös, für die Analyse von personenbezogenen Daten aus polizeiexternen Datensammlungen auf breiter Basis, welche nur entfernt eine Verbindung zu einer Straftat vermuten liessen, bestünden auch in der Schweiz gesetzliche Grundlagen. Er bezeichnete diese aber nicht genauer.[211] Ähnlich verfuhr der Gesetzgeber bei der Ausarbeitung der Schweizerischen Strafprozessordnung: Zunächst stand in der Planungsphase zur Diskussion, die Rasterfahndung in die StPO aufzunehmen. In der Botschaft zur StPO hingegen wurde später, unter dem Titel der Datenbearbeitung, lediglich vage auf die gesetzliche Grundlage in Deutschland hingewiesen, ohne eine eigene Regelung innerhalb der StPO zu erlassen. Damit wurde die Frage nach der rechtlichen Zulässigkeit der Rasterfahndung in der Schweiz weiterhin offen gelassen.[212]

In seinem Urteil zu sog. „Antennensuchläufen im Rahmen einer Rasterfahndung gegen noch unbekannte Täterschaft“[213] ging das Bundesgericht kurz auf die Frage der Rechtmässigkeit von Rasterfahndungen ein. Die „Erhebung von Randdaten mittels Antennensuchlauf“ ordnete es dabei als „systematische Rasterfahndung“ ein und erlaubte diese unter gewissen Voraussetzungen.[214] Bezüglich der Zulässigkeit von Antennensuchläufen scheint damit eine dreigeteilte Abgrenzung nötig:

---

210 Vgl. SCHMID 2009a, S. 427 insb. Fn. 48.

211 Siehe die Stellungnahme des Bundesrats vom 7. Dezember 2001 i. S. Theophil Pfister.

212 Siehe dazu Begleitbericht EJPD 2001, S. 76; Botschaft StPO, S. 1159; RUDIN, S. 278. Der Gesetzgeber vergab hier m. E. eine gute Gelegenheit, zumindest die strafprozessuale Rasterfahndung transparent zu regeln.

213 Gemäss BGE 137 IV 340 E. 5.6 S. 348 werden dabei „Telefonie-Randdaten von zunächst *unbestimmt vielen* (möglicherweise sehr vielen) Teilnehmern erfasst und (vorerst anonymisiert) miteinander abgeglichen, um aus Randdaten verschiedener Tatorte oder Tatzeiten die *Schnittmenge* von konkret Verdächtigen zu ermitteln“. Siehe HEINIGER, S. 36 ff. zur Vorgehensweise bei Antennensuchläufen. Vgl. die Erläuterungen des EJPD vom 8. Juni 2011, S. 4 f.; Botschaft BÜPF 2013, S. 2749.

214 Die da sind: Dringender Verdacht der Begehung eines Verbrechens, Individualisierbarkeit der Gesuchten, Subsidiarität der Massnahme, blosse zunächst anonymisierte Randdatenerhebung und -auswertung, voraussichtlich kleine Schnittmenge (BGE 137 IV 340 E. 6.1 349 f.). Siehe dazu kritisch HANSJAKOB 2012, N. 14 ff.; HEINIGER, N. 53 ff.; ROOS/JEKER, S. 179 f.

- Erstens Antennensuchläufe, die keiner Rasterfahndung gleichkommen, sondern lediglich als Datenabgleich zu qualifizieren sind und deshalb auf der Grundlage des neugeschaffenen Art. 16 lit. e VÜPF durchgeführt werden können.
- Zweitens diejenigen, die einer Rasterfahndung je nach Konstellation zumindest ähnlich sind, aber den Anforderungen des Bundesgerichts gerecht werden.[215]
- Drittens diejenigen, die diese Voraussetzungen nicht einhalten. Derartige Antennensuchläufe wandeln den Randdatenabruf in eine Fahndungs- oder Verdachtsbegründungsmethode[216] und sind deshalb ohne angemessene Ermächtigungsgrundlage nicht zulässig.[217]

Unklar bleibt, ob das Bundesgericht Rasterfahndungen in der Strafverfolgung allgemein für zulässig hält, solange diese gemäss Anforderungskatalog des Bundesgerichts einem konventionellen Datenabgleich noch sehr nahe kommen[218] – oder ob seine Ausführungen lediglich begrenzt auf Antennensuchläufe zu verstehen sind. Zumindest scheint aus dem Urteil hervorzugehen, dass das Bundesgericht Rasterfahndungen zu rein präventiven Zwecken unter der jetzigen Rechtslage in der Schweiz nicht angewendet wissen will.[219]

5. Anlasslose Datensammlungen und verdachtsunabhängige Datenbanken

In Deutschland und der Europäischen Union entstand aufgrund der 2006/24/EG[220] und des Urteils des deutschen Bundesverfassungsgerichts BVerfGE 125, 360 (Vorratsdatenspeicherung) eine rechtspolitische Debatte über die

---

215 Nach HANSJAKOB 2012, N. 12, soll diese Sorte Antennensuchlauf nicht als Rasterfahndung gelten und somit unter Art. 273 StPO fallen. M. E. zu Recht a. A.: HEINIGER, N. 56; GLESS 2012, S. 14; ROOS/JEKER, S. 179.

216 GLESS 2012, S. 14; ROOS/JEKER, S. 180; HANSJAKOB 2006, N. 18 zu Art. 16 VÜPF mit einem Beispiel.

217 Für sie kann nach der hier vertretenen Ansicht Art. 16 lit. e VÜPF keine genügende, hinreichend bestimmte Ermächtigungsgrundlage bieten.

218 Man könnte diese Variation „Rasterfahndung light" nennen.

219 BGE 137 IV 340 E. 5.6 349. Siehe dazu auch BVerfGE 115, 320.

220 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

Zulässigkeit der Vorratsdatenspeicherung.[221] Demgegenüber beruht das anlasslose Speichern von Randdaten für die Dauer von sechs Monaten in der Schweiz bereits seit über zehn Jahren auf einer gesetzlichen Grundlage im BÜPF und mittlerweile auch in der StPO.[222] Im Gegensatz zu den Nachbarländern fanden bezüglich der Vorratsdatenspeicherung in der Schweiz bis zum neuesten Revisionsentwurf des BÜPF, in dem eine auf zwölf Monate ausgedehnte Aufbewahrungsdauer vorgesehen ist[223], kaum grössere Debatten statt.[224] Die verdoppelte Aufbewahrungsdauer wurde teilweise begrüsst, vehement als zu lange oder auch als wesentlich zu kurz kritisiert.[225]

Die rechtlichen Grundlagen für verdachtsunabhängige Register mit Personendaten in der Schweiz können platzbedingt lediglich anhand zweier Beispiele veranschaulicht werden:

Das Schweizer Informationssystem Ausweisschriften (ISA) wurde an sich nicht zu Ermittlungszwecken geschaffen, ja verbietet diesen Verwendungszweck sogar. ISA speichert in einer Datenbank seit 2003 die zur Überprüfung der Identität bei der Ausstellung eines Ausweispapiers erforderlichen Daten (Personalien, Foto und Fingerabdrücke). Auf diese Datenbank zugreifen dürfen nur diejenigen Schweizer Behörden, welche Ausweise ausstellen oder kontrollieren müssen. Die Datenbank steht für die Identifikation von Opfern durch Unfälle, Gewalttaten und Naturkatastrophen, jedoch nicht zu Fahndungszwecken zur Verfügung. Die Klärung der Identität einer Person über eine Abfrage der Datenbank ist nur mit deren Einverständnis erlaubt.[226] Insofern unterliegt sie zwar einer Zugriffsre-

---

221 Siehe zu dieser Debatte etwa BIENDL, S. 4; GLESS 2012, S. 14; MÖSTL, S. 225; ROSSNAGEL, S. 1238 f.; SIMON D., S. 200 ff.; THIEL, S. 323 ff.; OEHMICHEN, S. 933; WEBER/WOLF/HEINRICH, N. 7 ff. Siehe weiterführend zur Vorratsdatenspeicherung bspw. SZUBA, S. 47 ff.; SIMON D., S. 200 ff.; ZIMMER, S. 109 ff.

222 Art. 15 Abs. 3 BÜPF; Art. 27 VÜPF; Art. 273 StPO. Vgl. GLESS 2012, S. 13 f.; WEBER/WOLF/HEINRICH, N. 13.

223 Botschaft BÜPF 2013, S. 2686 und 2697 f.

224 WEBER/WOLF/HEINRICH, N. 14. Siehe auch AB 2000 N 1208 und AB 2000 S 721.

225 Siehe die Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF, S. 42 ff. Bereits das Postulat der Sicherheitspolitischen Kommission des Ständerats vom 21. Februar 2005 und die Motion Rolf Schweiger vom 24. März 2006 forderten verlängerte Fristen. Vgl. WEBER/WOLF/HEINRICH, N. 16 f.

226 Art. 28 lit. i und k sowie Art. 30 Abs. 2 und 3 der Verordnung über die Ausweise für Schweizer Staatsangehörige vom 20. September 2002 (VAwG; SR 143.11).

gelung, die indessen nicht ganz so streng ist wie vermittelt.[227] Die bereits vorhandenen Ausnahmen weisen darauf hin, dass im Bedarfsfall durchaus ein Spielraum für zusätzliche (oder ausgeweitete) Ausnahmen bestehen könnte.[228]

Ist die Kriminalitätsbekämpfung mithilfe des ISA (noch) nicht erlaubt, besteht bereits eine andere Datenbank, welche diesen Zweck ausdrücklich zulässt: Das DNA-Profil-Register CODIS (Combined DNA Index System) der Schweiz. Es wurde mit Inkrafttreten des DNA-Profil-Gesetzes[229] am 1. Januar 2005 in Betrieb genommen. Das CODIS ist eine Mischvariante von Verdachtsregister und verdachtsunabhängiger Datenbank. Es enthält Personenprofile von Straffälligen sowie von Tatverdächtigen – teilweise, etwa im Rahmen von Massenuntersuchungen, und zumindest vorübergehend, aber auch lediglich *potenziell* Verdächtige.[230] Dabei überrascht die für Schweizer Verhältnisse hohe Anzahl registrierter

---

227 Vgl. das Faltblatt „Schweizerpass" des Bundesamts für Polizei (fedpol), abrufbar unter: <http://www.schweizerpass.admin.ch/content/dam/data/passkampagne/flyer/falter_d.pdf>.

228 Die Motion Andrea Martina Geissbühler vom 2. Dezember 2020, welche der Polizei einen erweiterten Zugriff auf die ISA-Datenbank erlauben soll, haben National- und Ständerat jedenfalls bereits angenommen (siehe AB 2012 N 1280; AB 2013 S 192), siehe dazu den Artikel „Polizei soll auf Passfotos zugreifen können" in Tages-Anzeiger Online vom 14. März 2013; kritisch die Stellungnahme des Bundesrats vom 23. Februar 2011 i. S. Andrea Martina Geissbühler.

229 Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen vom 20. Juni 2003 (DNA-Profil-Gesetz; SR 363).

230 DNA-Proben dürfen Verdächtigen und anderen Personen entnommen werden, wenn dies erforderlich ist, um sie als Verdächtige auszuschliessen (Art. 3 Abs. 1 lit. a und b DNA-Profil-Gesetz). Massenuntersuchungen auf bestimmte Merkmale hin sieht das Gesetz explizit vor, um Personen als mögliche Täter zu erkennen oder auszuschliessen (Art. 3 Abs. 2 DNA-Profil-Gesetz). In die Datenbank dürfen nach Art. 11 Abs. 1 des DNA-Profil-Gesetzes u. a. die eines Verbrechens oder Vergehens Verdächtigten (lit. a) und verurteilte Personen (lit. b) sowie Spuren, sofern konkrete Anhaltspunkte bestehen, dass dies der Aufklärung eines Verbrechens oder Vergehens dienen kann, und tote Personen (lit. c i. V. m. Art. 4 DNA-Profil-Gesetz) aufgenommen werden. Die Löschung der DNA-Profile regelt Art. 16 DNA-Profil-Gesetz. Die relevanten Bestimmungen des DNA-Profil-Gesetzes wurden inhaltlich in die Art. 255 ff. StPO überführt, siehe FRICKER/MAEDER, N. 1 Vor Art. 255 StPO. Die DNA-Analyse und DNA-Profile können auch präventiven Zwecken dienen „und damit zum Schutz Dritter beitragen", siehe die Urteile des Bundesgerichts 1B.57/2013 vom 2. Juli 2013 E. 2.3 f. und 1B.685/2011 vom 23. Februar 2012 E. 3.4 f.; FRICKER/MAEDER, N. 7 ff. zu Art. 255 StPO mit weiteren Hinweisen.

Personenprofile: Ende 2012 (also sieben Jahre nach Inbetriebnahme von CODIS) waren es bereits 145'284 Personenprofile und 41'920 Tatortspuren.[231]

Ein weiteres Beispiel war das vom Bundesrat im Jahr 2010 wegen rechtsstaatlicher Bedenken gestoppte Programm Fotopass. Dieses Programm registrierte automatisch die Grenzübertritte aller Angehörigen von Staaten, die der Nachrichtendienst als besondere Gefahrenherde einstufte, im Informationssystem ISIS. Ein knappes Jahr nach der Einstellung des Programms Fotopass bestätigte der Nachrichtendienst, dass bereits das Nachfolgeprogramm ausgearbeitet werde.[232]

II. Raumüberwachung

Der Raumüberwachung wird in jüngerer Zeit aufgrund der immens grossen Fortschritte auf den Gebieten der Video-, Informations- und Kommunikationstechnologie ein immer höherer Stellenwert beigemessen. An dieser Stelle sollen insbesondere die Videoüberwachung realer öffentlicher Räume und die Überwachung sowie Sondierung virtueller Räume durch Einsatz neuerer Technologien thematisiert werden.

A. Videoüberwachung

Die reale Raumüberwachung erfolgt primär durch den Einsatz von Videoüberwachungssystemen, welche auch CCTV-Systeme (Closed Circuit Television)

---

231 <http://www.ejpd.admin.ch/ejpd/de/home/themen/sicherheit/ref_personenidentifikation/ref_dna-profile/ref_die_datenbank.html>; FRICKER/MAEDER, N. 22 Vor Art. 255 StPO; zur Anzahl Identifikationen: <http://www.fedpol.admin.ch/content/fedpol/de/home/themen/sicherheit/personenidentifikation/dna-profile/anzahl_identifikationen.html>. Sehr umfangreiche biometrische Personendatenbanken existieren z. B. auch in Schottland (die Scottish Digital Prisoner's Database), siehe NORRIS/ARMSTRONG, S. 218 und in Grossbritannien (die National DNA Database), siehe NORRIS, S. 147 f.; CROSSMAN. Der National DNA Index des FBI überschritt hinsichtlich der „offender profiles" im Jahr 2011 die zehn Millionen-Marke, was eine Zunahme von ca. zwei Millionen neuen Einträgen innerhalb eines guten Jahres entspricht (siehe dazu <http://www.fbi.gov/about-us/lab/codis/ndis-statistics>; CHESTERMAN, S. 257 f.; STEINBOCK, S. 11).

232 Siehe Stellungnahme des Bundesrats i. S. Bericht GPDel, S. 7752 und RENZ in Tages-Anzeiger Online vom 3. Mai. 2011. Zudem stand jüngst zur Debatte, ob DNA-Tests von „bestimmten Asylbewerbern" eingeführt werden sollen, siehe KLENGER in Tages-Anzeiger Online vom 17. April 2013.

genannt werden.[233] In London ist die praktisch flächendeckende Überwachung des öffentlichen Raums Realität geworden. Von London aus breitete sie sich rasch in ganz Grossbritannien aus.[234] In jüngster Zeit wird die Videoüberwachung vermehrt auch in der Schweiz eingesetzt.[235] Obwohl diese Massnahme nicht allseits auf Zuspruch trifft, scheint sie in der Schweiz einem Bedürfnis der Bevölkerung zu entsprechen oder von dieser zumindest akzeptiert zu werden.[236]

Im Begriff „Videoüberwachung" enthalten ist sowohl die direkte Übertragung eines Live-Streams von einem Aufnahmegerät zu Überwachungsmonitoren als auch die vorerst unbesehene Sammlung und Speicherung der durch die Kameras gewonnenen Daten und alle möglichen Kombinationen dieser beiden Ansätze. Zu unterscheiden sind drei Überwachungsvarianten[237]:

- Mittels der *observativen* Überwachung wird ein bestimmter Tatverdächtiger technisch beschattet. Sie ist immer vorübergehend, verdeckt und auf eine Person beschränkt.
- Die *nicht-personenbezogene* Überwachung dient hingegen der Steuerung von Personen und Verkehrsströmen. Sie lässt grundsätzlich keine Personenidentifikation zu.
- Die *dissuasive* Überwachung wird eingesetzt, um bestimmte Räume zu sichern. Sie wird in der Regel offen sichtbar betrieben. Mit ihrer Hilfe sollen

---

233 GRAS, S. 91. Die akustische Raumüberwachung wird einerseits noch sehr zurückhaltend eingesetzt und die Ausführungen zur visuellen Raumüberwachung lassen sich andererseits auf die akustische übertragen, siehe MÜLLER L. 2011, S. 11 mit Hinweisen. Sie soll hier deshalb als optionale Erweiterung der visuellen Videoüberwachung verstanden werden.

234 Siehe dazu NORRIS/MORAN/ARMSTRONG, S. 497; NORRIS/ARMSTRONG, S. 3 und 40 ff.; FARRINGTON ET AL. 2007, S. 22; LINGG, S. 22 ff.; ZEHNDER M., S. 16 f.; STUTZER/ZEHNDER, S. 110 f.; BÜLLESFELD 2002, S. 35 ff.; SCHRÖDER, S. 44 ff. Zur technischen Funktionsweise und den Abläufen dieser Systeme, siehe BÜLLESFELD 2002, S. 5 ff.; GRAS, S. 91 ff.; BORNEWASSER, S. 138 ff.; MÜLLER L. 2011, S. 15 ff.

235 Siehe ZEHNDER M., S. 18 ff. und LINGG, S. 25 ff.

236 Siehe bspw. LINGG, S. 62 und 82 f.; MÜLLER L. 2011, S. 2 mit zahlreichen Hinweisen. Vgl. SZVIRCSEV TRESCH/WENGER 2012, S. 108 f. (76% der befragten Personen befürworteten die Videoüberwachung öffentlicher Räume). Zur sich bereits wieder abkühlenden Stimmung in Grossbritannien, siehe NORRIS/ARMSTRONG, S. 60; WEBSTER, S. 10 f.; WOOD.

237 RUDIN/STÄMPFLI, S. 144 f. Siehe dazu ausführlich BÜLLESFELD 2002, S. 19 ff. Eine andere gebräuchliche, aber nach Ansicht von RUDIN/STÄMPFLI, S. 144, veraltete Unterteilung findet sich bei FLÜCKIGER/AUER, S. 924 und im Bericht EJPD 2007, S. 9 (insb. grenzen diese als zusätzliche Variante die „invasive Videoüberwachung" ab).

> Personen erkannt und präventiv davon abgehalten werden, Delikte (im überwachten Raum) zu begehen, oder die Ermittlungen nach einer geschehenen Tat erleichtert werden.

Mithilfe neuerer dissuasiver Systeme wird versucht, Verhaltensweisen und Verhaltensmuster sichtbar zu machen, um Bedrohungen vorzubeugen und in einem früheren Stadium eingreifen zu können. In Extremfällen, wie zum Beispiel in London, können sich in der Stadt bewegende Personen über Umschalten zwischen benachbarten Überwachungsräumen verfolgt werden. Diese Einsatzformen sind immer auch in Verbindung mit ihren Einsatzgebieten zu beurteilen. Dazu gehören erstens öffentliche Räume mit abstrakter Gefahrenlage. Zweitens öffentliche Räume mit konkretisierbarer Gefahrenlage, das heisst vor allem neuralgische Kriminalitätsballungspunkte.[238] Drittens öffentliche Räume, für die eine konkrete Gefährdung durch eine spezifizierbare Bedrohung akut vermutet wird.[239]

Mit dem Begriff „Videoüberwachung" ist vorliegend, wenn nicht anders vermerkt, die dissuasive Überwachung gemeint, auf welcher der Fokus der Untersuchung liegt. Grundsätzlich soll der öffentliche Raum in einem weiteren Sinn als die geläufige Definition der Gesamtheit der im Eigentum des Gemeinwesens stehenden und/oder einer öffentlichen Aufgabe dienenden und in aller Regel jeder Person zugänglichen Areale, Gebäude und Sachen verstanden werden. Öffentlich zugängliche digitale „Räume" wie das Internet sollen zudem unter die verwendete offene Interpretation des öffentlichen Raums fallen.[240] Die Grenzen zwischen Orten oder Arten der Videoüberwachung sind indes, wie im Verlauf dieser Arbeit noch mehrmals festgestellt wird, fliessend, weshalb zu starre Unterscheidungen wenig zweckmässig sind.[241]

---

238 Vgl. ROGGAN 2001, S. 137; BARTSCH, S. 211.

239 Siehe zum Ganzen ausführlicher MÜLLER L. 2011, S. 26 ff. mit weiteren Hinweisen.

240 Siehe dazu Bericht EJPD 2007, S. 8 f. Vgl. FLÜCKIGER/AUER, S. 926; LINGG, S. 16. Die öffentliche Zugänglichkeit des Raums soll wie bei MÜLLER L. 2011, S. 8 f. den Untersuchungsgegenstand eingrenzen, die durch Private betriebene Überwachung jedoch höchstens am Rande behandelt werden. Ausführlich zum Begriff des öffentlichen Raums bzw. „public place" in Deutschland und den USA: BARTSCH, S. 18 f.

241 MÜLLER L. 2011, S. 25 f. hält daher die genannten Kategorien der Videoüberwachungsarten angesichts der technischen Fortschritte für gänzlich verzichtbar.

B. Überwachung im virtuellen Raum

Die Beobachtung einer steigenden Tendenz von Delikten, welche im, durch den oder mit einem Bezug zum virtuellen Raum begangen werden, scheint der Forderung nach dessen verstärkten Überwachung Nachdruck zu verleihen.[242] Um möglicherweise erlangte Vorteile (zum Beispiel bei der Kommunikation über digitale Kanäle oder beim Betreiben von Informationsplattformen für kriminelle Ideen im Internet) gegenüber staatlichen Behörden aufzuholen, sollen intelligente und automatisierte Such-, Ermittlungs- und Analysesysteme den virtuellen Raum transparenter und leicht erfass- und sondierbar machen. Zu repressiven Ermittlungszwecken scheinen virtuelle Überwachungsmassnahmen bereits öfters Anwendung zu finden.[243]

In der vorliegenden Arbeit wird, wie bereits angemerkt, von einer weiten Definition des virtuellen Raums ausgegangen. Das Internet und andere virtuelle Räume können auf vielfältige Weise als Erkenntnisquelle und Fahndungsmittel gebraucht werden. Die aufklärende oder ermittelnde Behörde kann den virtuellen Raum als Informations- oder Kommunikationsmittel benutzen. Sie kann passiv an Informationen gelangen, aktiv oder auch interaktiv Informationen beschaffen oder Geschehnisse beeinflussen. Bei der Einsatzvariante als Informationsmittel handelt die Behörde, ohne sich direkt zu beteiligen. Sie beobachtet aus der „virtuellen Ferne" oder hält bereits Geschehenes fest und ruft bestehende Daten ab (mittels Überwachung von Netzknoten, der Observation im weiteren Sinne des Verhaltens einer Zielperson respektive Zielgruppe oder sonstiger Datenerhebungsarten). Wählt die Behörde den zweiten Zugang und verwendet zur Raumüberwachung die digitalen Kanäle als Kommunikationsmittel, beteiligt sie sich passiv oder aktiv an den Geschehnissen. Sie beeinflusst die entstehenden Daten somit mittelbar oder unmittelbar. Zum Beispiel klinkt sie sich, offen oder verdeckt, in eine Diskussion eines Internet-Chatraums ein.[244]

Dieses Modell des Handelns im Internet kann als Basis dienen, staatliches Tätigwerden im virtuellen Raum zu beschreiben, aber es kann angesichts neuer Überwachungs- und Ermittlungstechnologien im virtuellen Raum die Situation nicht immer adäquat erfassen. So stehen der Behörde zur Einsicht oder Speiche-

---

242 Siehe PERREY, S. 2; NOWAK, S. 33. Fraglich ist hierbei, ob die Gefahren der Internetdelinquenz nicht vielfach übersteigert dargestellt werden, vgl. RÜTHER, S. 93 ff. und 99.

243 Vgl. PERREY, S. 86. Siehe dazu unten Erster Teil, Kapitel III.

244 Siehe ausführlich zum Ganzen: PERREY, S. 74 ff.; VALERIUS, S. 29 ff. und 35 ff.

rung der Daten aus virtueller Information oder Kommunikation vorderhand viele Ansatzpunkte offen: Sie kann die gespeicherten Daten mittels „Government-Software“ („Govware“) direkt vom Computer des Verdächtigen abrufen, sie kann vom Verdächtigen ausgelagerte, aber unter seiner (Teil-)Herrschaft verbleibende Speicherorte einsehen, versendete E-Mails beim Provider anfordern etc.[245] Neuere Technologien wie beispielsweise die „Deep Packet Inspection“ (DPI; „tiefe Paketanalyse“) erlauben zudem, die virtuelle Kommunikation in Echtzeit zu überwachen, zu beurteilen und zu manipulieren.[246] Zum einen dienen diese Technologien also oftmals mehreren Zwecken oder können technisch bedingt nicht immer auf bestimmte Einsatzfunktionalitäten beschränkt werden.[247] Zum anderen müssen die Vorgehensweisen der Behörden im virtuellen Raum um eine weitere Dimension, die Abgrenzung zwischen dem Sondieren von Daten innerhalb und ausserhalb der Systeme von Nutzern, erweitert werden. Das deutsche Bundesverfassungsgericht nennt erstere Variante in seinem Urteil zu „Online-Durchsuchungen“ (BVerfGE 120, 274) „technische Infiltration“ eines informationstechnischen Systems, letztere „heimliches Aufklären des Internet“.[248]

Für die erste genannte neuere Technologie kursieren viele verschiedene Begriffe. In der vorliegenden Arbeit wird für diese Art von Programmen der Sammelbegriff „Govware“ bevorzugt. Der teilweise synonym verwendete Begriff „Remote Forensic Software (RFS)“ scheint aus zwei Gründen irreführend: Erstens fiel dieser Begriff in Zusammenhang mit staatlichen Beteuerungen, man wolle das Spähprogramm direkt vor Ort auf das Zielsystem aufspielen und nicht über ein Netzwerk einschleusen.[249] Zweitens bedeutet „forensisch“ im juristisch-deutschen Sprachgebrauch „gerichtlich“. Die Spähprogramme sind freilich nicht per se auf den Einsatz innerhalb eines Strafverfahrens beschränkt. Der Begriff „Remote Forensic Software“ ist somit ungenau. Darin zeigt sich, wie unscharf die Trennung zwischen den Rechtsgebieten, der Gefahrenabwehr und Strafverfolgung geworden ist.[250] In Deutschland verbreitete sich zudem, vor allem in den

---

245 Eindrücke zu entsprechenden technischen Lösungen auf aktuellem Stand finden sich auf den Internetauftritten von Sicherheitsunternehmen (ein Bsp.: <http://www.ss8.com>).

246 Zur Definition, Geschichte und Funktionsweise der DPI: COOPER, 139-145; BEDNER, S. 4-8; WAGNER, S. 3 ff.; LSE BRIEFING, S. 21-23.

247 Siehe dazu unten Zweiter Teil, Kapitel I.D. und Dritter Teil, Kapitel I.G.

248 BVerfGE 120, 274 (276).

249 Siehe KREMPL in heise Online vom 3. August 2007.

250 Mehr zu dieser problematischen Entwicklung unten im Zweiten Teil, Kapitel I.I.

Medien, rasch die Bezeichnung „Bundestrojaner". In der Schweiz liest man gelegentlich „Trojaner Federal".[251] Diese etwas alltagssprachlichen Bezeichnungen mit dem Zusatz „Trojaner" für ein staatlich eingesetztes Spähprogramm scheinen zu negativ formuliert[252], sie umreissen die übliche Funktionsweise von Govware aber trefflich. Sogenannte „Trojaner", sind Programme, die unter anderem dazu benutzt werden, um sich Zugang zu fremden Computern zu verschaffen. Der Begriff „Trojaner" steht, in Anlehnung an das mythische trojanische Pferd, für ein fremdkontrolliertes Programm, das andere Programme vom Anwender unbemerkt in das Zielsystem einschleust.[253] Einmal im Zielcomputer eingeschleust, können diese Programme versteckten Aufgaben nachgehen, unerkannt im Hintergrund laufen. Sie können demjenigen, der sie einsetzt, erlauben, sich (unberechtigt) Zugang zu einem bestimmten Computersystem zu verschaffen, ohne dass der Anwender des Computers dies gutheisst oder überhaupt bemerkt. Ein Trojaner kann die anwendende Behörde somit in die Lage versetzen, sowohl auf alle Daten auf dem Computer zuzugreifen (sie anzusehen, zu kopieren, zu verändern etc.) als auch jegliche aus- und eingehende Kommunikation zu überwachen. Auch kann sie durch den Trojaner theoretisch nicht nur Daten, die sich auf infizierten Computern befinden, über das Internet auslesen, sondern viele andere Manipulationen am Zielsystem vornehmen, die zum Beispiel das Mitprotokollieren eingegebener Passwörter (sog. „Keylogging"), die Aktivierung der Webcam (zum Beispiel zur Wohnraumüberwachung) und die völlige Fernsteuerung des Zielsystems erlauben.[254] Govware ermöglicht insbesondere auch, verschlüsselte

---

251 Siehe zum Ganzen insbesondere BRAUN; BUERMEYER; GLESS 2012; HANSJAKOB 2011; JOTTERAND/MÜLLER/TRECCANI; MÉTILLE; STÖCKLI; TSCHENTSCHER; WEBER/WOLF/HEINRICH. Neutraler findet sich auch die Bezeichnung „Spähprogramm", siehe ZERBES, S. 34. Siehe zum technischen Hintergrund: BUERMEYER, S. 154 ff.

252 RHYNER/STÜSSI, S. 469, RISS/BERANEK ZANON, N. 3 und HANSJAKOB 2011, N. 2 f., weisen m. E. zutreffend darauf hin, dass der Begriff „Trojaner" üblicherweise Programme meint, die Hacker *illegal* verwenden. Die Behörde hingegen setzt die Govware, insofern eine entsprechende gesetzliche Grundlage besteht und sie innerhalb der vorgegebenen Schranken handelt, *legal* im Rahmen einer genau definierten staatlichen Aufgabe und ohne Absicht, Schäden zu verursachen, ein. Vgl. Botschaft BÜPF 2013, S. 2772.

253 Zu den Aufspielmöglichkeiten siehe BUERMEYER, S. 163 f.; RISS/BERANEK ZANON, N. 5; HANSJAKOB 2011, N. 11 f.; HANSEN/PFITZMANN; PFITZMANN/KÖPSELL 2009b, S. 154 ff.; SCHMIDT in heise Online vom 11. März 2007. Bei den Zielsystemen kann es sich freilich auch um Laptops, Smartphones etc. handeln, siehe TSCHENTSCHER, S. 384.

254 BUERMEYER, S. 155 ff. und 161 f.; HANSJAKOB 2011, N. 8 f.; JOTTERAND/MÜLLER/TRECCANI, N. 10; TSCHENTSCHER, S. 384 f.; HANSEN/PFITZMANN; BVerfGE 120, 274 (276 f.); RISS/BERANEK ZANON, N. 4; ZERBES, S. 23 und 34 f. Siehe zum Ganzen HANSJAKOB

Internettelefonie zu überwachen. Diese Programme versenden die zu übermittelnden Informationen mit „End-to-End-Verschlüsselung“ in vielen kleinen Datenpaketen über mehrere verschiedene Server. Die (verschlüsselte) Datenübertragung an sich ist zwar mitunter einer konventionellen Kommunikationsüberwachung zugänglich, den Inhalt der Datenübertragung zu entschlüsseln ist indes nahezu unmöglich oder äusserst aufwendig.[255]

Zusammenfassend können vier grundlegende Anwendungsformen von Govware unterschieden werden[256]:

- Variante 1: Die Behörde beschränkt sich darauf, über die Govware Kommunikationsinhalte, das heisst von einem an ein anderes Informationsverarbeitungssystem übertragene Daten, auszulesen (sog. „Quellen-TKÜ“). Sonstige Inhalte und Daten auf dem Computer bleiben unberührt oder werden zumindest nicht übermittelt, nicht gespeichert oder umgehend gelöscht. Analogien bestehen zur Observation und zur inhaltlichen Telefonüberwachung.
- Variante 2: Die Behörde beschränkt sich nicht auf Kommunikationsinhalte. Sie setzt die Govware zeitlich punktuell ein (sog. „Online-Durchsuchung“). Analog einer Hausdurchsuchung oder Beschlagnahme des Rechners bestimmt sie einen Zeitpunkt, an dem sie alle gewünschten Daten vom Zielcomputer überträgt und speichert (also einzelne Dateien kopiert oder den Datenträger

2011, N. 4 ff.; MÉTILLE, S. 7 f.; GLESS 2012, S. 16 ff.; JOTTERAND/MÜLLER/TRECCANI, N. 6-11; WEBER/WOLF/HEINRICH, N. 19-21; PLATZ, S. 839 f.; CCC Analyse.

255 Siehe dazu BUERMEYER/BÄCKER, S. 434; HANSJAKOB 2011, N. 4 ff.; PLATZ, S. 838; GLESS 2012, S. 12; KLESCZEWSKI, S. 742; BVerfGE 120, 274 (279); Botschaft BÜPF 2013, S. 2775 f. Auch die DPI-Technologie kann derartige Verschlüsselungen in der Regel nicht umgehen, siehe LSE-Briefing, S. 26. Skeptisch BRAUN, S. 681 und 685 mit weiteren Hinweisen, der zu bedenken gibt, dass die Anbieter derartiger Dienste sog. „Backdoors“ („Hintertüren“) für das Abhören auch verschlüsselter Datenübertragung offenhielten. Ähnlich BUERMEYER/BÄCKER, S. 434, die aber anmerken, neuere Verschlüsselungsmethoden könnten diese Vorkehrungen umgehen. Zur Funktionsweise der Internettelefonie, siehe KLESCZEWSKI, S. 741 ff. mit weiteren Hinweisen. Zu Firewalls und Verschlüsselungsmethoden, siehe TINNEFELD/BUCHNER/PETRI, S. 433 ff.

256 Siehe dazu BUERMEYER, S. 160 ff.; BUERMEYER/BÄCKER, S. 434; BRAUN, S. 681; KLESCZEWSKI, S. 744; ZERBES, S. 34 f. In Deutschland ist für die erste Variante die Bezeichnung „Quellen-Telekommunikationsüberwachung“ („Quellen-TKÜ“) in Abgrenzung zur sog. „Online-Durchsuchung“ und „Online-Überwachung“ für weitergehende Varianten üblich, siehe bspw. BVerfGE 120, 274 (308 f.).

komplett „spiegelt“).[257] Die Govware wird zeitgleich oder kurz vor dem Einsatz installiert und zeitgleich mit oder kurz nach Beendigung der Übertragung der Daten deinstalliert.

- Variante 3: Die Behörde beschränkt sich nicht auf Kommunikationsinhalte. Sie setzt die Govware über eine (längere) Zeitspanne ein, mit dem Ziel entweder Beweismittel zu sammeln, einem Verdacht nachzugehen oder einer Bedrohung vorzubeugen (sog. „Online-Überwachung“).[258] Dieser Einsatz von Govware bedeutet eine anhaltende (oder vielfach wiederholte) heimliche Durchsuchung.[259]
- Variante 4: Die Behörde überwacht das System oder die Systeme einer Zielperson im Sinne eines Monitorings.[260] So könnten Risikopersonen von (neuerlichen) unkonformen Tätigkeiten im virtuellen Raum abgehalten werden. Das wäre unter anderem eine nur logische Ausdehnung der Begleitmassnahmen von Verdachtsregistern.

Einen anderen Ansatz verfolgen DPI-Technologien. Sie haben nicht wie die Govware das Computersystem selbst als Ziel, sondern die aus- und eingehende Kommunikation zwischen Computersystemen. Sie dringt nicht in ein Zieldatenverarbeitungssystem ein. Zusätzlich ermöglicht sie aber, den virtuellen Raum verdachtsunabhängig zu durchforsten.

Vorläufig kann etwas ungenau festgehalten werden, dass Govware ein bestimmtes Datenverarbeitungssystem, den Herrschaftsraum einer Person und alles betrifft, was sich darin befindet und was darin passiert, wohingegen die DPI-Technologien das Handeln und Kommunizieren einer Person im virtuellen Raum ausserhalb seines eigenen Datenverarbeitungssystems betreffen.

Aus rechtlicher Sicht bedeutsame Merkmale für die Einschätzung von Online-Überwachungsmassnahmen sind somit vor allem die Zugänglichkeit des überwachten Raums der Information und Kommunikation (frei verfügbar, privater

---

257 BUERMEYER, S. 160. Vgl. PLATZ, S. 843. Der Einsatz von Govware findet aber in aller Regel heimlich, vor dem Betroffenen verborgen statt, siehe RUX, S. 832 und PLATZ, S. 839. Deshalb ist diese Analogie und der Terminus „Online-Durchsuchung“ ein wenig missverständlich, weil er (unzutreffend) an eine offene, angekündigte Massnahme erinnert, siehe m. E. zutreffend BUERMEYER, S. 154; PETRI, G N. 355; THIEL, S. 270.

258 Vgl. BUERMEYER, S. 160 ff.

259 Vgl. PETRI, G N. 355.

260 Vgl. GLESS 2012, S. 18 f.; BUERMEYER, S. 160 f.

Rahmen, besonders geschützt), welche die Behörde beabsichtigt zu erlangen, die Zielgerichtetheit (konkrete Person, Personengruppen, raumbezogen) und der Grad der Heimlichkeit der jeweiligen Massnahme. Bis zum Extremfall der weitflächigen, verdachtsunabhängigen Sondierung der Kommunikation im virtuellen Raum und der informationstechnischen Systeme aller Staatsbürger scheint es, zumindest im Schweizer Rechtsraum, ein weiter Schritt. Auch weniger ausgedehnte Überwachungsstrategien können indes gravierende Eingriffe in die Rechte Betroffener bedeuten. Die folgenden Ausführungen ein wenig vorwegnehmend, führt besonders die beträchtliche Streubreite (mitgesammelte Daten Dritter, Zufallsfunde etc.) der eingesetzten Methoden zu unbefriedigenden Situationen.[261] Derartige Massnahmen sind demnach vor allem zur Gefahrenforschung gebraucht zumeist als unverhältnismässig einzustufen, sofern für sie überhaupt eine genügende gesetzliche Ermächtigungsgrundlage besteht.[262]

1. Zielgerichtete vs. verdachtsgewinnende Überwachung

Bei der gezielten Überwachung vertiefen die sicherheitspolizeilichen oder strafverfolgenden Behörden gewonnene Hinweise oder ermitteln gegen eine bestimmte Person. Sie überprüfen oder „beobachten" bekannte Gefahren-Hot-Spots, die gesamte oder eine spezielle Aktivität einer oder mehrerer verdächtiger Personen im virtuellen Raum oder dringen in die Computer dieser Personen ein. Die verdachtsgewinnende Variante konzentriert sich weniger darauf, potenziell gefährliche Personen zu überwachen, als vielmehr potenziell gefährliche Aktivitäten, Verhaltensweisen und Merkmale aufzuspüren. Sie entspricht damit dem postmodernen Präventionsgedanken besser. Wesentliches Unterscheidungsmerkmal zur zielgerichteten Variante liegt im Ausgangspunkt vor ihrem Einsatz. Die verdachtsgewinnende Überwachung startet lediglich mit einem unbestimmten Rahmen (dem ungefähren Thema der zu verhindernden Bedrohungen) und ohne speziellen Verdacht beziehungsweise mit dem simplen und sehr abstrakten Grundverdacht, dass Straftaten im und über den virtuellen Raum geplant und verübt werden. Einsatzziel ist, einen nicht vordefinierten Verdacht oder Verdächtigen zu ermitteln, also nicht bereits vorhandene Informationen zu vervollständigen, sondern bewusst zufällig neue, unbekannte Informationen zu entdecken. Diese Art der Überwachung ist auf sorgfältig entwickelte Erkennungstaktiken abweichenden Verhaltens angewiesen. Wegen der Datenmenge und Unüber-

---

261 ZERBES, S. 361 f.; HASSEMER 1995, S. 483.

262 Siehe dazu unten Zweiter Teil, Kapitel I.C.

sichtlichkeit des virtuellen Raums kann diese Vorgehensweise insbesondere dort kaum noch manuell ausgeführt werden. Der menschliche Benutzer muss entsprechende Sondierungsprogramme benutzen. Mittels dieser Programme kann der virtuelle Raum nach vorgegebenen Kriterien durchsucht werden, was erst eine systematische Verdachtsforschung im virtuellen Raum ermöglicht.[263]

Relativ zielgerichtete Vorgehensweisen schöpfen die potenziellen Kapazitäten der heutigen Data-Mining- und Computer-Technologie bei Weitem nicht aus.[264] Die zielgerichtete Überwachung kann auch der Gefahrenabwehr dienen. Grundsätzlich ist sie jedoch eher ein Werkzeug, das Ermittlungen unterstützt und einen nicht unerheblichen Zeitaufwand (Vorbereitung inkl. Hypothesenformulierung, Vorlaufzeit und Auswertung) bedingt.

Govware setzt in ihrem jetzigen Entwicklungsstadium in der Regel einen konkreten oder konkretisierbaren Vorverdacht voraus. Das Ermittlungsziel muss in dem Sinne vordefiniert sein, dass vor ihrem Einsatz die zu überwachende Person, Gruppe oder der zu überwachende Raum und in den Grundzügen das zu erwartende Resultat, die erwünschten belastenden Daten, feststehen. Theoretisch liessen sich diese Programme aber auch ohne näher bestimmten Vorverdacht einsetzen. Spielten Behörden ihre Govware auf allen informationstechnischen Systemen in der Schweiz auf, erhielten sie Zugriff auf immens grosse und aufschlussreiche Datenbestände. Stünde ein leistungsfähiges Analyse- und Auswertungsprogramm zur Verfügung, könnten sie auf diese Art und Weise eine flächendeckende Überwachung des schweizerischen virtuellen Raums erreichen. Es ist aber unwahrscheinlich, dass Govware in der Schweiz je in diesem Ausmass zur Anwendung kommen wird. Abgesehen vom zu erwartenden Widerstand aus der Bevölkerung dürfte eine grossflächige Verbreitung der Govware heute aus technischen Gründen äusserst aufwendig zu kontrollieren und zu beaufsichtigen, und damit kaum zu finanzieren sein – wobei anzumerken ist, dass es mit fort-

---

263 Ein Beispiel eines bereits älteren virtuellen Sondierungsprogramms ist das Programm DCS-1000 („Carnivore"). Carnivore ist ein sogenannter „Packet Sniffer". Es durchsucht und filtert Datenpakete des Internetverkehrs, speichert sie und sondiert diese für den Ermittler vor, kann jedoch immer nur einigermassen zielgerichtet eingesetzt werden und ist relativ rasch überfordert mit grösseren Datenmengen. Das Programm eignet sich deshalb vor allem zum Einsatz mit observationsähnlichem Charakter, nicht zu einer gesamtheitlichen oder stichprobenartigen Überwachung des virtuellen Raums. Siehe dazu ANDRES, S. 241 f.; STRÖM, S. 164 ff.; Christian Schwarzenegger im Interview bei WEMANS, S. 30 f.

264 STRÖM, S. 164. Zu anderen Methoden der Sondierung des virtuellen Raums: NOWAK, S. 17; VAN DER HILST, S. 12 ff.

schreitender technologischer Entwicklung realistischer wird, diese technische Hürde zu überwinden. Es wäre folglich in weniger zurückhaltenden Staaten als der Schweiz durchaus denkbar, dass Govware, sobald effizientere und präzisere Systeme der automatischen Datenverarbeitung zur Verfügung stehen, auf den Computer eines jeden Internetnutzers installiert wird oder werden muss und diese Daten durch ein Analyseprogramm durchsuchbar gemacht werden.

Jedenfalls ist der Einsatz von Govware in etwas kleinerem Rahmen zum Beispiel für das heimliche Monitoring von Eingetragenen in Registern oder von Personen und Gruppen, die einer Risikokategorie zugeordnet werden, durchaus eine denkbare polizeilich-präventive Option.[265]

2. Echtzeit-Überwachung

Das Echtzeit-Monitoring von potenziellen Gefahrenherden und andere Varianten der Echtzeit-Überwachung im virtuellen Raum sind die Domäne der DPI-Technologien. Rechtliche Bedenken und die Zulässigkeitsfragen zunächst aussen vor gelassen, ermöglicht die DPI-Technologie den Providern und den staatlichen Behörden, direkt oder indirekt über die Provider, einen fast umfassenden Echtzeit-Zugriff auf den Inhalt derjenigen Daten, die sie übertragen.[266] Für behördliches Vorgehen gegen die Kriminalität ergeben sich daraus theoretisch sehr interessante Ansatzpunkte:

1. Die Behörde könnte sich in die laufende Kommunikation eines Verdächtigen mit Dritten einklinken und dem virtuellen Gespräch „zuhören", ohne die eigene Anwesenheit zu verraten.
2. Sie könnte jegliche Kommunikationsinhalte zur späteren Auswertung oder Beweissicherung speichern oder vom Provider speichern lassen.
3. Sie könnte sehr direkte und umfassende Monitorings von bestimmten oder allen Nutzern anordnen, die je nach Bedarf heimlich stattfinden oder den Nutzer beispielsweise im Moment eines Fehltritts mit einer (personalisierten) Meldung (ver)warnen. Oder sie könnte den Nutzer, will er eine unerwünschte

---

265 Vgl. GLESS 2012, S. 18 f.

266 Zu den Hintergründen der DPI-Technik sei nur erwähnt, dass sie ursprünglich die Netzwerksicherheit gewährleisten sollte und die Provider in die Lage versetzt, gewisse Pakete prioritär zu bearbeiten resp. zu übermitteln sowie den Nutzern etwa personalisierte Werbung zu präsentieren. Ausführlich dazu BEDNER, S. 1 ff. und 9 ff.; COOPER, S. 139 ff. und 150 ff.

virtuelle Aktivität ausüben, direkt an einen Polizeibeamten oder verdeckten Ermittler umleiten lassen.

4. Bei länger andauernder Überwachung von Personen könnten Nutzerprofile ihrer Kommunikationsgewohnheiten erstellt werden.
5. Schliesslich könnte die Behörde die über einen Provider laufende Kommunikation beziehungsweise den gesamten Internetverkehr automatisiert nach Mustern (Stichwörtern, Kriterien, Merkmalen) durchsuchen.[267]

Diese Aufzählung von möglichen Verwendungsformen ist sicherlich nicht abschliessend, vermittelt aber ein Bild des vielfältigen Potenzials dieser Technologie. Staatliche Behörden zeigen grosses Interesse daran: Insbesondere in Grossbritannien wird intensiv diskutiert, ob Ermittlungsbehörden zum Einsatz von DPI-Techniken ermächtigt werden sollen.[268] DPI-Techniken kamen in einigen Staaten in der Kriminalitätsbekämpfung und wohl vor allem im nachrichtendienstlichen Bereich bereits mehrfach zum Einsatz.[269] Hängig sind zum Beispiel seit 2008 zwei Fälle, in denen die National Security Agency (NSA) der USA und das Telekommunikationsunternehmen AT&T unbefugt amerikanische Bürger mittels dieser Technologie ausgehorcht und massive Datenbanken mit den gesammelten Informationen angehäuft hatten.[270]

Jüngste, sehr ähnliche Beispiele von grossangelegten, anlasslosen Datensammlungen und -sondierungen im virtuellen Raum sind das PRISM der Vereinigten Staaten und das britische TEMPORA.[271] In der Schweiz sind keine entsprechen-

---

267 Zum Ganzen: BENDRATH, S. 4, 12 f. und 25 f.; BEDNER, S. 9 ff. und 16 f.; WAGNER, S. 4 ff.

268 Bspw. als tragende Säule des tot geglaubten Interception Modernisation Programme (siehe dazu ausführlich das LSE Briefing), das scheinbar unter dem neuen Namen Communications Capabilities Development Programme unterdessen wieder zur Diskussion steht, siehe STEWART in PCPro vom 20. Februar 2012. Sehr ähnlich auch das britische TEMPORA.

269 Siehe dazu WAGNER, S. 11 f.; BENDRATH, S. 25 f.; BEDNER, S. 3 und 16 f. jeweils mit Beispielen und entsprechenden Hinweisen. WAGNER, S. 7-9 beschreibt den Einsatz der DPI zu Zensurzwecken in China und Tunesien.

270 Siehe dazu <https://www.eff.org/issues/nsa-spying>.

271 Siehe dazu etwa die folgenden Zeitungsartikel: RÜESCH in NZZ Online vom 7. Juni 2013; STEIER in NZZ Online vom 7. Juni 2013; MACASKILL EWEN/BORGER JULIAN/HOPKINS NICK/BALL JAMES in The Guardian vom 21. Juni 2013; Artikel „Snowden enthüllt britische Spionage“ in NZZ Online vom 22. Juni 2013; Artikel „Nach «Prism» jetzt «Tempora»“ in NZZ Online vom 23. Juni 2013; STEIER in NZZ Online vom 12. Juli 2013; STEIER in NZZ Online vom 18. Juli 2013; GREENWALD in The Guardian vom 31. Juli 2013. Ähnliche Tendenzen sind auch in anderen Staaten zu beobachten, siehe MONROY/BUSCH, S. 6 f.

den Fälle von DPI-Einsätzen von staatlicher Seite her bekannt. Was nicht heisst, dass es zu keinen Einsätzen gekommen ist: die Govware-Fälle in der Schweiz waren auch längere Zeit nicht publik.[272]

3. „Selbstregulation"

Das Internet schützte abweichlerische Inhalte besser vor staatlicher Überprüfung, solange es wenig durchsichtig und schwerer sondierbar war. Kann der Staat hingegen den virtuellen Raum effizient, also zeit-, kostengünstig und einigermassen zuverlässig, auf unerwünschte Informationen durchsuchen, erlangt er damit die Möglichkeit, jene zu unterbinden. Diese Errungenschaft kann in einigen Fällen, beispielsweise bei extremistischen Inhalten, anzustreben sein, kann jedoch vom Staat ebenso gut missbraucht werden.[273]

Allen anderen Ländern voran lenken Singapur und China den virtuellen Datenfluss in von ihnen definierte Bahnen. Sie verknüpfen propagandistisch verkündete Normenkataloge und Wertvorstellungen, Listen als „politisch" eingestufter Inhalte im Internet und symbolische Zensur zu einem Apparat der „Selbstregulation". Beispielsweise sind staatliche Behörden in Singapur ermächtigt, über die (quasi monopolisierten) Provider jeglichen Inhalt für den Konsumenten zu sperren (Beispiel: „Content-Filterung", Blocken bestimmter Websites oder Dienste). Gleichzeitig sind sowohl Service Provider als auch Content Provider an den von staatlicher Seite herausgegebenen „Internet Code of Practice" gebunden. Weichen sie von dessen Richtlinien ab, können sie dafür zur Verantwortung gezogen werden. Politische Inhalte müssen als solche deklariert und der staatlichen Behörde gemeldet werden. Medienwirksam in Szene gesetzte Stichprobenkontrollen unerwünschter Zugriffe, Kommunikation oder Aufschaltung von Inhalten sorgen für die nötige symbolische Machtdemonstration. Die DPI-Technologie ist in diesem Zusammenhang entscheidend. Sie lässt die Provider die ihnen obliegenden Massnahmen und Anforderungen erfüllen und den Staat die erwähnten Kontrollen vornehmen. Staat und Provider können dabei Inhalte nicht nur filtern oder blockieren, sondern auch plakativ oder subtil verändern. Aus der breit ange-

---

272 Vgl. dazu für Deutschland BEDNER, S. 3. Zu den Fällen mit Einsatz von Govware in der Schweiz, siehe unten Erster Teil, Kapitel II.D.2.

273 Beispiel China: Dort werden etwa die Suchmechanismen der „algorithmic knowledge discovery" u. a. in Verbindung mit der DPI-Technologie dazu verwendet, die virtuellen Räume von den Meinungen von „Dissidenten" zu säubern. Bspw. können Blogs auf abweichende Inhalte überprüft werden, siehe CHAU/XU. Vgl. NOWAK, S. 18 f.

legten Sondierung von öffentlich zugänglichen Informationen kann sich eine Kultur der Zensur herausbilden. Auch zu einer regelrechten Echtzeit-Zensur kann die DPI verwendet werden. Tatsächlich kommt diese Methode von allen in dieser Arbeit vorgestellten Methoden der „Idealvorstellung" des panoptischen Gebildes am Nächsten. Die Überwachung soll durch ihr teilweise sichtbares, an beliebigen Stellen plötzlich erfolgendes Auftreten als allgegenwärtig erscheinen.[274] Das Ziel dieses Vorgehen ist es, bei den Betroffenen Selbstzensur hervorzurufen, was die Vorstufe zu einem „selbst" regulierten, vollkommen staatskonformen Verhalten sein kann.[275]

Aus rechtsstaatlicher Sicht mag das vor allem in Hinblick auf einige der hier angeführten Extrembeispiele von praktizierenden Zensurstaaten abzulehnen sein. Aus diesen Praktiken können sich intensive Eingriffe in die Meinungsäusserungs-, Informations- und Medienfreiheit ergeben.[276] Die einzelnen Teilstrategien dieser Kontrollmethode erweisen sich jedoch als derart pragmatisch anwendbare Instrumente, dass sie spätestens seit den Anschlägen im Jahr 2001 in fast allen Ländern in irgendeiner Form vorzufinden sind.[277] Als Taktik der Kriminalitätsbekämpfung wirkt die Internetfilterung in der Art einer situativen Prävention, die viel Gewicht auf die effektive Verhinderung, weniger auf Abschreckung (vor allem der Provider durch „Konventionalstrafen"), von unerlaubten Inhalten legt. Die Ansätze, unerwünschte Internetinhalte zu blockieren oder zu

---

274 Siehe zum Ganzen LEE. Ausführlich zum chinesischen Internetzensursystem: BECKER K. B., S. 99-155. Zur Content-Filterung und zum Blockieren und Manipulieren von Webseiten, siehe BEDNER, S. 12-14; WAGNER, S. 2. Zu den einzelnen Werkzeugen des Internetfilterns, siehe MURDOCH/ANDERSON; COOPER, S. 152 f. Als perfide Manipulationsgelegenheiten bieten sich u. a. an: Eine Vorgehensweise etwa lässt Abweichler auf ihren eigenen Websites öffentlich diffamieren und brandmarken, indem dort (leicht veränderte) peinliche Auszüge aus ihrer Kommunikation publiziert werden. Subtiler können regimekritische Inhalte zu regimefreundlichen Inhalten umgeschrieben werden (vgl. dazu WAGNER, S. 10 f.).

275 Ausführlich und mit zahlreichen Hinweisen BECKER K. B., S. 123, 156-163 und 165.

276 In der Schweiz wären u. a. die Art. 16 und 17 BV betroffen. Präventive Eingriffe in die Meinungsfreiheit sind „verpönt" bzw. verboten (HÄFELIN/HALLER/KELLER, N. 491 f. S. 158; MOHLER 2012, S. 165). Insofern sei auch angemerkt, dass ein „brainwashing" der Jugend nicht lediglich durch die Offenheit des Webs, sondern im Gegenteil wahrscheinlicher durch eine eingehende virtuelle Zensur geschehen kann. Diesen Aspekt scheinen z. B. CHAU/XU, S. 474 zu übersehen.

277 LEE, S. 91; BECKER K. B., S. 99. Für die Schweiz siehe den Bericht BJ inter net, S. 15: Bereits im Jahr 1996 empfahl das Bundesamt für Justiz einen „Ehrenkodex" inkl. „Selbstregulierungssystem" zu entwickeln, damit die Netzwerkbranche „ihren Beitrag zur Verhinderung von Straftaten auf Netzwerken" leisten könne.

löschen und damit jedem möglichen Konsumenten den Zugang dazu schlicht zu verweigern, können als Zensur bezeichnet werden[278], zugleich muss man aber anerkennen, dass die punktuell eingesetzte Internetfilterung von unerwünschten Inhalten durchaus legitim und wirksam sein kann. Durch sie wird versucht, sicherzustellen, dass unerwünschte Inhalte im Internet nicht verbreitet werden können. Sie kann lediglich mit einem gewissem Aufwand und gewissen technischen Kenntnissen umgangen werden.[279] Gerade auch Probleme, die aufgrund der landesübergreifenden Struktur des Internets entstehen, werden versucht mittels Internet-Filterung zu umgehen, indem unerwünschte Inhalte vom eigenen Staatsgebiet ferngehalten werden sollen. Das Filtern von Inhalten und Selbstregulierungsmechanismen können somit theoretisch etwas leisten, was das Strafrecht und konventionelle (Überwachungs-)Massnahmen im Bereich des Internets wahrscheinlich nie werden leisten können.[280] Indes hat diese Vorgehensweise wenig mit Ursachenbehebung zu tun. Vielmehr unterdrückt sie lediglich Symptome.[281] Die Internetfilterung als präventiv-polizeiliche Massnahme neigt zudem dazu, nicht nur Gefährdungen für Rechtsgüter zu verhindern, sondern auch Moralvorstellungen zu transportieren und erhalten.[282] Verhaltenskodizes in Zusammenarbeit mit den Providern aufzustellen, mag ein gutes Mittel für eine milde Inhalt-Filterung sein. Es ist jedoch nicht unproblematisch, selbstregulierende Tendenzen der Provider oder Internet-Unternehmen zu fördern. Diese können über den Zweck des Selbstregulierungsauftrags hinaus bereits Inhalte filtern, die den Anschein haben, von Sittlichkeitsnormen abzuweichen.[283]

---

278 So etwa OBERHOLZER 2004, S. 52.

279 Mit Training und den entsprechenden Ressourcen stellen aber auch diese Barrieren kein allzu grosses Problem dar, siehe unten Erster Teil, Kapitel III.G.

280 Vgl. OBERHOLZER 2004, S. 51 f. und PERREY, S. 194 mit weiteren Hinweisen. Skeptisch zur Selbstregulierung im Internet: VALERIUS, S. 27 f.

281 Vgl. unten Dritter Teil, Kapitel V.E.

282 LOBSIGER 2004, S. 67, der in diesem Fall eine rechtlich unzulässige „exekutivbehördliche Sozialgestaltung" sieht.

283 Vgl. sehr anschaulich die übervorsichtige, moralisierende Firmenpolitik bei Facebook, die dazu führt, dass bspw. aus europäischer Sicht harmlose Inhalte entfernt werden. Siehe dazu HILGENDORF, S. 831; AUF DER MAUER/STEINER.

C. Bilanz: Ambitionen und praktische Erfahrung

1. Videoüberwachung

Zur Lancierung von Videoüberwachungsanlagen im öffentlichen Raum und später zur Verteidigung ihres fortlaufenden Betriebs wird auf vielerlei Vorzüge hingewiesen. Angepriesen wird insbesondere, dass die Videoüberwachung die staatlichen Behörden unterstütze, ihre Arbeit vereinfache und fehlende personelle Ressourcen ausgleiche.[284]

Mit Videoüberwachungssystemen soll theoretisch sichergestellt werden, dass erstens problematische Ereignisse in einem bestimmten Raum sofort erkannt werden und darauf zeitnah reagiert werden kann. Zweitens wird damit bezweckt, die Strafverfolgungsbehörden bei der Aufdeckung und Aufklärung von Straftaten durch gesammelte Videoüberwachungsinformationen zu unterstützen, im Sinne einerseits der Verdachtsgewinnung und -erhärtung und andererseits im Sinne der Sachverhaltsfeststellung und Beweissicherung. Drittens sollen potenziell problematische Ereignisse abgewehrt werden, indem Personen abgeschreckt werden, im überwachten Raum Straftaten zu begehen oder sich in unerwünschter Weise zu verhalten (zum Beispiel durch eine gut sichtbare Platzierung von Kameras oder das Anbringen von Warnschildern, welche auf die Videoüberwachung hinweisen). Viertens soll das subjektive Sicherheitsgefühl der Bevölkerung in den überwachten Räumen wiederhergestellt werden, gezeigt werden, dass die Sicherheitsbedürfnisse des Bürgers ernstgenommen werden, und die Bürger sollen nicht zuletzt daran erinnert werden, wachsam zu sein.[285]

Es ist jedoch fraglich, ob diese Ziele in der Praxis durch den Einsatz von Videoüberwachung erfüllt werden können.[286] Überzeugender ist der fünfte, praktischere Verwendungszweck, den häufig die anwendenden staatlichen Behörden selbst in den Diskurs einbringen: Vorausschauend platzierte Live-Videoüberwachungsanlagen mit weiträumigem Blickwinkel vermitteln einen guten Überblick über die Szenerie und erlauben damit im überwachten Raum eine koordinierte und flexible Einsatzführung aus der Ferne (beispielsweise bei Demonstrationen,

---

284 Siehe die bei TÖPFER, S. 274 ff. wiedergegebenen Ansichten. Vgl. auch GRAS, S. 99.

285 BÜLLESFELD 2002, S. 34; GRAS, S. 99 ff.; STUTZER/ZEHNDER, S. 112; ZEHNDER M., S. 26 f.; MÜLLER L. 2011, S. 26-30 mit weiteren Hinweisen. Vgl. KAMMERER 2008, S. 168. Zur Platzierung von Kameras und Warnschildern, siehe etwa NORRIS/ARMSTRONG, S. 44 Figure 2 und 54 Figure 6.

286 Kritisch zur Zweckerfüllung der Gefahrenabwehr ROGGAN 2001, S. 137 f. und 139.

sportlichen Grossanlässen etc.).[287] Primär ist dies zwar ein Argument vor allem für die nicht-personenbezogene Überwachung, die aus rechtlicher Sicht weit weniger Probleme als die dissuasive Variante mit sich bringt. Da modernere Systeme der grossflächigen Überwachung mit weitem Winkel dank Fähigkeit der Kameras zu hochauflösendem Zoom nahtlos vom Personen- und Verkehrsstrom-Überwachungsmodus in den Personenidentifikationsmodus und vom reinen Live-Überwachungsmodus in einen Aufzeichnungsmodus mit Datenspeicherung wechseln können und umgekehrt, ist eine Unterscheidung jedoch nahezu entbehrlich geworden.[288]

Die praktische Wirkung der Videoüberwachung des öffentlichen Raums lässt sich anhand eines grossen Portfolios an einschlägiger Literatur und zahlreichen Evaluationsstudien, insbesondere aus Grossbritannien, aber zunehmend auch aus Kontinentaleuropa, beurteilen. Vorläufig kann aus dem vorhandenen Material zur Videoüberwachung des öffentlichen Raums der Schluss gezogen werden, dass diese als Instrument des Vorgehens gegen Kriminalität die in sie gesetzten hohen Ansprüche in fast allen Bereichen nicht erfüllt.[289]

Die Erkenntnisse aus einschlägigen Studien und die entsprechende Literatur können wie folgt zusammengefasst werden:

- *Die Videoüberwachung scheint auf einige sehr spezifische Deliktstypen sowie bestimmte Verhaltensweisen präventiv zu wirken, sie vermag vermutlich gewisses Handeln zu unterdrücken, namentlich dann, wenn sie in einem sehr beschränkten Raum eingesetzt wird.* Sie kann in denselben Deliktsbereichen die Strafverfolgung unterstützen, insofern die Anzahl und Grösse der überwachten Gebiete sehr übersichtlich bleibt.[290] Die Videoüberwachung kann in diesen Fällen zudem dazu führen, dass Kriminalität verlagert wird und gewisse Personen vom überwachten Raum fortgewiesen beziehungsweise ferngе-

---

287 Siehe TÖPFER, S. 275; GRAS, S. 127 f. mit weiteren Hinweisen.

288 Siehe oben Erster Teil, Kapitel II.A.

289 Gl. M. wie HEMPEL/TÖPFER, S. 17: „While mostly advocates and critics belief that visual surveillance technology works, these studies explain that CCTV has to be seen in broader social and political contexts and that every optimistically belief in the effectiveness of the technology is pure fantasy." Ebenso etwa HEMPEL, S. 117 ff.; FARRINGTON ET AL., S. 33 f.

290 Siehe GILL/SPRIGGS, S. 117; FARRINGTON ET AL., S. 33; DITTON/SHORT, S. 162; BARTSCH, S. 45; GRAS, S. 167 f. und 178.

halten werden.[291] Es handelt sich bei den betroffenen Deliktskategorien indes tendenziell um solche am unteren Ende des Spektrums des Strafbedürfnisses beziehungsweise um lediglich unkonformes Handeln (Beispiel: Diebstähle, kleinere Sachbeschädigungen, Zigarettenstummel-auf-die-Strasse-Werfen usw.). Die Effekte im Allgemeinen sind nicht zufriedenstellend. Insbesondere scheint die Videoüberwachung nichts oder nicht viel gegen impulsive Delikte, wie beispielsweise Gewaltdelinquenz, ausrichten zu können.[292] MICHAEL ZEHNDER fand in seiner Evaluationsstudie der Videoüberwachung auf dem Bahnhofplatz Luzern keine signifikanten Abschreckungseffekte.[293] Eine von CLIVE NORRIS und GARY ARMSTRONG in Grossbritannien durchgeführte Studie ergab zudem, dass in den nahezu 600 Stunden Videoüberwachung, welche untersucht wurden, nur in 45 Fällen auf irgendeine Weise interveniert wurde – nur in einem Fall von der Polizei.[294] Mehr als die Hälfte der Interventionen basierte auf einer relativ willkürlichen Einschätzung der Verhaltensweise einer durch den Überwachungsangestellten als verdächtig beobachteten Person. Lediglich in zwölf Vorfällen (24%) führte sie zu einer Verhaftung.[295]

---

291 Siehe BÜLLESFELD 2002, S. 60, welcher eine Studie anführt, in deren Rahmen ein relativ starker Verlagerungseffekt beobachtet werden konnte (31% Anstieg der Kriminalitätsrate in den Aussenbezirken durch die Überwachung der Innenstadt). Ähnliches ergab die Evaluationsstudie bzgl. des Luzerner Bahnhofs, siehe ZEHNDER M., S. 103. Nicht eindeutige Verlagerungseffekte entdeckten BORNEWASSER/SCHULZ, S. 87, in einer Studie in Brandenburg (dazu auch BORNEWASSER, S. 150, der daraus vor allem Unterdrückungseffekte ableitet). FARRINGTON ET AL. 2007, fanden keine Nachweise für Verlagerungseffekte in ihrer Evaluationsstudie. KUBERA, S. 134 ff., vermutet, auch der Verlagerungseffekt falle „strukturell und täterspezifisch unterschiedlich aus". Sehr ähnlich GRAS, S. 172 ff.

292 Siehe WELSH/FARRINGTON, S. 41, welche in ihrer Meta-Evaluation von 22 Studien eine durchschnittliche Reduktion der Kriminalitätsraten von (vernachlässigbaren) 4% feststellten und DIES., S. VII; GILL/SPRIGGS, S. 58 f., 120 und 34 (Table 3.5); BORNEWASSER, S. 150. KRABBENBORG, S. 61 f., wertet die Ergebnisse seiner niederländischen Studie zwar etwas optimistischer, aber auch dort beeinflusste die Massnahme vornehmlich den Fahrzeugdiebstahl oder Vandalismus. Ebenso GILL/SPRIGGS, S. 118; SCHRÖDER, S. 51. Nach Einschätzung von STEGMANN M., S. 84 ff. konnte in der bernischen Gemeinde Studen durch Videoüberwachung Sachschaden aus Vandalismus vermindert werden.

293 ZEHNDER M., S. 101.

294 NORRIS/ARMSTRONG, S. 166.

295 NORRIS/ARMSTRONG, S. 167 ff.

- *Die Ergebnisse aus den verschiedenen Studien sind meist gegensätzlich und wenig eindeutig.*[296] Zum Beispiel führten JASON DITTON und EMMA SHORT in Schottland eine Studie zum Effekt der Videoüberwachung auf offener Strasse durch. Sie verglichen dabei die Kriminalitätsrate vor und nach der Installation von 12 respektive 32 Kameras in Airdrie (1992; Kleinstadt) und Glasgow (1994; Grosstadt). Der Einsatz des CCTV-Überwachungssystems im öffentlichen Raum im Jahr 1992 in Airdrie war für Schottland eine Premiere. Die Autoren konnten in dieser Studie einen unerwarteten und interessanten Effekt beobachten: Während in Airdrie nach der Installation der Kameras die aufgezeichnete Kriminalitätsrate sank und die Entdeckungsrate stieg, geschah in Glasgow das genaue Gegenteil.[297] Sie schliessen daraus, auch wenn sie dieses Ergebnis relativieren, dass die Videoüberwachung situationsbedingt verschieden wirke.[298]

  Die Aussagekraft dieser Untersuchung hinsichtlich der beobachteten Effekte ist problematisch. Allgemein sind in einer derartigen Untersuchung verschiedene das Ergebnis potenziell verfälschende Faktoren zu berücksichtigen und auszuklammern.[299] Die Wirkung eines neuinstallierten Videoüberwachungssystem isoliert zu betrachten, ist praktisch nicht möglich und diese somit als Hauptursache etwa einer Veränderung der Kriminalitätsrate im überwachten Gebiet kaum plausibel nachzuweisen.[300] Können die Effekte nicht zuverlässig gemessen beziehungsweise eingeordnet werden, verbleibt den Studien immerhin, einen Beitrag zu leisten, indem durch sie Spekulationen abgeleitet werden können.[301] Dies kann hilfreich für die Weiterentwicklung von Kriminalitätskontrollmassnahmen oder für den Fachdiskurs sein. Problematisch in-

---

296 Siehe WELSH/FARRINGTON, S. 41 (nur in 11 der 22 Studien wurde ein gewünschter Effekt ersichtlich, in fünf sogar ein unerwünschter); FARRINGTON ET AL., S. 33 f.; ZEHNDER M., S.101 ff.; BÜLLESFELD 2002, S. 59 ff.; GRAS, S. 166 ff., 178 und 189; HEMPEL/TÖPFER jeweils mit Hinweisen auf Studien. Vgl. MÜLLER L. 2011, S. 243.

297 DITTON/SHORT, S. 162: Ein geringer Anstieg der Aufklärungsquote in Airdrie von 8% steht einer Reduzierung derselben in Glasgow von 4% gegenüber. Die Reduzierung der Kriminalitätsrate bezifferte sich in Airdrie auf 21%; in Glasgow erhöhte sich die Rate um 9%.

298 DITTON/SHORT, S. 167. Vgl. BARTSCH, S. 44.

299 NORRIS/ARMSTRONG, S. 64; BARTSCH, S. 45; GILL/SPRIGGS, S. 115.

300 Auch weil die Videoüberwachung meist in Verbindung mit anderen Massnahmen praktiziert wird (was die Zuschreibung von Effekten erschwert). Siehe GILL/SPRIGGS, S. 118 f.; WELSH/FARRINGTON, S. 42; BORNEWASSER/SCHULZ, S. 90 f.; KUBERA, S. 127 und 129.

301 NORRIS/ARMSTRONG, S. 94 f., meinen, dass neuere Evaluationen die Effekte der Videoüberwachung immer adäquater erfassen würden.

des ist ihre unreflektierte oder bewusst täuschende Verwendung, etwa für politische Zwecke.[302] Bezüglich der Videoüberwachung ist ausserdem immer zu beachten, dass sie, gemäss eigenem Anspruch, entweder zur Enthüllung von ansonsten im Dunkelfeld verbliebenen Straftaten führt oder potenzielle Täter durch Abschreckung von der Begehung von Delikten abhält. Beide Effekte können zwar als Erfolg gewertet werden. Indes machen sie dem jeweils anderen Ansatz den Erfolg streitig.[303] Werden mehr Straftaten entdeckt, schadet das der Bilanz der Abschreckung. Zieht man diesen Umstand in die Interpretation der Studien mit ein, präsentieren sich die Ergebnisse bezüglich der *Verhinderung* von Straftaten schlechter. Dasselbe gilt e contrario im Fall eines aufgedeckten Dunkelfelds.[304]

- *Bei der Erstinstallation der Videoüberwachung sind verstärkte „Einführungseffekte" zu beobachten.* Studien ergaben, dass die mit übertrieben kommunizierten Wirksamkeitsversprechen verkündete Einführung hohe Erwartungen in der Bevölkerung weckte und für einen raschen, indes nur kurzfristigen Abfall der Kriminalitätsraten in der Einführungsphase der Massnahmen sorgte. Teilweise wurden in dieser Hinsicht sogar vorgelagerte Effekte beobachtet (wenn etwa bereits im Vorfeld der Installation Werbung im grossen Stil betrieben wurde). Sobald sich die allgemeine Aufregung jedoch legte, normalisierte sich auch das Verhalten im nämlichen Raum wieder.[305]
- *Weitwinklige Kamerasysteme an gezielt gewählten Orten erleichtern die interventionsgebundene Einsatzführung.* Nur, wenn genügend polizeiliche Einsatzkräfte zur Intervention bereit stehen, kann das Überwachungssystem indes auf diese Art und Weise als vorteilhaftes Hilfmittel verwendet werden.[306] Videoüberwachung kann demnach als „Baustein operativer Polizeiarbeit" einen gewissen Nutzen erbringen.[307]

---

302 Vgl. BÜLLESFELD 2002, S. 62; GEHRING, S. 67.

303 Siehe DITTON/SHORT, S. 162 f.; GILL/SPRIGGS, S. 61; ZEHNDER M., S. 101 ff.

304 Siehe DITTON/SHORT, S. 172 insb. Fn. 13.

305 Siehe KUBERA, S. 127 und 129 („Placebo-Effekt"); BORNEWASSER/SCHULZ, S. 90; GRAS, S. 177 und 210 mit weiteren Hinweisen. Vgl. KAMMERER 2008, S. 77; MÜLLER L. 2011, S. 244. Auch die Grafiken 1 und 2 in DITTON/SHORT, S. 154 f. deuten darauf hin.

306 TÖPFER, S. 275 ff. mit weiteren Hinweisen. Vgl. GRAS, S. 127 ff.; MÜLLER L. 2011, S. 236.

307 TÖPFER, S. 280.

2. Überwachung des virtuellen Raums

Das heimliche Einschleusen von Govware in ein informationstechnisches System verspricht gegenüber konventionellen Überwachungs- beziehungsweise Ermittlungsmethoden einige Vorteile. Abgesehen davon, dass die Zielperson nicht vorgewarnt wird und dadurch den Untersuchungszweck nicht vereiteln kann (indem sie Daten beziehungsweise Datenträger vernichtet), können, befindet sich die Govware einmal auf dem System der Zielperson, viele Verschlüsselungstechnologien und Sicherheitsvorkehrungen umgangen werden. Daten und Kommunikation können live und direkt erhoben sowie abgehört und nebenher auch „flüchtige Daten" wie Passwörter, gelöschte Dateien und Erkenntnisse über das Nutzungsverhalten der Zielperson gewonnen werden.[308]

Das unentdeckte Aufspielen der Govware auf das Zielsystem ist indes eine Herausforderung, insbesondere, wenn dafür gesorgt sein soll, dass unbeteiligte Dritte nicht mitbetroffen werden. Neben dem unmittelbar „physischen" Installieren des Programms, fallen Lösungen in Betracht, die ein Aufspielen ohne direkten („physischen") Zugang zum Zielsystem zwar ermöglichen, ihre Erfolgswahrscheinlichkeit hängt aber unter anderem von Faktoren ab, welche die zuständige Behörde nicht beeinflussen kann. So können Sicherheitsvorkehrungen von einigermassen wachsamen Systemnutzern eine beachtliche Hürde darstellen.[309] Auch nach der Installation können zahlreiche Schwierigkeiten und Schwachstellen die Bedeutung dieser Methode schmälern.[310]

Demgegenüber sind auch die für einen Einsatz aufzuwendenden Mittel nicht zu unterschätzen. Es muss ein Programm geschrieben werden, das, um aufgespielt werden und um verborgen auf dem Zielsystem verbleiben zu können, die Sicherheitsvorkehrungen des Zielsystems (Firewall, Antivirensoftware etc.) umgehen

---

308 BVerfGE 120, 274 (279); BUERMEYER, S. 158 ff.; HOFMANN, S. 121; PLATZ, S. 839 Fn. 3 und 840; Botschaft BÜPF 2013, S. 2772. Wobei technisch versierte Verdächtige entsprechende Vorkehrungen in ihren Computersystemen vornehmen und damit trotzdem gewarnt sein dürften, siehe BUERMEYER, S. 165 f.

309 Siehe dazu PLATZ, S. 340 sowie BUERMEYER, S. 163 f. und 165, der die Infiltration für „schon mit wenig technischem Sachverstand relativ problemlos zu verstellen" hält. Vgl. DERS., S. 166 Fn. 83.

310 Siehe dazu die CCC Analyse. Vgl. PLATZ, S. 840; BUERMEYER, S. 164 f. Wobei der frühere Flaschenhals des übertragenen Datenvolumens bei den heute üblichen Abonnementen mit hohen Bandbreiten und ständiger Verbindung kaum noch Bedeutung haben dürfte. Freilich im Falle einer präventiven Überwachung von Personengruppen stellte sich auch hier die Frage der übersichtlichen Archivierung und der Lagerung der gesammelten Daten.

kann, ohne die noch zu besprechenden rechtlichen Vorgaben zu verletzen.[311] Die einsetzende Behörde muss die dafür benötigten Kapazitäten und Spezialisten verfügbar haben und, bis die entsprechenden Aufgaben erledigt sind, anderswo entbehren können. Alternativ kann sie Teile des Einsatzes (zum Beispiel das Schreiben des Programms, das Sammeln der Daten) an eine Drittbehörde mit den entsprechenden Ressourcen oder an Private auslagern, was jedoch, wie noch dargestellt wird, problematisch sein kann.[312]

Sehr ähnliche Probleme sind bei der DPI festzustellen. In einem DPI-Kit stecken viel Arbeit, eine Menge Programmroutinen und komplexes Equipment. Trotzdem, oder gerade deswegen, wird es sehr schwierig respektive sehr teuer sein, die DPI-Kits mit Upgrades auf demselben (hohen) technischen Niveau der von den Internetprovidern verwendeten Apparaturen und Programme oder neuartigen Dienste zu halten, das garantiert, dass die Masse an Informationen des Datenverkehrs in Echtzeit abgefangen und analysiert werden kann.[313] Erschwerend kommt hinzu, dass der Datenverkehr und die verschiedenen Dienste meist über mehrere unterschiedliche Anbieter laufen, von denen sicher einige ihren Sitz ausserhalb der Schweiz haben dürften.[314]

Die Kriminalprävention durch das Filtern oder Blockieren von Daten überzeugt wohl vor allem in der Theorie. Die Studien von MACKINNON und von ZITTRAIN/EDELMAN weisen jedenfalls darauf hin, dass die umfangreiche Internet-Zensur in China wenig statisch, willkürlich und sehr unvollkommen ist. Auch BECKER stellt viele systemimmanente Probleme und Umgehungsmöglichkeiten fest.[315]

---

311 Siehe HANSEN/PFITZMANN. Gemäss Botschaft BÜPF 2013, S. 2774, gaben Fachleute aus dem Polizeibereich an, für jeden Einsatz werde ein speziell auf das Zielsystem angepasstes Programm konzipiert.

312 KATZENSTEIN, N. 8 zu Art. 280 StPO misst technischen Überwachungstechnologien deshalb „marginale Bedeutung" in der Praxis zu. Vgl. ZERBES, S. 13 mit Hinweisen auf die Situation in Österreich.

313 LSE Briefing, S. 16 f. und 25 f.

314 LSE Briefing, S. 17 f.

315 BECKER K. B., S. 166-187 mit mehreren Beispielen und weiterführenden Hinweisen.

D. Gesetzliche Grundlagen in der Schweiz

1. Videoüberwachung

Die Kompetenzen im Bereich der Videoüberwachung liegen primär bei den Kantonen und Gemeinden, sofern bei der infrage stehenden Massnahme die typischen sicherheitspolizeilichen Zwecke der Gefahrenabwehr überwiegen, mithin untergeordnete repressive lediglich präventiv-polizeilichen Zwecken dienen.[316] Die Kantone beziehungsweise Gemeinden können in ihren Polizeigesetzen zudem darüber bestimmen, unter welchen Voraussetzungen eine repressive Verwendung der gestützt auf ihre Polizeigesetze präventiv-polizeilich erhobenen Daten zulässig sein soll.[317] Steht indes der Zweck der Strafverfolgung im Vordergrund, sind die strafprozessualen Bestimmungen des Bundes massgebend.[318] Vereinzelte nicht lediglich subsidiäre Kompetenzen des Bundes finden sich darüber hinaus namentlich im Bereich des Staatsschutzes, des Grenzschutzes und der Personenbeförderung.[319]

Die kantonale und kommunale Regelungskompetenz wurde in den letzten zehn Jahren rege in Anspruch genommen und die Videoüberwachung mittlerweile in

316 LIENHARD/HÄSLER, S. 118; SCHWEIZER 2008, Vorbemerkungen zur Sicherheitsverfassung, N. 12; Antwort des Bundesrats vom 25. Februar 2009 i. S. Margret Kiener Nellen; Bericht EJPD 2007, S. 25 und 29; HANSJAKOB 2010, N. 3 zu Art. 280 StPO; MÜLLER L. 2011, S. 195 mit weiteren Hinweisen. Vgl. Art. 4 Abs. 1 BWIS.

317 Womit sie dahingehend Beweisverwertungsverbote vorsehen können. Siehe dazu MÜLLER L. 2011, S. 196; WOHLERS, N. 4 zu Art. 139 StPO. Im deutschen Recht ist diese Frage umstritten, siehe zustimmend BARTSCH, S. 173 und ablehnend BÜLLESFELD 2002, S. 215.

318 MÜLLER L. 2011, S. 196 f. Das ist bspw. dann der Fall, wenn Videokameras nach Art. 282 ff. StPO zu Observationszwecken in Ermittlungsverfahren eingesetzt werden. Vgl. für Deutschland BÜLLESFELD 2002, S. 229; BARTSCH, S. 241.

319 Antwort des Bundesrats vom 25. Februar 2009 i. S. Margret Kiener Nellen. Ausführlich MÜLLER DISS, S. 197-200, mit Hinweisen und Beispielen. Teils kritisch MOHLER 2012, S. 78. Bspw. sieht das BWIS den (vorbeugenden) Einsatz technischer Überwachungsgeräte im öffentlich zugänglichen Raum in Art. 14 Abs. 2 lit. f vor. Art. 7 des Vorentwurfs des Polizeiaufgabengesetzes des Bundesgesetzes über die polizeilichen Aufgaben des Bundes vom November 2009 (Polizeiaufgabengesetz; PolAG) sollte eine umfassende Regelung für die sicherheitspolizeiliche Videoüberwachung auf Bundesebene schaffen, vgl. HANSJAKOB 2010, N. 3 zu Art. 280 StPO und den Bericht PolAG. Der Bundesrat hält das PolAG indes noch solange in der Schwebe, bis der Bericht zur Klärung der Kompetenzen in der inneren Sicherheit (Postulat Peter Malama vom 3. März 2010) vorliegt, siehe Medienmitteilung EJPD vom 30. März 2011.

den meisten Polizeigesetzen und entsprechenden Verordnungen normiert.[320] Restriktivere Erlasse erlauben die Videoüberwachung von öffentlichen Plätzen lediglich unter der Bedingung, dass diese Personen nicht zu identifizieren vermag und das Material weder aufgezeichnet noch aufbewahrt wird.[321] Offenere Erlasse erlauben beispielsweise, die Aufzeichnungen über einen bestimmten Zeitraum aufzubewahren und allenfalls zu Strafverfolgungszwecken zu verwenden.[322] Unter anderem aufgrund der betont föderalistischen Struktur der Schweiz besteht eine uneinheitliche Rechtslage.[323]

2. Überwachung des virtuellen Raums

Die Überwachungstätigkeit des Staats im Internet wirft regelmässig neue Fragen auf. Eingesetzte Massnahmen eröffnen meist kaum abschätzbare Problembereiche.[324] Govware gelangte in der Schweiz in wenigen Fällen auf Bundesebene (gestützt auf Art. 66 Abs. 2 BStP) und in einigen Fällen auf Kantonsebene, bekanntermassen im Kanton Zürich und in Westschweizer Kantonen, zur Anwendung.[325] In Deutschland und den USA kam Govware bereits öfters zum Einsatz.

---

320 Übersicht über die Erlasse auf Bundesebene und kantonaler Ebene: FLÜCKIGER, S. 216 f.

321 Ausführlich zur konkreten Rechtslage im Kanton Bern und den Gemeinden: STEGMANN M. Etwa das Polizeigesetz der Stadt Chur vom 24. Februar 2008 (PG Chur; Churer Rechtsbuch 411) in Art. 12.

322 So bspw. das Polizeigesetz des Kantons Bern vom 8. Juni 1997 (PolG Bern; Bernische Systematische Gesetzessammlung 551.1), das den Einsatz von Bildübermittlungs- und Bildaufzeichnungsgeräten an öffentlichen Orten (Art. 51a) sowie zum Schutz öffentlicher Gebäude (Art. 51b) inkl. Aufbewahrung und repressiver Verwendung (Art. 51e) zulässt, soweit die Überwachungsgeräte deutlich gekennzeichnet werden (Art. 51d). Zur vorgeschriebenen Kennzeichnung in bernischen Gemeinden, siehe STEGMANN M., S. 78.

323 Vgl. MÜLLER L. 2011, S. 360 mit weiteren Beispielen kantonaler Gesetze. Insofern hat sich der von BAUM, N. 29 befürchtete „«Flickenteppich» von 26 unterschiedlichen Regelungen" verwirklicht.

324 Vgl. HILGENDORF, S. 825 und 828. Siehe ausführlich unten Zweiter Teil, Kapitel I.D.-I.I.

325 Siehe STÖCKLI, S. 15; WEBER/WOLF/HEINRICH, N. 22; JOTTERAND/MÜLLER/TRECCANI, N. 2-4 und insb. N. 34; Botschaft BÜPF 2013, S. 2772 f.; den Artikel „Trojaner passen nicht zu einem Rechtsstaat" in Tages-Anzeiger Online vom 14. Oktober 2011 und SCHMID/BAUMGARTNER in NZZ Online vom 15. Oktober 2011. Dem Urteil i. S. der Zürcher Linksaktivistin Andrea Stauffacher (Bundesstrafgericht SK.2011.1 vom 8. November 2011/21. März 2012) sind indes keine Ausführungen zum Einsatz oder zur Zulässigkeit der Govware zu entnehmen. Zur Praxis und Rechtslage in Österreich, siehe ZERBES, S. 38 und OGH 13 Os 83/08t vom 27. August 2008. Vgl. auch TSCHENTSCHER, S. 388 f.

Die sich daraus ergebende Entrüstung in Deutschland brachte überhaupt erst die Schweizer Fälle ans Licht der Öffentlichkeit.[326]

a. De lege lata

Die Eingriffsschwere und der geheime Einsatz von Govware verlangen für die entsprechende Tätigkeit der staatlichen Behörden eine eindeutige Grundlage in einem formellen Gesetz.[327] In der Schweiz ist unklar, ob Art. 246 ff., 269 und 280 StPO diese Grundlage leisten können. Der überwiegende Teil der Lehre und Vertreter aus der Praxis gehen – nach der hier vertretenen Ansicht aus überzeugenden Gründen – davon aus, dass momentan weder im Regelungsbereich der StPO noch auf dem Gebiet der Gefahrenabwehr eine klare gesetzliche Grundlage für den Einsatz von Govware in irgendeiner Form besteht[328] und zuvor wohl auch in keiner kantonalen StPO bestanden hatte[329]. Einige Stimmen aus der schweizerischen Praxis hingegen erachten die Art. 269 und 280 StPO als ausreichende Ermächtigungsgrundlage, Govware einzusetzen und vereinzelte Zwangsmassnahmengerichte scheinen, sollte denn ein derartiger Antrag gestellt werden,

---

326 Zu den Fällen und zur Diskussion in Deutschland: Urteil des BGH StB 18/06 vom 31. Januar 2007; Urteil des Landesgerichts Landshut 4 Qs 346/10 vom 20. Januar 2011; das wegweisende Urteil des BVerfGE 120, 274; BUERMEYER (mit Hinweis auf weitere deutsche Urteile, siehe S. 162 f.); BRAUN; ALBRECHT F.; HOFMANN; den Artikel „Staatstrojaner: Behörden spähten 100mal Computer aus" in Spiegel Online vom 15. Oktober 2011.

327 KATZENSTEIN, N. 16 zu Art. 280 StPO; HANSJAKOB 2010, N. 2 zu Art. 280 StPO; BRAUN, S. 681; ZERBES, S. 42; SCHWEIZER 2008, N. 46 zu Art. 13 BV mit Hinweisen auf die Rechtsprechung des EGMR; Botschaft BÜPF 2013, S. 2777 f. Vgl. JAGGI, S. 2.

328 Gl. A. wie HANSJAKOB 2011, N. 14 ff.; DERS. 2010, N. 2 zu Art. 280 StPO; KATZENSTEIN, N. 16 zu Art. 280 StPO; HEIMGARTNER, S. 41; ZERBES, S. 38. Dieser Ansicht sind auch RHYNER/STÜSSI, S. 469 und WEBER/WOLF/HEINRICH, N. 25 f., soweit es nicht bloss um die Überwachung von Gesprächen gehe, da sich diese unter Art. 269 StPO subsumieren lasse. Offen lässt die Frage SCHMID 2009b, N. 4 Vor Art. 269-279 StPO und N. 8 zu Art. 280 StPO. Siehe auch die Äusserungen aus Lehre und Praxis bei STÖCKLI, S. 15 ff.

329 GOLDSCHMID, S. 90 (Kanton Bern); HEIMGARTNER, S. 41 (insb. Fn. 248 und 249) mit weiteren Hinweisen. Im Kanton St. Gallen verweigerte der zuständige Bewilligungsrichter den Strafverfolgungsbehörden in einem Fall aus dem Jahr 2006 (siehe GVP 2006 Nr. 106, S. 295 f.), den E-Mail- und Chat-Verkehr sowie den Festplatteninhalt mittels Govware zu durchsuchen. Vgl. dazu PLATZ, S. 839 f.

vorerst eine allfällige Genehmigung, zumindest bei schweren Fällen, nicht ausschliessen zu wollen.[330]

Art. 269 Abs. 1 StPO erlaubt zwar, den Post- und Fernmeldeverkehr zu überwachen[331], worunter die Überwachung der Kommunikation direkt an der Quelle im Zielcomputer fallen könnte (Variante 1; „Quellen-TKÜ"). Umstritten ist aber, ob die Bestimmung den Vorgang des Eindringens in den Zielcomputer – ein grundsätzlich rechtswidriges Verhalten im Sinne von Art. 143bis StGB (unbefugtes Eindringen in ein Datenverarbeitungssystem) – ausdrücklich erlauben muss oder ob die Ermächtigung zur Überwachung diesen Vorgang umfasst.[332] Umstritten ist zudem, ob Art. 280 StPO unterstützend einspringen kann. Diese Bestimmung sieht zwar den heimlichen Einsatz „technischer Überwachungsgeräte" vor, jedoch lediglich zur Aufzeichnung von Bild und Ton, von Vorgängen oder zur Feststellung von Standorten von Personen und Sachen. Die Durchsuchung von Datenbeständen auf einem informationstechnischen System fügt eine Dimension hinzu, die Art. 280 StPO wohl nicht abdeckt.[333] Die Govware unter dem Globalbegriff „technische Überwachungsgeräte" und über eine extensive Auslegung von Art. 280 StPO einzusetzen, scheint somit problematisch.[334] Zur Durchführung einer Online-Durchsuchung beziehungsweise Online-Überwachung kann sich die Behörde schliesslich auch nicht auf die Art. 246 ff. StPO zur Durchsuchung von Aufzeichnungen berufen. Letztere hat, im Gegensatz zu Ersterer, offen, also nur mit Wissen des Betroffenen, stattzufinden.[335] Hingegen dürfte Art.

---

330 Siehe dazu die Äusserungen aus der Praxis bei STÖCKLI, S. 17. JOTTERAND/MÜLLER/TRECCANI, N. 15 und 24 f. sehen in den Art. 269 und 280 StPO, ausgenommen für den „unlimitierten Zugang" auf alle Systemperipherien und die „komplette Kontrolle" über den Computer, grundsätzlich eine genügende gesetzliche Grundlage. Auch MÉTILLE, S. 7 f., vertritt diese Ansicht unter gewissen Vorbehalten.

331 Wozu auch bspw. die Internet-Telefonie gehört. Siehe HANSJAKOB 2011, N. 14.

332 HANSJAKOB 2011, N. 15 f. ist der Ansicht, dass Art. 269 StPO diese Ermächtigung nicht mit umfasse. So auch der Erläuternde Bericht BÜPF, S. 43; Botschaft BÜPF 2013, S. 2773. A. A. sind neben JOTTERAND/MÜLLER/TRECCANI, N. 15 und MÉTILLE, N. 37, auch RHYNER/STÜSSI, S. 469 und WEBER/WOLF/HEINRICH, N. 25. MÉTILLE, N. 27 verweist analog auf Art. 280 StPO, der die heimliche Installation von Mikrofonen oder Kameras in Wohnungen oder Fahrzeugen auch nicht ausdrücklich von der Strafbarkeit nach Art. 186 StGB ausnehme.

333 Vgl. BRAUN, S. 684. Die Anwendungsbereiche von Art. 280 StPO sind zudem abschliessend aufgezählt, nicht unter diese subsumierbare Varianten sind nicht zulässig, siehe KATZENSTEIN, N. 12 f. zu Art. 280 StPO und HEIMGARTNER, S. 40.

334 Vgl. Martin Steiger bei STÖCKLI, S. 17.

335 HANSJAKOB 2011, N. 21 f.; Botschaft BÜPF 2013, S. 2779. Die „transparente Vorgehensweise" stellt ein wesentliches Element der Art. 246 ff. StPO dar, siehe HEIMGARTNER, S. 41.

269 StPO hinsichtlich der *zielgerichteten* Überwachung von Kommunikationsinhalten und Randdaten im Strafverfahren eine genügende gesetzliche Grundlage für den Einsatz von DPI-Technologien darstellen, da mit diesen gerade nicht in Datenverarbeitungssysteme eingedrungen wird. Für Funktionen, die über das reine Überwachen der Kommunikation hinausgehen, würde diese Grundlage hingegen nicht ausreichen.[336]

b. De lege ferenda

Im Bereich der Gefahrenabwehr gestaltet sich die Lage klarer: Eine gesetzliche Grundlage für den präventiven Einsatz von Govware ist zurzeit nicht vorhanden.[337] Der in der ursprünglichen Fassung der Revisionsvorlage BWIS II vorgesehene E-Art. 18m, der den zuständigen Bundesbehörden diese Methode erlauben sollte, wurde im Überarbeitungsprozess zur dritten Vorlage aufgegeben.[338] Indes soll VE-Art. 22 Abs. 1 lit. g des neu zu schaffenden Nachrichtendienstgesetzes (NDG) den präventiven Einsatz von Govware gesetzlich verankern.[339]

Hinsichtlich des Einsatzes von Govware im Strafverfahren sieht die kommende Revision des BÜPF und der StPO Änderungen vor, mit denen diese an die technischen Entwicklungen angepasst werden sollen.[340] Die Revision soll die StPO

---

336 Mittels DPI können etwa Daten in Echtzeit verändert, umgeleitet oder unterdrückt werden, siehe BEDNER, S. 2 und oben Erster Teil, Kapitel II.B.2.

337 Vgl. Botschaft BÜPF 2013, S. 2771.

338 E-Art. 18m BWIS sollte unter dem Titel „Geheimes Durchsuchen eines Datenverarbeitungssystems" lauten: „Lassen konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin ein ihm oder ihr zur Verfügung stehendes und gegen Zugriff besonders gesichertes Datenverarbeitungssystem benutzt, kann dieses vom Bundesamt durchsucht werden. Die Durchsuchung kann ohne Wissen des mutmasslichen Gefährders oder der mutmasslichen Gefährderin erfolgen." (Entwurf BWIS, S. 5148 f.) Siehe dazu die Zusatzbotschaft BWIS II 2010, S. 7851; den Bericht zum Vorentwurf des Nachrichtendienstgesetzes vom 8. März 2013, S. 5 ff.; WEBER/WOLF/HEINRICH, N. 30. Vgl. HANSJAKOB 2011, N. 28 f. und analog die ausführliche, abschlägige Beurteilung einer ähnlichen, angestrebten Gesetzesänderung in Deutschland durch das BVerfG in seinem Urteil BVerfGE 120, 274 (insb. 315 ff.).

339 Erlaubt werden soll (genehmigungspflichtig) das heimliche Eindringen in Computersysteme und Computernetzwerke, um dort vorhandene oder von dort aus übermittelte Informationen zu beschaffen (Ziff. 1) und den Zugang zu Informationen zu stören, zu verhindern, oder zu verlangsamen, falls diese auf kritische Infrastrukturen verwendet werden (Ziff. 2). Siehe den Vorentwurf NDG vom 8. März 2013 und den Bericht Vorentwurf NDG, S. 36 ff.

340 Der Bundesrat verabschiedete die Botschaft zur Revision des BÜPF am 27. Februar 2013.

unter anderem durch eine ausdrückliche gesetzliche Grundlage für den Einsatz von Govware im Strafverfahren ergänzen.[341] Der entsprechende E-Art. 269ter StPO in seiner jetzigen Form ist zu Recht restriktiver und klarer gefasst als noch VE-Art. 270bis StPO, welcher zunächst in die Vernehmlassung gegeben wurde. VE-Art. 270bis StPO hätte Strafverfolgungsbehörden ermächtigen sollen, aktiv in das zu überwachende Datenverarbeitungssystem einzudringen, spezielle Informatikprogramme einzuführen und allenfalls zusätzliche Programme zu verwenden, um Antivirenprogramme zu umgehen.[342] Diese offen formulierte Regelung wurde von vielen Seiten kritisiert.[343] Im Ergebnis kann man sich der Einschätzung von GLESS anschliessen, dass der VE-Art. 270bis StPO den Anforderungen des Bestimmtheitsgrundsatzes nicht genügt hätte.[344] Die überarbeitete Ermächtigungsnorm von E-Art. 269ter StPO statuiert deshalb stärker einschränkende Bedingungen und umschreibt das zulässige Vorgehen ausführlicher und klarer. Zugelassen wird in der neuen Fassung das Abfangen und Ausleiten von Kommunikationsinhalten und Randdaten unter den Bedingungen von Art. 269 Abs. 1 StPO (dringender Tatverdacht, Schwere der Straftat, Subsidiarität) bei Delikten, die unter den Straftatenkatalog von Art. 286 Abs. 2 StPO (verdeckte Ermittlung) fallen, und unter Beachtung der (doppelten) Subsidiarität hinsichtlich Art. 269 StPO.[345] Auch die Genehmigung durch ein Zwangsmassnahmegericht wird für den Einsatz vorausgesetzt (E-Art. 274 Abs. 4 lit. c StPO).[346] Eine gesetzliche Grundlage für eine Online-Durchsuchung oder sonstige weitergehende optionale Funktionen der Govware (beispielsweise Wohnraumüberwachung durch das Einschalten der Webcam oder des Mikrofons des Zielcomputers, Keylogger etc.) werden mit dieser überarbeiteten Norm ausdrücklich nicht geschaffen.[347]

Gestützt auf E-Art. 269ter StPO dürfte der *technisch einwandfreie* Einsatz von Govware zur Überwachung von Kommunikationsinhalten und Randdaten in Strafverfahren de lege ferenda grundsätzlich zulässig sein. Fraglich ist, ob die analoge Regelung im Vorentwurf des NDG dem Bestimmtheitsgebot genügt. Der Wortlaut zumindest deutet darauf hin, dass der Gesetzgeber keine der aufge-

---

341 Botschaft BÜPF 2013, S. 2701 f.

342 Erläuternder Bericht BÜPF, S. 42.

343 Siehe dazu die Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF, S. 55-59; Botschaft BÜPF 2013, S. 2773; STÖCKLI, S. 16; GLESS 2012, S. 17.

344 GLESS 2012, S. 19.

345 E-Art. 269ter StPO. Siehe Botschaft BÜPF 2013, S. 2701 f., 2771 f. und 2776 ff.

346 Vgl. Botschaft BÜPF 2013, S. 2776.

347 Botschaft BÜPF 2013, S. 2702 und 2772.

zeigten Varianten oder möglichen Funktionen von Govware grundsätzlich ausschliessen möchte.[348] Jedenfalls scheint mit der verworfenen Ermächtigungsnorm in der Revisionsvorlage des BWIS II der nachrichtendienstliche beziehungsweise präventiv-polizeiliche Einsatz von Govware noch nicht vom politischen Tisch zu sein.

Für die verhältnismässige und vernünftige Anwendung dieser gesetzlichen Grundlagen werden die Zwangsmassnahmengerichte und Beschwerdeinstanzen zu sorgen haben. Zumindest scheint die vereinfachende Meinung, Govware könne den „Prinzipien eines Rechtsstaates niemals entsprechen"[349] zu weit zu gehen. Ausnahmefälle, in denen der Einsatz von Govware sowohl nutzbringend als auch rechtsstaatlich vertretbar sein dürfte, sind durchaus denkbar.[350] Offene Fragen bleiben aber, ob die Öffentlichkeit den Einsatz dieser Zwangsmassnahme anerkennt – wofür indes die Schwierigkeiten bei der Revision des BÜPF (und des BWIS), sich auf die neuen Artikel zu einigen, nicht gerade sprechen –, ob diese heimliche Überwachungsmassnahme unter restriktiver Auslegung der genannten Voraussetzungen den Ermittlungsbehörden den erhofften Mehrwert (auch hinsichtlich des personellen und finanziellen Aufwands) liefern kann und ob der praktische Einsatz aus technischen Gründen den gesetzlichen Vorgaben gerecht werden kann. So verursachten zum einen technische Schwierigkeiten der jüngst in der Schweiz und Deutschland eingesetzten Versionen der Staatstrojaner massive rechtliche Probleme. Zum anderen entfallen essentielle Voraussetzungen, sobald der Einsatzzweck der Govware ausserhalb des Strafprozessrechts liegt, im Zwielicht der fliessenden Übergänge der Rechtsgebiete eingesetzt wird oder ausserhalb eines Strafverfahrens gewonnene Erzeugnisse der Govware im Strafverfahren verwertet werden sollen.[351]

---

348 Das strapaziert das Bestimmtheitsgebot in Anlehnung an die bundesgerichtliche Rechtsprechung zum Videoüberwachungsartikel im PolG ZH (BGE 136 I 87 E. 8.3 S. 114 ff.) m. E. arg. Insbesondere geht aus der Bestimmung nicht hervor, ob lediglich eine Spiegelung der Daten zulässig sein soll oder auch eine permanente Infiltration inkl. Überwachung über längere Zeiträume. Was spräche aufgrund dieses Wortlauts etwa dagegen, den Bordcomputer des Autos einer Zielperson, der über einen mobilen Internetzugang verfügt, per Govware zu infiltrieren und bspw. die aktuellen Daten des Navigationsgeräts auszulesen?

349 So der ehemalige Präsident der Piratenpartei Schweiz, Denis Simonet im Artikel „Trojaner passen nicht zu einem Rechtsstaat" in Tages-Anzeiger Online vom 14. Oktober 2011.

350 In diesem Punkt gl. A. wie MÉTILLE, S. 8 und JOTTERAND/MÜLLER/TRECCANI, N. 40 sowie HANSJAKOB 2011, N. 31.

351 Diese Problembereiche werden unten im Zweiten Teil diskutiert.

III. Technische Evolutionen, neue Lösungswege und bleibende Schwachstellen

In den vorangegangen Kapiteln wurden bereits einige Schwachstellen und Schwierigkeiten beim Einsatz der vorgestellten Kriminalitätsbekämpfungstechnologien besprochen. Viele der Effekte, Vorteile und Erleichterungen, die sich die Öffentlichkeit und mit dem Vorgehen gegen Kriminalität betraute Behörden erhoffen, können mit diesen Technologien nicht erbracht werden. Fraglich ist, ob eventuell mit sich in Entwicklung befindlichen Technologien einige dieser Probleme beseitigt werden können. Ihnen könnten Probleme inhärent sein, die zu lösen oder auszugleichen nicht möglich ist. Abgesehen davon ist es sehr wahrscheinlich, dass neue Technologien gleichzeitig neue Probleme mit sich bringen und neue Ansprüche an die Bandbreite der Funktionalität aller beteiligten Personen und bestehender Systeme stellen.

A. Exkurs: Praxisbeispiele kombinierter Systeme und Portale

Im Rahmen eines Exkurses werden zunächst die Projekte des mittlerweile eingestellten amerikanischen Information Awareness Office (IAO), welches eine prägende Rolle hinsichtlich vernetzter Überwachungssysteme einnahm, und des INDECT, das ganz im Sinne der amerikanischen Projekte für die Europäische Union an einem ähnlichen Überwachungssystem arbeitet, dargestellt werden. Da INDECT einen Grossteil des Spektrums neuerer Technologien abdeckt, von den laufenden Sicherheitsprojekten der Europäischen Union am weitesten fortgeschritten und zweckdienlich dokumentiert ist, eignet es sich gut zum Exempel und soll in den nachfolgenden Darlegungen stellvertretend für die technische Evolution herbeigezogen werden.

1. Das Information Awareness Office und seine Nachfolger

Das Programm des Information Awareness Office (IAO; vormals Terrorism Awareness Office) der amerikanischen DARPA (Defense Advanced Research Projects Agency) löste in der letzten Planungsphase um das Jahr 2003, als es reif für die tatsächliche Umsetzung war, grosse Proteste aus. Geschaffen wurde diese Behörde als Antwort auf die Anschläge vom 11. September 2001. Eingestellt wurde das Projekt vom Kongress der Vereinigten Staaten im September 2003. Dennoch wurden viele der Teilprogramme unter neuem Namen in anderen Behörden weiterverfolgt. Überbleibsel des IAO ist zum Beispiel das FACTS-System (Factual Analysis Criminal Threat Solution), welches im Wesentlichen

dazu geschaffen wurde, alle möglichen Arten von (öffentlichen und nicht-öffentlichen) Registern und Datenbanken auf Stichworte durchsuchen zu können. Es sollte ein Vorreiterprogramm auf dem Gebiet der ganzheitlichen Überwachung zum Zwecke der Kriminalitätsbekämpfung, insbesondere zur Bekämpfung des Terrorismus, werden.[352]

Bestrebungen, jegliche Art von Bedrohungen durch automatische Überwachungstechnik in einem möglichst frühen Stadium bekämpfen zu können, bestehen indes nicht nur im amerikanischen Raum. Einige der Projekte der Vereinigten Staaten mögen zwar prominenter im öffentlichen Bewusstsein vertreten sein, die Informationsbeschaffungs- und Datenanalyseprojekte etwa der Europäischen Union (Beispiel: INDECT) stehen in ihren Ansprüchen an die Funktionalität und Effektivität denjenigen der USA indes in nichts nach. Im Rahmen dieser Projekte sollen die Schwachstellen der bisherigen Informationsverarbeitungsmethoden ausgeräumt sowie nützlichere und präzisere Ergebnisse mit überarbeiteten Prozessen und Systemen erzielt werden. Abhilfe schaffen soll diesbezüglich insbesondere die *Kombination* von (automatisierter) Überwachung, Datenbanken und Verdachtslisten. Die denkbaren Möglichkeiten der Verknüpfung und Vernetzung dieser Instrumente sind vielfältig und zumeist auf den ersten Blick (potenziell) ungemein hilfreich. Folglich werden entsprechende Technologien vielfach als Antwort auf viele Fragen der Sicherheit und Kriminalität kommuniziert.[353]

2. Das europäische Projekt INDECT

INDECT ist die Kurzform von „Intelligent information system supporting observation, searching and detection for security of citizens in urban environment". Der Arbeitstitel des am 1. Januar 2009 in Angriff genommenen und 60 Monate laufenden Projekts sagt bereits viel über dessen Inhalt aus: Es soll ein intelligentes, also weitgehend automatisiertes und möglichst autonomes Informationssystem[354] entwickelt werden, welches die Sicherheit von Bürgern im städtischen Umfeld schützt. Gemäss offizieller Projektbeschreibung soll dieses Ziel erreicht

---

352 CHESTERMAN, S. 231, welcher der Ansicht ist, der Start ähnlicher Programme und Projekte sei langfristig kaum aufzuhalten. Siehe ausführlich zum IAO und ähnlichen Programmen: FIENBERG, S. 201 f.; STRÖM, S. 25 ff.; MINOW ET AL., S. 15-20; BRODEUR/LEMAN-LANGLOIS. Auch PRISM (siehe oben Erster Teil, Kapitel II.B.2.) tritt in die Fussstapfen des IAO.

353 Siehe etwa die Projektbeschreibung INDECT.

354 Teilweise können heutige Programme bereits autonom in dem Sinne agieren, dass sie ihre Vorgehensweise an neue Gegebenheiten selbst anpassen, also während des Ausführens der Anweisungen lernen. Siehe dazu unten Erster Teil, Kapitel III.D. und III.E.

werden, indem eine Plattform für die Registrierung und den Austausch von operativen Daten, die Akquisition von Multimedia-Inhalten, für das intelligente Verfolgen aller Arten von Informationen und das automatische Aufspüren von Bedrohungen und Erkennen von abnormalem Verhalten oder Gewalt zur Verfügung gestellt wird.[355] Der Entscheid des Rats der Europäischen Union 2006/971/EG zur Durchführung des Siebten Rahmenprogramms (FP7) vom 19. Dezember 2006 bildet die Grundlage für das Projekt INDECT. Das Siebte Rahmenprogramm verfolgt unter anderem das Ziel, eine funktionierende Abwehr von Bedrohungen, und somit Sicherheit in der EU, über fünf auszubauende Bereiche zu gewährleisten: Die Identifizierung von Vorfällen, die präventive Verhinderung von Bedrohungen, den Schutz bestimmter Objekte oder Subjekte sowie einen Plan zur Antwort auf Krisen und die Aufarbeitung der Konsequenzen einer Krise oder eines Vorfalls.[356]

Praktisch alle diese Elemente des INDECT waren in Grundzügen bereits im Paket des IAO enthalten. Das IAO-Programm sollte kriminelle Vorbereitungshandlungen frühzeitig enthüllen und etwa terroristische Intentionen und Aktionen voraussehbar machen, die Identifikation von Menschen auf grosse Distanz ermöglichen sowie ein sehr ähnliches Instrumentarium an vernetzten Systemen entwickeln.[357] Entsprechend weiterentwickelt, soll dem Kriminalitätsbekämpfungsapparat mit INDECT *primär* ein neues und effektives Werkzeug in die

---

355 Siehe den Internetauftritt des INDECT unter <http://www.indect-project.eu/>. Neben INDECT befassen sich HUMABIO, SAMURAI, ADABTS und viele andere Projekte mit praktisch identischen Themen. Sehr ähnliche Ziele, jedoch beschränkt auf die intelligente Videoüberwachung, verfolgt das Projekt CamInSens, siehe unter <http://www.sra2.uni-hannover.de/caminsens/> und dazu D'ANGELO ET AL. Im einmal jährlich stattfindenden Wissenschaftswettbewerb TRECVID (Text Retrieval Conference – Video Retrieval Evaluation) sollen Programme bzw. Algorithmen entwickelt werden, die automatisierte Prozeduren der Informationssammlung, -verarbeitung und -analyse ermöglichen oder verbessern, siehe <http://trecvid.nist.gov/>. Vgl. zum Ganzen HAYES 2009, S. 49 f. und ferner EBENDA, S. 9 ff.; MOECKLI/THURMAN, S. 4 ff.; COUDERT, S. 377; LISCHKA/REISSMANN in Spiegel Online vom 13. November 2012.

356 Entscheidung des Rats der Europäischen Union 2006/971/EG vom 19. Dezember 2006, S. 216 ff.

357 Das Leitziel des IAO: „… become much more efficient and more clever in the ways we find new sources of data, mine information from new and old, generate information, make available for analysis, convert it to knowledge, and create actionable options." (POINDEXTER). Zum Ganzen siehe FIENBERG, S. 200 ff.; SOLOVE 2008, S. 192; MOECKLI/THURMAN, S. 9 ff. Zu den einzelnen Programmen des IAO, siehe die Programmsektion auf dessen ehemaliger Website, abrufbar unter: <http://infowar.net/tia/www.darpa.mil/iao/programs.htm>.

Hand gegeben werden. Dem Projekt liegt die Überzeugung zu Grunde, Kriminelle hätten sich in den letzten Jahren gegenüber ihrem Konterpart, den mit der Kriminalitätsbekämpfung betrauten Behörden, einen technischen Vorsprung verschaffen können. Diesen technischen Vorsprung führen die Verfasser des Projektberichts insbesondere darauf zurück, dass Kriminelle einerseits auf mehr finanzielle Mittel zurückzugreifen und diese Mittel zudem schnell und präzise zuzuteilen vermöchten und andererseits die staatlichen Behörden den Rechtsstaat und die Menschenrechte zu achten hätten.[358] *Sekundär* soll ausserdem dem Bürger ein begrenzter Zugriff auf die INDECT-Plattform ermöglicht werden. Dadurch könne dieser allenfalls wichtige Informationen liefern oder sich selbst besser vor „dem Verbrechen" schützen.[359] Das Projekt INDECT konzentriert sich also in erster Linie auf die ersten drei Ziele des Programms FP7 der EU. Es wird beabsichtigt, diese über folgende Methoden zu erreichen:

- Die automatisierte Video- und Audioüberwachung des realen öffentlichen Raums.
- Die Observation von Verdächtigen.
- Den effizienten Austausch und Abruf von Informationen zwischen verschiedenen Datenbanken und Dienststellen.
- Die Überwachung des virtuellen Raums.

---

358 Siehe die Projektbeschreibung INDECT; den Bericht INDECT D9.4, S. 8. Zum Ganzen: Bericht INDECT D0.5. In dieselbe Richtung geht auch die einleitende Anmerkung im Bericht INDECT D1.1, S. 7: „This document has been reviewed by the members of Ethics Board appointed by the participants of the INDECT Project, with high stress on ethical issues and human rights." Vor allem aber der „funktionelle Datenschutz" erhält einen Platz auf der Traktandenliste der Forscher, indem sie sich in erster Linie darum kümmern, die Systeme einerseits vor unbefugten *Zugriff* auf die Prozesse und Archive und andererseits vor unberechtigtem *Gebrauch* der gesammelten Personendaten (durch grundsätzlich befugte Behörden oder Personen) abzusichern (siehe Bericht INDECT D9.4, S. 40). Zwar wurden im Mutterprojekt der EU (FP7) zwei begleitende Forschungsprojekte zur Beurteilung von Ethik, Moral und Menschenrechten auf die neuen Technologien begründet (diese Projekte heissen DETECTER und INEX, siehe <http://www.detecter.bham.ac.uk/> und <http://www.inexproject.eu/>; vgl. HAYES 2009, S. 21). Diese können durchaus sehr wertvoll sein. Inwieweit aber etwa auf deren Erkenntnisse bei der Entwicklung und der anschliessenden Implementierung der fertigen Systeme abgestellt wird, wird sich zeigen.

359 Das sind nicht unbedenkliche Ansätze der Selbstaktivierung, auf die später noch zu sprechen zu kommen sein wird (siehe unten Dritter Teil, Kapitel IV.A.).

B. Vernetzung, Koordination und optimierter Austausch

Überwachungssysteme neuerer Projekte sollen als Portale mit verschiedenen, auf den jeweiligen Nutzer abgestimmten Bereichen dienen. Das „Portal mit nutzerzentriertem Zugang" des INDECT beispielsweise vereinte eine vielseitige Zusammenstellung und Vernetzung verschiedener Arten von Datenbanken und Raumüberwachungsmassnahmen. Angestrebt wird also eine Art Meta-Register, das viele verschiedene Datenbanken kombiniert und Informationen sowie Hinweise zu Bedrohungen oder gefährlichen Personen(-gruppen) bestimmten Nutzerkreisen, unter anderem der Öffentlichkeit, übersichtlich darstellen könnte. Dies soll immer verknüpft mit Daten aus anderen Quellen und dem aktuellsten Stand der Raumüberwachung geschehen.[360]

Sollte diese Vernetzung technisch umsetzbar und praktisch anwendbar sein, könnten Informationen aus der Raumüberwachung routinemässig und ohne Kompatibilitätsprobleme mit den Inhalten (mehrerer) Datenbanken (Personendossiers, Indizien ungelöster Fälle etc.) abgeglichen werden, womit zum Beispiel überwachte Personen leichter bestimmten Kategorien (unauffällig, bedrohlich, verdächtig bezüglich Fall X, usw.) zugeordnet werden könnten.[361] Die sich in Entwicklung befindenden Systeme sollen in dieser Hinsicht einen möglichst stabilen Speicherplatz für umfangreiche Datensammlungen anbieten, sowie deren effizienten und akkuraten Abruf gewährleisten. Mithilfe von Vernetzungen mit und dem Zugriffsrecht auf verschiedene Verdachtsregister und andere Datenbanken sollen die Systeme die umfassende Information über eine Person ermöglichen und diese für Analysen benutzen oder der abrufenden Behörde nach bestimmten Kriterien geordnet bereitstellen können. Dadurch könnten beispielsweise komplizierte Beziehungsmuster erkannt und für den menschlichen Benutzer übersichtlich dargestellt werden.[362]

Ein weiteres Ziel des INDECT, das vorliegend nicht vertieft werden soll, besteht beispielsweise darin, den Polizeibehörden mittels mobilen Zugangstools des INDECT mit permanenter Verbindung zum Zentralmodul erlaubt werden, während einer Observation für sie wichtige Daten mit geringem Aufwand abzurufen und mit den Daten vor Ort abzugleichen (zum Beispiel könnten Bekannte oder „Ge-

---

360 Vgl. Bericht INDECT D9.4, S. 23.

361 Vgl. KURZ/RIEGER, S. 3. Zu dieser Schwachstelle bestehender CCTV-Systeme, siehe NORRIS/ARMSTRONG, S. 221.

362 Bericht INDECT D9.4, S. 20.

schäftspartner“ des Verdächtigen an Ort und Stelle identifiziert werden). Zudem soll das System die Polizisten mit bearbeiteten Karten versorgen, mit Hilfe derer sie zweckmässiger navigieren könnten. Weiter sollen Flugdrohnen („Unmanned Aerial Vehicles“, UAVs), wie sie zurzeit vor allem in der militärischen Aufklärung zur Anwendung gelangen[363], für Observationen zur Verfügung gestellt werden.[364]

Fraglich ist, ob die dargestellten Ansätze tatsächlich erfüllt werden können, und inwieweit die Bevölkerung Einsätze derartiger Technologien akzeptieren wird. Jedenfalls verstärken vernetzte und kombinierte Technologien die bereits angesprochenen Probleme der zunehmenden Entgrenzung und Vermischung von verschiedenen Tätigkeitsbereichen und Rechtsgebieten. Sie dürften daher rechtlich kaum eindeutig einzuordnen sein. Weiter führten sie insgesamt zu undurchsichtigen Vorgehensweisen, da die vielfältigen Datenverwendungs- und Verknüpfungsmöglichkeiten vom Bürger kaum noch zu durchschauen sein dürften.[365] Auch die Missbrauchsmöglichkeiten, welche derartige neue Technologien und die daraus entstehenden Konglomerate auf Seiten staatlicher Stellen, Privater oder unberechtigter Zugreifer eröffnen, sind gross.[366]

C. Verbesserte Echtzeit-Überwachung

Die Vernetzung einer automatisierten Überwachung mit Verdachtsregistern würde das Konzept, Straftaten durch Registrierte über die Kontrolle der ihnen erlaubten Bewegungsradien und der ihnen verbotenen Areale zu verhindern, theoretisch erheblich unterstützen. Speicherte ein Verdachtsregister neben den üblichen Daten den von der Behörde vorgegebenen Bewegungsraum, die dem Eingetragenen verbotenen Zonen und ein biometrisches Profil, könnten dessen Bewegungen etwa über Videoüberwachungsanlagen oder über die Analyse und

363 Für einen Überblick zu UAVs: MOECKLI in Analysen zur Sicherheitspolitik vom Juli 2010.

364 Bericht INDECT D9.4, S. 16 und D1.1, S. 8.

365 Siehe dazu unten Zweiter Teil, Kapitel I.I. und Vierter Teil, Kapitel IV.D.

366 SORELL, S. 7 und 20 verkennt hier m. E., dass die archivierten Datenmengen und die automatisierten Prozesse eines im Umfeld und der Kultur des Bekämpfungsstrafrechts angewendeten INDECT sehr problematische Züge annehmen könnten. Das in den Zielen und der Ausgestaltung praktisch deckungsgleiche Projekt MATRIX (Multistate Anti-Terrorism Information Exchange) aus Florida wurde 2005 wegen mangelndem Partizipationswillen anderer Bundesstaaten und Bedenken der Öffentlichkeit eingestellt, siehe dazu MOECKLI/ THURMAN, S. 12 f.; FIENBERG, S. 200 ff.

Verknüpfung von Daten aus verschiedenen Quellen nachverfolgt und Bewegungsprofile erstellt werden.[367] Vorstellbar wäre auch die Echtzeit-Übertragung des Aufenthaltsorts eines Registrierten auf einer digitalen Karte. Der Schritt hin zu einer Live-Visualisierung des Bewegungsprofils über das Internet ist nicht besonders gross.[368] Dasselbe Resultat könnte erreicht werden, indem den Behörden direkter Zugang zu Verkehrs- beziehungsweise Verbindungsdatenbanken etwa von Mobilfunknetzbetreibern erlaubt würde.[369] Letztere Methode versetzte Behörden in die Lage, Zielpersonen über ihre mobilen Geräte live zu orten, sofern die Zielpersonen diese bei sich tragen. Je nachdem wie umfassend auf private Datenquellen zugegriffen werden dürfte oder wie flächendeckend Videoüberwachungsanlagen vorhanden wären, könnten auch ein elektronischen Fussfesseln ähnlicher Effekt erreicht oder Kontrollmechanismen über Checkpoints unterhalten werden: Verlässt eine eingetragene Person das ihr zugesprochene Gebiet oder betritt sie ein ihr verbotenes Areal (zum Beispiel der Sexualstraftäter einen Kinderspielplatz, der mutmassliche Terrorist einen Flughafen oder der Hooligan ein Stadion) und wird dabei etwa von einer biometrischen Videokamera identifiziert, macht ein Alarm die zuständige Behörde oder den betreffenden Sicherheitsdienst auf diesen Verstoss aufmerksam.

Abgesehen davon könnten archivierte Bewegungsprofile dazu verwendet werden, die Handlungen registrierter Personen zu einem späteren Zeitpunkt für Ermittlungen in Straffällen beizuziehen, was durchaus hilfreich sein könnte. Jedoch müssten, um eine Ermittlung in einer Straftat wirklich sinnvoll unterstützen zu können, die Bewegungsabläufe des Registrierten über längere Zeitspannen gespeichert werden, womit diese Methode demselben Problem gegenüberstünde wie die Live-Überwachung: Die Masse an gesammelten Daten verbrauchte viele Ressourcen, wäre schwer handzuhaben und könnte höchstens von automatisierten Systemen effizient gemanagt werden.

---

367 Siehe dazu HORNUNG/DESOI, S. 154.

368 Siehe dazu STRÖM, S. 103 ff., insb. 107. Eine ähnliche Technik ist in das soziale Netzwerk „Facebook" integriert: In Kombination mit einem iPhone kann über die Plattform „places" der eigene Standort, sofern man diesen Dienst aktiviert lässt, von anderen Nutzern live abgerufen werden. Vgl. dazu etwa den Artikel „Auch Facebook weiss, wo du bist" in Tages-Anzeiger Online vom 24. August 2010; WEIGERT in netzwertig.com vom 19. August 2010.

369 KURZ/RIEGER, S. 12.

D. „Intelligent monitoring“

Die bis anhin hauptsächlich eingesetzten manuellen oder halb-automatischen Live-Überwachungssysteme versagen meist darin, eine bevorstehende Straftat frühzeitig vor der effektiven Tathandlung oder noch rechtzeitig vor dem Verschwinden des Täters zu erkennen. Dieser Schwachpunkt ist darauf zurückzuführen, dass die menschlichen Überwacher für die Früherkennung einer heiklen Situation das von der Kamera übertragene Geschehen auf dem Bildschirm, die Indizien der sich über virtuelle Kanäle abzeichnenden Bedrohungslage oder der in Datenbanken gespeicherten Informationen zutreffend deuten können und möglichst rasch eine Entscheidung treffen müssen (zum Beispiel, ob interveniert werden soll oder nicht).[370] Weiter müssen ausreichend menschliche Überwacher zur Verfügung stehen, um die Anforderung angemessen zu erfüllen. Ein Mensch kann nur eine bestimmte, lediglich geringe Anzahl an Monitoren mit Live-Bildern für eine bestimmte Zeitspanne aufmerksam und zuverlässig überwachen.[371] Ebenso fordern das Durchforsten, die Kontrolle und Analyse von Datenarchiven, der virtuellen Kommunikation oder von verschiedenen Verdachtsregistern den einzelnen Menschen stark. Die an mehreren Orten gespeicherte Masse an Informationen ist, wie bereits festgestellt, manuell kaum derart effizient zu bewältigen, dass akut drohende Gefährdungslagen dadurch zuverlässig verhindert werden könnten. Die Qualität einer manuellen Raumüberwachung oder Kontrolle von (Verdachts-)Registern hängt demnach stark von verfügbaren personellen Ressourcen ab.[372]

Bei diesen praktischen Problemen setzen die Projekte zu neuen und sich in Entwicklung befindlichen Systemen an. Nicht nur sollen entsprechende Prozeduren durch Automatisierung kosteneffizienter gemacht, sondern die Systeme überdies mit weiteren nützlichen Funktionen ausgestattet werden. So soll der Bediener das automatisierte System eine automatische (Vor-)Sondierung der Datenberge vornehmen lassen können. Im Projekt INDECT wird diese Technologie „intelligent monitoring” genannt.

Mit diesem Begriff wird der Anspruch erhoben, eines der zentralen Probleme der manuellen Überwachung zu lösen, indem das automatisierte System genau das leisten soll, was für ein rein auf menschlichen Überwachern basierendes System

370 Vgl. dazu etwa HOWELLS.
371 Siehe HORNUNG/DESOI, S. 153 f.; DEPARIS/DAVID, S. 6.
372 NORRIS/ARMSTRONG, S. 210 ff. Vgl. KAMMERER 2008, S. 192 f.

ineffizient wäre: Eine immens grosse Anzahl an Datenquellen bestenfalls nahezu synchron auszuwerten.[373] Wo beispielsweise aktuelle Raumüberwachungssysteme den Zielraum lediglich vergleichsweise rudimentär wahrnehmen können[374] und demnach zu schwach in der Analyse von gesammelten Daten und der Bewertung von Situationen sind, um eigenständig einigermassen verlässliche Ergebnisse zu liefern, soll es Systemen wie dem INDECT gelingen, die menschliche Beobachtungsgabe zu imitieren und deren Leistungsfähigkeit zu verbessern. Dadurch werde den Behörden ermöglicht, direkt gestützt auf die automatisierte Analyse Interventionen zu veranlassen. Dem menschlichen Überwacher käme innerhalb eines derartigen vollautomatisierten Systems kaum mehr als die Stellung einer Prüfinstanz zu.[375] Das heisst, das automatisierte System wertete die gesammelten Daten aus und würde weitere als erforderlich erachtete Daten aus anderen Systemen zur Analyse beiziehen. Würde das Rechenergebnis aufgrund der Daten daraufhin weisen, dass eine Situation besteht, die einer Handlung bedarf, sendete das System die betreffenden Informationen mit einem Alarm an den zuständigen menschlichen Benutzer. Dieser hätte in der Folge darüber zu befinden, ob tatsächlich Handlungsbedarf besteht.

Das automatisierte System träfe mithin die Auswahl der weitergeleiteten Daten und Informationen und entlastete damit den menschlichen Benutzer in seinem Arbeitsaufwand erheblich. Mit derart automatisierten Systemen könnten theoretisch auch anlasslos gesammelte Daten aus verschiedenen Quellen mit geringem Aufwand und grösster Präzision durchsucht und bewertet oder beispielsweise anhand von vorgegebenen Kriterien sondiert werden.[376]

E. Perfektionierung des Selektionsverfahrens

1. Algorithmic Knowledge Discovery

Weiterentwickelte, verbesserte Sondierungsverfahren sollen eine weitere Errungenschaft laufender Forschungsprojekte werden. Die für diese Methoden gebräuchliche Bezeichnung lautet *Algorithmic Surveillance* oder allgemeiner *Algo-*

---

373 Vgl. dazu etwa THÜR, S. 101 f.

374 Einige Bsp. dazu finden sich bei BÜLLESFELD 2002, S. 13 ff.

375 Siehe Bericht INDECT D9.4, S. 13.

376 Siehe zum Ganzen SKILLICORN 2008b, S. 11; GRAHAM/WOOD, S. 538; COUDERT, S. 378; GATES, S. 78 f.; BARTSCH, S. 22; KAMMERER 2008, S. 190; MÜLLER L. 2011, S. 17 f.

rithmic Knowledge Discovery.[377] Die Bezeichnung „Erkenntnisforschung" trifft den Sinn der „Knowledge Discovery" ziemlich gut. Mit dem Zusatz „algorithmisch" wird zum Ausdruck gebracht, dass die Suche auf mathematischen Kriterien basiert und dementsprechend automatisiert durchgeführt werden kann. Der Begriff meint mithin insbesondere verbesserte, automatisierte Varianten der Datenverarbeitung über den Abgleich von extrahierten Eigenschaften.

Personen oder Objekte automatisch zu identifizieren oder einen Vorfall sichtbar zu machen, können zum Beispiel bereits heutige Videoüberwachungstechnologien teilweise.[378] Mit aktuellen Projekten sollen diese Fähigkeiten stark erweitert werden: Es soll ermöglicht werden, vorgegebene Kontextkriterien zu suchen und abzugleichen, folglich Suchläufe zu initiieren, die zugleich Daten sammeln, sondieren und analysieren. Das gesetzte Ziel geht darüber hinaus, biometrische Eigenschaften oder Objekte sowie Personen zu erfassen, die an einen Ort als bedrohlich empfunden werden. Es sollen vielmehr zusätzlich Bewegungsabläufe von Personen und Objekten analysiert, Anomalien und unübliches Verhalten erkannt, problematische Verhaltensweisen vorausgeahnt und dadurch bedrohlichen oder kritischen Situationen mit entsprechenden Interventionen vorgebeugt werden („automatic detection of threats").[379] Auch virtuelle Sondierungsprogramme könnten immens von in diese Richtung weiterentwickelten Algorithmen profitieren.[380]

Die Vernetzung vieler verschiedener Datenbanken, deren Umfang und die Leistungsfähigkeit zukünftiger Analysesysteme erlauben somit zumindest in der Theorie, Datenbestände nach einem bestimmten Muster vielschichtiger und deshalb effizienter zu erstellen und zu durchforsten. Hinzu kommt, dass sie durch ihre einfach bedienbaren Suchmasken und die übersichtliche Darstellung der hierarchisch nach Wahrscheinlichkeit des Zutreffens geordneten Ergebnisse den Zeitaufwand für Beweisausforschungstätigkeiten (sog. „fishing expeditions")

---

377 Vgl. etwa NORRIS/MORAN/ARMSTRONG, S. 497; SKILLICORN 2008b, S. 11; INTRONA/WOOD.

378 Siehe dazu NORRIS/ARMSTRONG, S. 212 ff. und 216 ff.; BIER/SPIECKER GEN. DÖHMANN, S. 611 mit weiteren Hinweisen.

379 Siehe Bericht INDECT D9.4, S. 12, 38 f. („[biometrics] not only as collection of methods for identification/recognition of individual offenders but also for automated detection of criminal behaviour of anonymous people."); COUDERT, S. 377 f.; HORNUNG/DESOI, S. 153.

380 Siehe BENDRATH, S. 14 ff. zu den erweiterten Möglichkeiten der DPI durch verbesserte Algorithmen.

stark verringern könnten.[381] Neben den sehr umfangreichen Datensammlungen könnten insbesondere die Ausbreitung und der Ausbau von Verdachtsdatenbanken für Rasterfahndungen hilfreich sein. Die dort gespeicherten Profilinformationen enthalten potenziell wertvolle Informationen, die mittels Kriterien verknüpft werden können.[382] Neue Technologien wecken auch grosse Hoffnungen in die zukünftige Funktionalität der Massendatenverarbeitung. Jeder Schritt in die Richtung eines Abbaus von Hürden, umfassende und detaillierte Verdachtsregister und andere personenbezogene Datenbanken zu schaffen und vernetzt anwenden zu dürfen, öffnet der Massendatenverarbeitung viele vorher verriegelte Türen.

Möglicherweise können die automatisierten Systeme die strukturimmanenten Schwachstellen der Rasterfahndung durch die angesprochene Datenquantität, Vernetzung, schnellere Datenverarbeitung oder ähnliche Fortschritte beheben. Das automatisierte Verfahren stimmt indes mit dem halb-automatischen *in der Struktur* überein (Probleme der Profilerstellung, Angewiesenheit auf zuverlässige Merkmale oder Kriterien etc.).[383] Systemimmanente Probleme, inbesondere etwa sobald komplexere Straftaten oder komplexere Tätergruppen analysiert werden sollen, könnten daher bestehen bleiben.

2. Biometrische Personenidentifikation

Der hauptsächlich angestrebte Zweck des Einsatzes von Technologien, die biometrische Daten nutzen, zur Kriminalitätsbekämpfung wäre es, Zielpersonen, zum Beispiel mutmassliche Terroristen oder andere Personen, die auf Fahndungslisten beziehungsweise in Verdachtsregistern verzeichnet sind, aus (gros-

---

381 Siehe dazu POPP/POINDEXTER; SKILLICORN 2008b, S. 11 f.; BARTSCH, S. 21; CROSSMAN, S. 117 f.; die Versprechungen im Bericht INDECT D9.4. Vgl. auch HORNUNG/DESOI, S. 154. Zu bestehenden, noch ausbaufähigen intelligenten und vernetzten Videoüberwachungssystemen siehe etwa WOOD in Blog vom 21. Februar 2009 und BRADSHER in The New York Times Online vom 12. August 2007.

382 Bsp.: Das Kriterium „befindet sich einer Hooligandatenbank" ergäbe verknüpft mit dem Kriterium „telefonierte in der Nähe des Stadions zum Tatzeitpunkt" vielleicht die Identität des Täters eines im räumlichen und zeitlichen Umfeld eines Fussballspiels geschehenen Gewaltakts.

383 Vgl. kritisch SKILLICORN 2008b, S. 12 f. Bezüglich der Abgrenzbarkeit über Charakteristiken von „Kriminellen und Terroristen" gegenüber „normalen" Bürgern in der Gesellschaft aber grundsätzlich positiv eingestellt, SKILLICORN 2008b. S. 74 f.

sen) Menschenmassen heraus identifizieren zu können.[384] Die überraschend geringe Verlässlichkeit heutiger biometrischer Personenidentifikationssysteme unter realen Bedingungen und insbesondere, wenn grössere Personengruppen zu sondieren sind, ist jedoch faktisch aus technischen Gründen schwer zu beheben.[385] Ausserhalb von Versuchsanordnungen ist zudem kaum abzuschätzen, ob und allenfalls wieviele, Soll-Treffer das biometrische System nicht erkennen konnte (Falsch-Negative).[386]

Personenidentifikationsprozesse setzen zunächst ein qualitativ sehr gutes Vergleichsmuster voraus.[387] Aber hochwertige Aufnahmen einer Person reichen alleine zumeist nicht aus, diese mit einer ausreichend hohen Wahrscheinlichkeit zu identifizieren, weil die entsprechenden Algorithmen sehr schnell zu kompliziert zu handhaben und korrekt anzupassen sind.[388] Bereits in isolierten Versuchsanordnungen erreichen Systeme zur automatisierten Personenidentifikation keine genügende Verlässlichkeit, vor allem, sobald die Zahl an zu vergleichenden Mustern in der abgeglichenen Datenbank anwächst. So verbuchten bis heute Versuche von automatischen Abgleichungsmechanismen und -systemen, die in einer Datenbank aufgeführte, gesuchte Personen über die biometrische Gesichtserkennung von Kameras finden sollten, meist Misserfolge.[389] Probleme

---

384 INTRONA/NISSENBAUM, S. 20. Siehe etwa auch bei Drucksache 17/9003 vom 16. März 2012, S. 12 f., die laufenden Projekte „GES-3D – Multi-Biometrische Gesichtserkennung“ und „MisPel – Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten“.

385 INTRONA/NISSENBAUM, S. 3, 40 und 47. Vgl. SKILLICORN 2008b, S. XV; GROEBNER, S. 174; INTRONA/WOOD, S. 195 f.; KAMMERER 2008, S. 171 f. mit weiteren Hinweisen. Tatsächlich gelingt es auch Menschen oft nicht, ihnen unbekannte Personen auf Videoüberwachungsaufnahmen mithilfe von Vergleichsmustern zu erkennen und zuzuordnen.

386 INTRONA/NISSENBAUM, S. 12 f. Ohnehin entgehen biometrischen Überwachungssystemen Personen, von denen keine Musterdaten zum Abgleich vorliegen (insofern aus der Sicht des Systems Richtig-Negative).

387 INTRONA/NISSENBAUM, S. 40.

388 Vgl. DUNSTONE/YAGER, S. 53 ff. und 241 ff. Hindernisse können bspw. ein unvorteilhafter Kamerawinkel, Veränderungen des Aussehens der Person gegenüber dem Vergleichsmuster und viele andere Verfälschungen der Aufnahme darstellen.

389 Für eine Übersicht und Besprechung von The Face Recognition Vendor Tests (FRVT) 2002 und 2006, The facial recognition grand challenge (FRGC), BioFace II, FaceIt (Identix), Australian SmartGate FRS und der BKA-Fotofahndung, siehe INTRONA/NISSENBAUM. Zum Gesichtserkennungssystem Mandrake in London und anderen ernüchternden Beispielen, siehe KAMMERER 2008, S. 205-209, 219-221 und 224. Zu einem gescheiterten Experiment mit biometrischen Kamerasystemen in Tampa, Florida, siehe GATES. Im Gegensatz dazu

bereiten insbesondere „biometrische Doubles“ (das heisst sehr ähnlich aussehende Personen), tiefe Bildqualitäten der Überwachungsaufnahmen, Altersunterschiede von Mustern in der Datenbank und in Überprüfungsmustern sowie schwer kontrollierbare Umgebungen (hinsichtlich Ausleuchtung etc.).[390] Herrschen nicht experimentale Idealbedingungen, fällt die Wahrscheinlichkeit für zutreffende Ergebnisse sehr tief aus, wodurch derzeitige biometrische Identifikationssysteme in der Raumüberwachungspraxis hinsichtlich des genannten Hauptzwecks noch wenig nutzbringend eingesetzt werden können[391], wobei aber zu berücksichtigen ist, dass ihre Leistungsfähigkeit kontinuierlich steigt und der gleichzeitige Einsatz mehrerer kombinierter Erkennungstechnologien zuverlässigere Resultate verspricht.[392]

3. Automatisiertes Erahnen von Verhaltensweisen

Neuerdings sollen von den Überwachungssystemen zusätzlich zur Personenidentifikation bestimmte Verhaltensweisen automatisch unterschieden und isoliert voneinander spezifisch abgearbeitet werden können. Es geht dabei nicht mehr alleine um das Sichtbarmachen von Verhaltensweisen, sondern um das Erkennen und Voraussagen unterschiedlich eingestufter Verhaltensweisen.[393] Nun wurde aber bereits ausgeführt, dass heutige automatisierte Systeme mit ihren Kapazitäten kaum in der Lage sind, zuverlässig das Erscheinungsbild einer Person gesamthaft oder intuitiv einzuschätzen. Die automatisierte Verhaltensanalyse und das Erkennen von Bedrohungen sind schwieriger zu realisieren.[394] Ohne relativ ausgereifte, etablierte und nahezu perfekte kriteriengestützte Auswertungsmethoden scheinen diese Technologien, wie bereits festgestellt, wenig nutzbringend einsetzbar.

hätten sich die automatisierten Verfahren zur Autokennzeichenerkennung als „relativ zuverlässig“ herausgestellt, meint PETRI, G N. 565 mit weiteren Hinweisen.

390 INTRONA/NISSENBAUM, S. 38 ff.

391 INTRONA/NISSENBAUM, S. 3; INTRONA/WOOD, S. 189; INTRONA, S. 83 ff.; GATES, S. 80; Bericht BKA Fotofahndung, S. 5 f., 20 ff. und 27; Bericht EJPD 2007, S. 17. Siehe auch BARR ET AL., S. 1 ff., die zudem einen Überblick über Lösungsansätze und die zukünftige Ausrichtung bieten.

392 INTRONA/NISSENBAUM, S. 26, 36 und 38 f.

393 Vgl. Bericht INDECT D1.1, S. 8. Siehe bspw. auch das von OLTRAMARI/LEBIERE vorgestellte System und STEIER in NZZ Online vom 29. Oktober 2012.

394 Bereits die Definition „gefährlichen oder atypischen Verhaltens“ scheint schwer zu objektivieren. Vgl. dazu den diesbezüglichen Fragebogen des Projekts INDECT, der an die polnische Polizei abgegeben wurde: Bericht INDECT D1.1, S. 13 f. und insb. S. 16 f. sowie 18 f.

In einer 2004 veröffentlichten Studie kamen TROSCIANKO ET AL. zum Schluss, dass Voraussagen über das Verhalten beobachteter Subjekte grundsätzlich machbar, wenn auch nicht perfekt seien.[395] Die im Rahmen der Studie durchgeführten Experimente mit einerseits einer Gruppe von (mehr oder weniger) erfahrenen Überwachungsangestellten (Experten) und andererseits von Psychologiestudenten im ersten und zweiten Jahr (Laien)[396] ergaben folgende Erkenntnisse: Den Versuchspersonen wurden 15 Sekunden lange Sequenzen aus realen Videoüberwachungsaufnahmen vorgeführt. Die Aufnahmen zeigten Personen, deren Verhalten entweder zu einem Vorfall führte oder nicht. Die Videosequenzen wurden jeweils kurz vor dem Vorfall beziehungsweise kurz bevor erkenntlich geworden wäre, dass kein Vorfall geschah, gestoppt. Die Versuchspersonen mussten daraufhin beurteilen, was als Nächstes geschehen werde. Je nach Versuchsanordnung konnten die Versuchspersonen Verhalten mit anschliessendem Vorfall von Verhalten mit harmloser Folge mit einer Trefferquote von ca. 80-90% unterscheiden. Mit einer Trefferquote von 34% beziehungsweise 31% konnten die Versuchspersonen den Ausgang der auf der Videosequenz dargestellten Situation korrekt beziehungsweise nahezu korrekt beschreiben.[397] Diese Ergebnisse, so die Verfasser der Studie, würden darauf hinweisen, dass relativ zuverlässige Aussagen über die Intention einer Person aus ihrem unmittelbar vorhergehenden Verhalten abgelesen werden könnte, und zwar mit der gleichen Präzision von erfahrenen Videoüberwachern wie von Laien.[398] Daraus leiten sie ab, dass objektivierbare Kriterien existierten, mit Hilfe derer auch ein automatisiertes Programm kriminelles Verhalten voraussagen könne.

Die Frage, was diese Kriterien sind, wird in der Studie nicht beantwortet, sondern lediglich festgehalten, dass wohl bestimmte Bewegungen der überwachten Person Rückschlüsse auf ihr intendiertes Verhalten zulassen. Zudem wird in der Studie auf die Notwendigkeit zukünftiger Forschung verwiesen, um einen derar-

---

395 TROSCIANKO ET AL., S. 96. Vgl. zu dieser Studie PATON WALSH in The Observer vom 22. Juli 2001.

396 Die vorgenommene Einordnung in Experten und Laien kann kritisiert werden: Ein Psychologie-Student könnte in der visuellen Verhaltensanalyse durchaus gleich fähig sein wie ein erfahrener, aber wohl in Psychologie ungebildeter Videoüberwachungsangesteller. Insofern sind die Gruppen etwas unglücklich gewählt. Zumindest eine dritte Gruppe mit erfahrenen Verhaltenspsychologen hätte die Studie wohl aussagekräftiger gemacht.

397 TROSCIANKO ET AL., S. 90 und 93 ff. Als korrekte Beschreibung galt bspw. „female in white top hits other female", als nahe dran „white top going to fight with someone".

398 Eine mögliche Erklärung dafür sei, dass die vorgegebenen Kriterien automatisierbar seien und daher nicht stark von der Erfahrung beeinflusst würden (TROSCIANKO ET AL., S. 96).

tigen Kriterienkatalog zusammenstellen zu können.[399] Die Erkennungsrate des Vorliegens eines Vorfalls war zwar mit einer Trefferquote von ca. 80-90% relativ hoch. Dieser „Erfolg" ist aber wohl durch eine bedenklich hohe Falsch-Positiv-Rate von ca. 40% und eine in der Realität wenig praktikable sechsstufige Bewertungsskala erkauft.[400]

Zu ähnlichen Schlussfolgerungen wie die Studie von TROSCIANKO ET AL. kommt das im Rahmen des „Telematics Applications Programme" unter der Schirmherrschaft der Europäischen Kommission durchgeführte Projekt CROMATICA.[401] Im Rahmen dieses Projekts befassten sich Forscher bereits in der zweiten Hälfte der Neunzigerjahre unter anderem mit Videoüberwachungslösungen in Untergrundbahnhöfen, die abnormale Verhaltensweisen beziehungsweise Bedrohungen automatischen erkennen lassen sollten. Zwar waren lediglich relativ rudimentäre Verhaltensmuster, nämlich abnorme Bewegungen (vor allem die Bewegung gegen den Strom) und Positionierung (zum Beispiel in der Nähe von Notausgängen) Inhalt des Experiments, *diese* konnte das untersuchte automatische Überwachungssystem aber mit einer Quote von deutlich über 90% der Fälle erkennen.[402]

Die Ergebnisse aus der vorgestellten Studie von TROSCIANKO ET AL. sind wohl eher zurückhaltend zu interpretieren und die bei GMÜR angeführten Studienergebnisse zur Gefährlichkeitsprognosestellung ebenso mehrdeutig.[403] Beim Vorausahnen von Bedrohungen teilen die neuen Systeme die Probleme der herkömmlichen Rasterfahndung, des Profilings und der Prognosestellung: Die Profilerstellung beruht auf Erfahrung sowie Intuition und liefert (sinnvolle) Hypothesen oder Ermittlungsansätze, jedoch nicht beispielsweise unmittelbar identifizierbare Täter.[404] Kriterienkataloge können die Erfahrung und Intuition nur unzureichend ersetzen. Wenn schon ausgewiesene Experten auf dem Gebiet der Profilerstellung abweichendes Verhalten oder zukünftige Abweichler nicht zuverlässig vorausahnen oder identifizieren können sowie bis anhin keine krite-

399 TROSCIANKO ET AL., S. 96.

400 Siehe TROSCIANKO ET AL., S. 90.

401 Projekt TR1016 „Crowd Management with Telematic Imaging and Communication Assistance" (CROMATICA) wurde am 31. März 1999 beendet, siehe DEPARIS/DAVID, S. 22.

402 DEPARIS/DAVID, S. 15 und 19.

403 GMÜR, S. 1312.

404 DITTMANN 2003, S. 81; NEDOPIL, S. 361 f.; HOFFMANN/MUSOLFF, S. 154 f. Vgl. KUNZ 2011, S. 56 f. Ausführlich zum Profiling, siehe bspw. HOFFMANN/MUSOLFF und (kritisch) KRASMANN, S. 276 ff.

riengeleitete Prognosemethode mit wirklich überzeugenden Trefferquoten entwickelt werden konnte[405], dann dürfte dies auch bei automatisierten Systemen jedenfalls in absehbarer Zeit nicht gelingen.[406]

Der Vorteil automatisierter Systeme liegt in deren hoher Rechenkapazität. Das heisst, das automatisierte System kann die *vorgegebenen* Kriterien und Algorithmen effizienter und verknüpft anwenden; es bleiben jedoch dieselben Kriterien, die der Mensch in seiner Lagebeurteilung verwendet. Der Nutzen von automatisierten Selektions- und Analyseverfahren hängt somit wesentlich von den Fortschritten in der Disziplin des Profiling ab. Auch ist die menschliche Intuition ein nicht unwichtiges Element beim „psychologischen Täterprofil".[407] So ist zu bezweifeln, dass automatisierte Systeme zwischen verdächtigem Verhalten und etwa dem desorientierten Verhalten eines Fremden zu unterscheiden vermögen. Die Merkmale beider Verhaltensarten überschneiden sich.[408] Missdeutungen von aus verschiedenen Datenbanken extrahierten Informationen und Missverständnisse bei darauf gestützt erarbeiteten (Bedrohungs-)Analysen und Personenprofilen dürften sehr häufig auftreten.[409]

Um diesem Problem entgegenzuwirken, könnten indes, meint SKILLICORN, neuere Systeme mit verbesserten Ausgabekategorien versehen werden. Viele der heutigen Technologien sagten auch für eine eigentlich inkompatible Eingabe *irgendetwas* voraus. Künftige Systeme könnten hingegen mit der Fähigkeit ausgestattet werden, Ergebnisse einer Voraussage (zum Beispiel kriminelles Verhalten) über eine bestimmte Rangzuordnung zu markieren. Der Nutzer sähe dann, welche Ergebnisse das System als plausibel berechnet hat. Darauf gestützt kann er entscheiden, welche es wert sind, weiterverfolgt zu werden.[410] Indem das System auf die Kategorisierung der Resultate programmiert wird, kann zwar nicht

---

405 GMÜR, S. 1311 mit zahlreichen Hinweisen; KAMMERER 2008, S. 204. Vgl. DITTMANN 2003, S. 81 und NEDOPIL, S. 361, welche v. a. der Prognose künftiger Delinquenz eines mutmasslichen Täters sehr skeptisch gegenüberstehen.

406 SKILLICORN 2008b, S. 68 f. A. A. TROSCIANKO ET AL., S. 96.

407 Anders beim empirischen Täterprofil, in welchem Intuition und Erfahrung keine Rolle spielen, siehe DITTMANN 2003, S. 81.

408 A. A. sind die Verfasser des Berichts INDECT D1.1, S. 8. Im Bericht wird aber nirgends ein plausibler Nachweis der praktischen Machbarkeit dieser Behauptung angeführt. Siehe NORRIS/ARMSTRONG, S. 144 f. für dasselbe Problem bei der althergebrachten (nicht automatisierten) Videoüberwachung

409 Vgl. MINOW ET AL., S. 39 f.

410 SKILLICORN 2008b, S. 312.

die Ursache des Problems behoben, jedoch könnten vielleicht zumindest einige falsche Ergebnisse, die etwa zu falschen Ermittlungsschlüssen führen, frühzeitig erkannt werden. Zudem könnte dieses Vorgehen dazu beitragen, viele für die Profilerstellungsforschung nützliche Daten zusammenzutragen. Die wissenschaftliche Auswertung dieser Daten könnte die Forschung womöglich vorantreiben, und zuverlässige objektivierbare Kriterien in bestimmten Bereichen könnten dadurch vielleicht tatsächlich gefunden werden.

F. Kostenpunkt und mangelnde Kapazitäten

Vielfach wird vorgebracht, Überwachungstechnologien könnten Behörden entlasten, indem sie das Problem chronischen Personalmangels lösten. Dagegen ist einzuwenden, dass die Komponenten der Systeme angeschafft und durch geschultes Personal betrieben, gewartet und von Zeit zu Zeit über Upgrades aktualisiert werden müssen.[411] Die Datenverarbeitungssysteme der Behörden „up-to-date" zu halten ist keine günstige Angelegenheit. Die Sondierung und Analyse von Daten setzen je nach zu überwachendem realem oder virtuellem Raum, Netzwerk oder System entsprechend hochgerüstete Hardware voraus. Die gesammelten Daten bedürfen zudem eines Speicherorts, sollen sie archiviert werden. Je nach benötigter Datenart und -qualität fallen nicht unerhebliche Datenmengen an, für die genügend Speicher zur Verfügungen stehen muss. Beispielsweise braucht, nach eigener Schätzung der Projektmitarbeiter, *eine einzelne* Videoüberwachungskamera des INDECT in *minimaler* Aufnahmequalität (bzgl. Auflösung und Bild pro Sekunde) bei Nonstop-Betrieb pro Tag über fünf Gigabyte Speicherplatz, bei maximaler Aufnahmequalität über 42 Gigabyte.[412] Frag-

---

411 Siehe dazu den Bericht INDECT D9.4, S. 14 f.: Die einmaligen Kosten eines INDECT-Systems mit zehn Knotenpunkten, einer Zentralstation, fünfzehn Kameras und zehn Mikrofonen belaufen sich auf geschätzte 114'000 Euro (je nach technologischer Entwicklung muss mit einem Zuschlag von bis zu 50% der Kosten gerechnet werden). Die Wartung eines derartigen Systems kostet ca. 1'000 Euro pro Monat. Nicht berücksichtigt sind dabei die Betriebskosten, die wesentlich höher anzusetzen sein dürften als die Wartungskosten. Zu den Kosten herkömmlicher Videoüberwachungsanlagen, siehe GRAS, S. 95 ff. Siehe LINGG, S. 70 zu den Kosten der Videoüberwachungsanlage auf dem Bahnhofplatz Luzern. Zur notwendigen Aus- und Weiterbildung des die verschiedenen Technologien einsetzenden Personals der Behörden, siehe ROTERT, S. 439 f.

412 Bericht INDECT D1.1, S. 41 f. Hinzu kämen sieben Gigabyte pro Tag und Standort für die zusätzliche Audioüberwachung. Hochgerechnet auf eine Grossstadt mit 1000 Kameras, käme man auf über fünf beziehungsweise 42 Terabyte Video- plus sieben Terabyte Audio-

lich ist, inwieweit die schlechteste Aufnahmequalität für die manuelle und die automatisierte Analyse ausreichen. Die Minimalbildrate von 5 Bildern pro Sekunde scheint für die meisten Zwecke wenig brauchbar zu sein: Von polnischen Polizisten, die ein Testsystem aus dem Projekt INDECT verwendeten, verlautete, dass mindestens 15 Bilder pro Sekunde gewünscht wären.[413] Um automatisierte Bildanalysetechnologien (z. B. Gesichtserkennungsprogramme) zweckmässig zu verwenden, muss jedenfalls ein möglichst hoher Bildstandard vorliegen.[414]

Abwägungen zwischen der Anzahl Videokameras, der Aufnahmequalität und der Aufbewahrungsdauer der Aufnahmen sind unvermeidbar. Wahrscheinlich wird sich dieses Problem aber mit steigender Speicherkapazität auf zunehmend kleinerem Raum in der Zukunft lösen. Für die virtuelle Überwachung besteht es bereits heute praktisch nicht mehr.[415] Für Kleinstädte, wie das schottische Airdrie[416] aus der oben angeführten Studie von GILL/SPRIGGS, scheint es indes fraglich, ob sich der Einsatz eines INDECT-Systems lohnte.[417] Auch daraus ergibt sich, dass sich Raumüberwachungssysteme in der Schweiz vor allem als Instrument zum gezielten Einsatz an wenigen, neuralgischen Punkten eignen und diesbezüglich zur Koordination der Einsatzleitung bei geplanten Interventionen beitragen können.

Bereits zielgerichtete Einsätze von Überwachungssoftware und simple Antennensuchläufe sind teuer. Die Behörden müssen mit den heute verfügbaren Mitteln, die sehr wahrscheinlich aufwendigere Auswertung der gewonnen Daten nicht eingeschlossen, mit 10'000 Euro aufwärts pro Govware-Einsatz (exkl. Datenauswertung) rechnen.[418] Bei gross angelegten Rasterfahndungen sind die Kos-

Daten pro Tag. Siehe auch SIMON D., S. 244 mit weiteren Hinweisen, zu den riesigen Datenaufkommen der Vorratsdatenspeicherung. Vgl. dazu auch ROTERT, S. 437.

413 Siehe Bericht INDECT D1.1, S. 20.

414 Siehe dazu INTRONA/NISSENBAUM, S. 3, 21 und 40.

415 Siehe BRUCE SCHNEIER in Blog vom 6. März 2006.

416 Gemäss <http://www.scrol.gov.uk/> waren in Airdrie im Jahr 2001 36'326 Einwohner verzeichnet.

417 GILL/SPRIGGS, S. 120 kamen zum Schluss, dass die hohen (Unterhalts-)Kosten der von ihnen untersuchten CCTV-Anlagen im Verhältnis zum Erfolg nicht angemessen waren. Zu den Folgekonflikten (zwischen Politik, Gemeinwesen, Sponsoren und Privaten), die die Finanzierung der laufenden Kosten mit sich bringt, siehe GRAS, S. 223 f. mit Hinweisen.

418 HANSJAKOB 2011, N. 32. Siehe auch Botschaft BÜPF 2013, S. 2772 („der Einsatz von Govware ist ein komplexes Unterfangen und ausserordentlich kostenintensiv"). Gemäss SCHMID/BAUMGARTNER in NZZ Online vom 15. Oktober 2011 kostete im Fall Andrea Stauffacher ein entsprechendes Mietgerät der deutschen Firma Digitask die Bundesanwalt-

ten kaum abschätzbar; sicherlich aber weitaus höher.[419] Auch Register zu führen, ist zuweilen alles andere als günstig.[420] Vielfach ziehen in diesem Bereich bereits auf den ersten Blick unscheinbare Posten überraschend hohe Kosten nach sich.[421]

G. Umgehungstaktiken

Trotz aller Neuerungen, Verbesserungen und Leistungssteigerungen sind Überwachungs-, Registrierungs- und Massendatenverarbeitungstechnologien verhältnismässig leicht zu umgehen. Meist reichen simple und leicht erhältliche Mittel aus, um eine Identifizierung im virtuellen oder realen Raum zu verhindern. Dabei ist erstaunlich, wie gut die rudimentärsten Verschleierungswerkzeuge (Verkleidung, Internetzugang im Internetcafé anstatt zu Hause, schnell wechselnde IP-Adressen etc.) und -taktiken („unverdächtige" Verhaltensweisen etc.) wirken. Bereits eine Kappe und Brille verhindern eine verlässliche Identifikation (biometrische Gesichtserkennung) durch eine Videoüberwachungskamera, insbesondere, wenn diese in einem zu hohen Winkel installiert ist. Dasselbe gilt, wenn sich der Verbrecher etwa die Dunkelheit zunutze macht.[422] Nicht zu übersehen

schaft 26'000 Euro. Vgl. dazu BUERMEYER/BÄCKER, S. 434. Siehe zu den Gebühren für einzelne Überwachungshandlungen im virtuellen Raum auch den Entwurf der Änderungen der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs. Kritisch dazu auch GAUTIER/BUSCH, S. 51 f.

419 Siehe dazu PEHL, S. 257 f. Ebenso verursacht die Vorratsdatenspeicherung hohe Kosten, siehe dazu ZIMMER, S. 214 ff. mit weiteren Hinweisen.

420 Vgl. etwa hinsichtlich des Aufwands öffentlicher Verdachtsregister ZGOBA ET AL., S. 35 ff. (geschätzte fünf Millionen Dollar Betriebskosten im Jahr 2007 des Sexualstraftäterregisters des Bundesstaats New Jersey).

421 Zum Beispiel beliefen sich die Kosten fürs Versenden von E-Mails des Departement of Corrections von Florida an Sexualstraftäter mit Meldepflicht zur Verifizierung ihres Aufenthaltsorts in einem Jahr (2006/2007) auf 11'800 Dollar, siehe OPPAGA 2008, S. 4.

422 Siehe STRÖM, S. 119 f.; HEYMANN, S. 74; INTRONA/NISSENBAUM, S. 20; Bericht BKA Fotofahndung. Vgl. KAMMERER 2008, S. 223 f. Komplexere Täuschungsvarianten und Beispiele taktischen Vermeidungsverhaltens finden sich bei DUNSTONE/YAGER, S. 251 ff.; FUCHS ET AL., S. 16-19; MARX 2003, S. 374 ff.; KAMMERER 2008, S. 338 ff. Die Überwachung des Internetverkehrs (etwa mittels DPI-Technologie) kann bis zu einem gewissen Grad durch den Gebrauch von Anonymisierungs-Tools wie „Tor" (siehe <https://www.torproject.org/>) erschwert werden. Ein probates Mittel ist scheinbar auch, Nachrichten oder Inhalte als Bilder anstatt in Textform auszutauschen, siehe BECKER K. B., S. 180 f. Weitere Beispiele zu Taktiken und Ausweichaktivitäten im virtuellen Bereich finden sich bei LSE Briefing, S. 18; BECKER K. B., S. 172 ff.; GLESS 2012, S. 4; SZUBA, S. 36; SIMON D., S. 246 f.; PFITZMANN/KÖPSELL 2009a, S. 545 f.; VALERIUS, S. 24 f.; und auf <prism-break.org>.

ist ferner, dass sich automatisierte High-Tech-Systeme für die Überwachung oder Analyse von Low-Tech-Handlungen oftmals nicht eignen. Zwar können sie E-Mails mit verdächtigen Phrasen automatisch abfangen, den Inhalt eines normalen Briefs einzusehen bleibt ihnen aber verwehrt. Zudem erkennen im virtuellen Raum auch moderne Systeme gerade die einfachsten „Kodierungen" nicht. Unverdächtige Ausdrucksweisen zu benutzen, verhindert in der Regel, durch ein Überwachungssystem entdeckt zu werden. Eines der Ziele von INDECT bezüglich der virtuellen Raumüberwachung ist es deshalb, automatisierte Systeme so zu programmieren, dass diese die semantische Bedeutung, den Doppelsinn sprachlicher Kodierung erkennen.[423] Das wäre ein bedeutender Fortschritt. Ansonsten bräuchte es, um diese Art der Kodierung zu verstehen und zu übersetzen, nach wie vor den menschlichen Ermittler. Ein automatisiertes System wie INDECT muss aber bis zu einer bestimmten Verarbeitungsstufe, namentlich bis zu einem ausreichenden Grad der Vereinfachung und der übersichtlichen Darstellung der Informationen, autonom arbeiten können, um einen Mehrwert zu erbringen. Menschen sind in diesem Sinne *inkompatibel* mit automatisierten Systemen, wenn Letztere eine Aufgabe nicht äusserst verlässlich lösen. Mit grossen Datenbergen kann der Mensch nicht umgehen. Liefern sie dem menschlichen Ermittler zum Beispiel die gesammelten Berge kodierter Kommunikation nicht entkodiert oder teilweise falsch entschlüsselt zu – weil sie darauf nicht ansprechen oder diese nur allgemein als grundsätzlich verdächtig einstufen – überfordert die manuelle Auswertung den Menschen, er bremst in der Folge den Prozess aus und vermindert den Nutzen der Kooperation zwischen Maschine und Mensch in beträchtlichem Masse. Die Prozesse hinter einer von automatisierten Systemen ausgegebenen Analyse einer Bedrohungssituation dürften überdies auch für technisch erfahrene menschliche Anwender kaum nachvollziehbar sein und daher Auswertungsfehler des Systems nicht sofort oder nie erkannt werden, was die auf entsprechend fehlerhaften Ergebnissen beruhenden Folgehandlungen vorbelasten wird.[424] Zuweilen dürften dadurch Ressourcen etwa auf fehlleitende

---

423 Bericht INDECT D9.4, S. 22. Ausführlich zu sprachlichen und kommunikativen Umgehungsstrategien der Zensur BECKER K. B., S. 182-187 mit zahlreichen Beispielen und weiterführenden Hinweisen. Bsp. für „alltagssprachliche Kodierungen" finden sich bei SKILLICORN 2008a, S. 427; STRÖM, S. 60. Ein Mensch sollte auf den inneren Gehalt derartiger Andeutungen aus dem Kontext schliessen können, ein automatisiertes System wohl (noch) nicht von selbst. Vgl. ROTERT, S. 439. Teilweise kann derartigen Täuschungsversuchen mit „Tricks" entgegen gewirkt werden, siehe SKILLICORN 2008a, S. 447 f., zumindest solange jene vom Gegenspieler nicht wiederum durchschaut werden.

424 Vgl. KAMMERER 2008, S. 204 f.; INTRONA/WOOD, S. 183.

Ermittlungsansätze und auf die anschliessende Fehlersuche im System verwendet werden und ein erheblicher Mehraufwand entstehen.

Insofern scheitert die neue Generation der Raumüberwachungssysteme nicht einzig an dem etwa vom INDECT Projekt proklamierten technischen Vorsprung Krimineller, sondern vielfach an wenig eleganten, simplen Täuschungstechniken.[425] Erschwerend kommt sicherlich auch ein gewisser Gewöhnungseffekt hinzu. Solange die Raumüberwachung in einem Bereich unüblich ist, weiss der Delinquent womöglich noch nicht, wie er darauf reagieren soll. Ihm passieren Fehler oder er verhält sich nicht vorsichtig genug.[426] Kennt er hingegen erst einmal die Funktionsweise, die Fähigkeiten, die Kriterien für die Beurteilung abweichenden Verhaltens und die Standorte der Überwachungsknoten (beziehungsweise die toten Winkel der Sichtfelder der Kameras), kann er sich diesen Gegebenheiten anpassen. Sich der Überwachung zu entziehen, wird dadurch zur Routine. Insbesondere den als aussergewöhnlich gefährlich einzustufenden Personen muss man wohl eine gewisse Kreativität zuerkennen. Gerade diese dürften folglich in der Lage sein, die Systeme zu täuschen oder gar für eigene Zwecke zu missbrauchen.[427]

H. Hinderlicher Fortschritt

Die Behauptung, dass staatliche Behörden ihrem Gegenpart, den Kriminellen, im technischen Instrumentarium und Wissen hinterherhinken, kann zutreffen, ist im Allgemeinen aber anzuzweifeln.[428] Der rasante technische Fortschritt im virtuellen Bereich bringt zwar immer neue Kommunikationsmöglichkeiten mit sich, an welche die Instrumente angepasst werden müssen. Zumindest für einige Zeit, je nachdem wie schnell der Staat sein Repertoire anpasst, kann es sein, dass neue

---

425 Es ist zu bezweifeln, dass eine Sicherheitstechnologie je so sicher sein wird, dass keine Hintertüren ausfindig gemacht werden könnten. Auf neue Sicherheitstechniken folgen in der Regel immer auch neue Überlistungstechniken (und umgekehrt). Besonders die weite Verbreitung eines Systems macht es angreifbarer (vgl. MARX 2003, S. 372). Den überwachenden Behörden stehen wiederum meist wesentlich grössere Ressourcen (leistungsfähigere Computersysteme, mehr Personal etc.) zur Verfügung, vgl. FUCHS ET AL., S. 16.

426 Darauf weist bspw. die Studie DITTON/SHORT hin, bei der die Kriminalitätsrate sich im videoüberwachten Bereich zuerst verringerte, nach einer gewissen Zeit aber wieder auf das frühere Niveau stieg.

427 Vgl. CUSSON, S. 73 f.; HEYMANN, S. 65; NOGALA 1998, S. 260; PFITZMANN/KÖPSELL 2009a, S. 543 und 546; KAMMERER 2008, S. 347 f.; LSE Briefing, S. 24.

428 PERREY, S. 185. Vgl. die Projektbeschreibung INDECT.

Technologien einer Kontrolle durch automatisierte Systeme nicht zugänglich sind.[429] Ungleich dem realen Raum, wo eine Kamera mit veralteter Technik Geschehnisse trotzdem aufzeichnen kann, können virtuelle Sondierungs- und Überwachungsprogramme inkompatibel mit technischen Neuerungen des virtuellen Raums werden.[430]

In der Regel stehen den staatlichen Behörden indes wesentlich grössere Ressourcen zur Verfügung als Kriminellen.[431] Kundige Personen können die derzeitigen virtuellen Überwachungssysteme verhältnismässig leicht ausmanövrieren, aber nicht primär deshalb, weil ihnen die neuere Technologie zur Verfügung stünde. Die Probleme der Überwachung des virtuellen Raums ergeben sich daraus, dass Daten leicht zu manipulieren sind und dass sich im virtuellen Raum bewegende Nutzer oft vorsichtig vorgehen sowie um diese speziellen Beschaffenheiten der Virtualität wissen. Beachtet der Delinquent im virtuellen Raum verhältnismässig simple Verhaltensregeln (unter anderem die Nutzung bestimmter Programme und Systeme zu vermeiden oder die häufig ohnehin integrierten Verschlüsselungsoptionen zu aktivieren) und eignet sich ein gewisses Fachwissen an, ist er gegen den Grossteil der virtuellen Überwachungsmassnahmen geschützt.[432] Neue Schwachstellen der technisierten Kriminalitätsbekämpfung finden sich zudem immer wieder.[433] Davon abgesehen setzte eine einigermassen flächendeckende, staatliche Präventivüberwachung digitaler Inhalte und Kommunikation eine umfassende Datenbank voraus, und das dazu eingesetzte Überwachungssystem müsste grösser und schneller sein und bleiben als die zu kontrollierenden informationstechnischen Systeme (beispielsweise als die gesamte Internetinfrastruktur in einem Staat).[434]

---

429 Vgl. BECKER K. B., S. 187; LSE Briefing, S. 25. In diese Richtung geht auch das Argument des „rechtsfreien Raums", siehe dazu unten Vierter Teil, Kapitel V.B.

430 Siehe dazu LSE Briefing, S. 17 und 25 f. Analog stelle man sich bspw. vor, Videoüberwachungssysteme wären darauf angewiesen, regelmässig auf eine neue Energieversorgung umgerüstet werden zu müssen.

431 Vgl. RÜTHER, S. 93 ff.

432 Siehe dazu PERREY, S. 185; ANDRES, S. 242; COMPUTERGRUPPE H48, S. 202 ff.

433 Vgl. anstatt vieler den STREBEL in NZZ am Sonntag vom 10. Oktober 2004.

434 LSE Briefing, S. 20.

I. Fehleranfälligkeit und Datenmissbrauch

Technische Defekte oder unwirtliche Umgebungen (zum Beispiel die Dunkelheit für die Kamera) sind kostspielige Faktoren, aber grundsätzlich beheb- oder anpassbar (zum Beispiel könnte die Kamera mit einer Nachtsicht- oder Infrarotfunktion bestückt werden). Auch weiter fortgeschrittene Methoden des Data Mining und des Datensammelns von INDECT und Co. haben jedoch mit einigen Grundsatzproblemen zu kämpfen. Eines liegt in angezapften Datenquellen, die fehlerhaft sind. Ohne *verlässliche* Datenbanken über Personen, Sachen, Sachverhalte, Verhaltensweisen etc. können diese Instrumente eine nutzbringende Analyse grosser Datenbestände nicht anspruchsgerecht leisten.[435] Fokussieren Systeme auf das Sammeln möglichst vieler Informationen, vernachlässigen hingegen Vorkehrungen der Qualitätssicherung, entstehen mangelhafte Datenarchive.[436] Erst wenn es gelingt, automatisierte Systeme Datenbestände sehr zuverlässig analysieren zu lassen, also die vorhandenen Daten besser zu interpretieren und effizienter zu gewichten, sollte über Methoden nachgedacht werden, *mehr* Informationen zu gewinnen. Falschinformationen und schlechte Datenqualität in staatlichen Datensammlungen sollten über entsprechende Vorkehrungen so weit wie möglich vermindert werden.[437] Die Nützlichkeit einerseits der Instrumente des Data Mining und andererseits der Datenbanken kann an ihren nicht korrekten Einträgen gemessen werden.

Diesbezüglich ist auch darauf hinzuweisen, dass bei komplexer Technik Vorgänge bis zum gewünschten Resultat zumeist sehr viele Verarbeitungsstadien umfassen, was sie sehr fehleranfällig macht, da sich in jedem Stadium mehrmals Gelegenheiten ergeben, falsche Daten zu erfassen, Fehler zu generieren, verzerrende Daten zu berücksichtigen, Ungenauigkeiten zu übersehen oder Ähnliches. Die ursprünglichen Fehlerquellen lassen sich vom Resultat aus zurück forschend nurmehr schwer eruieren.[438] Wenig hilfreich ist dabei insbesondere, dass der Mensch nicht komplett aus den Prozessen auszuklammern ist. Er nimmt zwingend Einfluss auf den Prozess; sei es beim Schreiben des Programms, beim Si-

---

435 FIENBERG, S. 213: „Data mining tools can't make up for bad data and poor matches, […]"; NOWAK, S. 19; Bericht GPDel, S. 7724; BELSER, S. 7 ff. N. 12 ff. mit weiteren Hinweisen. Vgl. HEYMANN, S. 175.

436 Bericht GPDel, S. 7667; Stellungnahme des Bundesrats i. S. Bericht GPDel, S. 7749. Vgl. CHESTERMAN, S. 227 f.; HEYMANN, S. 163; HOWELLS, S. 46.

437 ROSSNAGEL/BEDNER/KNOPP, S. 538.

438 Vgl. bspw. MINOW ET AL., S. 37 ff.

cherstellen von Spuren und Sachbeweisen (zum Beispiel Videoüberwachungsaufnahmen) oder später bei der Analyse der Indizien, der Beurteilung des Falls oder der Eintragungsanordnung in ein Register.[439]

Der Wahrheitsgehalt der durch technisierte Methoden produzierten Erzeugnisse und Hinweise wird vielfach überschätzt.[440] So birgt zum Beispiel die DNA-Spuren-Analyse überraschend viele Fehlerquellen.[441] Es ist deshalb nicht völlig unwahrscheinlich, dass einige Einträge in DNA-Datenbanken zum Zeitpunkt des Eintrags verfälscht sind[442] und damit die darauf beruhenden Ermittlungshandlungen oder Präventionsanstrengungen negativ beeinflussen. Dasselbe gilt analog für andere Register, Massendatenverarbeitungs- und Überwachungstechniken.[443]

Die technischen Methoden bergen zudem das Risiko des Missbrauchs in sich. Als Beispiel zu nennen wären unerlaubte Zugriffe auf bestimmte Datenbanken oder auf die aus Überwachungen gewonnenen Informationen durch staatliche Behörden oder durch Dritte (Private oder andere Staaten).[444] Ferner ist immer daran zu denken, dass Daten leicht zu manipulieren sind, sei es, indem erhobene Daten respektive Informationen (ungewollt) verändert oder indem falsche gestreut werden. Beide Arten von Manipulation müssen nicht bewusst, etwa aus Übereifer einer Behörde oder aus krimineller Absicht geschehen. Zum Beispiel kann eine Videoüberwachungsaufnahme aus Versehen nachträglich mit dem Computer so bearbeitet werden, dass die aufgezeichnete Situation anders wirkt oder Angaben einer Person, die beispielsweise in einem Verdachtsregister vermerkt oder aus frei verfügbaren Internetquellen zusammengetragen werden, können eine simple Lüge sein.[445] Insofern wirken sich Informationen aus Datenbanken ohne genügende Aufsicht und ohne Pflicht zur korrekten Angabe sowie Vorkehrungen, welche das Erfassen der Wirklichkeit fördern, negativ auf darauf-

---

439 NEUHAUS, S. 539 Fn. 23; SPINNER, S. 271; MARX 2007 (Fallacy 6); NOGALA 1989, S. 106.

440 Sofern von *Wahrheitsgehalt* gesprochen werden kann, siehe unten Dritter Teil, Kapitel V.D.

441 Siehe dazu ausführlich NEUHAUS und BIEDERMANN/VUILLE mit Herleitungen.

442 Analog kritisch bezüglich fMRT-Hirnbildern: HASLER, S. 44.

443 Siehe NOGALA 1998, S. 164 f. mit weiteren Hinweisen.

444 Vgl. CHESTERMAN, S. 75 f. zu „Lecks" in Datenbanken. Bsp: Archivierte Bankdaten von Steuerflüchtigen oder mittels Govware gesammelte Personendaten. Dem Missbrauch durch staatliche Behörden kann möglicherweise mittels Anordnung zu Transparenz und mit genügenden rechtlichen Überprüfungsmechanismen entgegengewirkt werden. Siehe zu Datenmissbrauch und Systemsicherheit: KURZ/RIEGER, S. 38-44; LSE Briefing, S. 26 und 55 f.; SIMON D., S. 255 ff.; INTRONA/NISSENBAUM, S. 46 f.; ROSSNAGEL/BEDNER/KNOPP, S. 538 f.

445 Vgl. YOUNG 2004, S. 10 ff.

folgende Prozeduren und andere Datenbanken aus. Unentdeckte Manipulationen in frühen Informationsverarbeitungsstadien können mithin auch noch viel später zu Folgefehlern und Schwachstellen führen.[446]

J. Verlagerungseffekte

Verlagerungseffekte sind zugleich ein angestrebter Zweck und ein fundamentales Problem der dargestellten Kriminalitätsbekämpfungstechnologien.[447] Verlagerungseffekte können, in begrenztem Mass, sowohl bei der Überwachung virtueller und realer Räume als auch, stärker, bei Verdachtsregistern beobachtet werden. Am stärksten äussern sie sich bei Massnahmen, welche sich auf offene (im Gegensatz zu verdeckten) oder öffentliche Methoden verlassen.[448] Fällt der Entscheid zugunsten situativ positionierter Überwachungs-Hotspots, sorgen die Verlagerungseffekte häufig für ein Auseinanderklaffen der Schere zwischen sozial Bevor- und Benachteiligten, weil die aufwendige Überwachung von potenzialarmen Räumen sich aus vielen Perspektiven nicht lohnt.[449] Ein vermuteter und befürchteter Verlagerungseffekt wirkt zudem als Katalysator der Ausweitung der Überwachungstechnologien, da beispielsweise Gemeinden oder Quartiere, welche an überwachte Gegenden angrenzen, Videokameras aufstellen lassen, um zu verhindern, dass sich „die Kriminalität" in ihr Gebiet verlagert.[450]

---

446 Vgl. MINOW ET AL., S. 37 und 40.

447 Vgl. STUTZER/ZEHNDER, S. 114; YOUNG 1999, S. 22 und 136; GRAS, S. 204.

448 Zum Verlagerungs- bzw. Verdrängungseffekt der Raumüberwachung, siehe etwa FLÜCKIGER, S. 221; GILL/SPRIGGS, S. 72; HEMPEL/TÖPFER, S. 15; LINGG, S. 43 ff.; MÜLLER L. 2011, insb. S. 246; STUTZER/ZEHNDER, S. 113 f. und 127; ZEHNDER M., S. 28 f. und 39 f.; Erster Teil, Kapitel II.C.1. Zu demjenigen bei Verdachtsregistern: Bericht HRW, S. 7 f.; MOECKLI/KELLER, S. 242; BGE 137 I 31 E. 6.5 S. 47 f.

449 Vgl. GRAS, S. 201 ff. und 210.

450 KAMMERER 2008, S. 45, 65 ff., 101 und 342; GRAS, S. 34. Vgl. STUTZER/ZEHNDER, S. 115.

IV. Schlussfolgerungen

A. Informationsverarbeitung, Datenbanken und Verdachtsregister

1. Fehleinschätzungen und leere Phrasen?

Unterschätzen sollte man das *theoretisch* grosse Potenzial der Informationsverarbeitungsmethoden nicht; ebenso wenig sollte man aber die *praktischen* Möglichkeiten und *tatsächlichen* Effekte überschätzen. Computergestützte, automatisierte Datenabgleiche sind, um nur ein Beispiel zu nennen, sicherlich sehr hilfreich. Die spezielleren Datenverarbeitungstechnologien wie Rasterfahndung, Massendatenverarbeitung und Vorratsdatenspeicherung erbringen den erhofften zusätzlichen Nutzen aber nicht immer.

Äussern sich Ermittler, wie dargestellt, oft sehr positiv zu technischen Überwachungsmassnahmen, hält im Gegensatz dazu das Gutachten des MPI zur Vorratsdatenspeicherung nüchtern fest, die gegenwärtige Lage sei „gekennzeichnet durch eine noch sehr unsichere statistische Datengrundlage, das Fehlen systematischer empirischer Untersuchungen und sehr unterschiedliche Einschätzungen bei den unmittelbar betroffenen Praktikern".[451] Die Frage, ob die Vorratsdatenspeicherung für staatliche Behörden einen konkreten Mehrwert verschafft, ist momentan unklar. Vorerst lassen sich zwei Schlüsse ziehen: Einerseits werden der Nutzen und der Aufwand einer Rasterfahndung, Vorratsdatenspeicherung und ähnlicher Werkzeuge vielfach falsch zugunsten dieser Methoden eingeschätzt.[452] Andererseits dürfte es wohl künftig mit neuen Techniken möglich sein, Datenbanken, Raumüberwachung und Massendatenverarbeitung effizienter

---

451 ALBRECHT H. J. ET AL., S. 218. Zum Nutzen der Vorratsspeicherung, siehe auch SZUBA, S. 174 ff. und 180, SIMON D., S. 242 ff., insb. 247 f. und 259 (je skeptisch), ZIMMER, S. 205 ff. (grundsätzlich Nutzen zusprechend), MÖSTL, S. 227 ff. und WEBER/WOLF/HEINRICH, N. 6 (je Nutzen zusprechend) jeweils mit weiteren Hinweisen. Das BVerfG misst der Vorratsdatenspeicherung für die effektive Strafverfolgung und Gefahrenabwehr „besondere Bedeutung" zu, siehe BVerfGE 125, 260 (322 f.). Ähnlich Botschaft BÜPF 2013, S. 2697.

452 Ob beispielsweise die im Jahr 2002 angelaufene Operation „Genesis" in der Schweiz (Bekämpfung der Kinderpornografie im Internet) bezüglich des Kosten-Nutzen-Faktors ein Erfolg war, ist schwer zu beurteilen. Siehe zu dieser Operation die Medienmitteilung fedpol vom 25. Juli 2003 und den Bericht der Arbeitsgruppe Genesis. Für weitere Beispiele, siehe ALBRECHT H. J. ET AL., S. 94 ff. Siehe auch HOFFMANN/MUSOLFF, S. 271.

zu kombinieren und damit eventuell die kriminalitätsbekämpfende Informationsverarbeitung insgesamt zu verbessern.

Ähnlich werden auch Verdachtsregister häufig zu ihren Gunsten falsch eingeschätzt und mit leeren Phrasen gerechtfertigt. Zum Beispiel sind zwar geringe positive Wirkungen der öffentlichen Sexual Offender Register, Straftaten zu verhindern, nicht auszuschliessen, hingegen auch kaum zu belegen. Maureen Kanka, die Mutter von Megan, verteidigte das Megan's Law, angesprochen auf die dargestellten pessimistischen Studienergebnisse, wie folgt: „The purpose of the law was to provide an awareness to parents. It was put there for parents to know where the offenders are living. It's doing what it was supposed to do. We never said it was going to stop them from reoffending or wandering to another town."[453] Diese Argumentation greift indessen ebenso wenig wie diejenige, welche Natalie Simone Rickli zur Bekräftigung ihrer parlamentarischen Vorstösse, ein Schweizer Pädophilenregister zu schaffen, anbringt: „Der Täter muss wissen, dass er jederzeit kontrolliert werden kann."[454] Beide Standpunkte sind bezüglich einer Rechtfertigung derartiger Register irrelevant, wenn trotz der gesteigerten Wahrnehmung der Eltern gleich viele Kinder Opfer von Sexualstraftaten werden und den Täter die kommunizierte, „jederzeitige fremde Kontrolle" seiner selbst, aus welchem Grund auch immer, nicht interessiert beziehungsweise ihn nicht daran hindert, Sexualstraftaten zu begehen.

2. Empirische Gefährlichkeitsprognosen und die Übersichtlichkeit

Bei Verdachtsregistern tritt die Frage, *was* die Person getan hat, in den Hintergrund. Dies birgt vor allem für die öffentlichen Register viel Potenzial für Widersprüche, Fehler und Ungerechtigkeiten in sich: Mittels der öffentlich abrufbaren Einträge lässt sich kaum erkennen, welcher Eingetragene schwere Verfehlungen begangen hat und welcher nicht. Zwar kennen beispielsweise die meisten Sexualstraftäterregister in den Vereinigten Staaten eine Markierung der Eingetragenen mit bestimmten Gefährlichkeitsstufen (zum Beispiel Trennung zwischen „Sexual Offender" und „Sexual Predator"). Vielfach ist diese Markierung aber die einzige Information zur begangenen Tat.[455] Ohne eine gründliche

---

453 Siehe LIVIO in nj.com vom 7. Februar 2009.

454 Aus der Begründung ihrer parlamentarischen Initiative (09.423).

455 Siehe Bericht HRW, S. 55 ff.; LOGAN, S. 604 ff. mit Beispielen. Das Register von Florida begnügt sich mit dieser zweistufigen Unterscheidung. Andere Staaten sehen mehrstufige Klassifizierungen vor oder stellen kurze Angaben zu den verletzten Normen bereit. Siehe

Sichtung der Rechtsgrundlagen des jeweiligen Bundesstaates und/oder des zugrundeliegenden gerichtlichen Entscheids bleibt dem Nutzer – jedenfalls dem Rechtslaien, den dieses System in erster Linie ansprechen soll – indes verborgen, inwiefern der Eingetragene gegen das Gesetz verstossen haben soll. Leichte und schwere Straftaten und Tatgruppen auseinander zu halten, stellt sich als schwierig heraus, selbst wenn gewisse Angaben zu den verletzten Normen publiziert werden. Ohne weitergehende Informationen etwa zur Strafhöhe im Urteil, zu den Umständen, die zu der Tat geführt haben usw. hat der Nutzer keine Handhabe, sich selbst ein differenziertes Bild vom Registrierten zu machen. Die vorhandenen Daten sind aus dem Kontext gerissen – nicht mehr als Momentaufnahmen.[456] In gleicher Weise beschränken auch Terrorlisten die Hintergrundinformationen zu den einzelnen Einträgen auf das aus der Sicht der betreibenden Stellen Nötigste. Derartige Register geben daher häufig ein lückenhaftes Bild des Eingetragenen, seinen strafbaren Handlungen und den Hintergründen des Eintrags.[457] In Ermangelung genügender Informationen bleibt dem Nutzer nichts anderes übrig, als den Registereinträgen zu vertrauen oder sie anzuzweifeln. Eine tieferreichende Interpretation lassen sie nicht zu. Wer sicher gehen will, wird annehmen müssen, dass von jedem, der in einem derartigen Register vermerkt ist, eine Gefahr ausgeht.[458] Dementsprechend wird sicherheitshalber allen Registrierten wie einer akuten Gefahr gegenüber getreten, auch wenn ein Register tatsächlich gefährliche Personen nicht lückenlos oder fehlerfrei auflistet. Eine undifferenzierte und unnachsichtige Haltung gegenüber den Eingetragenen kann daher zu unfairen Situationen führen[459], die Öffentlichkeit grundlos verunsichern oder auch in falsche Sicherheit wiegen und in der Bevölkerung Anlass zu Misstrauen gegenüber dem Staat beziehungsweise dem Sanktionsregime geben, wenn Unzulänglichkeiten der Register aufgedeckt werden.[460]

<http://sex-offender-registry-review.toptenreviews.com/> für eine Übersicht der bereitgestellten Informationen.

456 Bericht HRW, S. 5 f. und 55 ff. Dasselbe Problem stellt sich bei der Raumüberwachung, siehe KAMMERER 2008, S. 160 f.

457 Siehe dazu etwa BARTMANN, S. 94.

458 Vgl. SCOTT/GERBASI, S. 496.

459 Vgl. etwa Bericht HRW, S. 7, 44, 71 und 78 ff.

460 Das ist nicht zuletzt deshalb so, weil die Bevölkerung durch ihr in Zweifelsfällen sicherheitsbewusst-berechnend unnachsichtiges Verhalten selbst in Misskredit gerät, sich aber eigentlich Ungefährlichen gegenüber ja wohl nicht unfair verhalten möchte.

Ein anderer Aspekt dieser Schwachstelle betrifft auch nicht-öffentliche Register: Die Aufnahme von Tätern in ein Verdachtsregister basiert, insbesondere im anglo-amerikanischen Raum, direkt auf Tatbestandsvoraussetzungen, auf rudimentären Prognoseinstrumenten (wie den Basisrückfallraten von Tätergruppen oder vereinzelt, in wenigen Bundesstaaten der USA, auf einer kriterienbasierten Checkliste[461]), oder auf zuweilen sehr vagen Geheimdienstinformationen, welche gar kein oder nur geringes Ermessen bei der Interpretation zulassen, sondern lediglich eine Zuordnung erfordern.[462] Zudem legt die amerikanische Gesetzgebung zum öffentlichen Verdachtsregister, aus Sicherheitsüberlegungen, deren Anwendungsbereich als sehr weit und die Registrierungsdauer als sehr hoch fest.[463] Die Aufnahme eines Sexualstraftäters in ein amerikanisches Register bedarf oft keiner Begutachtung durch einen Psychiater oder keiner Eintragsempfehlung, die von diesem infolge eines positiven Befundes der Gefährlichkeit des Täters erteilt würde. Stattdessen reicht für die Annahme der Gefährlichkeit oft bereits aus, dass der Täter die Norm verletzt hat.[464] Auf die Verletzung der Vorschrift folgt zwingend und ohne weitere Beurteilung die Registrierung. Somit

---

461 Siehe etwa HARCOURT, S. 7 ff. Zur Problematik dieser „statistischen Gefährlichkeitsprognose", siehe NOWARA, S. 104 f.; DITTMANN 1997, S. 129; NEDOPIL, S. 287 und 290 f. Wobei bzgl. der Abstellung auf Basisrückfallraten von keiner „Prognose" gesprochen werden kann, wenn man mit GMÜR, S. 1308, davon ausgeht, dass dieser Begriff nur für „*überzufällige* richtige Voraussagen" zu gebrauchen ist. Siehe auch HASLER, S. 122 f. zur Kritik am revidierten DSM-V, das neu auch „Risiko-Syndrome" umfasst. Dazu auch STALLMACH in NZZ Online vom 16. April 2013.

462 LOGAN, S. 598; SCOTT/GERBASI, S. 500. Ein typisches Beispiel für ein derartiges „Subsumtionsinstrument" (mit umfangreichem Katalog von Straftaten) ist die Formulierung der Artikel zum Sexualstraftäterregister der „Florida Statutes" des Senats von Florida (Statute 943.0435), abrufbar unter: <http://www.flsenate.gov/laws/statutes/2011/943.0435>.

463 Bericht HRW, S. 3. Ebenso bspw. die UN-Terrorliste, siehe SULLIVAN/HAYES, S. 86 ff.

464 LOGAN, S. 603, nennt dies die „compulsory method" und grenzt diese von der „discretionary method" ab. Vgl. MAZZUCCHELLI, S. 1338. Das individuelle Rückfallrisiko etwa ist dafür praktisch unerheblich, was primär zählt, ist die Basisrückfallquote der Tätergruppe oder die Einschätzung der Gefährlichkeit der Tätergruppe insgesamt. Demnach wird der Öffentlichkeit eine Liste von Personen zugänglich gemacht, deren Täterkategorie aus rein statistischer Sicht (somit abstrakt) oder auch politischer Sicht (somit subjektiv) gefährlich ist.Vgl. LOGAN, S. 604. Es muss aber bedacht werden, dass die Taten des notorischen Wiederholungstäters (also mit hoher Rückfallrate) nicht per se „gefährlich" sein müssen. Die Basisrückfallquote beschreibt nicht die Gefährlichkeit der zu erwartenden Tat und versagt damit darin, ein zuverlässiges Prognoseinstrument für die Eintragung in das Register darzustellen. Hierin wird eines der Probleme des „Täterstrafrechts" ersichtlich, vgl. HEINRICH, S. 118. Zum Täterstrafrecht siehe auch KUNZ 2010b, S. 10 ff.

konstatiert die verletzte Gesetzesnorm *selbst* die Gefährlichkeit des Täters durch einen Katalog (objektiver) Kriterien, welcher nur wenig richterliches Ermessen zulässt. Weil sich aber Kriterienkataloge, welche keine Ermessensentscheide vorsehen, nicht eignen, Einzelfälle adäquat zu erfassen, kann nicht verhindert werden, dass prognostisch ungefährliche Täter trotzdem in Register aufgenommen werden.

Diese Eintragungspraxis mag insbesondere für die USA gelten. Indes sind die Eintragungsvoraussetzungen mutmasslicher Terroristen oder gewaltbereiter Störer an Sportveranstaltungen in nicht-öffentliche Register auch in der Schweiz vielfach sehr ähnlich tief angesetzt.[465] Die unzulängliche Differenzierung und die oft vagen gesetzlichen Grundlagen der öffentlichen und nicht-öffentlichen Register führen dazu, dass absurde Einträge nicht selten sind.[466] Die genannten Register beinhalten folglich nicht nur Straffällige mit schlechter Prognose oder Personen, von denen eine akute und konkrete Gefahr ausgeht, sondern schlicht Personen, welche die weitgefassten Kriterien erfüllen; grundsätzlich unabhängig von einer nachhaltigen Prognosestellung oder Risikoanalyse. Obschon tatsächlich Gefährliche mit auf der Liste sein werden, dürfte sich ein beträchtlicher Teil der Eingetragenen bei einer individuellen und sorgfältigen Prognosestellung oder Gefährlichkeitsüberprüfung als ungefährliche, fälschlicherweise eingetragene Personen (falsch-positiv) herausstellen.[467] Abgesehen davon verändern sich Personen über die Zeit. Der Eintrag in einem Verdachtsregister ist hingegen eine (mehr oder weniger akkurate) Momentaufnahme. Die Systematik von Verdachtsregistern lässt kaum Platz für die Erfassung von Entwicklungen einer Person.

---

465 Als Schweizer Beispiel ist etwa das ISIS mit seinen „mechanischen Regeln zur Eingabe und Datenpflege" zu nennen, siehe Bericht GPDel, S. 7723.

466 Bspw. die Sechsjährige, welche in einer derartigen Datenbank als mutmassliche Terroristin geführt wurde, siehe dazu den Artikel „Gestatten: Terroristin, sechs Jahre alt" in 20 Minuten Online vom 29. Juni 2010.

467 Ein Grundsatzproblem: Will man möglichst restlos alle Gefährlichen erfassen, kommt man nicht umhin, zur Sicherheit auch einige Ungefährliche („Falsch-Positive") mit auf die Liste zu nehmen. Umgekehrt entgehen dem Register einige Gefährliche („Falsch-Negative"), wenn man die Liste kurz hält. Siehe DITTMANN 1997, S. 127 ff.; NEDOPIL, S. 288 ff.; HAYES 2009, S. 50; MINOW ET AL., S. 39; INTRONA, S. 85; SINGELNSTEIN/STOLLE 2012, S. 71, wonach Schätzungen aus der Praxis zufolge darauf hinwiesen, dass ca. die Hälfte aller per Prognose als gefährlich Eingestuften falsch-positiv seien. Dessen waren sich scheinbar auch zwei Richter des Obersten Gerichtshofs der USA im Entscheid Connecticut Departement of Public Safety v. Doe, 538 U.S. 1 (2003) vom 5. März 2003 bewusst, siehe dazu SCOTT/GERBASI, S. 496 und 501.

Verdachtsregister weisen schon deshalb viele nicht der Wirklichkeit entsprechende, weil überholte, Einträge auf.[468]

3. Praktikabilität

Aus den vorangehenden Ausführungen lässt sich ein weiterer allgemeiner Nachteil für Verdachtsregister (öffentlich oder nicht-öffentlich) ableiten: Die unzureichende Gefährlichkeitsprognose oder unbedachte Einträge aufgrund von vagen Kriterien betreffen unmittelbar die Praktikabilität eines Verdachtsregisters. Mit jedem Eingetragenen, der als gefährlich eingestuft wird, obwohl er es in Wirklichkeit nicht ist, verliert das Register an Effizienz, indem die wenigen konkret und akut Gefährlichen in der Masse der aufgrund falscher Einschätzung als gefährlich Registrierten untergehen. Eine Liste, auf der jeder hypothetisch Gefährliche vermerkt wird, ist hinsichtlich ihres Mehrwerts für eine effektivere Gefahrenabwehr belanglos und nützt auch der repressiven Ermittlung kaum. Die Stärke eines Registers liegt vielmehr in dessen Übersichtlichkeit und Verlässlichkeit.[469] Umfasst es weniger, dafür tatsächlich nur akut gefährliche Personen, können diese gemieden, kontrolliert oder paralysiert werden. In diesem Sinne kann die Bedrohung durch sie, mehr oder weniger, wirksam eliminiert werden. Ab einer gewissen Quantität von Registrierungspflichtigen indessen fällt es selbst den Registrierungsbehörden schwer, den Überblick zu behalten: Im Bundesstaat Kalifornien entzogen sich der Kontrolle der Registrierungsbehörden 861 von 6'995 (12%) der zu beaufsichtigenden, nicht weggesperrten Eingetragenen.[470] Bedenkt man, dass dieses System Ersttäter und geschickte Delinquenten nicht erfasst, ist das eine ziemlich hohe Zahl. Bereits die Reduktion der ver-

---

468 Vgl. GROEBNER, S. 66.

469 Vgl. Bericht GPDel, S. 7724 und ausführlich BELSER, S. 7 ff. N. 12 ff. mit weiteren Hinweisen. Das gilt auch hinsichtlich einer Verknüpfung mit anderen Technologien, bspw. mit automatisierten Fahndungsmethoden über biometrische Erkennungssysteme. Datenbanken, die aus Sicherheitsüberlegungen zu viele Falsch-Positive mitlisten, wiegen vielmehr in falscher Sicherheit. Prioritäten zu setzen, fördert im Gegenteil die Leistungsfähigkeit derartiger Systeme. Siehe dazu INTRONA/NISSENBAUM, S. 39.

470 OPPAGA 2008, S. 7. Vgl. zum Ganzen Bericht HRW, S. 9 und 45 f. In grossen Städten sind derart viele Personen registriert, dass es schon eine Herausforderung für einen Anwohner sein dürfte, alle Registrierten in einem grösseren Quartier identifizieren zu können. Einige bundesstaatliche Behörden in den USA scheinen diese Probleme erfasst zu haben und versuchen neustens nur noch einige wenige der Sexualstraftäter (die konkret gefährlichen) im öffentlichen Register zu publizieren. Sicherlich ein Schritt in die richtige Richtung. Siehe dazu Bericht HRW, S. 62 f.

schwundenen Eingetragenen auf diese Zahl erforderte einen grossen Aufwand: Der zuständigen Behörde mussten mehr Ressourcen zugeteilt werden, die diese unter anderem dafür nutzte, eine neue Abteilung zu gründen, welche ausschliesslich mit der Aufgabe betraut ist, die untergetauchten Personen aufzuspüren. Darüber hinaus erhielt die Behörde einen umfassenderen Zugriff auf Informationen aus anderen Sexualstraftäterregistern und aus Bundesstaaten- und Bundesdatenbanken. Zudem ermöglichte sie der Öffentlichkeit, Eingetragene, die sich der Kontrolle der Behörden entziehen, per Internet zu melden.[471] Ob sich dieser Aufwand tatsächlich lohnt, ist schwer abzuschätzen. Aus den erwähnten Zahlen lässt sich etwa nicht ablesen, ob sich unter den Eingetragenen, die sich der Aufsicht entziehen, besonders häufig aktuell Gefährliche befinden. Zumindest ist zu bezweifeln, dass sich diese höheren Kosten und grösseren Eingriffe rechtfertigen. Kompaktere Register würden das Problem wohl eher beheben, ohne die Sicherheitslage im Verhältnis zum jetzigen umfangreicheren Register negativ zu beeinflussen.[472]

Ein weiteres Beispiel, das potenziell gravierendere Folgen nach sich hätte ziehen können, wäre es nicht im letzten Moment verhindert worden, war der Versuch Umar Farouk Abdulmutallabs im Jahr 2009, ein Flugzeug auf dem Weg von Amsterdam nach Detroit zu sprengen. Zwar waren von mehreren Seiten Hinweise auf sein bevorstehendes Attentat eingegangen, unter anderem hatte die amerikanische Botschaft in Nigeria eine Terrorwarnung an die Nachrichtendienste gesandt, und Abdulmutallab war auf eine der amerikanischen Terroristenlisten gesetzt worden. Er ging jedoch in der riesigen Masse an dort verzeichneten, mutmasslichen Terrorverdächtigen, von denen grösstenteils keine akute Gefahr ausging, unter und schliesslich vergessen.[473]

---

471 OPPAGA 2008, S. 3.

472 Der Bericht OPPAGA 2012 verzeichnet vor allem einen markanten Anstieg der Anzahl registrierter Personen von 28% (18'607 auf 23'813) zwischen 2005 und 2012. Der Rückgang von einem Prozent weniger beaufsichtigten Flüchtigen innerhalb von vier Jahren (2008: 861 bei 6'995, 2012: 693 bei 6'111; siehe OPPAGA 2008, S. 7 und OPPAGA 2012, S. 10) ist minimal im Verhältnis zum dafür betriebenen Mehraufwand, siehe dazu OPPAGA 2012, S. 3 f.

473 Siehe CHESTERMAN, S. 227 f. Im Gegensatz zur amerikanischen Terrorliste, führte die UN-Terrorliste nie über 500 Einträge (siehe Bericht S/2012/968, N. 68). Neue Listungsanträge der Mitgliedstaaten gingen in den letzten Jahren nur sehr selten ein, weshalb seitens des Sicherheitsrats und der Monitoring Group im Gegenteil befürchtet wird, dass das Sanktionsregime bedeutungslos werde. Sie ermutigten die Mitgliedstaaten deshalb wiederholt, Lis-

4. Unaufmerksamkeit und der Nebel um den Einzugsbereich

Diese Beispiele leiten über zur Diskussion einer weiteren Schwachstelle von Verdachtsregistern: Wie der Bundesrat in seiner Antwort auf die Motionen Rickli richtig argumentiert, verleitet der Anspruch, gefährliche Personen möglichst lückenlos zu erfassen, dazu, gegenüber Nicht-Registrierten unaufmerksam zu sein.[474] Die Verdachtsregister lenken den Fokus der Prävention oder der Repression, also der Öffentlichkeit, der Polizei oder der Ermittler auf die *Eingetragenen*. Dadurch gelangen diese zur naheliegenden, vermeintlich logischen Überlegung: „Wer registriert ist, ist gefährlich und wer nicht registriert ist, ist nicht gefährlich!" Nicht-Registrierte können jedoch wesentlich gefährlicher als Registrierte sein. Zum einen haben nicht registrierte Tatwillige noch keine therapeutischen oder andere resozialisierende Massnahmen durchlaufen. Auch wurde ihnen keine Prognose gestellt.[475] Zum anderen dürfte gerade bei nicht-registrierten Wiederholungstätern zu vermuten sein, dass sie besonders gefährlich sind. Immerhin konnten sie bis anhin unentdeckt Straftaten begehen. Eingetragene Ersttäter hingegen weisen nicht die gleichen Rückfallraten wie eingetragene Wiederholungstäter auf. Das Konzept des Verdachtsregisters geht in diesen Punkten von falschen Annahmen aus.[476] Verdachtsregister vermögen gefasste Täter, gemeldete Störer und selektiv mutmasslich verdächtige oder gefährliche Personen aufzulisten. Sie lenken dadurch aber nicht selten von einer möglicherweise *ernst zu nehmenden* zugunsten einer *hypothetischen* Gefahr ab.[477]

Als Illusion stellt sich auch das präventive Konzept heraus, den Aufenthaltsort und Bewegungsradius der Registrierten bekannt zu geben. Es ist naiv, anzunehmen, ein tatwilliger Registrierter wäre, um ein Delikt zu begehen, an seinen eingetragenen Standort gebunden. Die Suchmatrix etwa der Internetregister in den USA umfasst lediglich einen Radius von einigen Kilometern, was unter dem Gesichtspunkt der oben besprochenen Übersichtlichkeit durchaus zweckmässig ist. Warum aber sollte der Kriminelle sich an irgendeinen Radius halten? Vielmehr

tungsvorschläge einzureichen (bspw. unlängst in der S/RES/2083 (2012), S. 2). Siehe dazu SCHULTE, S. 51 f. mit weiteren Hinweisen.

474 In der Stellungnahme des Bundesrats vom 7. Mai 2008 i. S. Natalie Simone Rickli auf den Punkt gebracht: „Solche Datenbanken vermitteln bloss eine Scheinsicherheit, weil sie nur die bereits verurteilten Täter erfassen." Ebenso Stellungnahme des Bundesrats vom 15. Mai 2013 i. S. Natalie Simone Rickli. Vgl. HEYMANN, S. 67.

475 Stellungnahme des Bundesrats vom 7. Mai 2008 i. S. Natalie Simone Rickli.

476 Vgl. dazu HARCOURT, S. 164.

477 Ähnlich fürs überschiessende Sammeln von Daten im Allgemeinen: VAN DER HILST, S. 21.

wird er seine Tat ausserhalb seiner „Verdachtszone“ begehen.[478] Darin ist also eine weitere Schwachstelle der Verdachtsregister auszumachen. Indem ein Eingetragener seine Delikte ausserhalb seines Einzugsbereichs verübt, lenkt er den Verdacht von sich selbst ab. Er wird es folglich tunlichst vermeiden, im eigenen Umfeld zu delinquieren. Vielmehr wird er Straftaten in anderen Gebieten begehen. Die Ironie ist, dass das Verdachtsregister in diesem Fall dem Tatwilligen sein Handwerk sogar erleichtert: Verlassen sich Prävention und Ermittlungen zu sehr auf das Register, fällt derjenige, welcher für das Begehen einer Tat seinen registrierten Einzugsbereich verlässt, aus dem Raster und bleibt möglicherweise gänzlich unbeachtet. Der Fokus der Ermittlungen, aber auch der Gefahrenabwehr, liegt auf den eingetragenen *Ansässigen* – eine willkommene Ablenkung für den „Tattouristen“, gibt es für ihn doch keine bessere Konstellation als diejenige, in der bestimmte, auf ihn hinweisende Indizien übersehen oder nicht berücksichtigt werden, weil andere Personen scheinbar verdächtiger sind. Durch das Verdachtsregister belastet werden somit in erster Linie die ansässigen Registrierten, auch wenn für begangene Delikte auswärtige verantwortlich sind. Der „Nebel“ ausserhalb des Verdachtsradius des Verdachtsregisters schützt diese. In diesem Sinne unterschätzen Befürworter von Verdachtsregistern die Eingetragenen und potenzielle Täter. Die Meldepflicht für längere Aufenthalte in einem anderen Gebiet als zum Beispiel dem Wohnort vermag daran kaum etwas zu ändern. Dieses bisher ungelöste Problem sorgt dafür, dass durch Verdachtsregister mindestens ebenso viel Verwirrung verursacht wird, wie durch sie Klarheit geschaffen werden soll.[479]

Die Nützlichkeit eines Verdachtsregisters hängt demnach wesentlich davon ab, wie kompakt gehalten und wie sorgfältig es geführt wird. Je umfangreicher ein Register ausgestaltet sein soll, desto ungleich grösser sind zudem die Ressourcen, die für ein einigermassen verlässliches Funktionieren und die Pflege des Registers aufzuwenden sind. Der Bundesrat hält dementsprechend den Aufwand „für den Aufbau, die Führung sowie die verlässliche Aktualisierung“ eines nichtöffentlichen Pädophilenregisters mit Informationen über Wohn-, Arbeitsort und

---

478 Dies scheint öfters der Fall zu sein, siehe dazu die Studien im Bericht HRW, S. 115 ff.

479 Siehe zum Ganzen: Bericht HRW, S. 115 ff. und die Antwort des Bundesrats vom 7. Mai. 2008 i. S. Natalie Simone Rickli, in der m. E. richtigerweise angemerkt wird, dass von einem in der Nachbarschaft wohnenden Eingetragenen keine grössere Gefahr ausgehe als von einem 30 Kilometer entfernt lebenden.

Aussehen der Person für unverhältnismässig. Das bestehende Strafregister erfülle die Aufgaben in Verbindung mit der Fahndungsdatenbank Viclas besser.[480]

B. Raumüberwachung

1. Überwachung des realen Raums

Der Ansatz der Kriminalitätsbekämpfung durch Videoüberwachung des öffentlichen Raums klingt zunächst vielversprechend. Jedoch kann die Videoüberwachung die vorgegebenen Ziele mit den heute gebräuchlichen technischen Mitteln nicht oder nur bedingt erreichen. In der Praxis waren die Aufnahmen bis anhin, aufgrund von Technologie- und Ressourcendefiziten, für die Präventions- und Repressionszwecke (z.B. für das Verhindern von Straftaten durch sofortiges Eingreifen oder zur Verwendung als Beweise in Strafverfahren) wenig verwertbar.[481]

Ein präventives Eingreifen, das heisst etwa jemanden „in flagranti" aufgrund einer Live-Überwachung eines Gebiets von der Begehung von Straftaten abzuhalten, scheitert zumeist an der begrenzten menschlichen Aufmerksamkeit und am unzulänglichen menschlichen Einschätzungsvermögen der Lage. Ein Mensch kann ab einer gewissen Anzahl von Bildschirmen die Ereignisse darauf nicht genügend aufmerksam verfolgen, um Gewähr zu bieten, dass er daraus die tatsächlich problematischen Ereignisse fehlerlos zu identifizieren vermag.[482] Insofern steigt die Chance, rechtzeitig zu intervenieren, je kleinräumiger überwacht wird und je weniger Videokameraübertragungen zu kontrollieren sind.[483] Dasselbe Bild zeichnet sich für das Erkennen, Aufdecken und Aufklären von Straftaten mithilfe von archivierten Videoüberwachungsaufnahmen: Die schiere Masse an gespeicherten Aufnahmen ist kaum zu bewältigen – je schwieriger, desto län-

---

480 Stellungnahmen des Bundesrats vom 7. Mai 2008 und 15. Mai 2013 i. S. Natalie Simone Rickli.

481 Siehe NORRIS/ARMSTRONG, S. 210 ff. Insbesondere der repressive Verwendungszweck verlangt eine gewisse Aufbewahrungsdauer der Aufzeichnungen (siehe etwa BGE 133 I 77 E. 5.2-5.2.2 S. 84 f.). Das führt zu schwer zu bewältigenden Datenmengen.

482 DITTON/SHORT, S. 165; NORRIS/ARMSTRONG, S. 211; NORRIS/MORAN/ARMSTRONG, S. 499; GRAS, S. 213 ff. mit Hinweisen. KAMMERER 2008, S. 143 f. ist zuzustimmen, dass die menschlichen Defizite der Bediener in der Praxis das wesentliche Problem darstellen und nicht eine tiefe Bildauflösung oder fehlende Zoomfähigkeit des Systems.

483 KAMMERER 2008, S. 148 f.

ger die Aufnahmen aufbewahrt bleiben sollen. Eine effiziente Sondierung der Daten ist derzeit wenig praktikabel.[484]

Eine (personelle) Entlastung der staatlichen Behörden, im Sinne eines „Outsourcing" der Aufgaben, kann durch die Videoüberwachung wohl dann bewirkt werden, wenn deren Betrieb an private Sicherheitsfirmen ausgelagert wird.[485] Eines der Probleme, welche die Auslagerung von Aufgaben einer Behörde auf verschiedene Sicherheitsanbieter mit sich bringt, ist sicherlich die erstaunlich hohe Inkompatibilität der je nach Unternehmen sehr unterschiedlichen Aufnahme- und Speichersysteme. Dadurch steigt der Auswertungsaufwand nach Übergabe an die Strafverfolgungsbehörde zusätzlich markant an, da die Daten zuerst harmonisiert und für das von der Behörde verwendete System aufbereitet werden müssen.[486]

Der Einsatz zur Prävention durch Abschreckung kann unter Umständen punktuell erfolgversprechend sein.[487] So können sich *bestimmte Delikte* in einem überwachten Gebiet wohl tatsächlich für eine gewisse Zeit – bis deren Unzuverlässigkeiten im Erfüllen der anderen beiden Zwecke erkannt werden – in ein anderes (unüberwachtes) Gebiet verlagern.[488]

Können die dargestellten praktischen Hürden überwunden werden, kann die Videoüberwachung womöglich erstens zur Aufklärungsrate, Sachverhaltsfeststellung und als Beweismittel im Strafverfahren Dienste leisten.[489] Zu berück-

---

484 NORRIS/ARMSTRONG, S. 210 ff.; GILL/SPRIGGS, S. 115 f.; SCHRÖDER, S. 50. Teilweise a. A. sind DITTON/SHORT, S. 167, welche die Archivierung der Aufnahmen für verhältnismässig kostengünstig, hilfreich und praktikabel halten. Ihr Urteil bezieht sich jedoch auf die Studie in Glasgow, in welcher lediglich noch einigermassen überschaubare 32 Kameras zum Einsatz kamen. Auch TÖPFER tendiert gestützt auf Aussagen aus der Praxis zu einer eher positiven Beurteilung der Videoüberwachung als „Personalsubstitut".

485 Vgl. TÖPFER, S. 277 f.

486 Siehe dazu KAMMERER 2008, S. 170 ff.

487 Es wird versucht, diesen Zweck durch plakatives Positionieren der Kameras und diesbezügliche Warnschilder umzusetzen. Kritisch anzumerken bleibt, dass die „abstrakte Möglichkeit der Abschreckung" von der Begehung gewisser Delikte durch die Videoüberwachung, so etwa BIER/SPIECKER GEN. DÖHMANN, S. 616, ohnehin schwerlich zu widerlegen ist.

488 Siehe dazu MÜLLER L. 2011, S. 245 f. mit weiteren Hinweisen. Skeptisch BORNEWASSER, S. 150 und 152.

489 Dieser Nutzen ist umstritten und wenig untersucht. Zumindest hinsichtlich medienwirksamer Kriminalitätsereignisse wird öfters von Erfolgen berichtet, siehe LINGG, S. 27 und 48 f. mit Beispielen. Freilich ist aus der Perspektive des Aussenstehenden schwer überprüfbar, inwieweit die Videoüberwachungsmassnahmen tatsächlich zum Erfolg beigetragen haben. Zum Nutzen für die Strafverfolgung (Sachverhaltsfeststellung, Beweismittelgewinnung,

sichtigen sind dahingehend aber mögliche „Lern- und Anpassungsprozesse von kriminellen Verhaltensmustern“.[490] Zweitens kann die Einsatzleitung geplanter, ereignisbezogener Interventionen von Live-Bildern aus dem Zielareal profitieren. Ein Live-Stream liefert in diesem Fall einen nützlichen Überblick über die Situation, den sich die Einsatzleitung auf andere Weise kaum verschaffen könnte (zum Beispiel eine Komplettansicht eines Platzes aus der Vogelperspektive). Die zur Verfügung stehenden Polizeikräfte können dadurch effizienter und flexibler geführt werden, was auch fehlendes Personal insofern ausgleichen kann.[491] Die reale Raumüberwachung kann folglich dort erfolgreich sein, wo die polizeiliche Behörde bereits Personen vor Ort hat und die potenziellen Bedrohungen schon im Vorfeld bekannt sind oder auf sehr bestimmte beziehungsweise bestimmbare Möglichkeiten eingeschränkt werden können.

Aus polizeikritischer Sicht motiviert die Videodokumentation eines Einsatzes zudem die Polizeikräfte vor Ort, nicht ungerechtfertigt oder unverhältnismässig einzugreifen. Aus behördlicher Sicht ist vorteilhaft, dass die Aufnahmen allenfalls als Beweis dafür vorgebracht werden können, dass verhältnismässig interveniert wurde. Der Nebeneffekt kann sich indes auch nachteilig auswirken. Dokumentieren heisst in diesem Zusammenhang überprüfbar, aber auch anschaulich kritisierbar machen. Insbesondere kann die Anwesenheit einer Videokamera wohl allgemein den Tatendrang der Polizei hemmen, da jedes noch so geringfügige Fehlverhalten der Beamten vor Ort bildlich festgehalten werden und einer späteren Beurteilung der Aufsichtsinstanzen, der Politik, der Medien und der Öffentlichkeit ausgesetzt sein könnte. Zögerliches oder bewusst zurückhaltendes Agieren von Polizisten kann sich jedoch in gewissen Situationen durchaus sehr nachteilig auswirken.[492] Der den Überwachungmassnahmen inhärente Symbolismus zeigt sich, wenn ein von GOOLD befragter Polizist feststellt, das Verhalten der Polizeipatrouillen habe „to *look* right“.[493]

Identifizierung von Tätern, Opfern und Zeugen), siehe etwa BGE 133 I 77 E. 5.2 S. 84; GRAS, S. 129 f.; MÜLLER L. 2011, S. 240 f. mit weiteren Hinweisen.

490 STUTZER/ZEHNDER, S. 127; ZEHNDER M., S. 28.

491 TÖPFER, S. 280, ist diesbzgl. m. E. zuzustimmen.

492 KAMMERER 2008, S. 152. Siehe dazu auch GOOLD. Man denke vielleicht an Einsätze, bei denen die Schwellen zwischen zurückhaltendem, verhältnismässigem und zu hartem Eingreifen fliessend sind, bspw. einen Raufhandel, den die Polizei zu wenig überzeugt auflöst, weil eine Videokamera die Szene aufnimmt.

493 GOOLD, S. 194.

Eine damit verbundene, weitere Komplikation beruht darauf, dass die Überwachungskamera jeweils nicht das gesamte Geschehen, die Umstände der Situation, die Geschichte hinter einer Handlung oder die Ereignisse ausserhalb ihres (engen) Blickfelds erfassen kann. Der Betrachter sieht diejenige Szene, auf welche die Kamera im Moment der Aufnahme fokussiert. Aus diesen Aufnahmen kann kein exaktes Abbild der vergangenen Wirklichkeit gewonnen werden, sondern lediglich ein retrospektiv rekonstruierter, unvollständiger Ausschnitt aus einer Chronik, die gewollt oder ungewollt auf vielerlei Arten manipuliert sein kann und dadurch eventuell falsche Geschehensabläufe suggeriert.[494]

2. Überwachung des virtuellen Raums

Virtuelle Raumüberwachungsmassnahmen laufen häufig im Verborgenen ab, weswegen deren Resultate meist nicht an die Öffentlichkeit gelangen.[495] Die Probleme sind jedoch in der Theorie bekannt. So wird die effiziente Überwachung des virtuellen Raums dadurch gestört, dass der virtuelle Raum fast unendlich gross, flüchtig und dezentral aufgebaut ist. Das Internet basiert auf einer Vernetzung von vielen, an verschiedenen Orten liegenden Zugangs- und Speicherpunkten. Inhalte, die am Ort ihrer Einspeisung straffrei sind, können anderswo strafbar sein. Zudem ist die Kooperation zwischen den Behörden verschiedener Staaten nicht immer unproblematisch.[496] In verschiedenen Rechtsordnungen kommen den staatlichen Behörden sehr unterschiedlich weit gehende Kompetenzen zu, im Internet Überwachungs- und andere Gegenmassnahmen zu ergreifen. In Verbindung mit dem je nach Staat abweichenden Verständnis darüber, was der Auftrag, kriminelles Handeln zu verhindern, alles beinhaltet, der regional unterschiedlichen Einschätzung von Grundrechten und der fast universellen Verfügbarkeit von Internetinhalten führen diese Gegebenheiten im Bereich des Internets zu praktischen Schwierigkeiten und rechtlich teils wenig überzeugenden Resultaten.[497]

---

494 Um auf das Zitat des Polizisten bei GOOLD zurückzukommen: Das Verhalten *unter* dem Auge der Kamera muss gut aussehen, nicht hingegen, was *ausserhalb* des Kamerawinkels geschieht.

495 Vgl. NOWAK, S. 6. VAN DER HILST, S. 12 f. führt einige Bsp. aus europäischen Staaten auf, die stark den Eindruck vermitteln, die *zielgerichtete* Überwachung der Kommunikation misslinge öfters oder sei grösstenteils nicht signifikant nützlich für Ermittlungen.

496 Zum Ganzen PERREY, S. 185 f.; NOWAK, S. 18; ROTERT, S. 437; VALERIUS, S. 23 f. und 27.

497 Siehe dazu OBERHOLZER 2004, S. 52 ff. mit Beispielen aus der Rechtsprechung; LOBSIGER 2004, S. 66; Schwarzenegger im Interview bei WEMANS, S. 28 f.; HILGENDORF, S. 829.

Technologien zur Überwachung des virtuellen Raums eignen sich in erster Linie für die repressive Ermittlung – insbesondere in Delikten, die ausserhalb des virtuellen Raums begangen werden und die mehr zufällig und nebensächlich einen Bezug zum virtuellen Raum aufweisen. Beispiele sind Drogendeals, die über Mobiltelefone vereinbart werden oder Wirtschaftsdelikte, bei denen sich kompromittierende Daten auch auf einem Computer befinden. Reaktive virtuelle Massnahmen, die erst nach der Tat oder aufgrund eines hinreichenden Tatverdachts eingeleitet werden, sind meist sehr zielgerichtet und konkret. Derart eingesetzte Überwachungstechnologien stellen für die Ermittlungsbehörden ein sicherlich sehr hilfreiches, ergänzendes Instrument neben vielen anderen Ermittlungsinstrumenten dar.

Sollen virtuelle Überwachungstechnologien hingegen zur präventiven Gefahrenabwehr gebraucht werden, versagen sie häufig. Das Spektrum der Deliktskategorien, in denen sie zweckmässig angewendet werden können, ist beschränkt. Einen grossen Nutzen verspricht man sich von ihnen beispielsweise bei der Überwachung von extremistischen Internetseiten oder im Einsatz gegen Pädophile, die sich die virtuellen Kanäle zunutze machen (einerseits zur Begehung von Delikten, andererseits etwa zur Kontaktaufnahme mit Opfern[498]) – also bei Delikten, die durch Personen begangen werden, die entweder ihre Gefährlichkeit bewusst propagieren, sich tatsächlich höchst verdächtig verhalten (vielleicht im Trugschluss, dass alles in der virtuellen Welt anonym geschieht?), bei Handlungen, die dazu prädestiniert sind, von einfachsten Programmen bemerkt zu werden oder bei Delikten im virtuellen Raum, die unbedarft begangen werden.[499] Automatisierte Techniken können dabei immerhin erste Hinweise liefern. Diesen muss danach in meist sehr aufwendiger Arbeit nachgegangen werden.[500]

Der Taktik des Blockierens von Inhalten zur Gefahrenabwehr ist immer irgendwie zu umgehen, wenn auch mit Aufwand und einer gewissen Bereitschaft, Unrechtes zu tun. Das macht die virtuelle Zensur zu einem Mittel gegen die überwiegende Anzahl Personen, die sich nicht kriminell verhalten, weniger zu einer Strategie der Verhütung von tatsächlichen Gefahren respektive der Enttarnung oder Überführung gefährlicher Personen.[501]

---

498 Vgl. BGE 134 IV 266.

499 Diese beiden letzten Voraussetzungen treffen zum Beispiel auch oft auf das unerlaubte Herunterladen urheberrechtlich geschützter Erzeugnisse zu.

500 Vgl. LSE BRIEFING, S. 24.

501 Siehe dazu unten Vierter Teil, Kapitel V.

Virtuelle Sondierungsprogramme stossen heutzutage rasch an ihre Grenzen, sowohl in ihrer Kapazität als auch in ihrer Funktionalität. Die aufzuwendenden Ressourcen zur anlasslosen oder präventiven Überwachung des virtuellen Raums sind immens.[502] Als Antwort wird etwa im Rahmen des Projekts INDECT versucht, neue Wege der effizienten Datenauswertung und der ökonomischen Datenlagerung zu erschliessen, indem es der Vernetzbarkeit mit anderen Systemen eine hohe Priorität zuerkennt. Neuere Systeme sollen den Datenverkehr im Internet zudem anlasslos und möglichst ganzheitlich, eben nicht nur auf eine Zielquelle ausgerichtet, durchforsten und automatisch auswerten. Das automatisierte System soll dem Bediener melden, wenn eine Situation oder eine Person die vorgebenen Kriterien erfüllt. Zudem soll durch das System Verdächtiges *ermittelt* werden: Es wäre nicht an einem Ausgangspunkt (verdächtige Situation oder Person) anzusetzen, sondern fände diesen selbst. Somit wären die Fähigkeiten dieser Systeme vor allem zur Unterstützung der *präventiven* Gefahrenabwehr oder zur Verdachtsforschung wesentlich höher als diejenigen von bestehenden Systemen. Vorderhand scheint es daher aussichtsreich zu sein, neuere DPI-Technologien mit automatisierten Analyseprogrammen zu kombinieren. Diesbezüglichen Realisierungsversprechen ist aber skeptisch gegenüber zu stehen.[503]

Die Vorteile automatisierter Systeme sind im virtuellen grösser als im realen Raum, da sich der Ermittler oder Präventionsbeauftragte im virtuellen Raum mit weitaus umfangreicheren und zahlreicheren Datenquellen konfrontiert sieht.[504] Zudem ändern Webseiten ihre Adressen, Foren lösen sich auf und formieren sich andernorts neu, Daten werden gelöscht und verschoben etc. Ein menschlicher Fahnder kann bestenfalls Stichproben durchführen und entdeckt deswegen wichtige Hinweise oder Relationen nicht selten zu spät (von Zufallstreffern einmal abgesehen).[505] Die manuelle Suche von Hinweisen im virtuellen Raum ist mühselig, zeitaufwendig und anfällig für das Übersehen von Details und Beziehun-

---

502 Siehe etwa ROTERT, S. 437.

503 Die Autoren des LSE-Briefing, S. 25 kommen daher zum Schluss: „[DPI] will be more of a wish list of performance and operational requirements than a realistic scheme that is tightly defined specified."

504 Vgl. bspw. die von BECKER K. B., S. 166 beschriebene Situation in China. Die Datenfülle ist überwältigend: Immer mehr Personen nutzen das Internet auf immer mehr Arten, siehe etwa LATZER ET AL., S. 7 ff.

505 Das kann für die Behörde auch von Vorteil sein, siehe unten Vierter Teil, Kapitel V.B.

gen.[506] Das diesbezügliche Konzept neuer Projekte hingegen soll durch ein sehr zeiteffizientes Abarbeiten des jeweiligen Auftrags und durch Vernetzungen innerhalb der Teilsysteme überzeugen. Erreicht werden soll dieser Anspruch durch eine jeweils angepasste Modifizierung der Algorithmen des Data Mining und eine allgemein vielseitige Struktur des Systems. Die Bandbreite der zum Beispiel von INDECT unterstützten Techniken im Durchkämmen und Überwachen des virtuellen Raums soll vom Aufspüren „unüblicher" Informationen über das Ermitteln und Kartografieren von in irgendeiner Weise suspekten Webseiten bis zum Erkennen bestimmter (verdächtiger) Verhaltensmuster in der digitalen Kommunikation reichen. All diese Funktionalitäten sollen dem Nutzer eine Entscheidungshilfe bereitstellen. Dabei soll das System weitgehend kompatibel zu anderen Systemen sein.[507]

Ein immer aktueller werdendes Thema ist sicherlich auch der Zugriff auf soziale Netzwerke und Konsumentendaten. Das amerikanische IAO sah vor, dass jegliche Datenquelle für die Kriminalitätsbekämpfung nutzbar sein sollte. Dazu hätten neben den erwähnten virtuellen Plattformen und Archiven auch Konsumentendaten gehört. Das IAO war, anders als INDECT sowie andere Systeme und Programme, direkt mit Gesetzesänderungen verknüpft, die zu derartigen Zugriffen ermächtigt hätten. Es scheiterte aber letzlich. INDECT und ähnliche Systeme müssten sich den bestehenden Rechtsgrundlagen unterordnen. Theoretisch wären sie aber durchaus dazu fähig, Datenquellen ähnlich umfassend zu erschliessen. Momentan können sie wohl mehr, als sie dürfen.[508] Die Systeme sind fähig, behördenfremde Datensammlungen zu durchsuchen, unabhängig davon, ob dies erlaubt ist oder nicht. Forscher bemühen sich um die Verbesserung der Mittel zur digitalen Überwachung und Kontrolle und erschliessen somit Schritt für Schritt weitere Territorien der virtuellen Welt. Neue Data-Mining-Technologien können theoretisch ohne Weiteres sogenannte Community-Plattformen (das heisst Internet-Foren, soziale Netzwerke wie Facebook, Blogs etc.) automatisch auf verdächtige Inhalte absuchen. Bei Treffern können zudem direkt nützliche Informationen an die zuständigen Behörden weitergeleitet werden. Auch werden Fort-

---

506 Weil mehrere Personen oder Dienststellen an verschiedenen Bereichen der Ermittlungen beteiligt sind, ist z. B. auch eine schlechte Kommunikation zwischen diesen für Fehler verantwortlich.

507 Zum Ganzen: Bericht INDECT D9.4, S. 17 f., 19 f. und 22.

508 Gl. M. wie Thomas Hansjakob zur Govware im Interview bei STÖCKLI, S. 16. Die umfangreichen Datensammlungen des amerikanischen PRISM und des englischen TEMPORA waren trotzdem möglich.

schritte in der Durchforstung der Kommunikation (E-Mail etc.) gemacht.[509] Auch der Abruf von Nutzerdaten bei den zahlreichen Internetdiensten ist für Ermittlungsbehörden sehr attraktiv.[510] Viele Internetdienste archivieren beinahe jede Information, die sie im Stande sind zu sammeln. Anbieter, die mehrere Dienste betreiben (beispielsweise Google), verknüpfen zudem personenbezogene Daten und Informationen aus verschiedenen Diensten.[511] In einer Gesellschaft, die nicht nur einen nicht unwesentlichen Teil ihrer Korrespondenz und Verrichtungen über den virtuellen Raum abwickelt, sondern auch viel Zeit darin verbringt, kann sich aus der Kombination dieser Nutzerdaten ein sehr umfassendes Bild einer Person ergeben.[512]

C. Versprechen der nächsten Technologiegeneration

Einige der zunächst positiv scheinenden Auswirkungen der postmodernen Kriminalitätsbekämpfungstechnologien, auch der nächsten Technikgeneration, stellen nur oberflächlich Erfolge dar. Die Hürden der Wirksamkeit und Effizienz

---

509 Siehe CHAU/XU, S. 479 und 480 (Grafik einer möglichen Funktionsweise). Theoretisch könnten z. B. die Profilbilder oder Fotos auf Facebook automatisiert nach Merkmalen eines biometrischen Musters durchsucht werden. Es könnte in dieser Weise auch nach Personen, die bspw. durch eine Videoüberwachungsanlage aufgezeichnet wurden, gefahndet werden.

510 Siehe etwa AL-FAROUQ ABO YOUSSEF, S. 92 ff.; MONROY/BUSCH, S. 5 f.; SCHULZKI-HADDOUTI, S. 34; HENRICHS/WILHELM 2010a, S. 36: „Die Kombination der in den polizeilichen DV-Systemen gespeicherten Datenbestände mit den Daten in den SNS [Social Network Services] ergibt einen taktischen und operativen Mehrwert von erheblichem Ausmass." Für einige Praxisbsp., siehe HENRICHS/WILHELM 2010b, S. 218 f.; SCHULZKI-HADDOUTI, S. 35 f.; MONROY/BUSCH, S. 6 (u. a. mit Hinweis auf das EU-Projekt VIRTUOSO: <http://www.virtuoso.eu/>). In den USA bestehen seit dem Patriot Act auch die rechtlichen Grundlagen, auf diese Informationen zuzugreifen. In den Nutzungsbestimmungen vieler grosser amerikanischer Internetdienstleister finden sich Klauseln, die amerikanischen Behörden die Extraktion von geschützten Nutzerdaten (nicht nur amerikanischer Nutzer) erlauben. Diese Ermächtigung wird scheinbar rege benutzt, siehe etwa die aktuelle Diskussion um die Überwachungprogramme der NSA. Vgl. etwa RÜESCH in NZZ Online vom 7. Juni 2013; eine geleakte Version der „Facebook Law Enforcement Guidelines" aus dem Jahr 2010: <https://www.eff.org/files/filenode/social_network/Facebook2010_SN_LEG-DOJ.PDF>.

511 Siehe dazu bspw. den Internettelefonie-Dienst Skype <http://www.skype.com/de/legal/privacy/> (insb. Punkt 1) oder den Internetdienstanbieter Google <http://www.google.ch/intl/de/policies/privacy/> (ausdrücklich: „Unter Umständen verknüpfen wir personenbezogene Daten aus einem Dienst mit Informationen und personenbezogenen Daten aus anderen Google-Diensten.").

512 Vgl. unten Vierter Teil, Kapitel IV.D.

sind hoch, sobald ein gewisser Anspruch besteht, die Ziele der jeweiligen Massnahmen genauer, überlegter und der Erscheinung Kriminalität angemessen komplex zu definieren.[513] Die Beurteilungsebene, die zählt, ist eine tiefere, als die häufig vermittelte. In der Beurteilung der Effizienz und der Nützlichkeit postmoderner Technologien sind nicht lediglich vordergründige Ziele einzubeziehen. Am Ende bestimmt nicht, wie häufig Ein- beziehungsweise Ausreisesperren verhängt wurden oder wie hoch eine eingefrorene Geldsumme ist, nicht die Anzahl an registrierten oder überwachten Personen oder die Menge an in Ermittlungsverfahren verwendeten Verkehrsdaten die Nützlichkeit und Wirksamkeit dieser Instrumente, sondern, ob und welchen kriminellen Handlungen damit vorgebeugt werden kann, welche verhindert oder leichter verfolgt werden können. Selbst wenn ein kombiniertes, allgegenwärtiges Überwachungssystem in der Lage wäre, von jeder Person in einem Gebiet ein umfassendes Bewegungsprofil zu erstellen, folgt daraus eben nicht automatisch, dass dadurch kriminelle Aktivitäten weniger oft vorkämen. Eventuell verhindert der Einsatz einer Technologie eine bestimmte Form von (kriminellem) Verhalten, fördert dafür indes andere (vielleicht schwerwiegendere) Aktivitäten. Eventuell vereinnahmt und blockiert sie auch Ressourcen auf einen bestimmten Teilbereich oder reserviert sie für Ermittlungs-/Präventionsmassnahmen, deren Effektivität zweifelhaft oder unüberprüft ist, wodurch die Aufwendungen in anderen Bereichen oder für dringlichere Angelegenheiten fehlen. Ein konkretes Beispiel: Der Bericht des BKA zu Mindestspeicherfristen betont die Relevanz der Vorratsdatenspeicherung für die Identifizierung von Bestands-/Kundendaten, die hinter einer IP-Adresse stehen im Bereich der Verhinderung und Ahndung von Kinderpornografie. Der Wegfall dieses Ermittlungsansatzes ist indes nicht zwingend als Lücke zu interpretieren, sondern kann gleichsam Chance sein, dass die darauf verwendeten Ressourcen für andere, vielleicht nachhaltigere Ermittlungsansätze und Strategien im Bereich der Kinderpornografie frei werden. Vielleicht für solche, die dieses Problem näher an der Wurzel packen können.[514] Eine Fülle an Ermittlungsansätzen zur Ver-

---

513 Bspw. anhand von Leitzielen wie: Gewaltdelikte X im Park Y langfristig und mit höchstens leichten Verlagerungseffekten in den Raum Z um eine bestimmte Mindestanzahl verringern.

514 Siehe dazu ALBRECHT H. J. ET AL., S. 222: „Insbesondere gibt es bislang keinen Hinweis dafür, dass durch eine umfängliche Verfolgung aller Spuren, die auf das Herunterladen von Kinderpornografie hindeuten, sexueller Missbrauch über den Zufall hinaus verhindert werden kann." Weiter ist anzuzweifeln, dass aus den Spezialfallstaaten mit weitläufigen Zensurapparaten nützliche Erkenntnisse für die Internet-Filterung als Kriminalitätsbekämpfungsinstrument abzuleiten sind (zum Beispiel für den Bereich der verbotenen Gewaltdarstellung, der rechtsextremen Inhalte oder der Verbreitung von harter Pornografie). Eine

fügung zu haben, muss nicht immer vorteilhaft sein, sondern kann auch zu schlecht zugeteilten Ressourcen führen.

Zum Beispiel bedingt eine feststellbare Verminderung der Kriminalitätsrate durch *aktive* Prävention (schnelle Intervention) mittels Videoüberwachung, dass die staatlichen oder privaten Überwachungsunternehmen das Personal äusserst sorgfältig und gezielt auswählen oder dann besonders gut ausbilden sowie im Verhältnis zu den zu überwachenden Monitoren ausreichend viele Leute einsetzen. Idealerweise würde vor jedem Bildschirm ein auf das Erkennen von kriminellem Verhalten spezialisierter Psychologe sitzen, der in kurzen Abständen abgelöst werden müsste. Diese Forderung ist in der Praxis freilich nicht realisierbar. Personal, welches den an sich hohen Anforderungen gerecht wird, beziehungsweise dessen dahingehende Ausbildung und Schulung, ist teuer. Demnach gestaltet sich die potenziell wirklich nützliche, weil funktionierende, *manuelle* Live-Videoüberwachung für ein einigermassen kostenorientiertes Unternehmen wenig interessant.[515]

Dasselbe gilt analog für den virtuellen Raum. Insgesamt kann aus den vorangegangenen Ausführungen gefolgert werden, dass präventive Überwachungsmassnahmen im virtuellen Raum die eigentliche Zielgruppe oft ebenso verfehlen wie diejenigen im realen Raum. Zumindest scheint das Potenzial von Überwachungsmassnahmen im virtuellen Raum längst nicht vollständig ausgeschöpft zu werden oder erforscht zu sein. Insbesondere im Bereich der Massendatenverarbeitung und der Vernetzung von Datenbanken sind einige – problematische – Varianten denkbar, welche den staatlichen Behörden möglicherweise entscheidende Vorteile im virtuellen Raum verschaffen könnten. Automatisierte Systeme, welche diesen Anforderungen gerecht werden, liegen in naher Zukunft und aus technischer Sicht durchaus im Bereich des Möglichen. Analog zu den Raumüberwachungssystemen und bestenfalls mit diesen kombiniert, wäre zum Beispiel auch ein automatisiertes Verdachtsregister mit Live-Überwachung wohl grundsätzlich realisierbar. Es ist demnach angezeigt, sich bereits heute darüber Gedanken zu machen, ob, inwieweit und in welchen Bereichen wir funktionierende automatisierte Systeme einsetzen würden, stünden diese bereit.[516]

Lehre daraus könnte immerhin sein, dass unerwünschte Inhalte jeglicher Art mit dieser Vorgehensweise nie ganz zu verbannen sind und der Zugang dazu nie komplett zu verwehren ist, fast unabhängig davon, wie allgegenwärtig und mächtig der Zensurapparat ist.

515 Für ein Beispiel der tiefen Löhne und hohen Arbeitszeit: NORRIS/ARMSTRONG, S. 103 f.

516 Vgl. etwa INTRONA/WOOD, S. 195.

Die heute und in naher Zukunft verfügbaren Informationstechnologien ergänzen das Instrumentarium der strafverfolgenden und gefahrenabwehrenden Behörden zweifellos. Einige dieser Technologien leisten ihren Dienst als hilfreiche Werkzeuge des Benutzers, sie können indes im Gebiet des Vorgehens gegen Kriminalität die Erkenntnis- und Einschätzungsfähigkeiten weder des menschlichen Theoretikers noch des menschlichen Praktikers ersetzen. HELMUT SPINNER zeigt die Vorzüge und Grenzen der postmodernen Techniken treffend auf: Sie steigern die Verarbeitungskapazität und -geschwindigkeit stark. Demgegenüber tragen sie wenig zur Wissenserzeugung in der Kriminalitätsursachenforschung und zur Prognose von kriminellen Geschehnissen bei und besitzen kaum oder keine Urteilskraft für kognitive und moralische Bewertungen.[517]

Zumindest in der Theorie sollen mittels automatisierter Systeme, basierend auf angeblich wissenschaftlichen Kriterien, problematisches Verhalten oder sich anbahnende Bedrohungen augenblicklich erkannt und ausgewertet oder sogar vorausgeahnt werden. Wie ist es aber möglich, dass durch Kriterien beziehungsweise Prädiktoren eine Bedrohung oder Ähnliches derart genau vorausgeahnt werden kann, dass diese Vorahnung ein staatliches (präventives) Eingreifen rechtfertigt? Wohl gar nicht. Viele Protagonisten sind hinsichtlich der Realisierung von Versprechen seitens der Forschung im Bereich der „algorithmic knowledge discovery" wahrscheinlich zu zuversichtlich. Das Potenzial, objektivierbare Kriterien zu finden sowie in Computersprache zu übersetzen, welche die Wirklichkeit (Personen, Taten, Vorfälle, Bedrohungen etc.) adäquat erfassen, und damit die Fähigkeit automatisierter Sondierungen sowie Analysen, wird teils zu optimistisch eingeschätzt.[518] Insbesondere in Bezug auf die sicherheitspolizeiliche Rasterfahndung beziehungsweise Massendatenverarbeitung sind passende Kriterien – also solche, die bestenfalls alleine die gesuchte Person aus einer grossen Personengruppe erfolgreich zu identifizieren vermögen – wohl schwer in einer objektivierten, computertauglichen Weise herauszuarbeiten. Die beiden Voraussetzungen dafür widersprechen sich in grundsätzlicher Weise: Die Kriterien müssten einerseits allgemein genug sein, um alle Verdächtigen zu erfassen, andererseits derart spezifische Eigenschaften betreffen, dass die Verdächtigen nach einer Rangliste ihrer Verdächtigkeit präsentiert werden könnten. Ergebnis-

---

517 SPINNER, S. 264.

518 SKILLICORN 2008b, S. 68 zum Anspruch, die künftige Wirklichkeit (Verhaltensweisen, Bedrohungen) über Algorithmen verlässlich vorauszuahnen: „This scenario is pure fiction." Auch mit SIMON, S. 273 ist diesbezüglichem Optimismus skeptisch gegenüberzustehen.

se, welche beide Bedingungen erfüllen, liessen, beginnend bei dem hoffentlich sehr überschaubaren innersten Kreis der Verdächtigenrangliste, eine sinnvolle Folgeermittlung zu. Jedes andere Ergebnis einer präventiv-polizeilichen Rasterfahndung oder Massendatenverarbeitung bedeutet in erster Linie eine Verschwendung von wertvollen Ressourcen und einen Verlust an Vertrauen in den Staat durch die Bevölkerung, sobald – und insofern (ein anderer kritischer Punkt) – die dahingehend angestrengten, und teilweise übereifrigen, Fahndungsversuche der Behörden der Öffentlichkeit bekannt werden. Einsätze ohne sichtbaren Erfolg, die aber in Grundrechte eingreifen, sollten Unmut hervorrufen.[519]

Eine anderes Problem künftiger Errungenschaften durch automatisierte Systeme zeigt sich zugleich im theoretischen Vorzug kombinierter Lösungen: Kombinierte Systeme und Portale, welche die Bewegungen von Registrierten live nachvollziehen lassen, könnten zum Beispiel den ermittlungshemmenden Schatten ausserhalb registrierter Verdachtsradien lichten. Der angesprochene Schwachpunkt des „Verbrechenstourismus", das heisst des Delinquierens eingetragener Personen in fremden Nachbarschaften, könnte somit dadurch behoben werden, dass alle Videokameraaufnahmen beziehungsweise die Bewegungsprofile aller für eine ähnliche Straftat Registrierten effizient darauf durchsucht werden könnten, ob im Tatzeitpunkt einer von ihnen am Tatort oder in dessen Umgebung anwesend war. Der detektivische Aufwand des besorgten Bürgers zum umfassenden Selbstschutz würde sich indes mit dieser Weiterentwicklung kaum vermindern. Zwar wäre der Zugang zu Live-Überwachungsaufnahmen von Registrierten durchaus eine bequeme Methode, in aller Regel müsste der misstrauisch kontrollierende Bürger aber, analog zu professionellen Sicherheitsdiensten, sehr viel Zeit und Geduld investieren, nur um die Bewegungen *eines* Registrierten nachzuverfolgen. Dieses Beispiel veranschaulicht, dass funktionierende postmoderne Technologien immer auch zusätzlichen Aufwand beim Bürger und bei staatlichen Behörden verursachen, wenn die automatisierten Systeme zum einen Bedrohungen nicht zuverlässig, flächendeckend und lückenlos erfassen und zum anderen Prozesse nicht autonom und ohne Hilfe der Bürger (Aufruf zu Aufmerksamkeit, zum Melden von verdächtigen Personen oder Situationen etc.) oder staatlicher Behörden (Auswerten von gesammelten Datenhaufen, Befassen mit aufgedeckten Dunkelfeldern, Suche nach Eingetragenen, die sich der Kontrolle zu entziehen versuchen etc.) abgearbeitet werden können. Ohne die relativ um-

[519] Siehe BRAUN, S. 686 bzgl. des Skandals um den „Staatstrojaner"-Einsatz in Deutschland.

fassende Vernetzung und Koordination sind Einzelteile eines automatisierten Systems zudem weit weniger nutzbringend.

Zusammengefasst kann gefolgert werden, dass sich ein kombiniertes Portal vor allem bei Grosseinsätzen und in Ballungszentren von Grossstädten auszahlen kann, soweit eine Koordinationsstelle mit genügend Personalressourcen zur Bedienung der Anlage und zur Intervention vor Ort zur Verfügung steht. Ob die fortlaufende Automatisierung die Kosten des Einsatzes dieser Überwachungssysteme, Datenbanken und virtuellen Such- und Analyseprogramme senkt, wird sich zeigen. Wie aber eingangs erwähnt, fordern komplexere Systeme modernere Hardware und technisch besser ausgebildetes Personal. Sollten die postmodernen Technologien zudem tatsächlich zweckgemäss wirken, führten sie zu einer grossen Mehrzahl an entdeckten Delikten oder gefährlichen Subjekten und Bedrohungen. Nimmt man zudem an, das ohne technisierte Methoden nicht erfasste Dunkelfeld habe eine gewisse Ausdehnung, würden demnach tatsächlich effizientere und effektivere automatisierte Abläufe den Behörden zusätzliche Arbeitslast aufladen, was die vorübergehend gewonnenen, oft vorgebrachten Entlastungs- und Kompensationseffekte für die Behörden mindestens aufwiegen könnte.[520] Ob in diesem Problempunkt künftig ein Gleichgewicht zwischen der Effizienz der automatisierten Systeme und den begrenzt verfügbaren (menschlichen und finanziellen) Ressourcen gefunden werden kann, also eine „echte" Effizienz, lässt sich heute schwerlich beurteilen. Die jeweils neuen Varianten müssen ferner, was die Kosten betrifft, nicht nur an ihren Vorgängermodellen, sondern auch an anderen Alternativen gemessen werden und im direkten Vergleich mit diesen muss ihr Dasein gerechtfertigt werden können.[521]

---

520 Vgl. NOGALA 1998, S. 261, der in der Ressourcenknappheit bei den staatlichen Behörden die „«natürliche» *Wachstumsgrenze*" dieser Techniken sieht (NOGALA 1998, S. 298). Zu Entlastungs- und Kompensationseffekten, siehe NOGALA 1998, S. 62 und insb. 183 f. Siehe auch unten Vierter Teil, Kapitel V.B.

521 Das ist eine Frage der Erforderlichkeit in der Verhältnismässigkeitsprüfung, siehe dazu bspw. ausführlich hinsichtlich der Videoüberwachung, MÜLLER L. 2011, S. 248 ff. Siehe dazu auch WOOD.

ZWEITER TEIL:
GEDANKEN AUS RECHTLICHER PERSPEKTIVE

I. Ausgewählte Problemfelder

A. Aufklären frei verfügbarer Informationen

Das Internet steht der breiten Öffentlichkeit zwar seit längerem zur Nutzung bereit, es dehnte sich aber vor allem in den letzten zehn bis fünfzehn Jahren explosionsartig aus. Das Internet und seine Online-Dienste (E-Mail, VoIP, Internetforen etc.) entwickelten sich zu alltäglichen, kaum mehr wegzudenkenden Kommunikations- und Unterhaltungsmitteln.[522] Der Gedanke der völligen Unabhängigkeit des Internets[523] hat sich nicht durchgesetzt.[524] Vielmehr wird zuweilen warnend darauf hingewiesen, dass durch die Ausdehnung des Internets „rechtsfreie Räume" entstanden seien und gefordert, „[…] dass alles, was jedermann im Internet suchen und finden kann, der Polizei nicht verwehrt sein" dürfe.[525]

Das zunehmende polizeiliche Bedürfnis, das Internet auch verdachtsforschend zu durchkämmen, ist durchaus nachvollziehbar, dieser Tätigkeitsbereich „erfolgt jedoch derzeit weitgehend im polizeigesetzlich regelungsfreien Raum und betrifft eine unüberschaubare Vielzahl unverdächtiger Personen."[526] Aktivitäten im und im Zusammenhang mit dem virtuellen Raum nehmen einen nicht zu vernachlässigenden, wachsenden Teil unserer Lebensführung ein, wobei jede Aktion (bleibende) elektronische Spuren hinterlässt. Der virtuelle Raum ist, im Gegensatz zum realen Raum, einer automatischen Sondierung besonders leicht zugänglich. Suchende, sondierende oder analysierende Hilfsmittel können im

---

522 ZERBES, S. 19 f. und 39; KLESCZEWSKI, S. 737; PETRI, G N. 361; PERREY, S. 37 f., 51 f. und 65 f.; TESCHNER, S. 15 f.; SZUBA, S. 24 f.; LATZER ET AL.

523 Siehe dazu etwa die „Unabhängigkeitserklärung" von John Barlow (<https://projects.eff.org/~barlow/Declaration-Final.html>) anlässlich des World Economic Forum (WEF) am 8. Februar 1996 in Davos.

524 BENDRATH, S. 5 f.; GLESS 2012, S. 3 und 22; TESCHNER, S. 31 und 86.

525 So etwa HENRICHS/WILHELM 2010b, S. 218; ähnlich GERCKE/BRUNST, S. 315 f. Siehe dazu auch TESCHNER, S. 31 ff.

526 PETRI, G N. 362. Ähnlich LOBSIGER 2004, S. 69.

virtuellen Raum anders, etwa leichter oder effizienter, verwendet werden.[527] Beispielsweise begründet die Kenntnis der Behörde von der Existenz einer einschlägigen Website wohl in der Regel einen Anfangsverdacht[528], hingegen das anlassunabhängige Durchforsten[529], die *Suche* nach einschlägigen Websites, dürfte oftmals verdachtsforschende Züge annehmen. Bereits simple Recherchen über eine Internetsuchmaschine nach Stichwörtern können im Rahmen der Verbrechensabwehr problematisch sein.[530]

Öffentlich zugängliche virtuelle Räume könnten dadurch einem strengeren Regime unterworfen beziehungsweise einer intensiveren Überwachung ausgesetzt werden, lediglich, weil die technischen Voraussetzungen dafür im virtuellen Raum besser sind.[531] In diesem Sinne ist es sicherlich zu begrüssen, dass die neuere Rechtsprechung des Bundesgerichts, des deutschen Bundesverfassungsgerichts und des EGMR die Freiheitsrechte auch im virtuellen Bereich auf bestimmte Sammeltätigkeiten öffentlich frei verfügbarer Informationen ausweitet und die Gerichte versuchen, Leitlinien für die staatliche Überwachungstätigkeit zu entwickeln. Das Mitverfolgen einer öffentlichen Kommunikation, etwa der Konversation von Dritten in einem öffentlich zugänglichen Chat, gleicht nach dem Bundesgericht dem Patrouillieren von Polizeiangehörigen in Zivil und ist, „soweit die Beobachtung gezielt auf bestimmte Teilnehmer im Chat konzentriert wird, allenfalls als Observation zu qualifizieren".[532] Diese Analogie des Bundesgerichts zum Patrouillieren im realen Raum scheint durchaus einleuchtend. Das deutsche Bundesverfassungsgericht argumentierte ähnlich. Es hielt fest, dass die „Kenntnisnahme öffentlich zugänglicher Informationen […] dem Staat nicht grundsätzlich verwehrt" sei, auch dann nicht, wenn „auf diese Weise im Einzel-

---

527 OBERHOLZER 2004, S. 59, BELSER, S. 2 N. 4; HILGENDORF, S. 828 ff.; THÜR, S. 105 ff.; HENRICHS/WILHELM 2010a, S. 32 f.; BISCHOF/SCHWEIZER, S. 152; CHESTERMAN, S. 226.

528 ZERBES, S. 301.

529 Siehe dazu KANT/BUSCH, S. 40 f.

530 Urteil des Bundesverwaltungsgerichts A-7040/2009 vom 30. März 2011 E. 7.3; BISCHOF/SCHWEIZER, S. 154. Es scheint diesbzgl. auch nicht immer leicht, passende Analogien im realen Raum zu finden. Die folgenden Ausführungen gehen dennoch – oder gerade deswegen – davon aus, dass für den virtuellen und realen Raum ähnliche Grundsätze gelten sollen. Vgl. RUX, S. 832 und ebenso GLESS 2012, S. 21. Zudem scheint der Weg über eine Suchmaschine im präventiv-polizeilichen Bereich häufig genuin verdachtsforschend. Denkbare Ausnahmen finden sich in Fällen, in denen die Analogie zur Observation passend ist oder mit sehr spezifischen Kriterien nach einer sehr spezifischen Information gesucht wird.

531 Vgl. ZERBES, S. 20.

532 BGE 134 IV 266 E. 3.8.2 S. 278. Vgl. auch GLESS 2012, S. 15.

fall personenbezogene Daten erhoben werden können". Es fügte weiter hinzu, dass das heimliche Aufklären des Internets nicht stets in das allgemeine Persönlichkeitsrecht beziehungsweise das Recht auf informationelle Selbstbestimmung eingreife.[533] Einschränkend tendieren EGMR und Bundesverfassungsgericht hingegen dazu, das systematisierte Zusammentragen von Daten aus öffentlich zugänglichen Quellen zurückhaltend eingesetzt zu wissen. Systematische Sammlungen von öffentlich zugänglichen personenbezogenen Informationen halten nach Ansicht des EGMR dem Verhältnismässigkeitsprinzip in der Regel nicht stand.[534] Analog neigt das Bundesverfassungsgericht dazu, Eingriffe in das Recht auf informationelle Selbstbestimmung zu bejahen, wenn öffentlich zugängliche Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Beizug weiterer Daten ausgewertet" werden und „sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen" ergibt. Es verlangt in diesen Fällen eine spezielle Ermächtigungsgrundlage.[535] Die „reine Internetaufklärung"[536] und entsprechend die Überprüfung öffentlicher virtueller Inhalte nach verdächtigen Begriffen und Aussagen, suspekten Verhaltensweisen und Websites etc. dürften also, folgt man diesen Leitsätzen, wie im realen Raum in der Regel ohne spezielle Ermächtigungsgrundlage zulässig sein, solange die durchsuchten und interpretierten Daten sowie das Analyseergebnis nicht in Registern beziehungsweise Datenbanken langfristig abgespeichert werden, systematisch personenbezogen gesammelt oder mit Daten aus anderen Quellen kombiniert werden (was aber wiederum die Regel sein dürfte). Ausgenommen sind analog zum realen Raum die private Kommunikation beziehungsweise private, nicht

---

533 BVerfGE 120, 274 (276 f. und 344 f.).

534 Die Entscheide des EGMR Rotaru gg. Rumänien vom 4. Mai 2000, Nr. 28341/95, §§ 42 ff. und P. G. und J. H. gg. Vereinigtes Königreich vom 25. September 2001, Nr. 44787/98, §§ 56 ff. dürften ohne weiteres analog für den virtuellen Raum gelten, siehe BISCHOF/SCHWEIZER, S. 155.

535 BVerfGE 120, 274 (345). Vgl. GERCKE/BRUNST, S. 316. Eine ausdrückliche präventiv-polizeiliche Ermächtigungsgrundlage, Personendaten durch Auswerten öffentlich zugänglicher Quellen (systematisch) zu beschaffen, sieht in der Schweiz beispielsweise Art. 14 Abs. 2 lit. a BWIS vor. Siehe dazu auch Bericht Vorentwurf NDG, S. 25 f.

536 BVerfGE 120, 274 (345). Also soweit Inhalte, „die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten" betroffen sind (345).

öffentlich zugängliche Inhalte.[537] Diese Leitlinien sind aber noch weit davon entfernt, ausgereift zu sein.[538]

Neben der Diskussion um die frei zugänglichen Internetinhalte ist ein weiteres aktuelles Thema die Überwachung von Peer-to-Peer-Netzwerken (P2P-Netzwerke), die bezweckt, den illegalen Austausch von urheberrechtlich geschützten Inhalten zu verhindern. Die Überwachung dieses virtuellen Abschnitts übernehmen zumeist private Sicherheitsunternehmen, die im Auftrag der Unterhaltungsindustrie handeln.[539] Sie agieren in einem Umfeld von massenhaft begangenen Bagatelldelikten bei gleichzeitig hohem Strafpotenzial. Für die Schweiz sah das Bundesgericht in dieser Bearbeitung von Daten über P2P-Netzwerkteilnehmer eine unzulässige Persönlichkeitsverletzung gemäss DSG.[540] Die dafür notwendige gesetzliche Grundlage besteht nicht. Zwar wurden mehrere Konzepte, auch auf überstaatlicher Ebene, diskutiert, eine für alle Seiten akzeptable Kompromisslösung konnte aber noch nicht gefunden werden.[541]

---

537 PERREY, S. 181.

538 Ein offener Punkt besteht bspw. darin, welche staatlichen Verwendungszwecke die freiwillige Datenpreisgabe durch den Betroffenen umfasst, siehe KUTSCHA, S. 1043; PETRI, G N. 22; PROBST, S. 35 ff. Fraglich ist, ob nicht auch darauf abgestellt werden sollte, inwieweit die betroffene Person Kenntnis von der Veröffentlichung hatte (die Inhalte von ihr insoweit tatsächlich *freiwillig* verfügbar gemacht wurden) und inwieweit sie Veröffentlichungen unterbinden kann, siehe PETRI, G N. 22; SIMON D., S. 152. Zum Rechtsschutz gegen „ubiquitäre Datenbearbeitung" im Internet und in sozialen Netzwerken, siehe BISCHOF/SCHWEIZER, S. 157; SCHWEIZER 2008, N. 47 f. zu Art. 13 Abs. 2 BV; BELSER, S. 370 ff. N. 104 ff. Zu fehlenden Ermächtigungsnormen hinsichtlich des Aufklärens und Sondierens insbesondere von sozialen Netzwerken, siehe etwa PETRI, G N. 363; ZERBES, S. 29; ausführlicher HENRICHS/WILHELM 2010a; DIES. 2010b; MÜLLER G., S. 173 ff.; die Beiträge im Schwerpunktheft CILIP 1/2011: „Internet unter Kontrolle? Die Staatsgewalt im Web 2.0".

539 Siehe dazu anstatt vieler: CHOTHIA ET AL.; PIATEK ET AL.; ZIMMER, S. 49 ff. mit weiteren Hinweisen.

540 Siehe dazu BGE 136 II 508. Ähnlich das Urteil des Obergerichts des Kantons Bern BK 11 9 vom 22. März 2011.

541 Siehe dazu den Bericht Bundesrat i. S. Savary, S. 10 ff.

B. Informationsverarbeitung, Datenbanken und Verdachtsregister

Personendatenabgleiche mittels polizeieigener Datenbestände bedeuten meist geringfügige Grundrechtseingriffe.[542] In Kombination mit anderen Methoden steigert sich ihre Eingriffsintensität. Auch die Erhebung und Aufbewahrung erkennungsdienstlichen Materials und das Erstellen und Bearbeiten eines DNA-Profils zu Identifikationszwecken in einem weitgehend anonymisierten Informationssystem berühren die Garantien von Art. 10 Abs. 1 und 2 (Geheimsphäre und Persönlichkeitsschutz) beziehungsweise Art. 13 Abs. 2 BV (informationelle Selbstbestimmung), stellen nach bundesgerichtlicher Rechtsprechung aber regelmässig nur leichte Eingriffe dar.

Problematischer scheinen hingegen insbesondere die Probeentnahmen bei DNA-Massenuntersuchungen.[543] Dasselbe gilt für die Datenerhebung über Rasterfahndungs- und Massendatenverarbeitungsmethoden aus zumeist behördenfremden Datenbeständen, bei denen regelmässig grosse Mengen Informationen über viele an sich völlig unverdächtige oder sehr abstrakt verdächtige Personen, Vorgänge, Beziehungen usw. ohne direkten Tatbezug bearbeitet und, optional, beiläufig „auf Vorrat" gesammelt werden.[544] In der durch diese Methoden reduzierten Schnittmenge befinden sich in aller Regel noch immer viele Personen, die näher überprüft werden müssen, von denen aber bis auf die wenigen tatsächlichen Störer, Gefährder oder Straftäter keine der Personen mehr der aufgestellten Fahndungshypothese entsprechen.[545] Daraus können geringe bis schwerwiegende Eingriffe in die Grundfreiheiten von potenziell sehr vielen Personen resultieren.[546] Die Eingriffsqualität richtet sich dabei nach der Einzelfallkonstellation.[547]

---

542 PETRI, G N. 520. Zu beachten sind die Grundsätze der Datenbearbeitung: Der Grundsatz der Gesetzmässigkeit der Datenerhebung und -bearbeitung, der Richtigkeit bzw. Qualität, der Zweckbindung, Verhältnismässigkeit und Datensicherheit, siehe MOHLER 2012, S. 383 ff.

543 BGE 136 I 87 E. 5.1 S. 101; 134 III 241 E. 5.4 S. 247; 128 II 259 E. 3.1-3.3 S. 267 ff.; 120 Ia 147 E. 2a und b S. 149 f.; 107 Ia 138 E. 5a S. 145; Urteil des Bundesgerichts 1B.57/2013 vom 2. Juli 2013 E. 3; HÄFELIN/HALLER/KELLER, N. 370 S. 122; VEST, N. 22 zu Art. 32 BV. Siehe auch kritisch OEHMICHEN, S. 937 bzgl. sich ausweitender DNA-Datenbanken.

544 PETRI, G N. 531 f.; BVerfGE 115, 320 (341 ff.).

545 ROGALL, S. 617; ZSCHOCH, S. 51. Vgl. HANSJAKOB 2012, N. 11.

546 Siehe etwa BGE 137 IV 340; 133 I 77; 128 II 259; HANSJAKOB 2006, N. 19 zu Art. 16 VÜPF; RUDIN, S. 280; PETRI, G. N. 531 ff.; ZSCHOCH, S. 48 und 51 f.; BVerfGE 115, 320 (347 f.). Skeptisch gegenüber der Annahme schwerwiegender Eingriffe: ROGALL, S. 625 f. und 635.

Die präventiv-polizeiliche Rasterfahndung hat grundsätzlich das Potenzial, stärker und breiter in die Freiheiten von Personen einzugreifen als die strafrechtliche, da die Anlassschwellen im präventiv-polizeilichen Bereich tiefer sind. Sie unterstünde in der Schweiz zudem dem Datenschutzrecht.[548] In Anbetracht der Breite und der Intensität der Eingriffe in die Grundfreiheiten einer grossen Zahl Unverdächtiger – es werden sensible, personenbezogene Daten durchforscht und in einem zweiten Schritt individuell nachgeprüft –, könnte höchstens eine hinreichend bestimmte rechtliche Grundlage den Anforderungen des Legalitätsprinzips und der Datenschutzgesetze genügen.[549]

Dem Aufbewahren personenbezogener Daten in elektronischen Datenbanken kommt deshalb eine „hervorgehobene Bedeutung" zu, weil verschiedene Stellen automatisiert auf sie zugreifen und die gespeicherten Informationen in verschiedenen Zusammenhängen verwendet werden können.[550] Die für die Schweiz massgebliche Rechtsprechung verbietet zwar grundsätzlich Daten auf Vorrat zu speichern.[551] Diese Regel wurde jedoch in jüngerer Zeit abgeschwächt[552]:

Erstens gelten diese Grundsätze für verdachtsunabhängige Datenbanken und das Sammeln von Randdaten nur bedingt.[553]

547 PETRI, G N. 531 mit weiteren Hinweisen; ZSCHOCH, S. 51. Nach der Ansicht des BVerfG sind für die Beurteilung „die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen" massgebend, siehe BVerfGE 115, 320 (347).

548 RUDIN, S. 277 f.

549 KUBE, S. 56; RUDIN, S. 278.

550 PETRI, G N. 370: „Inbesondere längerfristige Speicherungen haben daher für den Betroffenen häufig unabsehbare Folgen."; SCHEFER, S. 62; SIMON D., S. 175 und 249; BVerfGE 115, 320 (341 f.); Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, § 121: „[…] the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data."

551 Siehe den EGMR in seinen Entscheiden Segerstedt-Wilberg u. a. gg. Schweden vom 6. Juni 2006, Nr. 62332/00, § 90 und Peck gg. Vereinigtes Königreich vom 28. Januar 2003, Nr. 44647/98, § 85. Ebenso das Bundesgericht in BGE 136 I 87 E. 5.5 S. 103 f. Siehe dazu SCHWEIZER 2009, S. 468; SCHWEIZER 2008, N. 44 zu Art. 13 BV; PROBST, S. 39; NOWAK, S. 36. Vgl. auch BVerfGE 125, 260 (320 f.)

552 SIMON D., S. 175 steht deshalb Beteuerungen, es gelte ein Verbot der Datenbevorratung, verständlicherweise kritisch gegenüber.

553 Vgl. OBERHOLZER 2003, S. 333. Siehe oben Erster Teil, Kapitel I.G.5.

Zweitens hat die Digitalisierung von Alltagsdaten in den letzten Jahren immens zugenommen. Internetaktivitäten, der Gebrauch des Mobiltelefons oder von Kundenkarten und viele andere Handlungen hinterlassen Spuren, die (vielfach personenbezogen) gespeichert werden. Können Behörden Zugriff auf diese Quellen nehmen, sind diese Archive nichts anderes als nützliche und willkommene Vorratsdatenspeicher. So wäre noch vor 15 Jahren die Vorratsdatenspeicherung von Mobilfunkdaten weniger problematisch gewesen. Die Nutzungsmöglichkeiten der Mobiltelefone waren begrenzt, mithin hielten sich die meisten Leute nicht lange damit auf. Die generierten Daten waren dementsprechend gering und auch Antennensuchläufe hätten zu kleineren Schnittmengen geführt. Heute besitzt und bedient praktisch jeder ein mobiles Kommunikationsgerät mit vielerlei Zusatzfunktionen: Diese Datenquelle ist heute also wesentlich ergiebiger, sowohl quantitativ als auch qualitativ. Es ist zu erwarten, dass diese Tendenz weiter zunimmt.[554] Die Eingriffsintensität hängt bei der Vorratsdatenspeicherung unter anderem von der Aufbewahrungsdauer, der Zweckbestimmung und der Einhaltung dieser ab.[555] Die in der Vernehmlassung zur Revision des BÜPF geäusserte Skepsis gegenüber der Verdoppelung der Aufbewahrungsdauer ist insofern durchaus verständlich, wenn man berücksichtigt, dass der Nutzen der Vorratsdatenspeicherung nicht ausgewiesen ist[556] und in anderen Ländern teils wesentlich tiefere Fristen diskutiert werden.[557]

Interessant vor allem hinsichtlich zukünftiger Ermittlungen sind zudem andere Datenbanken, die verdachtsunabhängig Personendaten archivieren. Das Bundesgericht entschied in einem Urteil über die Aufbewahrung von erkennungsdienstlichem Material über ein Strafverfahren hinaus[558], die Verwendung dieses Materials könne unter drei Voraussetzungen verhältnismässig sein: Erstens, wenn das Verfahren bloss vorläufig eingestellt worden sei. Diese Bedingung leuchtet ohne Weiteres ein. Zweitens, wenn der Betroffene ein strafrechtliches Delikt begangen und damit „tatsächlich einmal zur Erstellung des Materials Anlass gegeben“ oder

---

554 Siehe etwa KURZ/RIEGER, S. 51. Dasselbe gilt hinsichtlich Informationssammlungen anderer digitaler Datenquellen, vgl. oben Zweiter Teil, Kapitel I.A.

555 WEBER/WOLF/HEINRICH, N. 18; ROSSNAGEL/BEDNER/KNOPP, S. 537 f.; SIMON D., S. 225 ff. und 259; SZUBA, S. 179 f. Analog BVerfGE 125, 260 (insb. 318 ff.).

556 Siehe oben Erster Teil, Kapitel I.F.2.

557 WEBER/WOLF/HEINRICH, N. 18. Vgl. BVerfGE 125, 260. Siehe auch SZUBA, S. 262 ff. für einen europäischen Rechtsvergleich.

558 Siehe BGE 120 Ia 147. Zu beurteilen war die weitere Aufbewahrung von Fotos der damals verdächtigten Beschwerdeführerin nach der Einstellung des Strafverfahrens.

drittens, die betroffene Person „bloss durch seltsames Betragen Anlass für die Erhebung der Unterlagen gegeben“ habe.[559]

Die beiden letzteren Voraussetzungen lassen aufhorchen: Insbesondere dritte Voraussetzung dehnt den Grundsatz der Verhältnismässigkeit weit aus. Eine Person allein aufgrund der Tatsache, dass über sie erkennungsdienstliches Material vorhanden ist, zu verdächtigen, aber insbesondere die Datensammlungen bereits aufgrund von Auffälligkeiten zu erlauben, kann Probleme hervorrufen. Es (ver-) führt zu einer Aufrechterhaltung der Datensammlungen ohne triftigen Grund, also lediglich basierend auf vagen Hypothesen (auf Rückfallbasisraten, auf auffälligem Verhalten als Indikator für Delinquenzaffinität, auf Einträgen in Verdachtsregistern etc.), und damit zur Einrichtung von praktisch verdachtsunabhängigen, teils nahezu anlasslosen Datenbanken, insbesondere, wenn der Grund für den Eintrag längere Zeit zurückliegt. Namentlich mit der tiefen Schwelle des „seltsamen Betragens“ als Voraussetzung für die Aufbewahrung des Materials über ein Strafverfahren hinaus, ermutigt das Bundesgericht damit möglicherweise bedenklichere Methoden der Aufbewahrung von Vorratsdaten.

Das Bundesgericht entschied in diesem Fall aber trotzdem zugunsten der Beschwerdeführerin: Aufgrund des geringfügigen Delikts hielt es die weitere Aufbewahrung für unverhältnismässig.[560] Zudem beschränkte das Bundesgericht die Aufbewahrungsdauer im Allgemeinen auf eine Zeitspanne von fünf Jahren[561] und setzte damit einer ansonsten ausufernden Verwendung erkennungsdienstlichen Materials gewisse Grenzen.[562]

Der EGMR befand in einem ähnlich gelagerten Fall die pauschale und wahllose Aufbewahrung von Fingerabdrücken, zellularen Proben und DNA-Profilen von verdächtigten, aber nicht überführten Personen verfehle es, eine faire Balance zwischen konkurrierenden öffentlichen und privaten Interessen herzustellen. Eine derartige Aufbewahrung konstituiere einen unverhältnismässigen Eingriff in das Recht des Betroffenen auf Respektierung seines privaten Lebens und könne

559 BGE 120 Ia 147 E. 2.e S. 152.
560 BGE 120 Ia 147 E. 2.g S. 155.
561 BGE 120 Ia 147 E. 2.e S. 152.
562 Unter diese bundesgerichtliche Rechtsprechung fallen übrigens auch Aufzeichnungen der Raumüberwachung, falls diese in einem Strafverfahren beigezogen werden sollen, siehe BGE 133 I 77 E. 4.2 S. 83.

nicht als notwendig in einer demokratischen Gesellschaft angesehen werden.[563] Der EGMR sprach dem Schutz persönlicher Daten fundamentale Bedeutung für das Recht auf Respekt des Privat- und Familienlebens einer Person zu, weshalb staatliche Massnahmen zur Autorisierung der Aufbewahrung und des Gebrauchs von DNA-Informationen ohne die Einwilligung des Betroffenen einer sorgfältigen Beurteilung zu unterziehen seien. Dies gelte unabhängig davon, ob es sich bei den Informationen um DNA-Profile oder Zellproben handle, welche aber als besonders einschneidend zu qualifizieren seien, weil sie eine Fülle an genetischen und gesundheitlichen Informationen beinhalteten.[564]

Verdachtsregister und darauf gestützt erlassene Folgemassnahmen greifen teilweise massiv in verschiedene Schutzbereiche ein. Das wesentliche Merkmal von (mitunter) präventiv ausgelegten Verdachtsregistern ist, mutmasslich risikobehaftete Personen zu demobilisieren und sie bezüglich der von ihnen erwarteten Gefahr handlungsunfähig zu halten. Die UN-Terrorliste und andere Terrorlisten versuchen dieses Ziel über das Sperren von Finanzen und Reiseverbote, Register mit gewaltbereiten Störern über Reise-, Rayon- und Stadionverbote und Sexualstraftäterregister über Meldepflichten, Bewegungseinschränkungen und Verbotszonen zu erreichen. Neben Berührungspunkten mit Grundfreiheiten, verursacht durch das systematische Sammeln, Verarbeiten und Verwalten von personenbezogenen Daten[565], sind demnach Beschränkungen der Eigentumsrechte, verschiedener Teilgehalte der persönlichen Freiheit und von Verfahrensrechten, verursacht durch die Folgemassnahmen, in Betracht zu ziehen.[566] Sie schränken

---

563 Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, § 125.

564 Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, §§ 104 und 120.

565 SCHEFER, S. 62 f. Siehe Zweiter Teil, Kapitel I.B.

566 Siehe dazu BARTMANN, S. 127 f. und 278; MEYER, S. 76 ff.; SCHULTE, S. 322 ff.; DIGGELMANN, S. 311 f.; EMMERSON, N.13; SULLIVAN/HAYES, S. 25 ff.; OEHMICHEN, S. 934; BIANCHI, S. 903 ff.; Bericht HRW, S. 78 ff.; STUDER, S. 67 f.; SOÒS/VÖGELI, S. 159; MOECKLI/KELLER, S. 240; TRUNZ/WOHLERS, S. 193; MÜLLER J. O., S. 120 f.; BGE 137 I 31 E. 6.2 S. 45; 133 II 450 E. 10.2 S. 467; Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 5.3 f.; Entscheid des EGMR Nada gg. Schweiz vom 12. September 2012, Nr. 10593/08, §§ 149 ff., insb. §§ 199, 209-214. Zwischen Eintrag und weiteren Massnahmen zu trennen, kann bedeutsam sein: Hat der Eintrag keine direkten Konsequenzen, unterstützt dieser also lediglich die Ermittlungen eines (zukünftig angestrebten) Strafverfahrens gegen die mutmasslichen Täter, dürfte das Führen nicht-öffentlicher Register in der Regel weniger einschneidend, wenn auch mitunter nicht unproblematisch sein.

den „finanziellen Handlungsspielraum“[567] und/oder die Bewegungsfreiheit von gelisteten Personen teils erheblich ein.[568] Abgesehen davon zieht die Listung einer Person oder Organisation in einem Verdachtsregister häufig Nebenwirkungen auf die Lebensführung eingetragener Person oder auch Dritter nach sich, die den eingetragenen Personen oder Organisationen nahe- oder mit ihnen in Kontakt stehen. Zum Beispiel können von den Sanktionen der Terrorlisten betroffene Personen zwar unbehelligt ihrer Arbeit nachgehen, aber keinen Lohn dafür empfangen. Es kann ihnen zwar eine Haftentschädigung für unbegründete Untersuchungshaft vom Gericht ausgesprochen, aber nicht ausbezahlt werden. Eine faire anwaltliche Verteidigung (Finanzierung des Wahlverteidigers, Kommunikation per Post ohne die für den Erwerb der Briefmarken erforderlichen Mittel etc.) scheiterte in der Vergangenheit zuweilen an den eingefrorenen Finanzen und am strikten Bereitstellungsverbot.[569]

Nicht-öffentliche Terroristenregister sehen unter anderem schwer wiegende Folgemassnahmen des Eintrags vor (zum Beispiel eine tiefgreifende Personenüberwachung des ganzen Umfelds des Betroffenen), setzen mit ihrem Verdacht früh an und gestehen dem Betroffenen aus Gründen der Effizienz und Flexibilität, vor allem im Rahmen der Verdachtsforschung, geringe Verfahrensrechte zu.[570] Sie weiten die Datensammlung häufig auf „Drittpersonen“ aus, was ermöglichen soll, das (mutmasslich verdächtige) Umfeld des mutmasslichen Gefährders und dessen Beziehungen zu anderen Personen zu erfassen. Die personenbezogenen Informationen werden dabei sehr umfassend gespeichert und können zu einer nicht endenden, wuchernden Ausweitung des Verdachtsradius führen.[571] In dieser Hinsicht erkannte der EGMR wiederholt, dass bereits systematische Sammlungen öffentlich verfügbarer Informationen zu verschiedenen Aspekten einer betroffenen Person und ihrer Handlungen, Ansichten und ihres Umfelds etc. in

---

567 BARTMANN, S. 28 und 120 f. Ebenso MEYER/MACKE, S. 447.

568 Siehe dazu ausführlich BARTMANN, S. 116 f. und 120 ff.; SCHULTE, S. 322 ff; MEYER, S. 76 f.; SULLIVAN/HAYES, S. 35; DIGGELMANN, S. 303; Bericht HRW, S. 7 f.; MÜLLER J. O., S. 120 f.; den Fall Youssef Nada (BGE 133 II 450; Reisebeschränkung).

569 Für diese und andere Beispiele, siehe MEYER/MACKE, S. 447 ff.; BARTMANN, S. 122 ff. Zu ähnlichen Problemen der Sexualstraftäterregister, siehe Bericht HRW, S. 74 f., 80 und 117.

570 STEGMANN A., S. 162. Vgl. HAYES 2009, S. 50.

571 STEGMANN A., S. 172 f., S. 158 und S. 175 ff.; CHESTERMAN, S. 238. Eine derartige Ausweitung auf Bekannte eines Eingetragenen gereichte in Kanada etwa Maher Arar zum Verhängnis, siehe dazu den Bericht i. S. Maher Arar. Siehe auch den Vorentwurf des Polizeiaufgabengesetzes. Vgl. MOHLER/SCHWEIZER, S. 9 f.

die Privatsphäre eingreifen würden.[572] Auch sie sind also zu rechtfertigen und steigern die Eingriffsintensität insbesondere, wenn Betroffene über einen längeren Zeitraum erfasst bleiben.

C. Video- und Onlineüberwachungsmassnahmen

Das Bundesgericht hielt in seiner bisherigen Rechtsprechung Art. 13 Abs. 2 BV und 8 Abs. 1 EMRK von Videoüberwachungsmassnahmen für berührt, liess aber offen, ob Art. 10 Abs. 2 BV durch diese betroffen sein kann.[573] Die nicht personenbezogene Raumüberwachung sowie die dissuasive mit bloss bildlicher Personenerkennung (sog. Übersichtsaufnahme beziehungsweise Echtzeitbeobachtung ohne Personenbezug) berühren den Privatbereich der betroffenen Personen nach der Rechtsprechung des Bundesgerichts und des EGMR in der Regel solange nicht, wie sie keine direkte Identifizierung von Personen erlauben.[574] Präzisierend fügte der EGMR hinzu, er erachte lediglich bei der (automatischen) *Bearbeitung* der Personendaten (insbesondere bei der Erstellung von Bewegungsprofilen oder Modifikationen des Systems zur Verfolgung einer Person) die Privatsphäre des Betroffenen als tangiert.[575] Zudem stellte das Bundesgericht in BGE 128 II 259 bezüglich des DNA-Profil-Informationssystems fest, dass sich die Schwere eines Eingriffs in die informationelle Selbstbestimmung nach objektiven Kriterien beurteile. Nicht entscheidend sei, wie dieser vom Beschwerdeführer empfunden werde. Daraus ergibt sich, analog angewendet auf die Videoüberwachung, dass blosse Übersichtsaufnahmen (ohne Speicherung) nicht höher eingestuft werden, nur weil sich ein Betroffener subjektiv aufge-

---

572 Entscheide des EGMR Rotaru gg. Rumänien vom 4. Mai 2000, Nr. 28341/95, §§ 42 ff.; P. G. und J. H. gg. Vereinigtes Königreich vom 25. September 2001, Nr. 44787/98, §§ 56 ff.

573 BGE 136 I 87 E. 8.1 S. 112; 133 I 77 E. 3.2 S. 80 f.; Urteil des Bundesgerichts 1C.315/2009 vom 13. Oktober 2010 E. 2.2. Vgl. FLÜCKIGER, S. 208; BELSER, S. 401 f. N. 174.

574 BGE 133 I 77 E. 5.3 S. 85 und der EGMR in seinem Entscheid Perry gg. Vereinigtes Königreich vom 17. Juli 2003, Nr. 63737/00, §§ 38 und 40. Ebenso in seinen Entscheiden Uzun gg. Deutschland vom 2. September 2010, Nr. 35623/05, § 44; Calmanovici gg. Rumänien vom 1. Juli 2008, Nr. 42250/02, § 130. Siehe dazu FLÜCKIGER/AUER, S. 932 f. und 941; FLÜCKIGER, S. 209 f.; MOHLER 2012, S. 183. MÜLLER L. 2011, S. 120 f. hält hingegen dafür, bereits die „blosse Videobeobachtung" als Eingriff in Art. 8 EMRK zu verstehen. Vgl. zu dieser Problematik BARTSCH, S. 93 ff.

575 Entscheide des EGMR Perry gg. Vereinigtes Königreich vom 17. Juli 2003, Nr. 63737/00, § 40; P.G. und J. H. gg. Vereinigtes Königreich vom 25. September 2001, Nr. 44787/98, § 57; Amann gg. Schweiz vom 16. Februar 2000, Nr. 27798/95, § 65-67. Siehe dazu SCHWEIZER 2009, S. 465; FLÜCKIGER, S. 210. Ähnlich MÜLLER L. 2011, S. 207.

zeichnet fühlt.[576] Das Aufzeichnen und Aufbewahren von Übersichtsbildern alleine bedeutet gemäss Rechtsprechung des Bundesgerichts somit grundsätzlich keinen Grundrechtseingriff.[577] Der EGMR nimmt erst dann einen Eingriff in Art. 8 EMRK an, wenn Videoüberwachungssysteme im öffentlichen Raum systematisch und dauerhaft aufzeichnen.[578] Die Aufbewahrungsdauer der Aufzeichnungen bedarf indes einer gesetzlichen Regelung, welche die Verwendung des Bildmaterials präzis normiert.[579] Das Bundesgericht entschied in dieser Hinsicht, dass die Dauer von 100 Tagen bereits einen „nicht unerheblichen" Grundrechtseingriff (Art. 13 Abs. 2 BV) für Betroffene darstelle. Zudem verlangt es, der überwachte Raum sei mit Hinweistafeln zu markieren.[580]

Ein Teil der Literatur hingegen nimmt bereits bei blossen Übersichtsaufnahmen und bei der Echtzeitbeobachtung ohne Personenbezug Eingriffe in die informationelle Selbstbestimmung an.[581] Abgesehen davon scheint die Überwachung mit Identifikation und Aufzeichnung, sofern es sich bei den Zielpersonen um konkrete Störer beziehungsweise Personen mit konkretem Störungspotenzial handelt (wobei sich diese Form einer Observation auf öffentlichem Grund stark annä-

---

576 Siehe BGE 133 I 77 E. 5.3 S. 85; 128 II 259 E. 3.3 S. 269. Gl. A. BARTSCH, S. 115 ff., welche m. E. zutreffend argumentiert, diese subjektiv empfundene Beeinträchtigung lasse den Eingriffsbegriff an Kontur verlieren.

577 BGE 133 I 77 E. 5.3 S. 85.

578 Entscheide des EGMR Wisse gg. Frankreich vom 20. Dezember 2005, Nr. 71611/01, § 25; Perry gg. Vereinigtes Königreich vom 17. Juli 2003, Nr. 63737/00, §§ 38 und 40; Peck gg. Vereinigtes Königreich vom 28. Januar 2003, Nr. 44647/98, § 59. Vgl. MÜLLER L. 2011, S. 114 und 118 ff., welcher dieser Rechtsprechung kritisch gegenübersteht. Zur Diskussion, ob der EGMR insb. die Systematik und Dauerhaftigkeit der Aufbewahrung oder der Videoüberwachung an sich als wesentliche Beurteilungsgrundlage berücksichtigt, siehe MÜLLER L. 2011, S. 115 mit weiteren Hinweisen.

579 Siehe dazu ausführlich MÜLLER L. 2011, S. 226-231 mit weiteren Hinweisen.

580 BGE 133 I 77 E. 5.3 S. 85 und E. 5.5 S. 87. Diese Richtlinien des Bundesgerichts dürften gefestigt sein. So bestätigte es etwa die hunderttägige Aufbewahrungsdauer in BGE 136 I 87 E. 8.4. Die beurteilte, im PolG ZH angestrebten Zeitspanne von einem Jahr hielt es hingegen für unverhältnismässig. Siehe zur zulässigen Aufbewahrungsfrist MÜLLER L. 2011, S. 279 ff., für den eine hunderttägige Frist grundsätzlich die noch zulässige Höchstdauer markieren soll. Auch die Venice Commision 2007, S. 16 N. 83 verlangt, dem potenziell Betroffenen die Videoüberwachung kenntlich zu machen. Vgl. zum Ganzen FLÜCKIGER/AUER, S. 934. Ferner DIES., S. 941 f.

581 So bspw. BREITENMOSER, N. 13 zu Art. 13 BV; MÜLLER L. 2011, S. 121 und 131 mit weiteren Hinweisen. Vgl. FLÜCKIGER/AUER, S. 932. Für Deutschland: Ausführlich BÜLLESFELD 2002, S. 142 ff.; ROGGAN 2001, S. 135 f.; BARTSCH, S. 97 ff.; ZSCHOCH, S. 199.

hert)[582] oder wenn im zu überwachenden Raum eine akute (konkrete) Gefahr droht, grundsätzlich mit öffentlichen Interessen zu rechtfertigen zu sein. Es ist indes eine klare und auf den jeweiligen Einsatzort und die Einsatzsituation zugeschnittene Zweckbestimmung festzusetzen.[583] Vorausgesetzt ist freilich auch, dass Kantone und Gemeinden ihre kantonalen und kommunalen Vorschriften zur Videoüberwachung nicht restriktiver gefasst haben.

Geheime Online-Überwachungsmassnahmen können zu schwerwiegenden Eingriffen in den Geheim- und Privatbereich des Verdächtigen und von Drittpersonen führen, Persönlichkeitsverletzungen im Sinne des Datenschutzgesetzes und Störungen des „Computerfriedens" (Unverletzlichkeit des eigenen Computers) verursachen.[584] Je nach eingesetzter Version und Funktionalität der Überwachungstechnologie sind somit Eingriffe in die persönliche Freiheit (Art. 10 Abs. 2 BV), informationelle Selbstbestimmung, die Privatsphäre und den Datenschutz (Art. 13 BV) denkbar.[585] Weiter können durch ihren Einsatz wesentliche Verfah-

---

582 In diesen Fällen ist fraglich, ob die Neuerungen bzgl. automatisierter Verhaltensanalysen sich nicht sogar, unter bestimmten Bedingungen, positiv auf die Verhältnismässigkeit auswirken könnten, indem die Aufzeichnung erst startet, wenn ein derartiges Vorkommnis vorausgeahnt bzw. identifiziert und somit nur *zielgerichtet* aufgenommen wird. Es bietet sich diesfalls zum Vergleich die Koppelung der Überwachung an einen Bewegungsmelder an, siehe RUDIN/STÄMPFLI, S. 149.

583 RUDIN/STÄMPFLI, S. 146 f. fordern m. E. zu Recht eine sehr präzise Zweckbestimmung (z. B. die exakte Angabe des im Fokus liegenden Deliktstypus) jeder einzelnen Überwachungsanlage. Ebenso MÜLLER L. 2011, S. 217. Vgl. SCHWEIZER 2008, N. 49 f. zu Art. 13 BV. In dieselbe Richtung geht die Ansicht des Bundesgerichts in BGE 136 I 87 E. 8.3 S. 114 ff. Zu den an Kriminalitätsschwerpunkte zu stellenden Erfordernissen, siehe MÜLLER L. 2011, S. 265; BÜLLESFELD 2002, S. 206 f. Nach Ansicht von MÜLLER L. 2011, S. 265 können auch Räume, die „als zur Verübung von schweren Delikten besonders geeignet erscheinen", in denen aber noch kein „erhebliches Straftatenaufkommen" zu verzeichnen war, Kriminalitätsschwerpunkte darstellen. A. A. BARTSCH, S. 202 f.; BÜLLESFELD 2002, S. 206 f.

584 KATZENSTEIN, N. 1 f. zu Art. 280 StPO; SCHMID 2009b, N. 1 Vor Art. 269-279 StPO; JAGGI, S. 2; BIAGGINI, S. 266 f.; ZERBES, S. 38; PLATZ, S. 841 mit weiteren Hinweisen. Art. 179 ff. StGB stellt den strafrechtlichen Schutz gegen Eingriffe in die Geheim- und Privatsphäre, Art. 143bis StGB schützt den „Computerfrieden" analog dem Hausfrieden, siehe dazu INS/WYDER, N. 5 zu Art. 179 StGB; WEISSENBERGER, N. 3 zu Art. 143bis StGB. JAGGI, S. 2 sieht durch geheime Überwachungsmassnahmen „erfahrungsgemäss häufig" Drittpersonen ohne Bezug zu Straftat und Untersuchung mitbetroffen.

585 Siehe dazu JEAN-RICHARD-DIT-BRESSEL, N. 21 zu Art. 269 StPO; SCHMID 2009b, N. 1 Vor Art. 269-279 StPO; BELSER, S. 396 f. N. 162, 164 und S. 401 f. N. 174; ausführlich TSCHENTSCHER, S. 389 ff., auch zum Wert eines Grundrechts auf Computerschutz (dazu bspw. auch PETRI, G N. 8 ff.) analog deutscher Rechtsprechung für die Schweiz.

rensrechte (Informations-, Verteidigungs-, Mitwirkungsrechte) beschnitten werden, wodurch die betroffene Person etwa Aussageverweigerungsrechte nicht wahrnehmen kann oder Berufsgeheimnisse verletzt werden.[586] Schliesslich können organisatorische und technische Mängel zu unerwünschten Nebenwirkungen führen, die möglicherweise auch die Rechtsgüter Dritter tangieren und allgemein eine beträchtliche Streubreite der Massnahme nach sich ziehen.[587]

Die Online-Überwachung im Speziellen kann besonders schwerwiegende Grundrechtseingriffe bei betroffenen Personen und Dritten auslösen. Die zahlreichsten und intensivsten Eingriffe dürfte die ununterbrochene Infiltration über längere Dauer, die Aktivierung von Zusatzfunktionen und die Übernahme der Kontrolle über das informationstechnische System bedeuten.[588] Zudem spielen im rein präventiv-polizeilichen Bereich Beweisverwertungsverbote keine oder kaum eine Rolle, erst im (eventuell anschliessenden) Strafverfahren kann durch sie überschiessendes behördliches Handeln kompensiert werden.[589] An eine heimliche Online-Durchsuchung/-überwachung, wie sie im Vorentwurf des NDG vorgesehen ist, wäre dementsprechend ein extrem hoher Massstab anzulegen, unter anderem wären sehr hohe Anforderungen an den nachträglichen Rechtsschutz, die Achtung von Amts- und Berufsgeheimnissen und die Herausgabe sowie Löschung irrelevanter Unterlagen zu stellen.[590] Mindestens teilweise verdachtsforschende Varianten von Govware und DPI können deshalb lediglich unter überaus restriktiven Voraussetzungen zulässig sein.[591]

---

586 JEAN-RICHARD-DIT-BRESSEL, N. 21 zu Art. 269. Umstritten ist, ob auch dem Verbot der Selbstbelastung („nemo tenetur") widersprochen wird, siehe JAGGI, S. 2 (zustimmend); JEAN-RICHARD-DIT-BRESSEL, N. 21 zu Art. 269 StPO (ablehnend) jeweils mit weiteren Hinweisen.

587 ROGGAN 2009, S. 261; ZERBES, S. 337. Siehe ausführlicher unten Zweiter Teil, Kapitel I.D.

588 M. E. lediglich im Einzelfall und wohl selten vor dem Einsatz der Massnahme zu beurteilen scheint, ob die Erfassung der Kommunikation und deren Randdaten oder die einmalige Spiegelung des Zielsystems mittels Online-Durchsuchung schwerwiegendere Eingriffe nach sich ziehen.

589 BIAGGINI, S. 264.

590 HEIMGARTNER, S. 37. Vgl. analog THORMANN/BRECHBÜHL, N. 1 zu Art. 246 StPO mit weiteren Hinweisen.

591 Wie unten ausgeführt wird (siehe unten Zweiter Teil, Kapitel I.I.), ist infrage zu stellen, ob der sicherheitspolizeiliche Tätigkeitsbereich und das Strafverfahren wegen der zunehmenden Vermischung der Rechtsgebiete klar abzugrenzen sind, siehe etwa ZERBES, S. 361.

D. Rechtliche Konsequenzen technischer Probleme

Die untersuchten Registrierungs- und Überwachungsmassnahmen können in der Praxis teils zu sehr unbefriedigenden Konstellationen führen. Vielfach zeigen sich unerwartete oder ignorierte Problemstellen und Folgen erst, wenn die Massnahmen tatsächlich angewendet werden und sich bewähren müssen:

Können Merkmale beziehungsweise Suchkriterien von Rasterfahndungen, Massendatenverarbeitungen oder automatisierten Systemen Verdächtige tatsächlich nicht adäquat erfassen, führt dies entweder zu einer grossen Streubreite oder zu einem oftmals unbilligen Fokus auf bestimmte Personengruppen.[592] Ersteres Ergebnis kann (leichte) Eingriffe in die Grundfreiheiten sehr vieler Personen bedeuten[593], letzteres schwerwiegendere Eingriffe verursachen und allenfalls das Diskriminierungsverbot (Art. 8 Abs. 2 BV) tangieren.[594] Die Fähigkeiten der Technik, innerhalb der Gesetzesvorgaben zu arbeiten, beschränken somit die Einsatzmöglichkeiten dieser Methoden.

Hinsichtlich der Verdachtsregister können sich problematische Situationen insbesondere aus deren Fehleranfälligkeit[595] in Verbindung mit fehlenden oder unzureichenden Behelfen des Betroffenen ergeben, Einträge berichtigen oder löschen zu lassen, und den unwiderruflichen sozialen Nachteilen, welche die Veröffentlichung des Eintrags mit sich bringt.[596] In einem Modell wie dem Sexualstraftäterregister der Vereinigten Staaten sind Registrierte wegen der ausufernden Vorschriften der Gesetzgebung teilweise genötigt, fernab von grösseren Ballungsräumen zu leben. Viele finden zudem überhaupt schwer Wohnungen, was dazu führt, dass Registrierte nicht selten wegen ihres Eintrags obdachlos werden und bleiben.[597] Hier zeigt sich die bedenklichste Folge der vorgeschrie-

---

592 Vgl. ZERBES, S. 313 und 332. Siehe ausführlicher unten Vierter Teil, Kapitel III. Vgl. auch die Ausführungen zu den Fähigkeiten der Methoden im Ersten Teil.

593 Siehe etwa ZSCHOCH, S. 52. Vgl. BGE 137 IV 340; 133 I 77; 128 II 259.

594 ZSCHOCH, S. 52; MOECKLI/KELLER, S. 240; das Urteil des Verwaltungsgerichts des Kantons Bern VGE 21758 vom 17. Mai 2004 E. 6.2.8 mit weiteren Hinweisen (= BVR 2005 S. 97 ff.); BVerfGE 115, 320 (351 ff.).

595 Vgl. bspw. EMMERSON, N. 30; DIGGELMANN, S. 310 f. Zur Fehleranfälligkeit bei der Vorratsdatenspeicherung, siehe etwa ROSSNAGEL/BEDNER/KNOPP, S. 538.

596 STUDER, S. 68.

597 Siehe Bericht HRW, S. 3, 7, 102, 107 und 125; OPPAGA 2008, S. 5. Teils überschneiden sich die Radien von Kindergärten, Schulen, Spielplätzen usw. für die Eingetragenen derart unvorteilhaft, dass ganze Stadtteile zu Bannkreisen werden (in Orange County, Florida 95% des Wohngebiets). Siehe dazu Bericht HRW, S. 102 mit weiteren Hinweisen.

benen Melde- und Mitteilungspflicht: Eingetragene Sexualstraftäter werden zu Verbannten der Gesellschaft, zu Aussätzigen. Wo Bannkreise unter dem Aspekt der Reduktion von Tatgelegenheiten oder der *défense sociale* wünschenswert scheinen können, sind Registrierte ohne stabiles soziales Umfeld, insbesondere Obdachlose, von der zuständigen Behörde nurmehr schwer zu beaufsichtigen und kontrollieren, was freilich speziell dem Zweck, das Register unterstützend bei Ermittlungen einzusetzen, entgegen wirkt.[598]

Nicht-öffentliche Register erzeugen in der Praxis unter anderem Komplikationen, sobald die Betreiber Personendaten aus diesen Listen an Dritte (beispielsweise an Flughäfen, Finanzinstitute oder Stadionbetreiber) mit der Anweisung weitergeben, dass diese ihre Klienten anhand dieser Informationen zu überprüfen haben. Heikel scheint diesbezüglich insbesondere, dass private Unternehmen die ihnen diktierten Sanktionen bei einem Treffer selbst und sofort vollziehen müssen, wenn die ausführenden Mitarbeiter in den Unternehmen nicht ausreichend ausgebildet sind, die teilweise sehr weitreichenden Sanktionen angemessen und ordnungsgemäss einzuleiten. Abgesehen davon sind die von der Behörde, die das Register führt, zur Verfügung gestellten Daten, vielfach nur ein Name, in der Regel zu knapp, um einen fehlerlosen Drittvollzug zu gewährleisten. Zudem können Ungenauigkeiten oder Unachtsamkeiten bei der privatisierten Klientenüberprüfung schnell zu Verwechslungen führen. Das mag vielleicht banal klingen, bringt den Betroffenen in der Praxis aber in eine prekäre Lage, da er sich nur mit viel Mühe exkulpieren kann. Zum Beispiel bekommen nicht selten Personen mit demselben oder einem ähnlichen Namen wie ein Eingetragener fälschlicherweise die für diesen vorgesehenen Sanktionen zu spüren. Den vollziehenden Dritten stehen meist nicht genug Informationen zur Verfügung, um die Identität des Betroffenen festzustellen und von der Identität des Eingetragenen unterscheiden zu können. Diese Systemlücke schafft eine grosse Nachfrage nach professionellen Überprüfern und somit ein weiteres Feld im Bereich der Kriminalitätsbekämpfung, das der Privatisierung anheimfällt, weil die Vorgaben ansonsten schlicht nicht zu bewältigen wären.[599]

---

598 Bericht HRW, S. 116 f.; OPPAGA 2012, S. 1 und 6.

599 Siehe zum Ganzen KOCHER, S. 104 f.; BIANCHI, S. 897 f. Ein Verwechslungsfall ereignete sich im Jahr 2005 bspw. auch in Deutschland: Das Arbeitsamt resp. die Postbank (sie schoben sich die Verantwortung für die Verwechslung gegenseitig zu) zahlte Mohammed H. irrtümlicherweise kein Arbeitslosengeld mehr aus, weil er bei einem Listenabgleich angeblich

Dieses praktische Problem besteht auch bei anderen Datenbanken[600]; auch bei der öffentlichen UN-Terrorliste, wobei die Qualität der Einträge des Sanktionsregimes durch verschiedene Vorkehrungen über die Jahre verbessert werden konnte.[601]

Wo diese Schwachstellen mehr konzeptueller Natur sind, fallen bei Online-Überwachungstechnologien deren noch unausgereifte technische Architektur und eingebaute Kontrollmechanismen negativ auf. Die aus rechtlicher Sicht grundsätzlich positive Einschätzung der Govware und DPI im Strafverfahren kontrastiert stark mit deren praktischen Problemen. Können diese zukünftig nicht gelöst werden, ist die rechtliche Zulässigkeit jener Massnahmen in vielen Punkten zu relativieren. Deren technisch scheinbar schwer begrenzbare Fähigkeiten sind mit geeigneten rechtlichen Vorkehrungen einzuschränken.[602] Die heutigen Programme scheinen nicht in der Lage oder deren Benutzer nicht willens zu sein, sich streng auf definierte Ziele (vorbestimmte Datenbestände, Beschränkung auf die Überwachung der Kommunikation) zu fokussieren. Der überschiessende Funktionsumfang dieser Technologie besitzt eine hohe Missbrauchsgefahr. Er kann zudem dazu führen, dass unbeabsichtigt Funktionen eingesetzt werden, die von der gesetzlichen Ermächtigungsgrundlage respektive der Genehmigung im Einzelfall nicht gedeckt sind.[603] Der Übergang zwischen einer Ermächtigung, die Kommunikationsinhalte und Randdaten mittels Govware zu überwachen, und einer unzulässigen Online-Durchsuchung/-überwachung ist zudem fliessend[604], was im Zusammenhang mit der vorgesehenen Norm von E-Art. 269ter StPO zu berücksichtigen ist, um ansonsten in der Praxis vorprogrammierten Abgren-

als Registrierter identifiziert worden war. Siehe ausführlich zu diesem und ähnlichen Fällen MEYER/MACKE, S. 449.

600 Siehe etwa die Vorkommnisse in Grossbritannien bei NORRIS, S. 153, in dem falsche Auskünfte über ihre Vorbestrafung dazu führten, dass Betroffenene bei Bewerbungen um Arbeitsstellen abgelehnt wurden.

601 Siehe SCHULTE, S. 53 mit Beispielen.

602 GLESS 2012, S. 12 und 17 f.; Botschaft BÜPF 2013, S. 2775. Analog der intelligenten Videoüberwachung, siehe unten Zweiter Teil, Kapitel II.C.

603 BRAUN, S. 683; BUERMEYER/BÄCKER, S. 439; ALBRECHT F., N. 17; GLESS 2012, S. 12 und 18. Insbesondere wird durch die Technik nicht verhindert, dass die anwendende Behörde über die im Voraus bezeichneten Datenarten oder Bestände hinaus Daten durchsieht. Das Handeln der Behörden in der Sache des Urteils des Landesgerichts Landshut 4 Qs 346/10 vom 20. Januar 2011 bestätigt, dass bei manchen Beteiligten durchaus die Bereitschaft besteht, von übergeordneten Instanzen vorgegebene Rahmen nicht zu beachten. Siehe auch SIMON D., S. 255 ff. hinsichtlich der Speicherung von Vorratsdaten.

604 Vgl. ALBRECHT F., N. 6.

zungs- und Beurteilungsproblemen vorzubeugen. Ähnlich entgrenzend wirken bei neuen Technologien, wie etwa der DPI, die technischen Unzulänglichkeiten, Randdaten, Inhaltsdaten etc. zuverlässig auseinander halten zu können, also beispielsweise *ausschliesslich* Randdaten zu erfassen, während in den rechtlichen Grundlagen oft davon ausgegangen wird, dass dies stets möglich sei.[605] Abgesehen von diesem technischen Problem, können Randdaten in ihrer Kombination zuweilen genauso aussagekräftig sein wie Inhaltsdaten. Verbindungsdaten lassen oft Rückschlüsse auf die Person oder auf ein zukünftiges Verhalten der Person zu, da sich die Verbindungsnummern in der Regel klar einer Firma, einer Person oder einem Dienst zuordnen lassen. Aus einem Anruf beim spezialisierten Arzt, vielen Gesprächen in kurzer Zeit mit einer Person aus dem nahen Umfeld, den von mobilen Internetgeräten benutzten IP-Adressen der jeweiligen Hot-Spots oder aus mobilen Transaktionsdiensten (zum Beispiel Entrichtung von Parkgebühren) lassen sich viele grundsätzlich nützliche Hypothesen auf- und allenfalls auch Persönlichkeits- und Bewegungsbilder erstellen.[606]

Im bisherigen Einsatz der Govware traten ferner einige andere Problempunkte im Bereich der Datensicherheit auf, die auch in der Vernehmlassung zur Revision des BÜPF teilweise vorgebracht wurden.[607] Zunächst muss die über Netzwerke zu installierende Govware aktuelle Schutzvorrichtungen umgehen können. Diese zu überlisten dürfte ohne Mithilfe und Kooperationsbereitschaft der Hersteller dieser Schutzprogramme (zum Beispiel, indem diese bewusst Lücken für staatlich eingesetzte Spähprogramme offen lassen) auf lange Sicht eine gewisse Hürde darstellen.[608] Sollte es trotzdem gelingen, fragt sich zudem, inwieweit gewährleistet werden kann, dass das legitim als behördliches Werkzeug eingesetzte

---

605 COOPER, S. 144; PFITZMANN/KÖPSELL 2009a, S. 543; FREILING/HEINSON, S. 550 f.; LSE Briefing, S. 5 und 13-16, 22 und 35; ROSSNAGEL/BEDNER/KNOPP, S. 537 f.; OBERHOLZER 2004, S. 59.

606 PFITZMANN/KÖPSELL 2009A, S. 543 f.; LSE Briefing, S. 56; FREILING/HEINSON, S. 551 f.; HENSEL, S. 528 ff.; ROSSNAGEL, S. 1239; SIMON D., S. 227 ff. und 259; ZIMMER, S. 216 mit weiteren Hinweisen. Einige interessante Beispiele, insbesondere zu den Transaktionsdiensten, finden sich bei KURZ/RIEGER, S. 30-35. Vgl. bspw. auch den Internetdienst <www.maxmind.com>, mit dessen Hilfe IP-Adressen ungefähren geografischen Standorten zugerechnet werden können.

607 Siehe zum Folgenden insbesondere: Botschaft BÜPF 2013, S. 2773 ff.; die Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF, S. 55-59; BVerfGE 120, 274; BIERMANN in Zeit Online vom 10. Oktober 2011.

608 Besonders, da publik wurde, dass Staaten Govware einzusetzen bereit sind. Vgl. BUERMEYER, S. 158 zum „Schutzkonzept" von Virenscannern.

Programm, das im Kern ein potentes Schadprogramm bleibt (von Virenscannern schwer erkennbar, erlaubt kompletten Fernzugriff auf fremde Systeme), sich nicht (unkontrolliert) weiter ausbreitet oder nicht in falsche Hände gerät. Anstatt fremde Rechtsgüter zu schützen, würden dadurch allenthalben nicht zu unterschätzende Gefahren für solche geschaffen.[609] Das scheint offenbar nicht zu gelingen, konnte doch die Architektur einer bereits angewendeten Version der Govware nicht unter Verschluss gehalten werden.[610] Nicht auszuschliessen ist weiter, dass die Zielperson die entdeckte Govware gegen die Ermittlungsbehörde einsetzt, indem sie etwa bewusst täuschende Informationen übermittelt oder die Übertragung dazu nutzt, die Systeme der Ermittlungsbehörde zu infiltrieren.[611]

Grosse Probleme ziehen weiter Versionen des Staatstrojaners nach sich, welche die Datenübertragung und die von ihnen für die Behörde verursachte Sicherheitslücke im infizierten System nicht ausreichend gegen den Zugriff Unbefugter absichern. Die vor kurzem eingesetzte Govware in Deutschland (die Schweizer Behörden bezogen die Govware vom selben Anbieter) erfüllt diese Bedingung nach Einschätzung des Chaos Computer Clubs (CCC) nicht. Die von ihm untersuchten Versionen verfügten über unzureichende Verschlüsselungen bei der Datenübertragung; die Kommandos von der Steuerungssoftware an den Staatstrojaner über gar keine.[612] Das ist rechtlich insofern sehr bedenklich, als Unbefugte erstens übertragene Daten abfangen, zweitens übertragene Daten verändern oder drittens über die vom Staatstrojaner eröffneten Sicherheitslücken in das infizierte System eindringen können.

Unbefugte können durch diese Schwachstellen Kenntnis von den Metadaten (zum Beispiel wer Ziel der Überwachung war) oder vom Inhalt der Überwachung erhalten oder sich (unrechtmässig) Zugriff darauf verschaffen. Es ist

---

609 BRAUN, S. 684; Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF, S. 58; BVerfGE 120, 274 (325 f.); Artikel „Chaos Computer Club analysiert aktuelle Version des Staatstrojaners" des CCC vom 26. Oktober 2011 und CCC Analyse Teil 2. Diese Befürchtung halten im Gegensatz dazu im Rahmen der Vernehmlassung der BÜPF-Revision kontaktierte Fachleute aus dem Polizeibereich für unbegründet, siehe Botschaft BÜPF 2013, S. 2772. Vgl. auch sehr ähnlich Plenarprotokoll 17/132 des Deutschen Bundestages vom 19. Oktober 2011, S. 15604.

610 Siehe die CCC Analyse (inkl. offen gelegtem Quellcode). Das ist nicht besonders verwunderlich, wenn man bedenkt, wie viele Akteure, davon insbesondere auch solche aus der Privatwirtschaft, am Einsatz beteiligt waren und dass die Govware selbst immer auch Datenspuren hinterlässt und somit von kundigen Nutzern entdeckt und verwendet werden kann.

611 Siehe HANSEN/PFITZMANN.

612 Siehe CCC Analyse, S. 3 ff.; ebenso CCC Analyse Teil 2. Vgl. BRAUN, S. 684.

weiter nicht ausgeschlossen, dass die Daten unterwegs verändert werden, beispielsweise veranlasst durch unbefugte Zugreifer oder auch ohne Zutun durch Software-, Kopier- oder Übertragungsfehler.[613] Die Behörde verbindet sich nicht über eine direkte Leitung mit dem Zielcomputer. Der Kanal zwischen Behörde und Zielcomputer geht über (mehrere) Provider, Server und, falls die Anbieter der Govware in das Prozedere eingebunden sind, was bei den bekannten Fällen oft so gewesen zu sein scheint, durch die Hände Privater. Überwachungen, die über externe (private) Dienstleister durchgeführt werden, sind insbesondere dann ein Problem, wenn sie die gesammelten Daten auf Server im Ausland übertragen[614] oder die Übertragungssicherheit nicht in einem äusserst hohen Mass gewährleisten können.[615]

Ein interessanter Aspekt sind auch die Integrität des Zielsystems sowie dessen Schutzmechanismen.[616] Ohne staatlichen Behörden unlautere Machenschaften bei der Beweisgewinnung unterstellen zu wollen – alleine aus dem behördlichen Eindringen und Infizieren des Zielsystems können der Integrität dieses Systems gewisse Bedenken anhaften.[617] Das System scheint nicht besonders beziehungsweise nicht ausreichend gesichert (gewesen) zu sein. Diese Sicherheitslücke könnten Dritte ausgenutzt haben.[618] Neben den Behörden könnten Dritte sich des Systems bemächtigt oder es manipuliert haben. Hypothetisch könnten folglich Dritte die dem Besitzer des Systems zur Last gelegten Delikte begangen und die entsprechenden (fehlleitenden) Spuren auf seinem Computer hinterlassen haben. Fraglich ist, ob darauf gestützt gewonnene Beweise genuin belastet sind, weil hypothetisch die Möglichkeit der Manipulation bestand oder durch die Govware

---

613 HEIMGARTNER, S. 36; Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF, S. 58; BVerfGE 120, 274 (325 f.).

614 In den genannten Praxisfällen scheinen die Daten u. a. auf einen Server in den USA übertragen worden zu sein, was aus Datenschutzgründen ein zusätzliches Problem darstellen kann. Siehe dazu BRAUN, S. 682 und 684; CCC Analyse, S. 6; BUERMEYER/BÄCKER, S. 440.

615 Vgl. analog THORMANN/BRECHBÜHL, N. 1 zu Art. 246 StPO. Das betrifft insofern die Vertraulichkeit des Zielsystems, siehe BVerfGE 120, 274 (314).

616 Siehe dazu BVerfGE 120, 274 (314).

617 Die Authentizität der durch die Govware gewonnenen Daten kann nicht ausreichend gewährleistet werden, siehe PLATZ, S. 841.

618 BVerfGE 120, 274 (325 f.); CCC Analyse, S. 6; TSCHENTSCHER, S. 384. Analog verdeutlicht das Szenario die Problematik dieses Punkts, in dem bei einer heimlichen Durchsuchung einer Wohnung die Behörde versäumte, die Türe anschliessend wieder zu verriegeln und ein Dritter dies – ohne Wissen des Besitzers – ausnutzte, um entweder Gegenstände aus der Wohnung zu entfernen oder kompromittierende Beweise zurückzulassen, die bei einer zweiten Durchsuchung von den Behörden aufgefunden werden. Vgl. GLESS 2012, S. 21.

ermöglicht wurde. So scheinen zum Beispiel informatikkundige Kriminelle ihre heiklen Daten häufig auf fremden Systemen zu lagern oder zwischenzuspeichern – man denke an Bot-Netze oder an die Fremdbenutzung des verschlüsselten Arbeitscomputers durch einen Mitarbeiter, der das fremde Passwort in Erfahrung gebracht hat.[619]

E. Vorfeldermittlungen, Verdachtsschwellen und Verdachtsausweitung

Der Anlassgrund des Einsatzes einer präventiv-polizeilichen Massnahme kann sowohl eine konkrete als auch abstrakte Gefahr sein. Konkret ist eine Gefahr in der Regel, wenn der Schadenseintritt im Einzelfall mit einer gewissen Wahrscheinlichkeit zu erwarten ist (zwischen „irgendwann in überschaubarer Zukunft" und „in naher Zukunft", je nach Ansicht in Literatur und Rechtsprechung). Die Qualität der abstrakten Gefahr zeigt sich nicht in einer tatsächlichen Gefahr, sondern einer hypothetischen.[620] Die präventive Gefahrenabwehr operiert häufig im Vorfeld und ohne näher konkretisierte Verdachtsmomente. Das soll sie grundsätzlich dürfen, sie soll nicht immer akute Gefahrenlagen abwarten müssen.[621] Daraus ergibt sich jedoch nicht, dass sich jedwelche Variante postmoderner Kriminalitätsbekämpfungstechnologien dafür eignet, in diesem Umfeld präemptiven Handelns eingesetzt zu werden. Oftmals bedürfen diese entweder einer Konkretisierung und Eingrenzung des Gefahrengegenstands oder alternativ anderer begrenzender Prinzipien, um rechtlich zulässig eingesetzt werden zu können. Sie können alle auch ohne konkreten Anlass, konkreten Verdacht oder konkreten Anknüpfungspunkt verwendet werden, entfalten aber speziell in diesen Fällen äusserst breite Streuwirkungen, was die Gesamteingriffsqualität der Massnahme, die je nach Konstellation ohnehin bereits durch nicht unerhebli-

---

619 Vgl. zu dieser Schwachstelle die Äusserungen von Denis Simonet im Artikel „Trojaner passen nicht zu einem Rechtsstaat" in Tages-Anzeiger Online vom 14. Oktober 2011. Siehe auch PFITZMANN/KÖPSELL 2009a, S. 545; HANSEN/PFITZMANN; Andreas Pfitzmann bei KREMPL in heise Online vom 3. August 2007.

620 SCHWEIZER/SUTTER/WIDMER, S. 82 und 83 jeweils mit Hinweisen. Vgl. SIMON D., S. 262; THIEL, S. 51 f. und 65; BVerfGE 120, 274 (328 f.): „Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zukunft ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird."

621 ZERBES, S. 253, 255 und 261. Zur Verdachtsbindung im Strafverfahren: DIES., S. 325 ff.

che Eingriffe für den Betroffenen hoch sein kann, durch Eingriffe bei vielen Nicht-Störern stark erhöhen kann.[622]

Polizeiliche Massnahmen haben grundsätzlich das Störerprinzip zu beachten. Von diesem Prinzip darf in der Regel erst abgewichen werden, wenn es eine akute Gefahr zu beheben gilt.[623] Gemäss Auslegung des schweizerischen Störerprinzips durch den EGMR darf die präventive Gefahrenabwehr, sofern sie in Grundrechte eingreift, ausschliesslich zielgerichtet und lediglich ausnahmsweise gegen unbeteiligte Dritte eingesetzt werden.[624] Das Prinzip, in dieser Weise verstanden, könnte beispielsweise dem Einsatz einiger Varianten der öffentlichen Raumüberwachung durch Videokameras widersprechen[625], indem es sie unverhältnismässig werden lässt, sobald das entsprechende System nicht nur leicht in die Rechte der Unbeteiligten eingreift und keine akute Gefahr vorliegt. Angesichts dieser Rechtsprechung des EGMR kann ausschliesslich ein sehr begrenzter Anwendungsbereich der Videoüberwachung vom Störerprinzip ausgenommen sein, da die Videoüberwachung in den meisten Fällen einen stark präventivpolizeilichen Charakter aufweist, welchen sie nur schwerlich vermeiden kann.[626] Wo sie eine grosse Anzahl an Personen betrifft, steigt die Wahrscheinlichkeit, dass zumindest einige davon völlig unverdächtig sind (Nicht-Störer).[627] Ob an neuralgischen Kriminalitätsschwerpunkten (zu einer bestimmten Zeit) eine gegenwärtige, konkretisierbare Gefahr angenommen werden kann, muss daher im Einzelfall abgewogen werden. Die Konstruktion einer akuten Gefahr an öffentlichen Orten über die Schwere einer rein hypothetischen oder unwahrscheinlichmöglichen Bedrohung, mithin begründet über abstrakte Argumente, scheint hingegen nicht haltbar.[628]

---

622 PETRI, G N. 53 f.; ZERBES, S. 43; ZIMMER, S. 211 f.; BVerfGE 115, 320 (354 f.); 125, 260 (318 f.). Indes zu beachten BGE 133 I 77 E. 5.3 S. 85: Der *individuelle* Grundrechtseingriff wiegt nicht „schwerer, weil eine grosse Anzahl von Personen betroffen ist".

623 Siehe dazu HÄFELIN/MÜLLER/UHLMANN, S. 569 ff. und 575. Vgl. PETRI, G N. 524 und 562; SIMON D., S. 101.

624 Vgl. weiter oben in der Einleitung, Kapitel IV.A.

625 Wobei die folgenden Ausführungen analog auf andere postmoderne Kriminalitätsbekämpfungstechnologien übertragen werden können.

626 Gl. A. wie BÜLLESFELD 2002, S. 87 ff. A. A. ist bspw. ROGGAN 2001, S. 139.

627 Insofern ist in erster Linie zu berücksichtigen, wie intensiv und wie grossräumig überwacht wird. Gl. A. wie MÜLLER L. 2011, S. 141 f. Vgl. BÜLLESFELD 2002, S. 80 und S. 102 f.

628 Im Kern gl. A. wie BARTSCH, S. 211, welche „tatsächliche Anhaltspunkte für die Begehung von Straftaten" und eine „deutlich überdurchschnittliche" Straftatenhäufung im überwach-

Auch bei anderen technischen Methoden reicht eine allgemeine Bedrohungslage in der Regel nicht aus, deren Einsatz im Vorfeld einer nicht näher konkretisierten Gefahr zu rechtfertigen. Konkrete Tatsachen sollten für eine hinreichend wahrscheinliche Gefahr sprechen.[629] Verdachtsforschung soll, vor allem, wenn die Ergebnisse in anschliessenden Strafverfahren verwendet werden sollen, tunlichst vermieden werden.[630] Dass derartige Beschränkungen in diesem Gebiet jedoch nicht immer ganz einfach vorzunehmen sind, lässt sich anhand zweier jüngerer Beispiele aus der Rechtsprechung des deutschen Bundesverfassungsgerichts verdeutlichen: Um der präventiv-polizeilichen Rasterfahndung einen entsprechenden rechtlichen Rahmen vorzugeben, sahen die Bundesländer in Deutschland üblicherweise, neben anderen einschränkenden Regelungen, eine *gegenwärtige* Gefahr als Bedingung der Durchführung vor.[631] An sich wäre damit eine qualifiziert konkrete, akut drohende Gefahr gemeint gewesen. Mit der dramatisierten, scheinbar vollkommen neuen Bedrohungslage nach den Anschlägen vom 11. September 2001 indessen wurde diese Schranke teilweise relativiert. Einige Gerichte stellten fortan nurmehr geringe Anforderungen an die Gegenwärtigkeit der Gefahr. Sie zogen das hohe Schutzgut und den zu erwartenden enormen Schaden als Surrogate für die Bedingung des zeitnahen Eintritts der Gefahr bei.[632] Am Beispiel dieser Auslegungsvarianten wird die Schwierigkeit einer sorgfältigen und auf Notfälle begrenzten Verwendung der sicherheitspolizeilichen Rasterfahndung und allgemeiner das den dargestellten postmodernen Kriminalitätsbekämpfungsinstrumenten inhärente Entgrenzungspotenzial ersichtlich. Den Einsatz der *präventiv-polizeilichen* Rasterfahndung von einer restriktiv verstandenen Bedingung der konkreten, gegenwärtigen Gefahr abhängig zu machen, hiesse, ihr praktisch keine denkbaren Anwendungsfälle zu überlassen. Sie kann nur ausnahmsweise nicht gefahrenforschend tätig sein und braucht zudem eine gewisse

ten Gebiet für die Qualifikation eines Kriminalitätsschwerpunkts voraussetzt. Ein wenig offener sieht dies BÜLLESFELD 2002, S. 102 und 107. Ähnlich MÜLLER L. 2011, S. 263 f.

629 BVerfGE 115, 320 (Leitsätze 1 und 2); KUTSCHA, S. 1043 f.; ROGGAN 2009, S. 262; RUDIN, S. 281; MEYER, S. 76 f.; SCHULTE, S. 330.

630 Siehe etwa BGE 129 II 462 E. 5.3; 1A.49/2007 E. 5.1; Botschaft StPO, S. 1216; MÜLLER L. 2011, S. 161 und 276 f.; ROGALL, S. 624.; ZERBES, S. 338.

631 Siehe ZSCHOCH, S. 191 ff.; ROGALL, S. 634 f.

632 Siehe dazu KUBE, S. 56 ff.; BVerfGE 115, 320 (321 ff.).

Anlaufzeit, die den rechtzeitigen Einsatz in Fällen *akuter* Gefahren meist vereiteln dürfte.[633]

Ähnlich hatte das Bundesverfassungsgericht im Rahmen seines Urteils BVerfGE 120, 274 über Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen zu befinden. Diese sollten die Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen insbesondere aus informationstechnischen Systemen und den Umgang mit den erhobenen Daten regeln.[634] Das Bundesverfassungsgericht befasste sich eingehend mit Faktoren, die die Intensität der Grundrechtseingriffe durch den Einsatz von Govware einschätzen lassen:

1. Die staatliche Datenerhebung aus komplexen Systemen berge bereits bei einmaligen und punktuellen Zugriffen ein „beträchtliches Potential" zur Ausforschung der Persönlichkeit des Betroffenen.[635]
2. Der Eingriff sei als besonders schwer zu qualifizieren, wenn eine längerfristige Überwachung die laufende Erfassung von Daten und ein Nutzungsprofil des Betroffenen ermögliche.[636]
3. Die Heimlichkeit der Massnahme und die Streubreite des Programms intensivierten den Eingriff.[637]

---

633 BVerfGE 115, 320 (363) und das kritische Minderheitsvotum der Richterin Haas (S. 376 ff.); ZSCHOCH, S. 209; SIMON D., S. 166 f.; VOLKMANN; S. 220; THIEL, S. 247 f. mit weiteren Hinweisen. Zur Kritik der Interpretation der „gegenwärtigen Gefahr" in diesem Urteil des BVerfG, siehe PETRI, G N. 42.

634 BVerfGE 120, 274 (275). Das Bundesverfassungsgericht befand die zu beurteilenden Vorschriften des Verfassungsschutzgesetzes für unvereinbar mit dem Grundgesetz und somit nichtig.

635 BVerfGE 120, 274 (322 ff.): Damit werde ein Datenbestand zugänglich, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen könne, das naheliegende Risiko einer Gesamtschau auf die betroffene Person (weitreichende Rückschlüsse bis hin zu Verhaltens- und Kommunikationsprofilen) geschaffen, die Gelegenheit der Bürger an einer unüberwachten Fernkommunikation teilzunehmen beschränkt und eine beträchtliche Streubreite der Überwachung und des Eingriffs auf notwendigerweise einbezogene Dritte in Kauf genommen habe.

636 BVerfGE 120, 274 (323 ff.): Damit würden flüchtige Daten erfasst, möglicherweise auf weitere sensible Daten zugegriffen, die Rückschlüsse auf Vorlieben, persönliche Verhältnisse und Kommunikationsgewohnheiten des Betroffenen zuliessen, und durch das Umgehen von Verschlüsselungstechniken der informationelle Selbstschutz des Betroffenen vereitelt.

637 BVerfGE 120, 274 (325 f.): Es würden dadurch Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch Dritter begründet (bspw. könnten

Im Ergebnis kam es zum Schluss, der polizeilich-präventive Einsatz von Govware könne einen derart schwerwiegenden Grundrechtseingriff bedeuten, dass er, eine gesetzliche Grundlage vorausgesetzt, lediglich sehr zurückhaltend in Betracht zu ziehen wäre. Es mahnte namentlich, dass, sollen informationstechnische Systeme mit Govware infiltriert werden, einerseits mindestens zu erwarten sein müsse, dass dadurch bestimmte Informationen gewonnen werden können und andererseits, dass eine konkrete Gefahr absehbar drohe. Unausgereifte Hypothesen oder Vermutungen genügten nicht. Darüber hinaus müssten „geeignete Verfahrensvorkehrungen" zugunsten des Betroffenen gewährleistet werden.[638]

Das Potenzial der Eingriffsintensität und die technischen Gegebenheiten von Govware verlangen demnach eine ziemlich akute, konkrete Gefahr und eine Eingrenzung auf möglichst eine Zielperson und ein Zieldatenverarbeitungssystem vor dem Einsatz, nicht auf einen grösseren Personenkreis mit mehreren Systemen. Es dürfte aber vor allem im präventiv-polizeilichen und nachrichtendienstlichen Bereich aufgrund der kaum zu vermeidenden Streubreite der Überwachungstechnologien schwer sein, private und geschäftliche Geheimnisse zu wahren.[639]

Tiefe Anlassschwellen in einigen Bereichen der Gefahrenabwehr mögen zwar durchaus legitim sein. Nach Ansicht des Bundesgerichts sind unbestimmte Normen im Bereich der Polizeiaufgaben denn auch notwendig, damit polizeiliches Handeln flexibel an die jeweils vorherrschenden Situationen angepasst werden könnten.[640] Die Gefahr hinsichtlich der postmodernen Kriminalitätsbekämp-

Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen – einen „rein lesenden Zugriff infolge der Infiltration" gebe es nicht), was „den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen" könne. Ähnlich BVerfGE 115, 320 (354 ff.) zur Rasterfahndung.

638 BVerfGE 120, 274 (322). Gemäss Ansicht des BVerfG, „entspricht [dieser Grundrechtseingriff] im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt" (326). Dazu hielt es weiter fest: „Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen Tatsachen festgestellt sein, die eine Gefahrenprognose tragen […]" (328).

639 Vgl. BIAGGINI, S. 267.

640 BGE 136 I 87 E. 3.1 S. 90 f.

fungstechnologien besteht aber darin, dass sich zum Beispiel basierend auf anlasslosen Datensammlungen und nahezu verdachtsunabhängigen Datenbanken, die vielleicht keine (schwerwiegenden) Folgemassnahmen vorsehen, Einträge in andere Datenbanken und Register, die solche Folgemassnahmen vorsehen, veranlasst werden könnten. Ein *verdachtsschwacher* Eintrag kann dadurch, eventuell in Kombination mit anderen Einträgen in ähnlichen Datenbanken oder mit anderen vagen Verdachtsindizien, unbegründete oder unverhältnismässige Konsequenzen in die Wege leiten. Tatsächlich dürfte der Verdacht hingegen je schwächer, abstrakter und schwerer nachprüfbar werden, desto mehr dieser Schritte er durchläuft (falls nicht bei jedem Schritt eine sorgfältige Beurteilung vorgenommen wird), da der Anlassgrund zum Ersteintrag immer weiter in die Ferne rückt.[641] Eindrücklich zeigt sich dieses Problem beim Informationssystem HOOGAN: Polizeiliche Massnahmen der Gefahrenabwehr gestützt auf das BWIS und das Hooligan-Konkordat werden auf Anzeichen hin getroffen.[642] Die Anforderungen an das Beweismass sind dementsprechend deutlich tiefer als etwa im Strafverfahren[643]; so erfordert ein Eintrag in das Informationssystem HOOGAN keinen förmlichen strafprozessualen Beweis.[644] Als Grundlage der Eintragung reichen bereits glaubhafte Meldungen etwa von Stadionbesitzern aus.[645] Diese gesetzliche Regelung ist im Lichte des Erfordernisses eines qualifizierten Verdachts für die staatliche Bearbeitung von Daten und der Intensität des Grundrechtseingriffs bei der Verhängung von darauf basierenden Massnahmen nicht unbedenklich.[646] Auch die Eintrittsschwellen bezüglich der Anlassdelikte insbesondere in der revidierten Fassung des Hooligan-Konkordats sind tief. Bereits geringfügige Formen von gewalttätigem Verhalten und Gewalttätigkeiten reichen aus, solange der, wiederum definitionsbedürftige, Anknüpfungspunkt

641 Siehe dazu etwa den Bericht GPDel hinsichtlich ISIS.

642 Urteil des Bundesgerichts 1C.278/2009 vom 16. November 2010 E. 5.2 und 6.4. Ebenso Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 5.5 und 6.2.2. Vgl. den Wortlaut von Art. 24c Abs. 1 lit. a und b sowie Abs. 2 BWIS („nachweislich"; „angenommen werden muss"; „die Annahme begründen").

643 Urteil des Verwaltungsgerichts des Kantons St. Gallen B 2009/81 vom 22. September 2009 E. 3.1; HENSLER, S. 40.

644 Botschaft BWIS 2005, S. 5629; Urteil des Bundesgerichts 1C.88/2011 vom 15. Juni 2011 E. 3.5; Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 5.5 und 6.2.2. Eine rechtskräftige Verurteilung als Voraussetzung wurde im Nationalrat verworfen, siehe AB 2005 N 1944 ff. Vgl. zum Ganzen MOECKLI/KELLER, S. 239.

645 Siehe Art. 16 lit. c Bearbeitungsreglement HOOGAN.

646 SCHEFER, S. 63. Vgl. TROCHSLER-HUGENTOBLER/LOBSIGER, S. 334; STUDER, S. 67.

„im Vorfeld einer Sportveranstaltung […] oder im Nachgang dazu" erfüllt ist. Diese Anlassdelikte erfahren dadurch eine schwer begründbare Qualifizierung gegenüber ihren ohne diesen Bezug begangenen Pendants, und den anwendenden Behörden wird durch die offene und unbestimmte Formulierung „ein zu weites Tatbestands- und Rechtsfolgeermessen" eingeräumt.[647] Ob diese vagen Begrifflichkeiten durch verfahrensrechtliche Garantien und durch eine besondere Bedeutung des Verhältnismässigkeitsprinzips angemessen kompensiert werden können, darf erst einmal bezweifelt werden.[648]

F. Verwaltungsrechtliche Massnahmen und rechtsstaatliche Vorkehrungen

Bei den Massnahmen gegen gewaltbereite Störer gestützt auf das BWIS oder das Hooligankonkordat handelt es sich gemäss den entsprechenden Materialien um präventive, verwaltungsrechtliche Massnahmen.[649] Dieser Einschätzung schlossen sich Bundesgericht und Bundesverwaltungsgericht an und sprachen diesen Massnahmen keinen strafenden Charakter zu.[650] Ähnlich qualifiziert der UN-Sicherheitsrat die Sanktionen der UN-Terrorliste als rein administrativer Natur.[651] In der Konsequenz unterstehen die Massnahmen den kantonalen Ver-

---

647 Gl. A. wie MÜLLER J.O., S. 111 ff.

648 So aber das Bundesgericht in BGE 136 I 87 E. 3.1 S. 90 f. und im Urteil 1C.278/2009 vom 16. November 2010 E. 6.4.

649 Botschaft BWIS 2005, S. 5614 und 5626; Bericht KKJPD, S. 4 f.

650 BGE 137 I 31 E. 4.3 S. 42 („Sie weisen keinen pönalen, repressiven Charakter auf, werden nicht wegen Erfüllung von Straftatbeständen ausgesprochen und bezwecken nicht die Besserung der betroffenen Person."); Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 4.3. Ebenso Urteil des Bundesgerichts 1C.278/2009 vom 16. November 2010 E. 3.3 und 4.2 sowie bereits BGE 134 I 125 E. 4.1 S. 136 f.; Urteil des Verwaltungsgerichts Zürich VB.2008.00237 vom 19. Juni 2008 E. 4.3; MOECKLI/KELLER, S. 241; HENSLER, S. 40 ff.; NUSSBAUMER, S. 147; DAENIKEN, S. 57. M. E. zutreffend kritisch WERDER, S. 251 f., der insb. die unklare Terminologie und oberflächliche Beurteilung der Massnahmen durch das Bundesgericht beanstandet und MÜLLER J. O., S. 112 f. mit Beispielen, der diesen Massnahmen mindestens teilweise pönalen Charakter zuspricht. Subjektiv jedenfalls scheinen diese Massnahmen in der Öffentlichkeit überwiegend als strafend wahrgenommen und von den Betroffenen nur selten als „Nicht-Strafe" akzeptiert zu werden, siehe dazu HENSLER, S. 41 f. und zustimmend MÜLLER J. O., S. 113. Weiterführend zur Natur verwaltungsrechtlicher Sanktionen und zu den Folgen eines pönalen Charakters, siehe JAAG und HÄNER.

651 Siehe dazu SCHULTE, S. 68; SULLIVAN/HAYES, S. 28 und 82 ff.; MEYER, S. 76. M. E. zutreffend kritisch MEYER, S. 78; SULLIVAN/HAYES, S. 82 ff.; EMMERSON, N. 54-58; CHESTER-

waltungsverfahren oder den Verfahren eines politisierten Sanktionsregimes. Strafrechtliche und strafprozessuale Prinzipien (insbesondere die Unschuldsvermutung und Informationspflichten) gelten für den Betroffenen nicht, wenn die verwaltungsrechtliche Massnahme keinen pönalen Charakter aufweist.[652] Das kann zu unbefriedigenden Auswirkungen führen: Problematisch können beispielsweise Situationen sein, in denen aufgrund der Einträge in Verdachtsregister weitere Anstalten gegen die gelistete Person oder ihr Umfeld getroffen werden, das heisst wenn etwa Stadionbesitzer, Klubs etc. gestützt auf den ihnen zugänglichen HOOGAN-Eintrag zusätzliche private Massnahmen ergreifen (zum Beispiel Stadionverbote aussprechen)[653] oder wenn staatliche Behörden den Eintrag in einem Verdachtsregister als dringenden Tatverdacht für Überwachungsmassnahmen (beispielsweise den Einsatz von Govware) gegen den Betroffenen oder sein Umfeld heranziehen.[654] Das gilt insbesondere, wenn ein Eintrag beispielsweise aufgrund eines von einem privaten Stadionbesitzer ausgesprochenen Stadionverbots wegen Bagatellen ohne Zusammenhang zu gewaltätigem Verhalten vorgenommen wurde[655] oder wenn der Eintrag auf vagen nachrichtendienstlichen oder unzureichenden Informationen[656] basiert. Daraus können sich unter anderem verwechslungsanfällig Einträge und Verdachtszirkelschlüsse ergeben, die vom Betroffenen schwer auszuräumen sind.[657] Zudem ist auch zu fragen, was mit dem Eintrag und den darauf gestützt präventiv angeordneten Massnahmen geschehen soll, wenn ein parallel laufendes Strafverfahren in der gleichen Sache mit einem Freispruch endet oder beispielsweise mangels Beweisen eingestellt

MAN, S. 187 jeweils mit Hinweisen. Insbesondere die Voraussetzung der zeitlichen Beschränkung erfüllen die Sanktionen in der Praxis nicht.

652 Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 4.3; Urteil des Verwaltungsgerichts Zürich VB.2008.00237 vom 19. Juni 2008 E. 4.3; MÜLLER J. O., S. 112; MEYER, S. 77 f.; HÄNER, S. 22 ff. und 39 f.; NIGGLI/RIEDO, S. 52 ff. mit Hinweisen auf die Rechtsprechung des EGMR.

653 HENSLER, S. 44. A. A. SOÒS/VÖGELI, S. 161, welche diesen Punkt positiv bewerten.

654 BARTMANN, S. 121 ff. und 126; MEYER/MACKE, S. 449 f.;

655 Was bspw. gestützt auf Art. 3 Abs. 1 lit c. des revidierten Hooligan-Konkordats möglich wäre, siehe MÜLLER J. O., S. 115 f., der als Bsp. ein privates Stadionverbot wegen Urinierens oder Einführens einer Bierdose ins Stadion nennt. Ebenso ENGLER, S. 166; KLEINER, S. 45 f.

656 Zur Kritik an der diesbzgl. extensiven Erfassungspraxis des ISIS in den letzten Jahren, siehe Bericht GPDel, S. 7679, 7685 und 7692.

657 ENGLER, S. 166; KLEINER, S. 45 ff.; MOHLER 2008, S. 90 f. Vgl. auch den Fall A. L. im Bericht GPDel, S. 7692 ff.

wird.[658] Zu fordern scheint mindestens, dass die Behörde, welche die Präventivmassnahme und den Eintrag in das Register angeordnet hat, über den Ausgang des Strafverfahrens zu informieren ist, damit sie die (rechtskräftigen) präventiven Massnahmen im Sinne neuer erheblicher Tatsachen von Amtes wegen inhaltlich neu überprüft und allenfalls aufhebt.[659] Hinsichtlich der UN-Terrorliste hielt das Bundesgericht denn auch fest, dass ein eingestelltes oder mit einem Freispruch beendetes Strafverfahren zur Aufhebung der präventiv angeordneten Sanktion führen sollte.[660] Präventivmassnahmen sollten ausserdem nicht lediglich dazu dienen, aus pragmatischen Gründen die Prinzipien des Strafverfahrens zu umgehen und Verfahrensrechte des Betroffenen zu verwässern.[661]

Allgemein sind Terrorlisten und öffentliche Verdachtsregister oft (auch) politisch motiviert und werden nach politischen Vorgaben unterhalten. Es wird öfters versucht, sie der Kontrolle durch die Judikative möglichst zu entziehen. Es erstaunt insofern nicht, dass einerseits direkt beruhend auf den Eintrag harte Sanktionen veranlasst werden können und andererseits die öffentliche Brandmarkung der Gelisteten faktisch einen Teil der Motivation hinter den öffentlichen Registern ausmacht.[662] So vielversprechend indessen eine politisch-pragmatische Kriminalitätsbekämpfung scheinen mag, stellt sich diese Kombination im Nachhinein vielfach als kontraproduktiv heraus. Spätestens rächt sich dieses Vorgehen, wenn Pleiten an die Öffentlichkeit gelangen, es die „moralische Autorität" der vollziehenden Behörde kompromittiert und damit zu einer beschämenden und für keinen der Beteiligten willkommenen Situation führt.[663]

In dieselbe Richtung geht die Kritik an heimlichen oder schwer durchschaubaren Praktiken, die häufig Bestandteil vieler postmoderner Kriminalitätsbekämp-

---

658 Siehe dazu ausführlicher MÜLLER J. O., S. 115 mit einem Beispiel. Vgl. bereits STUDER, S. 68. Sehr ähnliche Fragen stellen sich auch bezüglich der (oft unzureichenden) Revisionsmöglichkeiten bei öffentlichen Verdachtsregistern, siehe oben Zweiter Teil, Kapitel I.B.

659 Gl. A. wie MÜLLER J. O., S. 115 mit Hinweis auf eine entsprechende Aufhebungsverfügung aus dem Kanton Luzern. Ähnlich das Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 4.3. Analog BGE 136 II 447 E. 3.1 S. 451.

660 BGE 133 II 450 E. 9.2 S. 466.

661 Illustrativ aber zu diesem Bedürfnis der Ausspruch Gilles de Kerchoves (Koordinator für die Terrorbekämpfung der Europäischen Union) im Interview zur UN-Terrorliste bei KOCHER, S. 118 f.: „[…] wenn das Ganze völlig verrechtlicht wird, dann wird es zu einem stumpfen Instrument."

662 Siehe dazu mehr im Zweiten Teil, Kapitel I.G.

663 SCHEININ, N. 42 und Fn. 43.

fungstechnologien sind.[664] Die Heimlichkeit erhöht die Eingriffsschwere oft erheblich, da Betroffenen durch sie Rechtsschutzmöglichkeiten entgehen.[665] Weiter entziehen sich derartige Praktiken der öffentlichen Kenntnis und damit der Überprüfung und Legitimation durch die Bevölkerung. Steht der anwendenden Behörde zudem ein zu grosser Ermessensspielraum zu, sind die praktischen Einsatzbedingungen der Norm für potenziell Betroffene nicht vorherseh- und berechenbar, was hinsichtlich des Bestimmtheitsgebots, des Legalitätsprinzips und des Grundsatzes der Gewaltenteilung problematisch ist.[666]

Nicht-öffentliche Register, heimliche Datensammlungs- und Informationsverarbeitungstätigkeiten bergen die Gefahr in sich, sich einer externen Kontrolle weitgehend entziehen zu können.[667] Dies hat zur Folge, dass Personen vielfach nicht wissen, ob sie in einem Register eingetragen sind oder Daten über sie gesammelt werden oder wurden und in welchen Zusammenhängen diese Informationen verwendet werden. Zudem muss ihnen zunächst auch nicht immer bewusst sein, dass gegen sie Massnahmen verhängt sind.[668] Davon abgesehen wissen Aussenstehende nicht genau, welches die Registrierungskriterien sind und wer die Re-

---

664 Siehe bspw. das deutsche Bundesverfassungsgericht in BVerfGE 120, 274 (325): „In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmassnahmen die Ausnahme und bedarf besonderer Rechtfertigung." und ähnlich das Urteil des BGH StB 18/06 vom 31. Januar 2007 N. 5 ff. Siehe dazu ausführlich ZERBES, S. 43 ff.

665 Anstatt vieler: PETRI, G N. 51; PUSCHKE/SINGELNSTEIN, S. 113; SZUBA, S. 40; MÜLLER L. 2011, S. 138; BVerfGE 115, 166 (194); 125, 260 (335).

666 MÜLLER L. 2011, S. 360; KOCHER, S. 58 f.; MÜLLER J. O., S. 114; VETTERLI, S. 450 f. Vgl. GROEBNER, S. 56.

667 Siehe etwa KURZ/RIEGER, S. 40 ff. Dahingehend schlechtes Beispiel war die Eintragspraxis im ISIS, siehe Bericht GPDel; BELSER, S. 9 N. 18 f.; KREIS; SCHWEIZER in NZZ Online vom 22. Juli 2010; das Dossier „Neuer Fichenskandal" auf Tages-Anzeiger Online <http://www.tagesanzeiger.ch/dossiers/schweiz/dossier2.html?dossier_id=637>. Zu den Bedingungen der Rechtsprechung des EGMR bezüglich einer ordnungsgemässen Führung derartiger Register, siehe SCHWEIZER 2008, N. 46 zu Art. 13 BV.

668 Vgl. FIENBERG, S. 213; STRÖM, S. 33 und 37; NOWAK, S. 42 f.; BIER/SPIECKER GEN. DÖHMANN, S. 615. Art. 18 BWIS sieht lediglich ein einschränkbares Auskunftsrecht vor, grundsätzlich jedoch keine aktive Mitteilungspflicht der Behörde bei einer Eintragung (ausnahmsweise für die Hooligan-Register, siehe Art. 24a Abs. 10 BWIS). SCHWEIZER 2008, N. 44, 46 und 53 zu Art. 13 BV, hält diese Ausgestaltung des Auskunftsrechts m. E. zu Recht für „*mehr als fragwürdig*". Das Bundesgericht beurteilte eine ähnliche Bestimmung zwar als zulässig, jedoch grundsätzlich als schweren Eingriff in die Geheimsphäre, weswegen jene verfassungs- und konventionskonform auszulegen sei (BGE 109 Ia 273 E. 12 S. 298 ff. insb. 303). Zur Heimlichkeit der Vorgänge: STEGMANN A., S. 165. Zum selben Problem bei der Videoüberwachung: ROGGAN 2001, S. 139.

gistrierung durchführt. Dadurch werden somit auch Registrierungsfehler kaum bemerkt, obschon sie sehr folgenschwer sein können. Schliesslich ist teilweise schwer in Erfahrung zu bringen, ob, wo und wie die Löschung etwa falscher Einträge oder unrechtmässig gesammelter Personendaten anhängig zu machen oder überhaupt möglich ist. Das Potenzial, Verfahrens- und Freiheitsrechte Einzelner zu verletzen, ist demnach gross.[669] Problematisch gestaltet sich insbesondere die Aufnahme einer Person in das Register, ohne sie vorher anzuhören, wenn unmittelbar gestützt auf die erfolgte Eintragung (verwaltungsrechtliche) Massnahmen gegen diese Person veranlasst werden können oder sonstige Konsequenzen direkt aus der Eintragung folgen (die für den Betroffenen nicht immer nachvollziehbar sind).[670] Dadurch, dass die Eintragung in diese Art der Register meistens auf ziemlich schemenhaften Verdachtsmomenten basiert, ist die Richtigkeit der Einträge zweifelhaft.[671] Besonders, wenn die Beweise oder Verdachtsmomente nur ungenügend – gerichtlich nicht verwertbar – überliefert sind.

Es wurde bereits dargestellt, dass die Verdachtsschwellen im BWIS und im Hooligan-Konkordat, vor allem in dessen revidierter Fassung, relativ tief angesetzt sind. Zudem kann es vorkommen, dass der Betroffene zum Zeitpunkt, in dem ihm seine Eintragung mitgeteilt wird, bereits deren Konsequenzen unterliegt, ohne dass er sich dagegen hätte wehren können.[672] Das sind gewichtige Kritikpunkte. Die kantonalen Gerichte und das Bundesgericht scheinen zwar durchaus bestrebt zu sein, über die sorgfältige Kontrolle der Sanktionsverfügungen im Einzelfall einen Ausgleich zu schaffen. Gemäss ihrer relativ einheitlichen Rechtsprechung müssen Verdachtsnachweise ausreichend begründet sein, im Einzelfall auf die Begründetheit geprüft werden, der betroffenen Person muss

---

669 Siehe zum Ganzen: STEGMANN A., S. 212; SOLOVE 2008, S. 194; STUDER, S. 68; STRÖM, S. 38 f.; CHESTERMAN, S. 239; sehr kritisch SCHWEIZER 2008, N. 46 zu Art. 13 BV. In Betracht kommt eine Verletzung der Rechtsweggarantie von Art. 29a BV oder des rechtlichen Gehörs von Art. 29 Abs. 2 BV. Das Bundesgericht stellte in BGE 109 Ia 273 E. 12 S. 303 fest, ohne Benachrichtigung sei der Rechtsschutz faktisch ausgeschlossen.

670 STUDER, S. 68; NOWAK, S. 41 f. Übliche Massnahmen sind bspw. Ein- und Ausreisesperren (z. B. gemäss Art. 24c BWIS; vgl. Bericht SIPOL, S. 71), eine „Spezialbehandlung" am (Flughafen-)Zoll (z. B. gestützt auf Terrorlisten; vgl. STEINBOCK, S. 50) oder Rayonverbote sowie Meldeauflagen (z. B. gemäss Art. 4 ff. Hooligan-Konkordat), je nach Gefährlichkeit der Täterkategorie.

671 STUDER, S. 68.

672 STUDER, S. 67 f. Dies berührt u. a. die Rechtsweggarantie von Art. 13 EMRK, siehe SCHWEIZER 2008, N. 47 zu Art. 10 BV, was aber unter Umständen hinzunehmen ist, siehe Urteil des Bundesverwaltungsgerichts C-560/2011 vom 15. April 2013 E. 8.3.

das rechtliche Gehör hinsichtlich der Massnahmeverfügung gewährt werden und dem Verhältnismässigkeitsprinzip ist besondere Bedeutung zuzumessen.[673] Trotzdem gesteht der Strafprozess dem Betroffenen wesentlich umfangreichere Mittel zu, sich am Verfahren zu beteiligen und damit auf dessen Ergebnis einzuwirken.[674]

Bei zielgerichteten (heimlichen) Online-Überwachungsmassnahmen oder Verdachtsregistern kann und soll folglich ein nachträglicher Rechtsschutz zumeist gewährleisten, dass betroffene Personen Verfahrensrechte beanspruchen können.[675] Schwieriger indes ist die nachträgliche Transparenz und ein ausreichender Rechtsschutz bei verdachtsunabhängigen Überwachungs- und Informationsverarbeitungsmassnahmen sicherzustellen, da kaum je alle einbezogenen Personen darüber informiert werden können, dass sie betroffen sind und deshalb eine Auswahl zu treffen ist, wem überhaupt der Rechtsschutz zustehen soll.[676] Freilich muss die betroffene Person dazu identifiziert werden, was wohl wiederum, durch die Kombination der verdachtsunabhängigen Methode mit Identifizierungstechniken, einen intensiveren Eingriff in die Grundrechte des Betroffenen bedeuten könnte.

Diese Probleme betreffen mehrheitlich auch präventiv-polizeiliche Verdachtsregister. Ein wesentlicher Bestandteil dieser Informationssysteme ist die Bearbeitung und Interpretation von Daten zur Verdachtsforschung beziehungsweise Verdachtsermittlung, was dahingehend ein Problem darstellt, als strafprozessuale Verfahrensgarantien eben nur im Strafverfahren gelten und der beschränkende Grundsatz polizeirechtlicher Gefahrenabwehr, das Störerprinzip, mangels einer

673 Siehe dazu etwa Urteil des Verwaltungsgerichts des Kantons Bern Nr. 100.2008.23334U vom 2. März 2009; Urteil des Rekursgerichts im Ausländerrecht des Kantons Aargau 1-PO.2010.1 vom 14. Oktober 2010, AGVE-2010-78; Urteile desVerwaltungsgerichts Zürich VB.2011.00465 vom 8. September 2011, VB.2009.00019 vom 26. Februar 2009 und VB.2008.00237 vom 19. Juni 2008; BGE 137 I 31; 136 I 87; Urteile des Bundesgericht 1C.278/2009 vom 16. November 2010 und 1C.453/2009 vom 12. Januar 2010. Vgl. MOECKLI/KELLER, S. 239 f.; MÜLLER J. O., S. 111 und 119 f.; SOÒS/VÖGELI, S. 158; TRUNZ/WOHLERS, S. 193 und 196. Aus praktischer Sicht kritisch zu den Verfahrensverzögerungen durch die Gewährung des rechtlichen Gehörs: HENSLER, S. 42.

674 ZERBES, S. 325.

675 Anstatt vieler ZERBES, S. 374.

676 Bsp. Rasterfahndung und Antennensuchlauf: BGE 137 IV 340 E. 6.1 S. 350; BVerfGE 115, 320 (353); RUDIN, S. 279; HEINIGER, N. 18 und 54. Vgl. auch Botschaft BÜPF 2013, S. 2764. Bsp. Videoüberwachung: BIER/SPIECKER GEN. DÖHMANN, S. 613.

klaren Abgrenzung von Störern und Nicht-Störern in diesem Bereich nicht ausreichend beschränkend greifen kann.[677]

Bei öffentlichen Verdachtsregistern bereitet nicht wie bei den nicht-öffentlichen Datenbanken und geheim ablaufenden Informationsverarbeitungsprozessen der *Ausschluss*, sondern die Einbindung der Öffentlichkeit Sorgen. Da öffentliche Verdachtsregister sehr intensive Grundrechtseingriffe bedeuten können, ist ausgleichend zu verlangen, dass sie einen diesen Eingriffen angemessenen Individualrechtsschutz bereitstellen.[678] In den Anfängen der Schwarzen Liste der UNO bestand der einzige, nachträgliche Rechtsschutz darin, eine Entlistungspetition über den Heimat- oder Aufenthaltsstaat an den Sanktionsausschuss zu richten.[679] Die Kriterien, auf denen der Listungsentscheid des Sicherheitsratsausschusses basiert, und die Überprüfungspraxis sind auch heute noch wenig transparent und nicht selten geprägt von politischen Motiven.[680] Eine angemessene Gefährlichkeitsabklärung bei schwerwiegenden Grundrechtseingriffen im Einzelfall scheint damit kaum hinreichend gewährleistet.[681] Mittlerweile implementierte der Sicherheitsrat über zahlreiche Reformen Verbesserungen am Rechtsschutzsystem. Diese Bestrebungen sind begrüssenswert, einige (wesentliche) Defizite wurden aber noch nicht ausgeräumt.[682] Zum Beispiel muss der Betroffene, der sich von der Liste streichen lassen will, gegen zumeist nachrichtendienstliche Informatio-

---

677 STEGMANN A., S. 142 und 146 f. jeweils mit Hinweisen; PETRI, G N 125 f. Vgl. MIDDEL, S. 106 f. Siehe auch den Bericht GPDel bzgl. ISIS.

678 MEYER 2010, S. 77; BARTMANN, S. 282.

679 DIGGELMANN, S. 311; MEYER, S. 81. Vgl. SCHULTE, S. 62 ff. Lange erfüllte das Sanktionsregime „nicht einmal das Minimum an prozeduraler Legitimation" (MEYER 2010, S. 81). Sehr ähnlich die Einschätzung des Bundesgerichts in BGE 133 II 450 E. 8.3 S. 464 f. und SCHWEIZER in NZZ Online vom 22. Juli 2010 zur Informationsverarbeitung im Staatsschutz.

680 SCHULTE, S. 49 ff.; MEYER, S. 76; BARTMANN, S. 93 f.; EMMERSON, N. 24 ff.

681 Gl. A. wie MEYER, S. 76 f.

682 MEYER, S. 81 und 84; SCHULTE, S. 64, 293 ff. und 453; BARTMANN, S. 96, 172 f. und 257 ff.; HÄFELIN/HALLER/KELLER, N. 1920a S. 627; SULLIVAN/HAYES, S. 31 ff.; EMMERSON, N. 31 f. und 54-58; KOCHER, S. 58 f.; BGE 133 II 450 E. 7.4 S. 462 f. und E. 8.3 S. 464 f. mit weiteren Hinweisen; Entscheid des EGMR Nada gg. Schweiz vom 12. September 2012, Nr. 10593/08, Concurring Opinion of Judge Malinverni, §§ 23 ff. Der Sonderberichterstatter BEN EMMERSON etwa kritisiert in seinem Bericht A/67/396, N. 34 ff., dass der Entlistungsvorschlag der als „quasi-unabhängig" bezeichneten Ombudsperson vom Sicherheitsratsausschuss oder vom Sicherheitsrat innert Frist abgelehnt werden kann (siehe dazu Bericht S/2012/968, N. 11 und Annex III, N. 10 sowie S/RES/1989 (2011), N. 23). Immerhin scheint der Sicherheitsrat aber grundsätzlich gewillt zu sein, Reformen am Sanktionsregime vorzunehmen, siehe etwa Berichte S/2012/305, S. 47 f. und S/2012/968, N. 9 ff.

nen aus Mitgliedstaaten antreten, die aus politischen Gründen und Überlegungen der nationalen Sicherheit möglichst vage gehalten werden.[683] Dieser aus rechtsstaatlicher Sicht abzulehnende Winkelzug verleitete den kanadischen Bundesrichter Russel Zinn in der Urteilsbegründung zum Fall Abdelrazik zu einer amüsant sarkastischen Metapher: „One cannot prove that fairies and goblins do not exist any more than Mr. Abdelrazik or any other person can prove that they are not an Al-Qaida associate."[684] So empfiehlt auch der Menschenrechtsrats-Sonderberichterstatter MARTIN SCHEININ nachdrücklich, „dass Sanktionen gegen eine Person nicht auf Erkenntnissen ausländischer Nachrichtendienste beruhen sollten, es sei denn, der Betroffene kann die Glaubwürdigkeit, Richtigkeit und Zuverlässigkeit der Informationen wirksam anfechten und es bestehen glaubhafte Gründe für die Annahme, dass die Informationen zutreffend und zuverlässig sind".[685] Entsprechende Verfahrensvorkehrungen bedürfen der Aufnahme in das Sanktionsregime und analog allgemein in Verdachtsregister. Freilich liegen nicht allen Listen Erkenntnisse ausländischer Nachrichtendienste zugrunde, ihr typisches Merkmal ist aber, dass sie sich auf knappe, vage und/oder unzuverlässige Hintergrundinformationen oder tiefschwellige Eintragsvoraussetzungen abstützen und dass die Streichung eines Eintrags zu veranlassen, vor allem aufgrund gegenüberstehender Sicherheitsüberlegungen, teilweise ein schwieriges Unterfangen ist.[686]

G. Stigmatisierung und andere Nebenfolgen

Die Veröffentlichung von Personendaten in einem Verdachtsregister (zum Beispiel einem öffentlichen Betreibungsregister oder einem Pädophilenregister) kann Betroffene der öffentlichen Blossstellung aussetzen.[687] Diese berührt die

---

683 EMMERSON, N. 25 und 38; BARTMANN, S. 94 und 173; MEYER, S. 75 (insb. Fn. 6). Die (meist sehr kurzen und oft lückenhaften) „narrative summaries" und „statements of case" sind nicht selten die einzigen Informationen, die dem Betroffenen zur Vorbereitung seiner Verteidigung zur Verfügung stehen.

684 Richter Russel Zinn, Reasons for Judgment and Judgment, Urteil des kanadischen Federal Court 2009 FC 580 vom 4. Juni 2009 (Abousfian Abdelrazik) N. 53. Vgl. KOCHER, S. 175.

685 SCHEININ, N. 74. Ausführlicher der EMMERSON, N. 40-52 u. a. mit Hinweisen auf das Urteil United Kingdom Supreme Court Ahmed and others v. HM Treasury vom 27. Januar 2010. Vgl. auch SULLIVAN/HAYES S. 13, Fn. 24.

686 Bericht HRW, S. 2 ff.; BARTMANN, S. 94 und 96; SCHULTE, S. 328.

687 DIGGELMANN, S. 310; BARTMANN, S. 126; MEYER, S. 77; Bericht HRW, S. 78 ff. Vgl. KUNZ 2011, S. 356 f. Siehe auch SCHWEIZER/BISCHOF, S. 281.

persönliche Freiheit (Willensfreiheit beziehungsweise psychische Integrität) und den persönlichen Geheimbereich Eingetragener.[688] Nicht nur dürfte die Rufschädigung gravierend sein und durch die Mitteilung sowie die weite Verbreitung über die Medien (namentlich auch das Internet) für die Aufrechterhaltung der Brandmarkung sorgen, sondern die Konsequenzen der Eintragung und das durch den Eintrag angerichtete soziale Übel sind auch kaum rückgängig zu machen. Das einmal gesäte Misstrauen wird der Betroffene auch nach einer allfälligen Streichung seines Eintrags schwerlich wieder loswerden können.[689]

Der EGMR kam in einem Urteil zu einem öffentlichen Konkursregister zum Schluss, dass die Privatsphäre des Betroffenen insbesondere verletzt werde, wenn ein öffentliches Register automatisch und ohne umfassende Kontrollinstrumente geführt werde.[690] Diese Rechtsprechung kann ohne Weiteres analog auf andere öffentliche Verdachtsregister angewendet werden.[691] Die amerikani-

---

688 Siehe BGE 119 Ia 99 E. 4.b S. 105; den Entscheid des EGMR Taiani gg. Italien vom 20. Juli 2006, Nr. 3641/02, § 41 („un blâme morale"), den Entscheid des EGMR Sciacca gg. Italien vom 11. Januar 2005, Nr. 50774/99, §§ 28 und 29; SCHWEIZER 2008, N. 18 zu Art. 10 und N. 45 zu Art. 13 BV; SCHWEIZER 2009, S. 466; BREITENMOSER, N. 17 zu Art. 13 BV mit Hinweisen; DIGGELMANN, S. 312.

689 Problematisch ist dies natürlich insb., wenn der Eintrag auf einem relativ leicht wiegenden Anknüpfungspunkt beruht oder zeitlich weit zurückliegt. Mit BARTMANN, S. 126 ist indes zu vermerken, dass dieser stigmatisierende Effekt stark von der verbreiteten Kenntnisnahme der Einträge eines Registers durch die Öffentlichkeit abhängt. Diese ist bei den Sexualstraftäterregistern in den USA hoch, bei der UN-Terrorliste wohl hingegen sehr gering.

690 Der EGMR stellte in seinem Entscheid Taiani gg. Italien vom 20. Juli 2006, Nr. 3641/02, § 31, Folgendes fest: „[…] l'inscription du nom du failli dans le registre entraîne en soi une ingérence dans le droit au respect de la vie privée des requérants qui, compte tenu de la nature automatique de ladite inscription, de l'absence d'une évaluation et d'un contrôle juridictionnel sur l'application des incapacités y relatives ainsi que du laps de temps prévu pour l'obtention de la réhabilitation, n'est pas «nécessaire dans une société démocratique» au sens de l'article 8 § 2." Ähnlich auch bereits BGE 107 Ia 52 (Veröffentlichung der Namen fruchtlos gepfändeter Schuldner im kantonalen Amtsblatt).

691 In seinem Entscheid Segi und Andere & Gestoras Pro-Amnistia und Andere gg. 15 Staaten der Europäischen Union vom 23. Mai 2002, Nr. 6422/02 und 9916/02 kam der EGMR indes zum Schluss, es liege kein genügender Bezugspunkt zur Konvention vor, insofern (mutmasslich terroristische) Organisationen lediglich auf eine öffentliche Terror-Liste gesetzt würden, ohne Namen natürlicher Personen zu nennen und ohne, dass daraus weitere Massnahmen ergingen.

schen Sexual Offender Register zum Beispiel versagen exakt in den vom EGMR beanstandeten Punkten.[692]

Gleich verhält es sich bei der UN-Terrorliste: Die Einträge beruhen grösstenteils auf stark zusammengefassten Geheimdienstinformationen, welche meist ausschliesslich der zuständigen Behörde des anzeigenden Staats vollständig zugänglich sind.[693] Die das Register betreibende Stelle tendiert dazu, sich einer quasiautomatischen Eintragung mit stark beschränkten oder fehlenden (richterlichen) Überprüfungsverfahren und Aufsichtsprozeduren zu behelfen und systembedingt unzuverlässige Einträge zu erfassen. Der EGMR sah weiter auch bei einer nichtöffentlichen DNA-Datenbank ein Risiko der Stigmatisierung Betroffener: Würden zu einer nicht verurteilten beziehungsweise nicht überführten Person gesammelte Daten gleich behandelt wie diejenigen einer verurteilten beziehungsweise überführten, aber nicht gleich wie diejenigen einer nicht verdächtigten Person, werde die Unschuldsvermutung verletzt. Speziell schädlich befand der Gerichtshof die zu beurteilende Behandlung von Jugendlichen aufgrund ihrer speziellen Situation und der Bedeutung ihrer Entwicklung und Integration in die Gesellschaft.[694]

Dieses Stigmatisierungsrisiko und auch das Risiko, weiteren Folgeeingriffen ausgesetzt zu sein, bestehen allgemein bei Massnahmen mit hoher Streubreite, durch die teilweise unbegründete Verdachtsvorwürfe ausgesprochen werden.[695]

---

692 Vgl. dazu auch den Entscheid F and Angus Audrey Thompson v Secretary of State for the Home Departement, [2008] EWHC 3170 (QB), E. 12 f., 18 und 33.

693 SCHULTE, S. 200 f.; EMMERSON, N. 25. Bei nachrichtendienstlichen Erkenntnissen handelt es sich zudem nicht um Rohmaterial, sondern um ein aufbereitetes Produkt, siehe SCHEININ, N. 56.

694 Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, §§ 122-124. Vgl. analog BGE 120 Ia 147 E. 3.b S. 155: Das entspricht einer unbegründeten strafrechtlichen Missbilligung, welche gegen die Unschuldsvermutung verstossen kann, „wenn die Behörden damit ausdrücken, die betroffene Person sei doch schuldig, obwohl sie freigesprochen oder das Strafverfahren eingestellt worden ist." Ebenso VEST, N. 13 zu Art. 32 BV.

695 PETRI, G N. 55; HARCOURT, S. 36; SIMON D., S. 255. So wurden bspw. im Rahmen der „Schläferfahndung" 140 ausländische Studenten vorgeladen, die sich letztlich als unverdächtig herausstellten, siehe BVerfGE 115, 320 (352). Auch die bei ALBRECHT P. A. 2003, S. 137 f. beschriebenen Überprüfungsaktivitäten (Befragen der Nachbarn oder des Arbeitsgebers, Durchwühlen der Abfalleimer etc.) können für den überprüften, mutmasslichen Verdächtigen (soziale) Nebenfolgen bedeuten (bspw. Misstrauen der Nachbarn, Entlassung durch den Arbeitgeber etc.), auch wenn er sich als unschuldig herausstellt.

Problematisch ist zudem die bereits angesprochene Drittwirkung eines Registereintrags für die Familie und Bekannte des Gelisteten. Sie laufen Gefahr, in den Sog der Sanktionen zu geraten, indem ihnen verwehrt wird, den Eingetragenen zu unterstützen (Beispiel UN-Terrorliste), sie selbst wegen ihrer Verbindung zum Registrierten zu naheliegenden Zielen für weitere Einträge werden (vor allem nicht-öffentliche Register weisen dahingehend eine beträchtliche Streubreite auf) und allgemein die Folgen der sozialen Isolation und Stigmatisierung auch sie belasten (das ist vor allem der Fall bei öffentlichen Sexualstraftäterregistern).[696] Die Vorbringen der Beschwerde führenden Betroffenen im erwähnten Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung demonstrieren ebenso anschaulich, wie durch Online-Überwachungsmassnahmen Verdachtsmomente sich kaskadenhaft von Person zu Person fortsetzen und welche Unannehmlichkeiten dadurch für die betroffenen Personen ausgelöst werden können.[697]

In diesem Zusammenhang sei schliesslich auf die in der Schweiz jüngst öfters angewendete Internetfahndung (Veröffentlichung von durch Videoüberwachung gewonnenen Aufnahmen von Verdächtigen im Internet durch staatliche Behörden) hingewiesen.[698] Die potenziell schwerwiegenden sozialen Folgen der Veröffentlichung der Aufnahmen für die betroffene Person kommen einer formellen Folgemassnahme gleich, vor allem wenn die Fahndung an sich nicht der einzige

---

696 Siehe dazu EMMERSON, N. 13; MEYER/MACKE, S. 464 f.; MEYER, S. 77; BARTMANN, S. 116 und 124 f.; SULLIVAN/HAYES, S. 11 und 92 f.; PETRI, G N. 92; Bericht HRW, S. 117. Vgl. CHESTERMAN, S. 183.

697 Problematisch ist dies vor allem für Berufsgeheimnisträger (bspw. Anwälte) oder Personen, die legitimerweise mit grundsätzlich verdächtigen oder verdächtig aussehenden Informationen in Berührung kommen (bspw. Journalisten). Siehe dazu TSCHENTSCHER, S. 384 f.; GLESS 2012, S. 9. Berufsgeheimnisträger sind gemäss Art. 271 StPO geschützt, nicht aber etwa andere Vertrauensverhältnisse zwischen Verdächtigen und Drittpersonen, die Zeugnisverweigerungsrechte begründen (Eheleute etc.), siehe GLESS 2012, S. 9 f.; Botschaft StPO, S. 1249.

698 Vgl. den Artikel „Hooligans am Internet-Pranger: Der erste hat sich gemeldet" in Tages-Anzeiger Online vom 13. August 2010 und auch OTT/KOLLBRUNNER in Der Bund Online vom 12. Juni 2013. Zu dieser Fahndungsart, siehe ausführlich MÜLLER L. 2011, S. 283-287 und BUCHER/HÄGGI jeweils mit weiteren Hinweisen sowie MOHLER 2012, S. 380; TRUNZ/WOHLERS, S. 190; PERREY, S. 88.

Zweck der Veröffentlichung war, sondern vermutlich nicht zuletzt ein abschreckendes Zeichen für andere gewaltbereite Störer zu setzen angestrebt wird.[699]

H. Beweiswert im Strafverfahren

Die Verwertung nachrichtendienstlich oder sicherheitspolizeilich gewonnener Erkenntnisse auf dem Weg der Verdachtsregister mit eigenen Sanktionsregimen entzieht sich strafprozessualen Garantien weitgehend. Die unmittelbaren (zum Beispiel das Flugverbot) und die mittelbaren Sanktionsfolgen (zum Beispiel die öffentliche Anprangerung) treten direkt ein, spätestens nachdem die betroffene Person ein Verwaltungsverfahren vergeblich durchlaufen hat. Polizeiliche Erkenntnisse aus einem strafrechtlichen Ermittlungsverfahren, die in Strafverfahren eingebracht werden, unterliegen im Gegensatz dazu den Beweisverwertungsverboten der StPO gleichermassen wie Erkenntnisse, die Strafverfolgungsbehörden im Strafverfahren sammeln.[700] Die Beweissammlung ist unzulässig, wenn keine angemessene Ermächtigungsgrundlage für den Einsatz einer technisch möglichen Ermittlungsmassnahme vorliegt oder darin normierte, wesentliche Voraussetzungen nicht beachtet wurden.[701] Stammen Beweise aus einem Einsatz von Überwachungstechnologien ohne rechtliche Grundlage oder Genehmigung, sind diese gemäss Art. 141 und 277 StPO im Strafverfahren grundsätzlich nicht verwertbar.[702] Zufallsfunde aus Überwachungen des Post- und Fernmeldeverkehrs sind gemäss Art. 278 StPO zu behandeln: Sie sind verwertbar, wenn sie überwachungsfähige Straftaten und Personen betreffen sowie eine Genehmigung beim Zwangsmassnahmegericht eingeholt wird.[703]

---

699 Die erfolgte Veröffentlichung der Aufnahmen bedient sich insofern einer ähnlichen Präventionslogik wie öffentliche Verdachtsregister. Das Anprangern von Tatverdächtigen als Zweck der Veröffentlichung bedeutet nach Ansicht von MÜLLER L. 2011, S. 103 eine „ausserordentlich schwere Persönlichkeitsverletzung". Vgl. SCHWEIZER 2008, N. 45 zu Art. 13 BV; VEST, N. 13 zu Art. 32; MOHLER 2012, S. 290.

700 GLESS 2011, N. 38 zu Art. 141 StPO. Vgl. BGE 134 IV 266 E. 5.2 S. 286 f. und auch 137 I 218 E. 2.3.4 S. 223 f.

701 GLESS 2012, S. 6; DIES. 2011, N. 1 zu Art. 141 StPO; WOHLERS, N. 1 zu Art. 141 StPO; VETTERLI, S. 461.

702 JEAN-RICHARD-DIT-BRESSEL, N. 3 ff. zu Art. 277 StPO; HANSJAKOB 2010, N. 1 ff. zu Art. 277 StPO; HÄRING, S. 236 ff. Vgl. BGE 137 I 218 E. 2.3.4 S. 223 f.; 133 IV 329 E. 4.4 S. 331.

703 Anstatt vieler: JAGGI, S. 8 f.; JEAN-RICHARD-DIT-BRESSEL, N. 1 ff. zu Art. 278 StPO. Umstritten ist hingegen, ob Erkenntnisse aus nicht genehmigten Überwachungsmassnahmen ei-

Schwieriger ist die Frage zu beantworten, wie mit aus dem Einsatz anderer Technologien generierten Zufallsfunden und mit Informationen zu verfahren ist, die ursprünglich ausschliesslich zu präventiv-polizeilichen Zwecken gesammelt wurden, später aber in einem Strafverfahren als Beweise verwendet werden sollen.[704] Präventiv-polizeiliche Informationsverarbeitungs- und Überwachungstechnologien, Datenbanken mit (verdachtsunabhängigen) Personendaten und Verdachtsregister sind dafür geschaffen, systematisch Informationen zu erheben[705] – aufgrund ihrer Streubreite häufig auch Zufallsfunde, die von Art. 278 StPO nicht erfasst sind.[706] Grundsätzlich auszuschliessen ist ihre Verwertung im Strafverfahren zwar nicht, Informationen aus einer unzulässigen (verdachtsunabhängigen) Beweisausforschung zu verwenden oder mit der polizeilich-präventiven Beweissammlung strafprozessuale Schranken zu umgehen, wäre aber als missbräuchlich einzuschätzen.[707]

Die Relevanz der aus einem (technisch) mangelhaften Einsatz der Govware gewonnenen Erkenntnisse dürfte vor Gericht wohl gering sein. Alleine die Manipulation des Zielsystems durch die Behörden kann die Beweiskraft der gewonnenen Daten schmälern oder entkräften.[708] Noch offen ist, ob vom Beschuldigten derart formulierte Schutzbehauptungen in Fällen des Einsatzes von Govware

nem absoluten Verwertungsverbot *mit Fernwirkung* unterstehen. Zustimmend: JEAN-RICHARD-DIT-BRESSEL, N. 4 zu Art. 277 StPO, HANSJAKOB 2010, N. 8 zu Art. 277 StPO; RHYNER/STÜSSI, S. 458; GLESS 2010, S. 154 ff.; DIES., N. 92 und 98 zu Art. 141 StPO; HÖHENER/VEST, S. 107 f.; HÄRING, S. 248 ff. mit weiteren Hinweisen. Ablehnend: BGE 133 IV 329 E. 4.5 S. 332 f. mit weiteren Hinweisen, in dem das Bundesgericht darauf abstellt, inwieweit der „ursprüngliche, ungültige Beweis Bestandteil sine qua non des mittelbar erlangten Beweises ist" und basierend darauf eine Interessenabwägung durchführt.

704 GLESS 2011, N. 38 und 104 zu Art. 141 StPO.

705 GLESS 2011, N. 104 zu Art. 141 StPO; PIETH, S. 123.

706 GLESS 2011, N. 104 zu Art. 141 StPO, die m. E. richtig darauf hinweist, die unumschränkte Verwertbarkeit dieser Informationen im Strafverfahren führte zu falschen Anreizen. Ebenso ALBRECHT F., N. 21; VETTERLI, S. 456 mit weiteren Hinweisen. A. A. ist JEAN-RICHARD-DIT-BRESSEL, N. 50 zu Art. 278 StPO.

707 Botschaft StPO 2005, S. 1237; GLESS 2011, N. 38 und 81 mit weiteren Hinweisen; VETTERLI, S. 453 f.; BGE 137 I 218 E. 2.3.2 S. 221 ff.; Urteil des Obergerichts des Kantons Bern BK 11 9 vom 22. März 2011 E. 2.4. Vgl. ferner HANSJAKOB 2010, N. 3 zu Art. 280 StPO. Für Deutschland, siehe PETRI, G N 356 (präventiv-polizeilicher Ergebnisse aus einer Online-Durchsuchung im Strafverfahren nicht verwertbar).

708 WEBER/WOLF/HEINRICH, N. 26; GLESS 2012, S. 13 und 16; PLATZ, S. 841, welcher der Ansicht ist, dass gemäss „herrschender Expertenmeinung bereits die Infiltration eine Modifikation des Zielsystems" darstelle. Ebenso BVerfGE 120, 274 (309 und 325). Siehe dazu auch Botschaft BÜPF 2013, S. 2773 ff.

regelmässig ausreichend stichhaltig sein können.[709] De lege ferenda sieht Art. 269ter Abs. 3 StPO denn auch speziell und ausdrücklich vor, dass unter Verletzung der normierten Einschränkungen erlangte Informationen nicht als Beweismittel verwendet werden dürfen, sondern vernichtet werden müssen.[710]

Polizeilich-präventiv gewonnene Informationen in ein Strafverfahren einzubringen, kann zudem insbesondere mit der geforderten klaren Zweckbestimmung für den präventiv-polizeilichen Einsatz technischer Überwachungsmassnahmen kollidieren.[711] Sollen zum Beispiel in einem bestimmten öffentlichen Raum bestimmte Straftaten mittels Videoüberwachung verhindert werden, stellt sich die Frage, wie mit zufällig erfassten Delikten ausserhalb der Zweckbestimmung der Videoüberwachung zu verfahren ist.[712] Derartige überführende Videoaufnahmen sollten in einem allfälligen Strafverfahren demnach nicht ohne Weiteres direkt verwertet werden dürfen. Das gilt verschärft, wenn die Raumüberwachung automatisiert oder grossräumig erfolgt und ausserdem das Geschehen nicht nur visuell festhält, sondern zusätzlich auch Geräusche mitschneidet.

Analog kann das Gesagte auch auf Informationen und Zufallsfunde aus der virtuellen Raumüberwachung und aus Informationsverarbeitungstätigkeiten übertragen werden. Eine Gleichbehandlung des aufgrund von Beweisen aus einer zielgerichteten Observation Angeklagten und des aus Informationen aus zweckentfremdeten präventiv-polizeilichen Methoden Angeklagten kann nur erreicht werden, wenn an die Beweise aus beiden Quellen im Strafverfahren der gleiche Massstab angelegt wird. Diesbezüglich besteht Bedarf an präzisen und

---

709 Ähnlich verhält es sich mit Wi-Fi-Netzwerken, die heute sehr verbreitet sind, sowohl zuhause als auch an öffentlich zugänglichen Orten. Das gilt insbesondere, wenn diese schlecht gesichert sind und folglich ohne grossen Aufwand „gehijacked" werden können (siehe anstatt vieler LSE Briefing, S. 18). Auch hier verringert der einfache Verweis darauf den Beweiswert. Siehe auch BGE 136 II 508 E. 6.3.3 S. 524 f.: „[…] zumal sich die Eruierung des Urheberrechtsverletzers in vielen Fällen als schwierig oder unmöglich erweisen würde, etwa wenn ein Drahtlosnetzwerk verwendet wird oder ein Computer mehreren Personen zur Verfügung steht."

710 Botschaft BÜPF 2013, S. 2776 und 2779. KUTSCHA, S. 1044 ist indes beizupflichten, dass auch derartige Verwertungsverbote nicht alle Eingriffe ungeschehen machen können.

711 Müller L. 2011, S. 278; Büllesfeld 2002, S. 213.

712 Wird diese beispielsweise installiert, um einen Parkplatz frei von Autodiebstählen zu halten, deckt stattdessen aber per Zufall einen kleineren Drogendeal auf, kann dann das entsprechende Aufzeichnungsmaterial als Beweis zur Verurteilung der am aufgezeichneten Delikt Beteiligten führen, kann es ausschliesslich Impulse geben für weitere Ermittlungen oder muss es eventuell sogar ignoriert werden?

ausdrücklichen Regelungen.[713] Im Bereich der präventiv-polizeilichen Videoüberwachung finden sich derartige Regelungen, wenn auch teilweise sehr extensive, die viele Optionen offen lassen, bereits oft in den Polizeigesetzen der Kantone und Gemeinden.[714]

I. Verschwimmende Tätigkeitsbereiche

Die postmodernen Kriminalitätsbekämpfungstechnologien begünstigen Tendenzen der Vermischung verschiedener Tätigkeitsbereiche. „Klassische rechtliche Kategorien"[715] und die Grenzen zwischen den Tätigkeitsbereichen werden zunehmend durchlässig und verschwimmen.[716] In der Literatur ist diesbezüglich öfters die Rede von einer „Verpolizeilichung".[717] Dieser Wandel ist aus mehreren Gründen kritisch zu betrachten[718]:

Die Entlehnung nachrichtendienstlicher Methoden zur polizeilichen Gefahrenabwehr, Kriminalprävention und Strafverfolgung bringt Anpassungsschwierigkeiten mit sich. Nachrichtendienstliche Strategien, Mittel und Techniken mögen sich durchaus für nachrichtendienstliche Aktivitäten eignen. Tätigkeiten der Informationssammlung und -verarbeitung sind *das* Metier nachrichtendienstlicher Behörden. In diesem Umfeld können vage Hinweise aus verdachtsforschenden Tätigkeiten nützlich und hilfreich sein. Ihnen werden dahingehend auch recht

---

713 STEGMANN A., S. 217 f. und 276 f. Analog für die Zufallsfunde bei der präventiv-polizeilichen Rasterfahndung, siehe ZSCHOCH, S. 195. Ähnlich HASSEMER 2000, S. 267; BÜLLESFELD 2002, S. 216, jedoch im Ergebnis mehr Spielraum zusprechend DERS. S. 217.

714 Siehe oben Erster Teil, Kapitel II.D.1. Art. 51e Abs. 3 des bernischen PolG bspw. erlaubt ausdrücklich die Verwertung von Zufallsfunden ohne Zusammenhang zur Anlasstat, vgl. STEGMANN M., S. 79. *Restriktivere* Verwertungsvorschriften der StPO dürften diesen kantonalen Regelungen indes vorgehen, siehe Urteil des Bundesgerichts 6B.334/2011 vom 10. Januar 2012 E. 4.3; VETTERLI, S. 452.

715 SIEBER, S. 34.

716 Siehe etwa ALBRECHT P. A. 2003, S. 96; KUNZ 2010b, S. 19 f.; SIEBER, S. 2, 34 und 36; SINGELNSTEIN/STOLLE 2012, S. 108 ff.; SZUBA, S. 44; MAEDER/NIGGLI, S. 452 f.; MOHLER 2012, S. 4 f., 56 ff., 85 f. und 372; CHESTERMAN, S. 244; KUBE, S. 64; NOGALA 1998, 168 f. Diese Tendenzen wurden weiter oben in der Einleitung, Kapitel IV.A. grob skizziert. Massgebende Faktoren dieses Wandels sind u. a. die agnostische Zweckvermengung sowie die genutzten Synergien und geschlossenen Fusionen der postmodernen Kriminalitätsbekämpfungstechnologien (siehe unten Zweiter Teil, Kapitel II.C. und Dritter Teil, Kapitel I.G.).

717 Siehe etwa NOGALA 1998, S. 311; ALBRECHT P. A. 2003, S. 95; SZUBA, S. 43; ausführlich SÖLLNER (insb. S. 62 ff.).

718 Gl. A. wie HEINRICH, S. 122 f. und 127 f.; ALBRECHT P. A. 2003, S. 43; SIMON D., S. 8.

weite Befugnisse und Spielräume zugestanden, indem ihr Tätigwerden nicht an das Vorliegen konkreter Verdachtsmomente gebunden ist.[719] Im Unterschied zu Polizeibehörden kommen ihnen jedoch grundsätzlich keine polizeilichen Exekutivkompetenzen zu.[720] Ihre Befugnisse, mehr in Erfahrung zu bringen als andere Behörden, schaden erst einmal kaum, solange keine über die Sammlung und Auswertung von Informationen hinausgehenden Interventionsbefugnisse zugestanden werden und die Informationen im nachrichtendienstlichen Umfeld bleiben, also nicht an Polizei- oder Strafverfolgungsbehörden weitergereicht werden.

Mit dem Einzug der dargestellten postmodernen Technologien in die Kriminalitätsbekämpfung werden nun aber Polizeibehörden mit nachrichtendienstlichen Mitteln ausgestattet.[721] Zum einen beruhen diese oft auf heimlichen, täuschenden oder verdachtsgewinnenden beziehungsweise -forschenden Methoden[722]: Viele Prozesse dieser Methoden laufen im Verborgenen ab, nicht selten ohne Überprüfungs- oder Mitwirkungsmöglichkeiten durch den Betroffenen.[723] Darunter fallen besonders die biometrische oder intelligente Videoüberwachung, Datensammlungen in nicht-öffentlichen Verdachtsregistern sowie rasterfahndungsähnliche Informationsverarbeitungs- und Datenverknüpfungstätigkeiten. Einige Methoden werden zudem bewusst täuschend eingesetzt, so etwa Govware, die in Zielcomputer eingeschleust wird, indem deren Schutzbarrieren umgangen werden, und die ermöglicht, die infizierten Systeme zu durchsuchen und manipulieren. Nicht zuletzt sind viele postmoderne Technologien stark proaktiv ausgerichtet. Sie werden daher oft verdachtsforschend und vorsorgend eingesetzt. Als Beispiele sind die Massendatenverarbeitung anhand verdächtiger Eigenschaften, die anlasslose Sondierung des virtuellen Raums anhand von Kriterien, die verdachtsunabhängige Speicherung von Daten auf Vorrat, die intelligente Videoüberwachung und rasterfahndungsähnliche Antennensuchläufe hervorzuheben. Zum anderen werden zunehmend Kooperationen zwischen Dienststellen angestrebt.[724]

---

719 Siehe den Erläuternden Bericht zum Vorentwurf BWIS II (insb. S. 6 ff.); THIEL, S. 388.

720 LOBSIGER 2008, S. 199 f.; SÖLLNER, S. 52. Siehe dazu aber die Stellungnahme des Bundesrats i. S. Bericht GPDel, S. 7746 ff. Zur immer stärker aufweichenden Trennung von Nachrichtendienst und Polizei in Deutschland, siehe ausführlich THIEL, S. 367 ff.; SÖLLNER, S. 16 ff, 52 ff. und 128 ff. Vgl. auch NOGALA 1998, S. 154 ff.

721 SIMON D., S. 197; SÖLLNER, S. 53; SINGELNSTEIN/STOLLE 2012, S. 109.

722 HASSEMER 1995, S. 483 benennt Heimlichkeit und Täuschung als „Kennzeichen nachrichtendienstlicher Tätigkeit". Siehe auch SZUBA, S. 43.

723 Vgl. ALBRECHT P. A. 2003, S. 97; SIMON D., S. 189.

724 Siehe VOLKMANN, S. 218; SIMON D., S. 197.

Diese Kooperationen können beispielsweise dazu führen, dass Informationen aus nachrichtendienstlichen Datenbanken polizeilich oder im Strafverfahren verwendet werden oder gemeinsame Datenbanken verschiedenen Behörden zugänglich sind und mit Informationen aus allen Tätigkeitsbereichen (Nachrichtendienst, Gefahrenabwehr, Strafverfolgung) angereichert werden.[725] Neben nachrichtendienstlichen Handlungsweisen und Methoden, zieht der Einsatz postmoderner Kriminalitätsbekämpfungstechnologien also auch zusehends eine Vermischung des Polizeirechts, des Prozessrechts und des Strafrechts nach sich.[726]

Neue Schnittstellen werden geschaffen und fliessende Übergänge toleriert oder begünstigt.[727] Alle Tätigkeitsbereiche werden auf das Konzept innerer Sicherheit ausgerichtet. Die postmodernen Technologien folgen operativ-pragmatischen Herangehensweisen, die an ihrer Effizienz gemessen werden und dadurch gebotene Grenzen ignorieren oder umgehen, und fördern jene.[728] Ohnehin besteht für die Polizeibehörde, die sowohl die Funktion der Sicherheits- als auch der Kriminalpolizei wahrnimmt, kaum „Abgrenzungsbedarf mehr zwischen Gefahrenabwehr und Kriminalpolizei".[729] Die üblicherweise *multifunktional* konstruierten und eingesetzten polizeilichen Eingriffsmittel entziehen sich zudem bisweilen der überinstanzlichen Kontrolle und Aufsicht, da die Staatsanwaltschaft und die Gerichte oft überlastet sowie „informatorisch abhängig"[730] von den ermittelnden Behörden sind und die Eingriffsmittel selten präzise bezeichnet und begründet

---

725 THIEL, S. 388; ZERBES, S. 285; OEHMICHEN, S. 939; SIMON D., S. 265; VOLKMANN, S. 218; SINGELNSTEIN/STOLLE 2012, S. 108 ff.; SIEBER, S. 33 f.; NOGALA 1989, S. 79 f. mit weiteren Hinweisen; SCHWEIZER in NZZ Online vom 22. Juli 2010; Erläuternder Bericht zum Vorentwurf BWIS II. Siehe THIEL, S. 390 ff. für Beispiele derartiger informationeller Zusammenarbeit in Deutschland.

726 HEINRICH, S. 117 und 121 ff., insb. 122; HASSEMER 2000, S. 256; KUBE, S. 64; STEGMANN A., S. 128 f.; ALBRECHT H. J. ET AL., S. 222 f.

727 Siehe etwa KATZENSTEIN, N. 10 zu Art. 280 StPO: „Der Übergang von polizeilichen Ermittlungen zur formellen Eröffnung eines Strafverfahrens ist in der Praxis oft fliessend und unscharf." Zur Vermischung von Strafverfahren und (präventiver) Vorermittlung durch JANUS, siehe STEGMANN A., S. 150 f.

728 Siehe dazu SINGELNSTEIN/STOLLE 2012, S. 68; ZERBES, S. 248 f., 281 ff. und 307 f.; STEGMANN A., S. 191 f. und 215 ff.; ALBRECHT P. A. 2003, S. 95; THIEL, S. 103 f. und 112. Vgl. auch VOLKMANN, S. 217; SZUBA, S. 45.

729 ZERBES, S. 284.

730 PUSCHKE/SINGELNSTEIN, S. 113.

werden müssen.[731]. STEGMANN hält in diesem Zusammenhang fest: „Die Technik des Zusammentragens verschiedenster Einzelinformationen kann sehr effektiv sein. Können aber ähnlich effektive Ergebnisse mit dieser Technik erzielt werden wie in einem Strafverfahren, liegt auf der Hand, dass das Anwenden dieser Technik eine Umgehung der Garantien des Strafverfahrens darstellt.“[732] Ähnlich äussert sich auch ZERBES: „Abfangen oder Infiltration der Kommunikation mutmasslicher Mitglieder verbrecherisch ausgerichteter Gruppen sind Eingriffe, die formal im Strafprozess geregelt sind, ihrer eigentlichen Funktion nach jedoch auf den Erhalt von Sicherheit ausgerichtet sind – ohne allerdings in die hierfür bislang entwickelten Grenzen präventiver Eingriffe hineinzupassen: Es handelt sich, weil heimlich ablaufende, um schwerwiegende staatliche Eingriffe jenseits eines Verdachts, aber auch jenseits einer akuten, sicherheitsrechtlichen Gefahr.“[733]

Das Ziel des Einsatzes postmoderner Kriminalitätsbekämpfungstechnologien besteht mitunter darin, vormals unerreichbare Milieus zu erfassen. Mit dem Ansinnen, lückenlos alle Vorgänge zu erfassen, um bei Bedarf auf entsprechend gewonnene Materialien zurückgreifen zu können, wird angestrebt, „rechtsfreie Räume“ abzubauen. Indem sich überschneidende Befugnisse der klassischen, funktionalen Unterteilung in Sicherheitspolizei und Strafverfahren, gesetzessystematisch verfehlte Ermächtigungsnormen und die unkomplizierte Kooperation zwischen verschiedenen Dienststellen gegenseitig verstärken, öffnet sich ein „neues Eingriffsfeld“.[734] Postmoderne Kriminalitätsbekämpfungstechnologien bewegen sich bevorzugt in diesen neuen Eingriffsfeldern. Die proaktive Krimi-

---

731 Siehe ALBRECHT P. A. 2003, S. 96; ZERBES, S. 284. Vgl. auch SIEBER, S. 33. Zur teils unvollständigen Aufsicht und Kontrolle der Tätigkeit der Staatsschutzorgane, siehe MOHLER 2009.

732 STEGMANN A., S. 199. Ebenso bzgl. der proaktiven Informationsbeschaffung bei der präventiven Videoüberwachung MÜLLER L. 2011, S. 277.

733 ZERBES, S. 323. In den vorangehenden Kapiteln wurden bereits mehrere Problembereiche dieser Entwicklungen dargestellt, so zum Beispiel der schwierige Umgang mit Früherkennungsmethoden und überschiessenden Funktionalitäten, die Beweisverwertung von Erzeugnissen, insbesondere von Zufallsfunden, aus präventiv-polizeilich eingesetzten Technologien im Strafverfahren, polizeirechtliche Massnahmen mit „sanktionsähnlichem Charakter“ (VOLKMANN, S. 218) oder mangelnde Rechtsschutzvorkehrungen.

734 ZERBES, S. 361. Vgl. auch SIMON D., S. 261. Wobei dieses freilich nicht „rechtsfrei“ gewesen sein muss, sondern vielleicht vielmehr unüberwacht oder von staatlichen Behörden unangetastet war und umgekehrt nicht zwingend „*un*rechtsfrei“, straftatenlos oder umfassend geregelt werden, nur weil staatliche Behörden es überwachen.

nalitätsbekämpfung mittels, zuweilen anlassloser, Präventivmassnahmen wird legitim, nicht als Ausnahme, sondern als übliche Vorgehensweise und unabhängig von einer konkreten oder akuten Gefahrenlage.[735] Die Gefahren*abwehr* setzt scheinbar zu spät an, geboten ist Gefahren*vorsorge*.[736] Reaktiv-repressive Strafverfolgung in geschehenen Straftaten reicht scheinbar nicht aus, gefragt ist proaktive Verfolgungsvorsorge in potenziell drohenden Straftaten.[737] Alle der hier dargestellten postmodernen Kriminalitätsbekämpfungstechnologien verfügen über dieses Potenzial: Beispielsweise sollen Verdachtsregister gefährliche Personen von zukünftigen Straftaten abhalten, erkennungsdienstliche Datenbanken und Vorratsdatenspeicher zukünftige Ermittlungen erleichtern, Videoüberwachungsanlagen zukünftige Straftaten, gefährliche Personen oder Situationen erkennen und aufzeichnen, Massendatenverarbeitungstechnologien potenziell Verdächtige aus grossen Personenpools aussieben und virtuelle Sondierungstechnologien Hinweise auf potenzielle Bedrohungen liefern. Darin ist ein typisch nachrichtendienstliches Element auszumachen: Zu bezweifelnde abschreckende Wirkungen einmal ausgeklammert, halten postmoderne Kriminalitätsbekämpfungstechnologien Gefahren nicht auf. Vielmehr bereiten sie die Abwehr oder Verfolgung vor. Die Abwehr selbst erfolgt aber in klassischer Polizeiarbeit.[738] In diesem Zusammenhang ist auch kritisch zu fragen, ob Ressourcen der Polizeibehörden durch lediglich vorbereitende Methoden, beispielsweise durch anlasslose Informationsverarbeitungstätigkeiten (Sammlung, Archivierung, Verwaltung, Analyse etc.), nicht übermässig beansprucht und dadurch anderen Bereichen teils unnötigerweise entzogen werden.

II. Schlussfolgerungen

Verallgemeinert lässt sich festhalten, dass alle der vorgestellten Mittel des Präventivapparats darauf konzentriert werden sollten, konkrete Täter und Störer ausfindig zu machen und nicht Personen, welche zu einer Tat (grundsätzlich) fähig wären. Postmoderne Kriminalitätsbekämpfungstechnologien sollten nur gestützt auf einen hinreichenden Tatverdacht oder konkrete Verdachtsmomente einge-

---

735 Vgl. etwa HENSLER; SOÒS/VÖGELI.

736 SINGELNSTEIN/STOLLE 2012, S. 68; HASSEMER 2006, S. 135 f. Siehe auch THIEL, S. 81 f.

737 Siehe dazu ZERBES, S. 285 ff.; THIEL, S. 66 f. und 134 ff.; SIMON D., S. 133. Vgl. ALBRECHT P. A. 2003, S. 95 f.; SZUBA, S. 296; PUSCHKE/SINGELNSTEIN, S. 118; SIEBER, S. 29.

738 ZERBES, S. 322 f.

setzt werden.[739] Die entsprechenden rechtlichen Grundlagen müssen genügend bestimmt und Verfahrensrechte (unter anderem Mitteilungs- und Berichtigungsrechte) ausdrücklich vorgesehen sein und geachtet werden. Die Tendenzen des Bekämpfungsstrafrechts führen jedoch dazu, dass in der alltäglichen Praxis nicht immer genügend differenziert wird. Der (potenzielle) Täter und nicht die Tat an sich gerät zusehends ins Zentrum des Blickfelds.[740] Täterprofile grenzen möglicherweise die Suche ein, wenn nach einem bestimmten Täter gefahndet wird. Sie helfen jedoch weniger bei der präventiv-polizeilichen Bedrohungserforschung, denn präzise Voraussagen sind vor allem eins: Glücksfälle.

Wie eingriffsintensiv die dargestellten Kriminalitätsbekämpfungstechnologien sind, hängt unter anderem auch wesentlich von ihren Folgen für die Zielpersonen sowie mitbetroffene Dritte und der jeweils herrschenden Umsetzungspolitik[741] ab. Folgeeingriffe und -massnahmen können, insbesondere auch angesichts der nicht unerheblichen Streuwirkungen auf an sich Unverdächtige, oftmals kaum vermieden und lediglich in geringem Masse durch organisatorische und strafprozessuale Vorkehrungen vermindert oder abgeschwächt werden. Um einer ausufernden Verdachtsausweitung und anderen Entgrenzungstendenzen[742] entgegenzutreten, ist es daher unerlässlich, den Einsatz der jeweiligen Kriminalitätsbekämpfungsinstrumente vorgängig genau und klar zu regeln und im Einzelfall sorgfältig zu planen. Gegebenenfalls ist nach der Planungsphase vom Einsatz abzusehen, wenn nicht garantiert werden kann, dass die vorgegebenen Schranken (etwa aus technischen Gründen) eingehalten werden können. PUSCHKE und SINGELNSTEIN ist deshalb zuzustimmen: „Je früher und unabhängiger ein Eingriff erfolgt, umso bestimmter muss die Regelung und umso gewichtiger müssen die Gründe hierfür sein.“[743] Eine vorausgehende, umfassende und bereichsspezi-

---

739 Vgl. ALBRECHT P. A. 2003, S. 171; SIMON, S. 274 und insb. 280; SCHWEIZER/MÜLLER, S. 386; MIDDEL, S. 335 ff.

740 Bei aller Opferzentrierung (Opferschutz, Opferinteressen, Ansprüche potenzieller Opfer etc.) geht teils vergessen: Der (potenzielle) Täter braucht den Schutz *vor dem Staat*, jener soll ihm nicht hilflos ausgeliefert sein. Vgl. dazu STEGMANN A., S. 214 f.

741 Z. B. hinsichtlich der noch hinzunehmenden Falsch-Positiven-Rate, siehe INTRONA/NISSENBAUM, S. 46.

742 Zu Tendenzen der Entgrenzung, siehe etwa HASSEMER 2006, S. 134; ISENRING/KESSLER, S. 34; KUNZ 2002, S. 728 ff.; KRASMANN, S. 313 ff.; NOGALA/SACK, S. 153; THIEL, S. 474 f.; SIEBER, S. 27 ff.; SINGELNSTEIN/STOLLE 2012, S. 107 ff; VOLKMANN, S. 217 ff.; ZERBES, S. 278 und 332 f.

743 PUSCHKE/SINGELNSTEIN, S. 118. Ähnlich der Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, §§ 104 und 112.

fische Zweckbestimmung ist in diesem Sinne sehr bedeutsam. Sie legt neben den Einsatzbedingungen auch klar fest, wofür die gesammelten Informationen verwendet werden sollen und dürfen.[744] Zweckbindungsklauseln scheinen ein gutes Mittel zu sein, die nachträgliche Verwendung von Erkenntnissen aus Videoüberwachungs- oder Onlinedurchsuchungsmassnahmen einzuschränken. Weiter kann das Risiko, dass Daten unzulässigerweise auf Vorrat erhoben[745] oder Informationen zweckentfremdet verwendet oder ausserhalb des Bearbeitungszwecks verknüpft werden, zumindest vermindert werden.[746] Indes stellt die Zweckbindung ein besonderes Problem bei rasterfahndungsähnlichen Methoden dar, da diese personenbezogene Daten aus verschiedenen Datenquellen in der Regel gerade nicht so verwenden, wie es die entsprechenden Datenbanken eigentlich vorsehen.[747]

A. Informationsverarbeitung, Datenbanken und Verdachtsregister

Gemäss der dargestellten Rechtsprechung des Bundesgerichts, des EGMR und analog der Rechtsprechung des deutschen Bundesverfassungsgerichts verursachen Informationsverarbeitungsprozesse insbesondere dann Grundrechtseingriffe, wenn sie (in mehreren Schritten) verknüpft oder für Kreuzabgleiche verwendet werden. Verdachtsunabhängige oder anlasslose Komponenten und Elemente, die es beispielsweise erlauben, Persönlichkeits- und Bewegungsprofile zu erstellen, intensivieren den Eingriff. Besonders hinsichtlich Datenverknüpfungen ist daher eine Zweckbindung der Ausgangs- *und* Verknüpfungsdaten zu verlangen.[748]

Ein Vorschlag zur Begrenzung der Eingriffsintensität von digitalen Datensondierungen (zum Beispiel mittels Data-Mining-Programmen) ist die stufenweise Anonymisierung der automatisiert erhobenen Daten. Je nach menschlichem Nutzer und je nach Gebrauchszweck werden diese Daten ausführlicher offenbart.[749] Ein Beispiel: Eine Kriminalbehörde hat mehr Befugnisse als ein Marktforschungsinstitut; die Verhinderung des Terrorismus legitimiert die unanonymi-

---

744 PETRI, G N. 37. Ausführlich bzgl. der Videoüberwachung: MÜLLER L. 2011, S. 219-222 und 226 ff.

745 Vgl. Bericht GPDel, S. 7721; Botschaft BWIS 1994, S. 1197 f.; PETRI, G N. 37.

746 Siehe PROBST, S. 12 f.

747 RUDIN, S. 278 f.; PETRI, G N. 531 f. und 562 f.

748 Siehe etwa PETRI, G N. 21 und 54; PROBST, S. 39.

749 FIENBERG, S. 207 ff.; für andere technische Begrenzungsmöglichkeiten: NOWAK, S. 21 ff.

sierte Einsicht in die kompletten, ein Strassenraub nur in eng begrenzte Daten. Derartige Vorkehrungen könnten unangemessene Verwendungspraktiken im Sinne der Verhältnismässigkeit eindämmen. Die Daten werden natürlich trotzdem erhoben, bevor sie je nach Anwender und Anwendungsart verschleiert werden. Somit können Behörden sie trotzdem verwenden, insofern Verwendungszwecke als verhältnismässig eingeschätzt werden. Die Bedingungen der Einsichtserlaubnis können in dieser Hinsicht stark variieren, wenn die Gesellschaft durch instabile Vorstellungen über Kriminalität geprägt ist.[750] Zudem kann die Missbrauchsgefahr dadurch nicht komplett verhindert werden. Rechtliche Barrieren (beispielsweise mittels enger Deliktskataloge und klarer Voraussetzungen für das Datensammeln durchgesetzt), welche bereits *vor* der Erhebung der Daten greifen, wären eine weitere Möglichkeit, die Achtung der Grundrechte zu gewährleisten – einmal erhobene Daten führen in Versuchung, sie auch zu verwenden.[751]

Wichtig ist zudem, dass die sich abzeichnende Weiterentwicklung etwa des Internets und des Mobilfunks nicht unberücksichtigt bleibt. Die Vorratsdatenspeicherung wird momentan noch häufig auf der Grundlage bereits wieder antiquierter Möglichkeiten und Gewohnheiten diskutiert. Neue Technologien wie das Voice-over-IP (VoIP), billige Flatrates für die mobile Internetnutzung, die rege und verbreitete Nutzung von sozialen Netzwerken und vielen anderen Diensten lassen Nutzer immer mehr Aktivitäten über mobile Geräte abwickeln. Für die nahe Zukunft dürfte demnach absehbar sein, dass ein Grossteil der technikaffinen Generation beinahe permanent mit dem Mobilfunknetz oder Internet verbunden ist.[752]

Eine unbestimmte Umsetzung der sicherheitspolizeilichen Rasterfahndung in die schweizerische Rechtsordnung wäre gemäss dem Legalitätsprinzip unzulässig, indes auch die Umsetzung einer restriktiv geregelten Variante wohl nur bedingt zu begrüssen. Es handelt sich bei ihr und ihrer Steigerung der Massendatenver-

---

750 Zum Verhältnismässigkeitsprinzip als lediglich „weiche“ Schranke, siehe unten Vierter Teil, Kapitel V.D.

751 Gl. A. wie OBERHOLZER 2003, S. 332; ähnlich NOWAK, S. 8 und 46 f. Jedoch auch diesbzgl. sollte man sich nicht der Illusion hingeben, diese (verfassungs-)rechtlichen Schranken wären absolut.

752 Vgl. dazu KURZ/RIEGER, S. 28; LSE BRIEFING, S. 15 ff. An dieser Stelle lediglich der Hinweis auf den Forschungsbericht von LATZER ET AL. und Grafiken des Bundesamts für Statistik zum massiven Anstieg der (mobilen) Internetnutzung in den letzten Jahren in der Schweiz (<http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04.html>).

arbeitung um Methoden, die grosse Verdachtsforschungspotenziale in sich bergen und theoretisch flächendenkend angewendet werden können.[753] Sie sind in einem „Klima der Furcht“[754] äusserst geeignet, entgrenzende Bedürfnisse abzudecken. Heute scheinen diese Methoden noch zu aufwendig, um im grossen Stil angewendet zu werden, was faktisch eine Schranke ausufernder Einsätze sein kann. Dies könnte sich (unter anderem mit INDECT) ändern.[755] Mit der Entwicklung neuer Automatisierungstechniken ist zu mutmassen, dass die sicherheitspolizeiliche Rasterfahndung und die Massendatenverarbeitung ohne klare, genügend bestimmte gesetzliche Vorschriften schwer unter Kontrolle zu halten sein werden.[756] Dafür versprechen ihre automatisierten Varianten zu schnelle Ergebnisse, welche zudem mühsame manuelle Ermittlungen scheinbar überflüssig machen.

Weniger kritisch zu beurteilen wäre die strafrechtliche Rasterfahndung. Solange sie strikt innerhalb des von den Grundrechten und den rechtsstaatlichen Prinzipien vorgegebenen Rahmens durchgeführt würde, könnte sie zwar durchaus in heikle Bereiche vordringen, leichte Eingriffe in die Freiheiten betroffener Personen dürften aber nach der zitierten bundesgerichtlichen Rechtsprechung zu rechtfertigen sein. Auch für sie ist indes eine hinreichend bestimmte gesetzliche Ermächtigungsgrundlage im schweizerischen Recht zu verlangen. In der Regel sollte dann ein für die strafrechtliche Rasterfahndung vorausgesetzter *hinreichender* Anfangsverdacht gegen bestimmte Personen beispielsweise verhindern, dass unspezifisch und unter Zuhilfenahme vager Kriterien nach Personengruppen gefahndet wird. Bestehen klare, hinreichend bestimmte Grundlagen und führt die zuständige Behörde das Verfahren in diesem Rahmen und unter Aufsicht übergeordneter Instanzen aus, scheint aus *rechtlicher Sicht* daher zunächst wenig gegen die strafrechtliche Rasterfahndung zu sprechen. Angesichts des Trends, Straftatbestände auf Vorbereitungshandlungen auszuweiten und Vorfeldermittlungen durchzuführen, überschreitet jedoch auch die *strafrechtliche* Rasterfahndung zusehends die Grenzen zwischen den Rechtsgebieten und gleicht in diesen Fällen stark ihrer präventiv-polizeilichen Variante. Eine derartige „präventiv-strafrechtliche“ Rasterfahndung umgeht qualifizierte Schranken des Polizeirechts.[757] Es wäre somit zu überlegen, sollten dereinst rechtliche Grundlagen für

---

753 Siehe etwa BVerfGE 115, 320 (355 ff.).
754 Siehe unten Dritter Teil, Kapitel I.
755 Vgl. WALDER/HANSJAKOB, S. 279.
756 Vgl. RUDIN, S. 282.
757 Vgl. ZERBES, S. 360 ff.

Rasterfahndungen in der Schweiz geschaffen werden, ob staatliche Behörden zu entsprechenden Befugnissen überhaupt ermächtigt oder wie zurückhaltend entsprechende Anträge genehmigt werden sollen. In diesem Zusammenhang scheint es einerseits begrüssenwert, dass das Bundesgericht pragmatisch versucht, postmodernen Technologien, die gesetzlich nicht geregelt sind, über den Weg der Rechtsprechung gewisse Grenzen vorzugeben, so etwa geschehen hinsichtlich Antennensuchläufen.[758] Andererseits wären konsequenterweise hinreichend bestimmte Ermächtigungsgrundlagen, in Form klarer gesetzlicher Grundlagen, für diese Methoden zu verlangen, und solange diese nicht bestehen, kein Einsatz gutzuheissen. Nur dergestalt kann eine klare Rechtslage entgrenzenden Einsätzen dieser Instrumente vorbeugen.

Verdachtsregister und polizeiliche Informationssysteme müssen strengen Anforderungen gerecht werden.[759] Dasselbe gilt für halb-öffentliche Verdachtsregister, welche häufig zusätzlich die problematischen Elemente der öffentlichen Register in sich vereinen.[760] Gestützt auf Verdachtsregister können verschiedene „Präventivmassnahmen" ausgesprochen werden und Nebenfolgen entstehen. Es wird dabei oft betont, es handle sich bei diesen Massnahmen um reine vorsorglichsichernde, verwaltungsrechtliche Massnahmen und gewisse, unbeabsichtigte Nebenfolgen für den Betroffenen seien systembedingt nicht zu verhindern. Der Kern der rechtlichen Kritik an Verdachtsregistern zielt genau auf diese Punkte ab: das (zuweilen fehlerhafte) Sammeln und Anhäufen von Personendaten, die Verwässerung von Verfahrensgarantien durch verwaltungsrechtliche oder politische Massnahmen mit teils pönalem Charakter und die zahlreichen (faktischen) Konsequenzen für den Betroffenen wie auch für Dritte, die teils bewusst als (symbolische) Nebensanktion ausgespielt werden (Prangerwirkung, soziale Isolation etc.).[761] Häufig betreffen Verdachtsregister sensibelste Daten (aus dem

---

758 Siehe oben Erster Teil, Kapitel I.G.4.

759 Siehe etwa STUDER, S. 68; SCHEFER, S. 63 f.; SCHWEIZER 2008, N. 53 zu Art. 13 BV.

760 Bspw. kennt aber Grossbritannien ein Sexualstraftäterregister, das, abgesehen von der relativ zurückhaltenden Auskunftspflicht an bestimmte fremde Behörden und ausgewählte Private (z. B. Schulen bei der Anstellung von Lehrkräften), ausschliesslich Merkmale eines nicht-öffentlichen Registers aufweist. Siehe oben Erster Teil, I.B.3.

761 Siehe etwa EMMERSON, N. 54 ff. MEYER, S. 77 meint, das Verfahren des UN-Sanktionsregimes trage zu „technokratische Züge", um behaupten zu können, die UN-Terrorliste verfolge bewusst auch eine Prangerwirkung. Diese symbolische Wirkung scheint öffentlichen Täterlisten m. E. aber faktisch kaum abzusprechen zu sein. Dabei ist m. E. nur zweitrangig erheblich, ob diese als (Neben-)Zweck bewusst verfolgt oder als Kollateralschaden in Kauf

Privatbereich) der Betroffenen. Dies erfordert erhöhte Vorsicht bei der Bearbeitung dieser Daten. Derartige Datenbestände bedürfen daher effektiver Kontrollmechanismen und der gewissenhaften Aufsicht durch eine unabhängige Stelle. Insbesondere auch Einträge in nicht-öffentliche Datenbanken bedingen ein sorgfältiges Vorgehen, da sie der unmittelbaren Aufsicht durch die Öffentlichkeit weitgehend entzogen sind.[762] Die Listen werden von meist mehreren Behörden mit Daten, darunter irrelevanten, unzuverlässigen oder fehlerhaften, angereichert. Sortiert keine ständige Überprüfungsstelle unnütze, hinderliche und unzulässig gesammelte oder gespeicherte Daten aus, geht die Übersicht verloren, entstehen „Registerleichen" und Sammlungen von Personendaten oder sonstigen Informationen, die keinen ausreichenden Anknüpfungspunkt aufweisen.[763] Eine richterliche Überprüfung greift meist nicht richtig oder zu spät, weil sie entweder im Regime nicht vorgesehen ist und folglich aus Sicht der betreibenden Institution richterliche Entscheide bezüglich einer verhängten Sanktion irrelevant sind oder die (sozialen) Folgen der Registrierung zeitlich mit der Eintragung zusammenfallen und mit einem Gerichtsurteil nur begrenzt rückgängig zu machen sind.[764] Vorsorgliche Massendatensammlungen und tiefe Schwellen der Datenarchivierungsvorschriften (zum Beispiel unbestimmte und stark vorgelagert ansetzende Eintrittsvoraussetzungen, wie „seltsames Betragen", „auffälliges Verhalten" oder der Kontakt zu anderen Eingetragenen) führen teils zu unbefriedigenden Konstellationen, insbesondere auch zu einer beträchtlichen Streubreite auf das Umfeld und Beziehungsnetz des Betroffenen. Dabei können die Listeneinträge weitreichende Konsequenzen entfalten. Neben mitunter massiven Einschränkungen der Bewegungs- und Handlungsfreiheit für den Betroffenen sind je nach Art des Registers beim Betroffenen und ihm nahestehenden Personen Ausgrenzungs- und Stigmatisierungseffekte zu erwarten oder zumindest nicht auszuschliessen. Die-

genommen wird. Vgl. Richard Barret, Koordinator des UNO-Monitoring Committee, im Interview bei KOCHER, S. 146.

762 STUDER, S. 67 f.; Bericht GPDel, S. 7666 f. Vgl. SCHWEIZER 2008, N. 42 und 44 zu Art. 13 BV.

763 Vgl. dazu den Bericht GPDel; BIGNAMI, S. 668; SPINNER, S. 271.

764 Die Rechtsprechung in der Schweiz zu Einträgen in Hooliganregister geht m. E. in die richtige Richtung, blieb aber nicht unkritisiert, da Massnahmen durch die Erfordernis, eine Verfügung zu erlassen, durch das rechtliche Gehör und durch die richterliche Kontrolle zu wenig zeitnah und flexibel eingesetzt werden könnten. Siehe oben Zweiter Teil, Kapitel I.F.

ses Argument mag zwar teilweise polarisierend benutzt werden[765], dürfte aber vor allem hinsichtlich umfassenderer Register im Bereich Sexualstraftäter oder gewaltbereiter Störer durchaus zutreffend sein.[766] Diese Nebenfolgen sollten mit geeigneten Vorkehrungen möglichst minimiert werden.[767] Zu beachten ist ferner, dass Verdachtsregister für diverse Arten von Datenabgleichen innerhalb oder ausserhalb eines Strafverfahrens und für die Begründung eines Tatverdachts zur Einleitung weiterer Massnahmen herangezogen werden können. Über die Anlasssache hinaus können Verdachtsregister und andere Datenbanken somit ausgezeichnet als (verdachtsbegründende) Hilfsmittel zu weiteren Ermittlungstätigkeiten in anderen und zukünftigen Sachen dienen und ohne Weiteres mit anderen Technologien und Methoden fusioniert angewendet werden.[768]

Während die öffentlichen Register einen degradierenden Effekt auf den Betroffenen oftmals bewusst anstreben, nehmen ihn nicht- beziehungsweise halböffentliche Register teilweise in Kauf, indem die Behörde dem Registrierten das zwischen ihnen herrschende Informationsgefälle aufzeigt. Dieser Fingerzeig kann aus zwei Gründen erwünscht sein: Zum einen macht die Behörde den Betroffenen darauf aufmerksam, dass sich weitere illegale Handlungen nicht lohnen, da man diese ohnehin bemerken werde. Diese Warnung macht dem Betroffenen zum anderen klar, dass ihn sein kriminelles Verhalten in diese Lage gebracht hat und die Gesellschaft ihn deswegen anklagt oder gar verachtet. Die Behörde, welche das entsprechende Register betreibt, bringt sich damit in eine (ihr wohl nicht zustehende) Vormachtstellung gegenüber dem Betroffenen.[769] Sie transportiert damit Moralvorstellungen in einem rechtlichen Vehikel, das für derartige moralische Anklagen tabu sein sollte.

Bei derart schwerwiegenden Eingriffen (bezüglich Intensität und Art) in verschiedene Rechte des Registrierten, wie sie öffentliche Verdachtsregister in der Lage sind zu verursachen, können lediglich sehr eingehende Vorkehrungen de-

---

765 So BARTMANN, S. 126 f. Auch mögen gewonnene Gerichtsverfahren zu „Schulterschlüssen" mit einzelnen Betroffenen führen, so MEYER, S. 77 – aber erst im Nachhinein und recht selektiv hinsichtlich medial wohlwollend und breit rezipierter Verfahren.

766 Vgl. SULLIVAN/HAYES, S. 91; DIGGELMANN, S. 310; MEYER, S. 77; Bericht HRW, S. 78 ff.; KUNZ 2011, S. 356 f.

767 Siehe etwa BARTMANN, S. 128; Bericht HRW, S. 130 f.

768 Werden Daten anlasslos und vorsorglich gesammelt, stehen sie bspw. im Fall, dass eine Person verdächtig wird oder sich eine Bedrohung ankündigt, bereits nutzbar zur Verfügung, vgl. NORRIS, S. 150.

769 Vgl. unten Vierter Teil, Kapitel IV.D.

ren Gebrauch rechtfertigen. Das vom Sicherheitsrat den Mitgliedstaaten vorgegebene Sanktionsregime der UN-Liste ist zu vollziehen, wobei nach Ansicht des EGMR regionale Vorkehrungen zu treffen sind, die Menschenrechte des Betroffenen zu wahren und die Verhältnismässigkeit der Massnahmen zu prüfen.[770] Angesichts der potenziell betroffenen, höchsten Rechtsgüter im Bereich der Terrorismusbekämpfung und der verhältnismässig überschaubaren Anzahl an Einträgen, scheint unter den Voraussetzungen, dass die Einträge auf klar umschriebenen, belastbaren Anknüpfungspunkten beruhen, humanitäre Freigabeklauseln offen stehen und dem Betroffenen zumindest nachträglich effektive Verfahrensrechte zugestanden werden, der Unterhalt der UN-Terrorliste weit weniger problematisch zu sein als noch in den ersten Jahren des Sanktionenregimes.[771] Der kontinuierliche Widerstand aus einigen Mitgliedstaaten (unter anderem der Schweiz) und von Gerichten auf allen Stufen beeinflussten das Sanktionsregime dahingehend stark. Der Sicherheitsrat scheint bemüht, die geforderten Verbesserungen vorzunehmen, was aus rechtsstaatlicher Sicht einen wichtigen Fortschritt darstellt.[772]

Der höchste Gerichtshof der Vereinigten Staaten betonte wiederholt das legitime öffentliche Interesse an der Registrierung von Sexualstraftätern und der Benachrichtigung des Umfelds des Registrierten über seinen Status und hält daran fest, dass die Registrierung nicht vom Rechtsgrundsatz „ex post facto" (entspricht dem Rückwirkungsverbot in der Schweiz) betroffen sein soll. Ausserdem setzt der höchste Gerichtshof der Eintragung *keine Pflicht zur Veranlassung einer individuellen Gefährlichkeitsprognose* voraus, jedoch schliesst er eine solche für die Zukunft nicht aus.[773] Im Gegensatz dazu entschied Grossbritanniens höchstes Gericht, dass die unbefristete und unwiderrufliche Registrierung gegen Art. 8 EMRK (Recht auf Privatsphäre) verstosse.[774] Die britische Rechtsprechung interpretiert die menschenrechtlichen Anforderungen an das Register somit gestützt auf die EMRK enger als diejenige der Vereinigten Staaten und anerkennt, dass gewisse Schranken bei der Anwendung dieses Instruments unerlässlich sind. Aufgrund der dargelegten Mängel, nicht sehr überzeugender kriminalitäts-

---

770 Entscheid des EGMR Nada gg. Schweiz vom 12. September 2012, Nr. 10593/08.

771 Gl. A. wie MEYER, S. 79 f. Ebenso SCHULTE, S. 326; BARTMANN, S. 126.

772 BGE 133 II 450 E. 7.4 S. 463.

773 Siehe die Zusammenfassung der Rechtsprechung bei SCOTT/GERBASI, S. 500.

774 Siehe den Entscheid des England and Wales High Court (Queen's Bench Division), F and Angus Audrey Thompson v Secretary of State for the Home Departement vom 19. Dezember 2008, [2008] EWHC 3170 (QB), insb. E. 11 und 33.

vermindernder Wirkung und einschneidender Folgen für Betroffene und Dritte scheint das Ansinnen der erwähnten parlamentarischen Vorstösse, ein Sexualstraftäterregister in die schweizerische Rechtsordnung einzuführen, kaum akzeptabel umzusetzen. Zumindest müsste eine ernsthafte und eingehende, individuelle Gefährlichkeitsprognosestellung im Einzelfall dazu beitragen, möglichst konkret gefährliche Personen aufzulisten.[775] Verdachtsregister profitieren von der *überschaubaren* Anzahl an Einträgen. Sie werden dadurch in der Praxis leichter zu handhaben. Daher und aus Verhältnismässigkeitsüberlegungen wären lediglich Täter einzutragen, welche schwerste Delikte begangen haben. Weiter wäre die Möglichkeit vorzusehen, den Eintrag zu revidieren und regelmässig durchgeführte Gefährlichkeitsüberprüfungen vorzunehmen, nach denen nach einer angemessenen Zeitspanne der Eintrag zu löschen wäre, wenn der Verurteilte sich gesetzeskonform betragen hat (kein Rückfall) und seine Prognose vorteilhaft ist. Der Eintrag darf mithin ohne regelmässige Überprüfung nicht zeitlich unbeschränkt existieren.[776] Jedenfalls wäre die Einführung einer gesetzlichen Grundlage – auch für ein unter restriktiven Regeln[777] geführtes – *öffentliches* Verdachtsregister gemäss der hier vertretenen Ansicht weder anstrebenswert noch mit der Schweizer Rechtsordnung zu vereinbaren.

B. Video- und Onlineüberwachungsmassnahmen

Der Einsatz von Videoüberwachungstechnologien bedarf einer klaren und bestimmten, bereichsspezifischen gesetzlichen Grundlage.[778] Besteht für die jeweilige Massnahme eine genügend bestimmte und kompetenzgerecht geschaffene rechtliche Grundlage, dürfte, im Lichte der heute in der Schweiz geltenden

---

775 Vgl. NOWARA, S. 110. Diese Anforderung ist bei den herrschenden Sicherheitsbedürfnissen (siehe dazu unten Dritter Teil) nicht leicht durchzusetzen, was etwa bei der Diskussion um die Verwahrungsprognosen in der Schweiz zu beobachten ist.

776 Vgl. GRUBER, N. 6 ff. zu Art. 369 StGB. Dies forderte aber die parlamentarische Initiative Natalie Simone Rickli vom 20. März 2009 (Löschung des Eintrags mit dem Tod des Registrierten).

777 Vgl. dazu Bericht HRW, S. 15 f.

778 BGE 136 I 87 E. 8.3 S. 114 ff.; BVerfG, NVwZ 2007, 688 (690); BAUM, N. 29; FLÜCKIGER, S. 213 ff.; MÜLLER L. 2011, S. 362 und ausführlich DERS., S. 201 ff. (insb. 203). Die Erwähnung etwa, „technische Mittel" einzusetzen, sei erlaubt, stellt keine genügende gesetzliche Grundlage für den Einsatz akustischer Überwachungstechnologien dar und auch die *verdeckte* Videoüberwachung des öffentlichen Raums bedarf einer ausdrücklichen formellgesetzlichen Ermächtigung, siehe MÜLLER L. 2011, S. 225 f.

Rechtsordnung und Rechtsprechung, die Videoüberwachung ohne Identifikations- und ohne Aufzeichnungsmöglichkeit, welche über eine Kurzspeicherung (mit unmittelbarer Löschung) hinausgeht, keine beziehungsweise lediglich leichte Grundrechtseingriffe bedeuten. Die (längerfristige) Aufbewahrung von Aufnahmen alleine führt noch nicht zu schweren Eingriffen, die Aufzeichnung von besonders schützenswerten Daten hingegen schon. Technische Zusatzfunktionen wie das Vergrössern und Fokussieren von Bildausschnitten und das Verfolgen von Personen intensivieren den Eingriff zusätzlich.[779] Die anlasslose Videoüberwachung sollte derart ausgestaltet sein, dass sie grundsätzlich nicht in Grundrechte eingreift. Abgesehen von einer perfekt funktionierenden, vollkommen automatisierten Videoüberwachung kommen dafür kaum Varianten in Betracht.[780] Ausnahmsweise findet bei Überwachungssystemen, welche *keine* Live-Sicht zulassen und wo weder manuelle noch automatische Analysen des Materials *vor* der Einleitung eines Strafverfahrens vorgenommen werden, das Störerprinzip keine Anwendung. In diesem Fall ist jene nicht als (sicherheits-) polizeiliche, sondern einzig als strafprozessuale Massnahme zu werten. Diese Form der Überwachung darf lediglich bezwecken, die Aufnahmen im strafrechtlichen Ermittlungsverfahren zu verwenden. Die bis dahin ungesichteten Aufnahmen dürfen erst auf dem Boden eines konkreten Anhaltspunkts konsultiert werden, etwa auf eine Anzeige hin.[781] Werden die Systeme (nebenbei) in anderer Weise betrieben oder werden deren Ergebnisse in anderer Weise verwendet, handelt es sich bei ihnen zwingend *auch* um polizeiliche Massnahmen der präventiven Gefahrenabwehr. In diesem Fall ist eine akute und konkrete Gefahrenlage im zu überwachenden Raum als Voraussetzung der Massnahme zu verlan-

---

779 Wobei zu bedenken ist, dass heutzutage kaum noch Systeme ohne derartige Zusatzfunktionen existieren dürften, vgl. ROGGAN 2001, S. 136; BÜLLESFELD 2002, S. 146 und 253; BARTSCH, S. 91 f. Insbesondere hochauflösend aufgezeichnete Übersichtsbildner sind nachträglich in der Regel so zu bearbeiten, dass eine Identifizierung möglich ist (vgl. BARTSCH, S. 95 mit Hinweisen). Indes sind natürlich auch neue Technologien denkbar, welche die Eingriffsintensität im Gegenteil reduzieren und somit allenfalls ausgleichen könnten (bspw. automatisches Unkenntlichmachen von Gesichtern etc.) – u. a. sog. „Privacy Enhancing Technologies", mit denen der Datenschutz und das Grundrecht auf informationelle Selbstbestimmung durch technische Vorkehrungen gefördert werden sollen, siehe dazu BIER/SPIECKER GEN. DÖHMANN, S. 614; BAUM, N. 43; LINGG, S. 19; KAMMERER 2008, S. 155; MÜLLER L. 2011, S. 21 f. und 142 jeweils mit weiteren Hinweisen und Beispielen.

780 Siehe dazu BVerfG, NVwZ 2007, 688 (691); BVerfGE 120, 378 (402 f.); ROSSNAGEL/DESOI/HORNUNG 2011, S. 696. Eine flächendeckende Überwachung ist nach Ansicht des Bundesgerichts ohnehin unverhältnismässig (siehe BGE 136 I 87).

781 So das Bundesgericht in BGE 133 I 77 E. 5.5 S. 87.

gen.[782] Im Regelfall hat die gesetzliche Grundlage daher die praktischen Einsatzbedingungen und möglichen Verwendungszwecke zu benennen und insbesondere einen im Voraus benannten Anlassgrund und eine klare Zweckbindung vorzusehen, damit Videoüberwachungstechnologien rechtssicher angewendet werden können.[783] Schwierigkeiten bereiten dabei vor allem die rasche technologische Weiterentwicklung und die (zukünftig) verfügbaren Varianten der smarten Überwachung. Das ist besonders problematisch, da für potenziell Betroffene gerade die Möglichkeiten *dieser* Technologien in der Regel verborgen bleiben.[784]

Generelle und absolute Aussagen zur Zulässigkeit der neuen Generation der Videoüberwachung und ebenso der anderen postmodernen Kriminalitätsbekämpfungstechnologien sind demnach schwerlich zu treffen. Um die Zulässigkeit einer Raumüberwachungsmassnahme sowie die Intensität der potenziellen Grundrechtseingriffe zu bestimmen und die Verhältnismässigkeit der einzelnen Methoden zu prüfen, sind deshalb jeweils die möglichen Einsatzgebiete und -formen der Überwachung immer im konkreten Einzelfall und unter Einbezug aller beeinflussenden Faktoren zu betrachten.[785] Es ist festzustellen, dass diesbezüglich in Polizeigesetzen mancherorts relativ grosses Ermessen zugestanden und teilweise bereits Raum für potenziell intensivere Methoden und Technologien offengelassen wird.[786] Die dargestellten, einschränkenden Entwicklungen in der Rechtsprechung des Bundesgerichts und des EGMR sind daher zu begrüssen.

Immer zu berücksichtigen ist, dass die weiter oben im Ersten Teil diskutierten Studien darauf hinweisen, dass die reale Raumüberwachung vor allem auf einige Arten leichter Delinquenz wirkt: Nicht nur die Eingriffe in die Grundrechte durch die Videoüberwachung können leicht sein, sondern auch die dadurch ver-

---

782 BARTSCH, S. 210; FLÜCKIGER/AUER, S. 938; ROHNER, N. 25 zu Art. 22 BV. Vgl. MÜLLER L. 2011, S. 195 und 227. In Betracht käme bspw. ein Park mit lebendiger Drogenszene oder ein abgelegenes Gebiet mit hohem Vandalismusrisiko, also Orte, an denen in erster Linie der Aufenthalt von Zielpersonen zu erwarten ist.

783 Ausführlich MÜLLER L. 2011, S. 211 ff., 219 ff. und 272 f. Ebenso ROSSNAGEL/DESOI/HORNUNG 2011, S. 697. Siehe auch BGE 136 I 87 E. 3.1 S. 90.

784 Siehe dazu MÜLLER L. 2011, S. 225 f. mit Hinweisen auf die Rechtsprechung des EGMR zu geheimen Überwachungsmassnahmen.

785 MÜLLER L. 2012b, S. 248; DERS. 2011, S. 257; FLÜCKIGER/AUER, S. 925; HORNUNG/DESOI, S. 158; ROSSNAGEL/DESOI/HORNUNG 2011, S. 697. Vgl. BGE 136 I 87 S. 114 f. E. 8.3. Ausführliche Besprechung des datenschutzrechtlichen und grundrechtlichen Kontexts sowie insgesamt der rechtlichen Zulässigkeit der Videoüberwachung des öffentlichen Raums in der Schweiz: MÜLLER L. 2011, S. 31-95, 97-193 und 195-306.

786 Vgl. etwa die Beispiele bei MÜLLER L. 2011, S. 224 f.

hinderten oder geahndeten Handlungen.[787] Oft schränken die gesetzlichen Grundlagen den Einsatz der Videoüberwachung nicht auf bestimmte Schweregrade von Straftaten ein. Beispielsweise dürfen nach bernischem PolG mittels Videoüberwachung Personen auch hinsichtlich Übertretungen verfolgt werden.[788] Diesen Punkt verschärfend, versuchen neuere Strategien, die gesellschaftlichen Sicherheitsbedürfnisse zu befriedigen, indem die polizeiliche Präventivabwehr bereits sehr früh bei „unerwünschten Verhaltensweisen" ansetzen soll.[789] Ob diesbezüglich eine angemessene Zweck-Mittel-Relation gegeben ist, also etwa das Herumlungern oder das Wegwerfen von Abfall den Eingriff in Grundrechte und den für die Installation, Instandhaltung und Kontrolle der Überwachung betriebenen Aufwand erfordert, ist fraglich – insbesondere dann, wenn als Nebeneffekt zusätzlich sich konform verhaltende Bürger überwacht oder eingriffsintensivere Technologien zugeschaltet werden.[790]

Dieselben allgemeinen Tendenzen, verfügbare technische Mittel ausreizen zu wollen, zeichnen sich im virtuellen Raum ab.[791] Ermächtigungsgrundlagen für Überwachungstechnologien setzen speziell in diesem Zusammenhang eine qualifiziert klare, bestimmte und formale gesetzliche Regelung voraus. Sie haben ansonsten die Tendenz einer Kontrolle zu entgleiten. Massnahmen im virtuellen Raum haben vielfach einen „neuen, eigenständigen Charakter".[792] Analogien zu anderen Massnahmen (im realen Raum) überzeugen oft nicht vollends, und einzelne Versatzstücke aus Vorschriften zu diesen anderen Massnahmen zu kombinieren, um die fehlende gesetzliche Grundlage zu ersetzen, ergibt zumeist keine

---

787 Das Bundesgericht scheint diese Tatsache teilweise zu berücksichtigen (z. B. in BGE 120 Ia 147 ff.). Vgl. BÜLLESFELD 2002, S. 212 ff.

788 Siehe dazu STEGMANN M., S. 79. Beschränken die kantonalen oder kommunalen Normen den Einsatz der Videoüberwachung hingegen auf Verbrechen und Vergehen, dürfen deren Aufzeichnungen im Strafverfahren nicht als Beweismittel verwendet werden, sofern eine Übertretung verfolgt werden soll, siehe MÜLLER L. 2011, S. 196. Skeptisch hinsichtlich der Verwertung von Aufzeichnungen zur Verfolgung von Übertretungen, DERS. S. 268 f.; BARTSCH, S. 210 f.; BÜLLESFELD 2002, S. 210 f.

789 BARTSCH, S. 40 ff., insb. S. 42 mit Hinweisen. Siehe dazu etwa LINGG, S. 65 f. und 80, die berichtet, dass die Videoüberwachung auf dem Bahnhofplatz Luzern wohl neben dem Zweck, kriminelle Handlungen und Bedrohungen zu verhindern und zu ahnden, mitunter auch darauf abzielte, „rauschtrinkende, alkoholisierte Jugendliche", Randständige und Abfallsünder vom Areal zu vertreiben.

790 Vgl. dazu etwa MÜLLER L. 2011, S. 222.

791 Vgl. etwa GAUTIER/BUSCH, S. 56.

792 Urteil des BGH StB 18/06 vom 31. Januar 2007 N. 10 zur Zwangsmassnahme der verdeckten Online-Durchsuchung.

befriedigende Lösung.[793] Es gestaltet sich demnach schwierig, die Eingriffsintensität bei verschiedenen Einsatzkonstellationen zu nivellieren und bei neu entwickelten Technologien entsprechende rechtliche Grundlagen zu finden oder zu schaffen sowie das rechtlich noch Zulässige mit einleuchtenden Gründen klar zu definieren.[794] Je nach der gewählten Einsatzart und denkbaren Modifikationen an den verwendeten Programmen variiert die Intensität des Eingriffs und der Folgeschäden, weshalb die jeweiligen Ausführungen immer mit einem Auge auf verschiedene Einsatzvarianten zu lesen sind.

Die meisten Varianten bedeuten gravierende Grundrechtseingriffe und sollten deshalb lediglich in Ausnahmefällen zum Einsatz gelangen. Es kann zudem momentan wohl lediglich geschätzt werden, inwieweit der Einsatz von Govware ein leichterer Weg als die herkömmliche Durchsuchung vor Ort ist, um an die gewünschten Zieldaten zu kommen.[795] Jedenfalls sind Online-Durchsuchungen und -überwachungen grundsätzlich in der Lage, „besonders massive Beeinträchtigungen" bei betroffenen Personen (Zielpersonen und miterfasste Dritte) zu bewirken.[796] Insbesondere die erhebliche Streubreite, unter anderem bedingt durch technische Schwachstellen, ist problematisch.[797] Für Online-Überwachungstechnologien, die zu präventiv-polizeilichen oder nachrichtendienstlichen Zwecken eingesetzt werden sollen, bleibt daher, analog zu den in diesen Bereichen einzusetzenden Rasterfahndung, sehr wenig Spielraum.[798] Die Beschränkung

---

793 Vgl. Urteil des BGH StB 18/06 vom 31. Januar 2007 N. 22; VETTERLI, S. 451 f.; Niklaus Ruckstuhl im Interview bei STÖCKLI, S. 17. Analog verwendet werden können hingegen die rechtlichen *Grundsätze* und *Überlegungen*, die für den realen Raum gelten.

794 Bzgl. der DPI stellen sich bspw. die Fragen, ob Tiefe der Inspektion gleich Eingriffsschwere bedeutet und wie tief tief genug ist, um einen Nutzen daraus ziehen zu können. Vgl. COOPER, S. 143 ff.; GLESS 2012, S. 10.

795 Einerseits scheint der Aufwand, Govware einzusetzen, beträchtlich, siehe Botschaft BÜPF 2013, S. 2772. Andererseits ist zu vermuten, dass deren Einsatz mit fortschreitender technischer Entwicklung einfacher zu bewerkstelligen sein wird und dementsprechend aus einer Effizienzperspektive betracht eine durchaus valable Option werden könnte, vgl. TSCHENTSCHER, S. 388.

796 Gl. A. wie ZERBES, S. 42 f.; Vgl. Botschaft BWIS II 2007a, S. 5110; BGE 122 I 182 E. 4.c S. 190. A. A. ist HOFMANN, 124, der die Online-Durchsuchung etwa gegenüber einer klassischen Durchsuchung als mildere Massnahme ansieht, da nicht die gesamte Wohnung des Betroffenen durchsucht werde, und der meint, der Computernutzer nehme die Infizierungsgefahr seines Computers in Kauf, wenn er sich des Internets bediene.

797 Anstatt vieler ROGGAN 2009, S. 261 f. Siehe oben Zweiter Teil, Kapitel I.D.

798 TSCHENTSCHER, S. 385. Vgl. für die präventiv-polizeiliche Rasterfahndung Zweiter Teil, Kapitel I.E. Zu erfüllende Bedingungen gemäss BVerfGE 120, 274 (327 f.): „Konkrete Ge-

dieser Instrumente in diesen von präventivem und proaktivem Handeln geprägten Bereichen auf dieselben restriktiven Voraussetzungen wie im Strafverfahren ist unter den heutigen Gegebenheiten schwer vorstellbar. Aus dem nicht bedingungsgerechten Einsatz aber sind eine grosse Streubreite hinsichtlich privater und geschäftlicher Informationen, die Miterfassung von ganzen Beziehungsnetzen und zahllose Zufallsfunde zu erwarten.

Abgesehen von diversen technischen Schwachstellen und unter restriktiven Voraussetzungen sind zulässige und rechtsstaatlich vertretbare Varianten von Govware und DPI aber durchaus denkbar. Momentan verhindern indes die angesprochenen technischen und praktischen Probleme sowie die fehlenden gesetzlichen Grundlagen, dass diese rechtskonform eingesetzt werden können.

In den bekanntgewordenen Fällen der schweizerischen und deutschen Behörden wurde Govware in verhältnismässig bescheidenem Umfang verwendet. Die (doppelte) Subsidiarität des vorgesehenen E-Art. 269ter StPO verlangt, dass weniger eingriffsintensive Varianten dem Einsatz von Govware vorgehen. Alternativen für die Überwachung und Speicherung der Netzwerkkommunikation (Quellen-TKÜ) existieren, wenn auch im Einzelfall abgewogen werden muss, ob diese das Ziel gleichermassen zuverlässig wie Govware-Programme erreichen können. Die Bereitschaft der Anbieter von Internetdiensten, mit staatlichen Behörden zu kooperieren, dürfte meist gegeben sein. Auch die DPI könnte in diesem Bereich mildere Einsatzvarianten anbieten.[799] Geht es lediglich um die Sicherstellung von Daten in einem bestimmten Zeitpunkt, scheint ferner die Beschlagnahme und Durchsuchung von Datenträgern (Art. 246-248 und 263 ff. StPO) eine schonendere, weil offen kommunizierte, Alternative.[800]

Die DPI-Technologie kann zwar in einiger Hinsicht eine weniger einschneidende Alternative als das Eindringen in informationstechnische Systeme mittels Govware darstellen. In anderer Hinsicht ist sie wesentlich problematischer, weil

fahr für ein überragend wichtiges Rechtsgut", „existenzielle Bedrohungslage", „hinreichende Eintrittswahrscheinlichkeit", „Annahmen und Schlussfolgerungen [besitzen] einen konkret umrissenen Ausgangspunkt im Tatsächlichen".

799 Siehe zu den Alternativen und der Kooperationsbereitschaft der Anbieter BRAUN, S. 685 mit zahlreichen Hinweisen; BENDRATH, S. 26. Anzumerken ist aber, dass diese Kooperationsbereitschaft weniger nützt, wenn gut verschlüsselte Datenübertragungen überwacht werden sollen, die auch die Backdoors der Anbieter umgehen können (vgl. oben Fn. 255), siehe TSCHENTSCHER, S. 385; BUERMEYER/BÄCKER, S. 434; LSE Briefing, S. 26 (bzgl. DPI).

800 Vgl. THORMANN/BRECHBÜHL, N. 1 zu Art. 246 StPO.

sie sich besser zur verdachtsunabhängigen Überwachung und Sondierung der Kommunikation mittels Algorithmen eignet. Es fragt sich diesbezüglich, ob es in näherer Zukunft technisch möglich sein wird, Govware und DPI in effizienter Art und Weise auf eine grössere Anzahl von Personen, auf bestimmte Kreise, Risikogruppen oder Risikokategorien, anzuwenden. Kombinationen mit anderen Überwachungstechnologien könnten zu sehr aussichtsreichen, jedoch höchst eingriffsintensiven Instrumenten führen. Zum Beispiel könnte das heimliche Online-Monitoring von Risikopersonen beziehungsweise virtuellen Risikoräumen oder das Online-Sondieren anhand bestimmter Risikokriterien mittels Govware und DPI grundsätzlich erfolgversprechende Ansätze der Kriminalitätsbekämpfung im virtuellen Raum bieten.[801] Die Feinjustierung der Inhalts-Filterung im Internet und des Online-Monitorings von Risikopersonen sind wohl, solange sie den Kern der betroffenen Grundfreiheiten nicht antasten, letztlich Geschmackssache und damit dem demokratischen Willen überlassen. Diese Strategien kamen im öffentlichen Diskurs aber noch verhältnismässig wenig zur Sprache.[802]

Die automatisierte, anlasslose Überwachung des virtuellen Raums mittels Methoden wie der Algorithmic Knowledge Discovery führten indes zu einem gigantischen Online-Überwachungspotenzial, falls es dereinst möglich sein sollte derartige Technologien erfolgreich einzusetzen. Effizient funktionierende anlasslose, verdachtsforschende und -gewinnende Govware- und DPI-Technologien wären auch aus rechtlicher Sicht sehr bedenklich.[803] Da automatisierte Programme heute jedoch (noch) nicht in der Lage sind, Daten derart zuverlässig zu sondieren, „dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte“[804], scheint eine derart anlasslose Verdachtsforschung, aber auch Verdachts*aus*forschung, lediglich aufgrund vager Verdachtsmomente in den Bereichen der Sicherheitspolizei und Strafverfolgung zu betreiben unzweckmässig – in der Regel unabhängig davon, welche Überwachungstechnologie zum Einsatz gelangt.[805] Werden verdachtsgewinnende Technologien technisch mangel-

---

801 Vgl. GLESS 2012, S. 18 f. zum Monitoring der Internetnutzung und <http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2012/ref_2012-06-21.html> zum Monitoring von Websites.

802 Vgl. PETRI, G N. 23 f.; THIEL, S. 57 und 64.

803 Vgl. LSE BRIEFING, S. 55.

804 BVerfGE 120, 274 (337).

805 Im nachrichtendienstlichen Bereich werden derartige Technologien bereits heute scheinbar sehr grossflächig angewendet (ob und wie erfolgreich, bleibe dahingestellt), siehe oben Erster Teil, Kapitel II.B.3. und III.A.

haft implementiert, müsste unter anderem vielfach eine hohe Falsch-Positiven-Rate in Kauf genommen werden.[806] Insgesamt kann angelehnt an die Leitlinien des deutschen Bundesverfassungsgerichts festgehalten werden, dass die Zielgerichtetheit, die im Voraus klar vereinbarte Zweckbestimmung und das Anknüpfen an eine ausreichend hohe Einschreitschwelle (Katalog mit schwersten Delikten, grundsätzlich kein Einsatz im Vorfeldstadium) diejenigen Punkte darstellen, die zuvorderst zu beachten sind.[807]

Die Authentizität, Integrität und Vertraulichkeit der gesammelten Daten sollte darüber hinaus in jedem Stadium gewährleistet sein: einerseits für die Glaubwürdigkeit der daraus abgeleiteten Informationen und Hypothesen und andererseits, um die Daten des Betroffenen und das Zielsystem nicht Unbefugten in die Hände zu spielen. Systeme Dritter dürfen nicht beeinträchtigt werden. Beispielsweise muss der Verbreitung von eingesetzter Govware vorgebeugt werden.[808] Von den postmoderne Kriminalitätsbekämpfungstechnologien einsetzenden Beteiligten ist zudem unbedingt eine unversehrte und vor unbefugten Personen geschützte Übertragung der Daten zu verlangen. Sie müssen jederzeit, bei jedem Schritt ein hohes Verschlüsselungsniveau gewährleisten und von ihnen geschaffene Sicherheitslücken des infizierten Systems, so diese denn unvermeidbar sind, für Unbefugte schliessen. Zudem ist unter anderem mittels technischer Vorkehrungen dafür zu sorgen, dass lediglich diejenigen Funktionen der Govware gebraucht werden, zu denen die gesetzliche Grundlage und der Genehmigungsentscheid im Einzelfall ermächtigen. Die anwendenden Behörden konnten in den erwähnten Praxisfällen letztlich nicht sicherstellen, dass keines der dargestellten Szenarien eintritt. Solange diese Sicherheiten in der Schweiz

---

806 SKILLICORN 2008a, S. 426, hält hohe Falsch-Positiven Raten für „ärgerlich" („annoying"). Vgl. NOWAK, S. 36. FIENBERG, S. 211 kommt diesbzgl. zum Schluss, die gross angelegten Durchsuchungen von Datenbeständen der virtuellen beziehungsweise digitalen Kommunikation liessen aus der Perspektive eines „risk-utility tradeoff" ein hohes Risiko des Eingriffs in die Privatsphäre erahnen, würden aber wenig Nutzen vorweisen.

807 BVerfGE 120, 274 (328 ff.); WEBER/WOLF/HEINRICH, N. 29; BRAUN, S. 685.

808 BRAUN, S. 684. Vgl. etwa BVerfGE 120, 274 (325 f.). Fraglich ist, ob eine staatliche Haftung bei Schädigungen des Zielsystems oder von Drittsystemen durch die eingesetzten Programme zweckmässig ist, siehe WEBER/WOLF/HEINRICH, N. 29; BRAUN, S. 685; ZERBES, S. 355 ff. (skeptisch); Zusammenfassung der Vernehmlassungen, S. 58.

aus technischen oder praktischen Gründen nicht erfüllt werden können, ist fraglich, ob der Einsatz derartiger Technologien zulässig sein kann.[809]

Neben technischen Vorkehrungen können auch geeignete Verfahrensvorkehrungen dazu beitragen, diese Punkte einzuhalten.[810] Die Verteidigungs-, Aussage- und Zeugnisverweigerungsrechte sollen durch Online-Überwachungstechnologien grundsätzlich geachtet und nicht ausgehöhlt werden.[811] Lediglich in Ausnahmefällen darf von ihnen unter strengen Bedingungen abgewichen werden. Von der einsetzenden Behörde ist daher zu verlangen, dass sie alle Übertragungen verschlüsselt, sicherstellt, dass Manipulationen der Daten erkannt werden und dass sie ihre Schritte protokolliert und dokumentiert.[812] Mit nachvollziehbar und lückenlos geführten Einsatzprotokollen schützt sich die Behörde gleichzeitig davor, die mühevoll zusammengetragenen Ergebnisse im Gerichtsverfahren nicht verwenden zu können (was nach dem doch erheblichen Aufwand einer derartigen Überwachung sehr frustrierend sein dürfte) und vor der öffentlichen Kritik, sie bespitzle unbescholtene Staatsbürger in unzulässiger Weise. In diesem Sinne noch wichtiger ist es, der Bevölkerung transparent zu kommunizieren, welche Online-Überwachungsmethoden der Staat anwendet oder in Betracht zieht, anzuwenden. Die jüngst häufiger auftretenden heimlichen Govware-Affären sorgen letztlich für einen schlechten Ruf der diese Technik einsetzenden Behörde. Das Geheimhalten der Methoden retrospektiv im Zeitpunkt, in dem ihr Einsatz aufgedeckt wird, mit dem Interesse zu rechtfertigen, staatliche Überwachungsmethoden Kriminellen nicht offenbaren zu wollen, überzeugt zuweilen nicht. Staatliches Handeln und die dazu benutzten Mittel bedürfen der Transparenz, selbst wenn diese Offenheit die Kriminalitätsbekämpfungsbehörden

---

809 Zweifelnd, dass „diese Erfordernisse in der Praxis umgesetzt werden können", ALBRECHT F., N. 18 und 19. Ebenso PFITZMANN/KÖPSELL 2009a, S. 542 und 544; ROSSNAGEL/BEDNER/KNOPP, S. 538 f. jeweils u. a. auch zur Vorratsdatenspeicherung. A. A. sind die in der Vernehmlassung zur Revision des BÜPF befragten Fachleute aus dem Polizeibereich, siehe Botschaft BÜPF 2013, S. 2774 f.

810 BVerfGE 120, 274 (331).

811 ZERBES, S. 99 ff.; GLESS 2012, S. 20.

812 PETRI, G N. 61 f.; GERCKE/BRUNST, S. 378; PFITZMANN/KÖPSELL 2009a, S. 544 f.; HANSEN/PFITZMANN; ROSSNAGEL/BEDNER/KNOPP, S. 539 f., jeweils auch zur Vorratsdatenspeicherung. Wobei die daraus entstehenden Daten und Dokumente dem Betroffenen und Dritten zum Nachteil gereichen können, wenn sie später (in einem anderen Zusammenhang oder Verfahren) zweckändernd gegen ihn oder Dritte verwendet werden, siehe PETRI, G N. 606. Zu analogen authentifizierenden Vorkehrungen hinsichtlich der Videoüberwachung, siehe KAMMERER 2008, S. 180 ff.

manchmal in benachteiligte Situationen bringen sollte.[813] Wird der Einsatz zudem lückenlos festgehalten, können nach getaner Arbeit die Ergebnisse und Protokolle auch dem Beschuldigten offengelegt werden, wodurch er zumindest im Nachhinein seine Verfahrensrechte in Anspruch nehmen und allenfalls Mängel, bestimmte Vorgehensweisen oder unzutreffende Hypothesen rügen oder entkräften kann. Unter diesen kontrollierten Bedingungen kann dafür gesorgt werden, dass Informationen, die unantastbare Kernbereiche etwa der Persönlichkeit betreffen oder von der jeweiligen Genehmigung nicht erfasst sind, in der Auswertungsphase unverzüglich gelöscht werden, sollte es nicht bereits während des Sammelvorgangs möglich sein, diese unberührt zu lassen.[814] Eine klare Rechtsgrundlage beziehungsweise klare Ermächtigungsnormen sollten deshalb zudem im Interesse der staatlichen Behörden liegen, weil die technische Massnahmen durchführenden und veranlassenden Personen allenfalls, je nach Fallkonstellation und eingesetzter Methode, strafrechtlich belangt werden können, wenn der Einsatz als rechtswidrig zu qualifizieren wäre.[815]

Die jeweilige Genehmigungsbehörde (und die entsprechende Beschwerdeinstanz) nimmt in diesem Verfahrenskomplex die wichtige Stellung ein, darüber zu wachen, dass gewisse Eintrittsschwellen gewahrt bleiben, diffuse Risiken nicht als Anlassgrund zu akzeptieren, und vage, ungenaue Anträge für Überwachungstätigkeiten abzulehnen.[816] Wird die Genehmigung erteilt, sind bereits geringere Abweichungen der einsetzenden Behörde von den Weisungen der Genehmigungsbehörde nicht zu tolerieren.[817] Das schränkt zwar die Flexibilität der Überwachungstätigkeit ein[818], ist aber der potenziell sehr hohen Eingriffsintensi-

---

813 Vgl. dazu BVerfGE 120, 274 (331); Urteil des BGH StB 18/06 vom 31. Januar 2007 N. 5 ff.; MEYER, S. 80 zu diesem Argument bei Terror-Listen.

814 BVerfGE 120, 274 (337); GLESS 2012, S. 19 f. und 22. Vgl. GLESS 2011, N. 11 und 48 zu Art. 139 StPO.

815 Vgl. etwa ALBRECHT F., N. 23.

816 Vgl. ISENRING/KESSLER, S. 34; SIMON D., S. 102; ZERBES, S. 334 f. und 367. Kritisch zum Abbau judikativer Kontrolle: ALBRECHT P. A. 2003, S. 150; SIMON D., S. 180 f. De lege ferenda als Genehmigungsbehörden sind im Strafverfahren das zuständige kantonale Zwangsmassnahmengericht (E-Art. 274 Abs. 4 lit. c StPO) und im Bereich des NDG das Bundesverwaltungsgericht (VE-Art. 25 NDG) vorgesehen.

817 Vgl. bspw. die überenthusiastische Behörde in der Sache des Urteils des Landesgerichts Landshut 4 Qs 346/10 vom 20. Januar 2011.

818 Bspw. dokumentiert ein digital geführtes Tagebuch den Tatablauf oder Vorbereitungshandlungen eventuell sehr detailliert, kann aber möglicherweise vor Gericht nicht verwertet werden, weil das Lesen des Tagebuchs von der Genehmigung nicht abgedeckt ist oder in Kernbereiche der Persönlichkeit eingreift.

tät heimlicher Online-Überwachungsmassnahmen geschuldet. Es sollen lediglich diejenigen Funktionen benutzt und diejenigen Schritte veranlasst werden, zu denen ausdrücklich ermächtigt wurde.[819] Das bedingt freilich, dass die Genehmigungsbehörde im Genehmigungsbeschluss, allenfalls in Absprache mit den einsetzenden Behörden oder Fachleuten, eindeutig den zulässigen Rahmen des Einsatzes von Online-Überwachungstechnologien definiert, sich Gedanken über möglicherweise auftretende Probleme macht und entsprechend Vorkehrungen, die vor und während des Einsatzes zu treffen sind, formuliert. Das dürfte insbesondere angesichts immer neuer Technologien und des herrschenden Zeitdrucks keine einfache Aufgabe sein.

C. „Intelligente" Überwachungssysteme und andere Fusionen

Smarte Videoüberwachungssysteme[820] vergrössern die Streubreite des Eingriffs, ermöglichen (automatisierte) Analyseverfahren sowie erfolgversprechende Vernetzungen mit anderen Technologien und laufen Gefahr, dass sie „Vorurteile intensivieren und perpetuieren", indem sie beispielsweise nach diskriminierenden Merkmalen suchen.[821] Greifen smarte Systeme auf automatisierte Sondierungsprogramme, kriterienbasierte Verhaltensanalysen und ähnliche Techniken zurück, müssen dadurch aber nicht zwangsläufig schwerere Grundrechtseingriffe entstehen.[822] Im Gegensatz zu den herkömmlichen, heute gebräuchlichen Überwachungssystemen muss sich die neue Generation der realen Raumüberwachung zum Beispiel theoretisch nicht auf ihre Archive verlassen, um wirksam funktionieren zu können. Automatisierte Systeme speichern die aufgenommenen Daten

---

819 GLESS 2012, S. 20 ff. Insbesondere ist etwa zu verhindern, dass Webcams eingeschaltet oder Nutzungsprofile durch Keylogger etc. erstellt werden, wenn dies von der jeweiligen Genehmigung nicht abgedeckt ist.

820 Zu diesem Begriff, siehe etwa GATES; KAMMERER 2008, S. 192. Auch „intelligente" Videoüberwachungssysteme oder „Thinking Cameras" genannt, siehe BÜLLESFELD 2002, S. 15; BIER/SPIECKER GEN. DÖHMANN, S. 610; ROSSNAGEL/DESOI/HORNUNG, S. 694; LINGG, S. 18; MÜLLER L. 2012a, S. 64.

821 ROSSNAGEL/DESOI/HORNUNG 2012, S. 460; HORNUNG/DESOI, S. 155 f.. Ähnlich auch MÜLLER L. 2011, S. 144.

822 Siehe dazu MÜLLER L. 2011, S. 138 f. Vgl. etwa BIER/SPIECKER GEN. DÖHMANN, S. 613 f. Das kann beispielsweise der Fall sein, wenn der Erkennung unerwünschter Verhaltensweisen keine diskriminierenden Charakteristiken zugrunde liegen, vgl. ROSSNAGEL/DESOI/HORNUNG 2012, S. 461. Indes ist äusserst fraglich, ob eine derart „saubere" Variante einer automatisierten Überwachung in näherer Zukunft realisierbar ist, gl. A. wie ROSSNAGEL/DESOI/HORNUNG 2011, S. 695 Fn. 9.

lediglich zweitrangig längerfristig ab. Der Anspruch ist vielmehr, vorgegebene Kriterien beziehungsweise Eigenschaften *direkt* abzugleichen, das heisst beispielweise abweichendes Verhalten zu erfassen oder Bedrohungen sowie Gefährder zu identifizieren.[823] Unerwünschte Verhaltensweisen oder gesuchte Merkmale sollen quasi-synchron zu ihrem Geschehen beziehungsweise Auftauchen im Blickfeld der Kameras erkannt und im Falle eines Treffers die zuständige Behörde augenblicklich alarmiert werden. Diese Verfahrensweise macht eine manuelle Sichtung des gesamten aufgezeichneten Materials in der Regel unnötig, da die Situation immer bereits automatisch sondiert und eine notwendige Intervention durch einen Alarm ausgelöst wird. Ein Vorfall muss somit höchstens kurzfristig, episodenhaft und zielgerichtet aufgezeichnet werden, um etwa als Beweis für ein geschehenes Delikt herbeigezogen zu werden. Insofern passende Merkmale vorgegeben werden und die Technologie verlässliche Abgleiche leisten kann, könnte dadurch verhindert werden, dass unbescholtene Personen mit über das pure automatische Sondieren hinausgehenden Massnahmen belangt werden. Funktionierende, nicht diskriminierende intelligente Videoüberwachungssysteme liefern somit theoretisch selektivere, verlässlichere sowie höherwertige Daten und können die gesammelten Informationen zuverlässiger vor Missbrauch schützen.[824]

Automatisierte Erkennungsverfahren hingegen bedeuten oftmals eine stark erhöhte Eingriffsintensität.[825] Schwere Eingriffe dürften insbesondere biometrische Identifikationstechniken, die Bewegungs- und Persönlichkeitsprofilerstellung und mit anderen Verfahren kombinierte Methoden darstellen (zum Beispiel der automatisierte Abgleich von beobachteten Personen mit Datenbanken, biometrische Zutrittskontrollen basierend auf Verdachtsregistern und durchgeführt über

---

823 Siehe bspw. Bericht INDECT D1.1, S. 8 oder das Projekt CamInSens unter <http://www.sra2.uni-hannover.de/caminsens/> und D'ANGELO ET AL.

824 BIER/SPIECKER GEN. DÖHMANN, S. 612, 614 und 616 f.; ROSSNAGEL/DESOI/HORNUNG 2011, S. 695.

825 ROSSNAGEL/DESOI/HORNUNG 2011, S. 695 f.; FLÜCKIGER/AUER, S. 939; BAUM, N. 40. Das gilt insbesondere, wenn sie etwa diskriminierende Merkmale oder abweichendes Verhalten identifizieren sollen, siehe MÜLLER L. 2011, S. 167 f; ausserdem, wenn etwa Gesichtserkennungssysteme bzw. Algorithmen aus technischen Gründen bestimmte Personengruppen leichter identifizieren können und diese deshalb öfters einer Folgebeurteilung unterzogen werden, siehe zu dieser Problematik INTRONA/NISSENBAUM, S. 41 und 45.

Videoüberwachungssysteme, die Massendatenverarbeitung über die Raumüberwachung).[826]

Hilfe, smarte Videoüberwachungssysteme einzuschätzen, leistet etwa das „Drei-Stufen-Modell" von ROSSNAGEL/DESOI/HORNUNG. Mit diesem Modell können sie hinsichtlich des potenziellen Schweregrads von Grundrechtseingriffen ähnlich wie bei der konventionellen Videoüberwachung abgestuft werden:

1. Übersichtsaufnahmen ohne Identifikations- beziehungsweise Individualisierungsmöglichkeiten (allenfalls erreicht durch wirksame Anonymisierungs- und Pseudonymisierungstechniken[827]), ohne zusätzliche Tools wie Zoomfunktionen oder akustische Sensoren und ohne Aufnahmespeicherung ziehen, wenn überhaupt, lediglich geringe Grundrechtseingriffe nach sich.
2. Sobald eine auffällige Person oder Situation vom System erkannt und dem menschlichen Überwacher mitgeteilt wird, dürfen eingriffsintensivere Hilfsmittel zugeschaltet werden. Der Überwachende darf zum Beispiel auf die auffällige Person zoomen oder die Situation aufzeichnen lassen.
3. Erst auf der dritten Stufe darf der Überwachende Identifizierungstechnologien, das heisst beispielsweise biometrische Programme, verwenden. Die dritte Stufe ist dann erreicht, wenn sich eine konkrete, unmittelbare Gefahrenlage oder ein konkreter Verdacht einer Straftat abzeichnet. Diese dritte Phase dient der Einsatzleitung und Beweissicherung.[828]

Kein oder nur ein leichter Eingriff wäre deshalb lediglich das Erkennen und Melden eines Vorfalls, der eine Intervention verlangt, an die sofort intervenierende Behörde, nicht aber die Meldung von genau umschriebenen Tatbeständen oder Bedrohungslagen an (sicherheits- oder gerichtspolizeiliche) Behörden. Die Grenze kann in dieser Unterscheidung aber bedenklich fliessend sein, was diesbezüglich sehr klare Regelungen nötig macht. Fraglich ist in dieser Hinsicht, ob

---

826 BIER/SPIECKER GEN. DÖHMANN, S. 616 f.; MÜLLER L. 2011, S. 17 ff., 139, 142 und 259 f. jeweils mit weiteren Hinweisen. Hinweistafeln vermögen zwar, insofern der Betroffene deswegen den überwachten Raum umgeht, bevorstehende Eingriffe in gewisse Grundfreiheiten zu verhindern, indes können dadurch andere Grundrechte verletzt werden. Zu Bewegungs- und Persönlichkeitsprofilen, siehe auch MÜLLER L. 2011, S. 56 f.

827 Siehe dazu etwa PROBST, S. 13 ff.

828 ROSSNAGEL/DESOI/HORNUNG 2011, S. 695 f. und 699 f. mit weiteren Hinweisen und Beispielen sowie DIES. 2012, S. 461. Nicht erfasst sind von diesem Modell die noch eingriffsintensiveren Verknüpfungen mit anderen Technologien (z. B. Fahndungsdatenbanken).

autonom-lernende Systeme als sehr problematisch oder im Gegenteil potenziell eingriffslindernd zu beurteilen sind. Theoretisch könnten autonom-lernende Systeme bestimmte Personen gezielter erfassen und damit die Freiheiten anderer Personen schonen. Indes erstellen derartige Systeme, um zu lernen, Profile (Persönlichkeit, Verhalten, Bewegung etc.). Sie sind darauf angewiesen, ihren Bestand an Mustern für positive und negative Befunde laufend zu vergrössern, um anhand dieser ihre Erkennungsleistung zu verbessern, einmal positiv identifizierte Personen einer eingehenderen Überwachung zu unterziehen und ihre Ergebnisse auch mit anderen intelligenten Überwachungstechnologien zu teilen.[829] Angesichts der heute wenig erfolgversprechenden Erfahrungen mit derartigen Systemen, scheinen die problematischen Seiten noch deutlich zu überwiegen.

Das Erstellen von Profilen ist auch bei anderen postmodernen Technologien ein Thema. Während die mittels Online-Überwachungsmassnahmen oder durch Vorratsdatenspeicherung gesammelten Daten in der Regel ohne Weiteres auf Persönlichkeits-, Verhaltens- und/oder Bewegungsprofile schliessen lassen[830], leuchtet ZSCHOCHS Ansicht, dass im Rahmen einer Rasterfahndung alleine keine Persönlichkeitsbilder, sondern lediglich Täterprofile erstellt werden, grundsätzlich ein.[831] Einzuwenden ist aber, dass je spezifischer die Eigenschaften der Personen vorgegeben sind, desto eher durch die anschliessende Datensammlungen persönlichkeitsrelevante Informationen gesammelt werden, durch welche in der Folgeauswertung umfassendere Profile erstellt werden können. Die Ausgangshypothese zu Beginn der Rasterfahndung besteht lediglich aus Täterprofilen, die Ausbeute zum Ende, die folgenden Analyseschritte und Überwachungsmassnahmen führen der einsetzenden Behörde aber weitaus mehr Informationen zu, mit denen sie diese Profile erweitern kann. Die Rasterfahndung *ermöglicht* somit

---

829 BIER/SPIECKER GEN. DÖHMANN, S. 615. A. A. sind ROSSNAGEL/DESOI/HORNUNG 2012, S. 461, die dafür halten, dass „selbstlernende Algorithmen" dazu beitrügen, diskriminierende Eingriffe zu vermeiden oder verringern. Vgl. BVerfGE 120, 378 (397 ff.). Ferner BVerfGE 125, 260 (Vorratsdatenspeicherung); BVerfGE 115, 320 (Rasterfahndung II).

830 Z. B. lassen Durchsuchungen von Smartphones mit Telefonbuch, Kalender, Fotogalerien, Nachrichtenspeicher etc. oder Sondierungen sozialer Netzwerke weitreichende Rückschlüsse über die Persönlichkeit und das Verhalten von Personen und Dritten zu, siehe BUERMEYER/BÄCKER, S. 437; BVerfGE 120, 274 (314); SCHULZKI-HADDOUTI, S. 36 ff. mit Hinweisen auf Studien zur Analyse und Auswertung von Daten aus sozialen Netzwerken. Ebenso die Vorratsdatenspeicherung über Bewegungen der betroffenen Person, siehe etwa <http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/>; NOCUN, S. 24 f. Vgl. auch ZERBES, S. 39.

831 ZSCHOCH, S. 208. Ebenso ROGALL, S. 625.

Bewegungs- und Persönlichkeitsprofile abzuleiten, insbesondere, wenn die gesammelten Daten zu den am Ende verbleibenden Personen oder zu allen einbezogenen Personen über die Fahndung hinaus gespeichert bleiben und in anderen Zusammenhängen oder späteren Ermittlungen erneut verwendet werden. In diesem Sinne können auch erhobene Randdaten (zum Beispiel im Rahmen eines Antennensuchlaufs) nachträglich und ohne konkrete Verdachtsmomente dazu benutzt werden, Bewegungen nachzuvollziehen oder auf die Persönlichkeit von Betroffenen zu schliessen.[832]

Aber auch ohne die Identifikation von Personen oder ohne die Aufzeichnung des Materials könnte die vermeintliche Fähigkeit automatisierter Systeme, unerwünschtes Verhalten zu erkennen und vorauszuahnen, genutzt werden.[833] Fraglich ist, inwieweit etwa automatisierte Verhaltensanalysen *ohne* Personenidentifikation einen intensiveren Eingriff in Grundrechte darstellen als die simple Beobachtung der Geschehnisse auf dem Bildschirm. Solange keine Komponenten einer darüber hinausgehenden Informationsverarbeitung miteingesetzt werden, das heisst die Verhaltensanalyse nicht der Fahndung nach ausgewählten Personengruppen oder Bedrohungen dient und keine zusätzlich intensivierenden Techniken verwendet werden, scheint eine Digitalisierung alleine einen Eingriff nicht zu intensivieren. Indes erleichtert sie freilich, die digitalisierten Informationen weiterzuverwenden und mit Informationen aus anderen Quellen zu verknüpfen.[834] Der automatisierte Alarm, der einer erkannten unerwünschten Verhaltensweise oder einem erkannten, gesuchten Merkmal folgt, dürfte jedenfalls nicht per se einen gravierenden Eingriff bedeuten, solange die sondierten Daten keiner Person zugeordnet werden können und die Daten unmittelbar nach der Erfassung gelöscht werden.[835] Jedoch überzeugt auch die Schlussfolgerung von FLÜCKIGER/AUER, dass sich, sobald vordefinierte Charakteristiken ins Spiel kommen oder das Geschehen und Personen automatisch verfolgt und/oder Bild-

832 GLESS 2012, S. 14.

833 Vgl. Bericht INDECT D1.1, S. 8. Der Zweck des sofortigen Eingreifens bei einem Vorfall und der Abschreckung durch mehrfaches erfolgreiches Eingreifen sowie einer offenen Platzierung der Kameras wäre damit weiterhin gewährleistet.

834 BIER/SPIECKER GEN. DÖHMANN, S. 612. ROSSNAGEL/DESOI/HORNUNG 2011, S. 694 f. halten hingegen bereits den Einsatz smarter Technologien für eingriffsintensiver als die konventionelle Videoüberwachung.

835 BVerfGE 120, 378 (399). Eine Negativselektion bestimmter Eigenschaften fällt nach Ansicht von BIER/SPIECKER GEN. DÖHMANN, S. 612 nicht darunter.

ausschnitte vergrössert werden, die Eingriffsintensität tendenziell erhöht.[836] Dies gilt im stärkeren Masse für die Kombination mehrerer Überwachungstechnologien. Durch derartige Koppelungen, insbesondere mit Varianten der Massendatenverarbeitung, finden personenbezogene Datenabgleiche statt, die wesentlich eingriffsintensiver sein können.[837]

Mittels smarter Technologien sollen vor allem unerwünschte Personen oder Personengruppen aus einem bestimmten Raum ferngehalten werden. Sowohl die konventionelle Videoüberwachung wie auch die Überwachung mit derartigen smarten Technologien können für jeden im überwachten Raum beziehungsweise für jeden, der diesen Raum wegen der Überwachung meidet, faktisch mehr oder weniger intensive Eingriffe in die Bewegungsfreiheit bedeuten. Besonders die mit anderen Technologien kombinierte Raumüberwachung kann die Bewegungsgewohnheiten von bestimmten Personen(-gruppen) in einem bestimmten Raum beeinflussen.[838] In derselben Weise kann die Versammlungsfreiheit (Art. 22 BV) verletzt werden, wenn Versammlungen faktisch durch die Überwachung eines (realen oder virtuellen) öffentlichen Raums verhindert beziehungsweise unterdrückt werden oder Personen dadurch oder etwa gestützt auf ein Verdachtsregister erlassene Fernhaltemassnahmen (faktisch) davon abgehalten werden, an der Versammlung teilzunehmen.[839] In gravierenden Fällen wäre wohl auch eine Verletzung der Niederlassungsfreiheit (Art. 24 BV) denkbar.[840] Auch die Automatisierung und Vernetzung von Raumüberwachung mit Verdachtsregistern, anderen Datenbanken und Massendatenverarbeitungstechnologien benötigen Restriktionen. Live-Kontrollen von Registrierten über die Raumüberwachung

---

836 FLÜCKIGER/AUER, S. 934. Ebenso BÜLLESFELD 2002, S. 146; ZSCHOCH, S. 198 ff.; ROSSNAGEL/DESOI/HORNUNG 2011, S. 695.

837 Siehe ZSCHOCH, S. 198 f. und 201; ROGGAN 2001, S. 135 f.; BARTSCH, S. 92.

838 BGE 132 I 49 E. 5.2 S. 56; FLÜCKIGER/AUER, S. 932; SCHWEIZER 2008, N. 35 zu 270; BAUM, N. 22. Vgl. ROSSNAGEL/DESOI/HORNUNG 2011, S. 698, die diese Problematik besonders bzgl. smarter Überwachungstechnologie hervorstreichen. Teilweise a. A. sind BÜLLESFELD 2002, S. 234 ff.; MÜLLER L. 2011, S. 153. Analog kann das Ausgeführte auf die virtuelle Überwachung anhand von Profilen übertragen werden: Bestimmte virtuelle „Orte" könnten typische Profilkriterien eines Täters darstellen – um nicht als Täter zu gelten, sollten diese gemieden werden. Siehe dazu NOWAK, S. 40.

839 ROHNER, N. 1, 6, 16 und 18 zu Art. 22 BV; FLÜCKIGER/AUER, S. 934 f. mit Hinweisen; MÜLLER L. 2011, S. 137; MOECKLI/KELLER, S. 240; DIGGELMANN, S. 312 f.; LSE BRIEFING, S. 55; BGE 137 I 31 E. 6.1 S. 44 f. Zur Versammlungsfreiheit im Allgemeinen: HÄFELIN/HALLER/KELLER, N. 532 ff. S. 172 ff.

840 Siehe etwa CAVELTI, N. 6 und 25 zu Art. 24 BV.

mittels (biometrischer) Personenidentifikation beispielsweise könnten sich als sehr nützlich für die kriminalitätsbekämpfenden Behörden erweisen, falls Technologien es erlauben würden, in dieser Weise eine gewisse Anzahl von Personen zuverlässig zu überprüfen. Diese kombinierte Variante könnte sowohl sichernd, indem überprüft werden könnte, ob sich Eingetragene ausserhalb ihres zugewiesenen Bewegungsradius aufhalten, als auch für Fahndungen oder Ermittlungen eingesetzt werden.

Die gesetzlichen Grundlagen der meisten schweizerischen Kantone respektive Gemeinden, welche die Videoüberwachung des öffentlichen Raums geregelt haben, liessen automatisierte Systeme zumindest in begrenzten Versionen zu.[841] Offenere Polizeigesetze, wie das Polizeigesetz des Kantons Zürich vom 23. April 2007 (PolG Zürich; Loseblattsammlung 550.1) in den §§ 32a-c, erlaubten bereits heute eine Installation visueller wie akustischer Raumüberwachungskomponenten eines automatisierten und vernetzten Systems. Der Regierungsrat des Kantons Zürich begründete diese offene Formulierung denn auch explizit mit dem technischen Fortschritt auf dem Gebiet der Überwachungsanlagen. Er habe damit gewährleisten wollen, dass in Zukunft ein gewisser Spielraum beim Einsatz neuer Technologien offen stehe.[842]

Diesbezüglich ist indes festzuhalten, dass das Bundesgericht in BGE 136 I 87 im Rahmen einer abstrakten Normenkontrolle unter anderem über die zu diesem Zeitpunkt noch weniger präzise bestimmte Raumüberwachungsvorschrift des Zürcher Polizeigesetzes zu befinden hatte. Es entschied, dessen offene Formulierung ohne jegliche Zweckangaben verhindere von vornherein, „klare Ziele und ein öffentliches Interesse an entsprechenden Überwachungsmassnahmen zu ermessen". Die fragliche Bestimmung lasse somit auch nicht zu, eine Zweck-Mittel-Relation zu bestimmen, die „vor dem Hintergrund eines Grundrechtseingriffs auf ihre Verhältnismässigkeit geprüft werden" könne. Die Bestimmung sei deshalb als „grenzen- und konturlose Blankettnorm" zu qualifizieren und könne folglich vor der Verfassung und der EMRK nicht standhalten.[843] Das Be-

---

841 Die Live-Sicht des INDECT lasse bspw. zu, Gesichter von Personen oder Autokennzeichen automatisch unkenntlich zu machen, siehe Bericht INDECT D1.1, S. 35 und D9.4, S. 12 f. Vgl. dazu BÜLLESFELD 2002, S. 17 f.; Bericht EJPD 2007, S. 10; PETRI, G N. 565 ff.

842 Antrag des Regierungsrates des Kantons Zürich vom 5. Juli 2006, Zürcher Amtsblatt 2006 (21. Juli 2006), S. 900.

843 BGE 136 I 87 E. 8.3 S. 114 ff. Namentlich genüge der allgemeine Verweis auf die generellen Aufgaben der Polizei den Anforderungen nicht. Die alte Bestimmung § 32 PolG lautete: „Die Polizei darf zur Erfüllung ihrer gesetzlichen Aufgaben allgemein zugängliche Orte mit

stimmtheitsgebot wirkt demnach einer zu extensiven Auslegung der entsprechenden gesetzlichen Grundlagen entgegen.[844] Insofern ist auch SCHWEIZER/MÜLLER zuzustimmen, dass bewusst offen formulierte Ermächtigungsbestimmungen für die Videoüberwachungen den Anforderungen an eine hinreichend bestimmte gesetzliche Grundlage vor allem für weiterentwickelte Überwachungssysteme kaum genügen würden. Zumindest für den Einsatz eingriffsintensiverer Technologien, durch welche zum Beispiel eine biometrische Identifikation ermöglicht wird, müsse eine sehr klare und konkretisierte gesetzliche Grundlage vorliegen.[845]

Aus diesen exemplarischen Überlegungen zu smarten Überwachungssystemen können allgemeine Schlüsse für kombinierte Methoden gezogen werden: Postmoderne Kriminalitätsbekämpfungstechnologien sind darauf ausgelegt, dass zwischen ihnen viele Synergien genutzt werden können.[846] Einzelne postmoderne Instrumente können deshalb nicht (immer) isoliert betrachtet werden. Meist können sie nur im Kontext des Gesamtinstrumentariums, in das sie eingebettet sind, beurteilt werden.[847] Dieser Kontext erschwert nicht nur die rechtliche Einordnung, sondern macht diese Komplexe insgesamt undurchsichtig. Die erforderliche „Gesamtschau" geht verloren, wenn diese Methoden, die für sich möglicherweise wenig aufsehenerregend oder eng begrenzt sein mögen, in der Öffentlichkeit lediglich je einzeln diskutiert werden.[848] Jegliche Fusion zwischen Rasterfahndung, Massendatenverarbeitung und Raumüberwachung sowie Verdachtsregistern und anderen Datenbanken steigert grundsätzlich die Intensität des Eingriffs. Bereits die Möglichkeit, diese Methoden und Technologien zu verknüpfen, können die Stärke des Eingriffs erhöhen.[849] Um lediglich einige weitere Beispiele anzusprechen: SCHEFER schätzt in erster Linie den Betrieb elektronischer Datenbanken „angesichts der vielfältigen technischen Möglichkeiten der Verknüpfung heute grundrechtlich derart sensibel" ein, dass er „besonders

technischen Geräten offen oder verdeckt überwachen und soweit notwendig Bild- und Tonaufnahmen machen." (BGE 136 I 87 E. 8 S. 111).

844 Siehe dazu ausführlich in Hinsicht auf die Videoüberwachung MÜLLER L. 2011, S. 201 ff.

845 SCHWEIZER/MÜLLER, S. 387. Ebenso BREITENMOSER, N. 36 zu Art. 13 BV; MÜLLER L. 2011, S. 225 jeweils mit Hinweisen.

846 CUSSON, S. 78; NOGALA 1998, S. 303 f. mit weiteren Hinweisen.

847 NOGALA/SACK, S. 146. Vgl. PETRI, G N. 533; VOLKMANN, S. 219.

848 RUDIN, S. 282. Ebenso HENSEL, S. 528. Vgl. auch SCHEFER, S. 63.

849 Siehe BVerfG, NVwZ 2007, 688 (691).

hohe Anforderungen“ bezüglich ihrer demokratischen Legitimation verlangt.[850] ZSCHOCH stellt fest, dass die Rasterfahndung in Kombination mit der Videoüberwachung zu einem qualifizierten, intensiveren Eingriff in die Grundrechte Betroffener führt als eine einfache Rasterfahndung.[851] Systeme wie INDECT könnten in dieser Hinsicht vielfältige Anwendungs- und Vernetzungsmöglichkeiten zur Verfügung stellen, welche die Zuverlässigkeit dieser Kombinationen erhöhen könnten.[852] Eine andere denkbare, problematische Kombination, die AL-FAROUQ ABO YOUSSEF anspricht, ist die Verbindung von Rasterfahndung und Standortdiensten.[853]

Die Suche nach der passenden Rechtsgrundlage für kombinierte Methoden hat daher stets auch das Gesamtbild zu betrachten. Eine Rundumüberwachung durch fusionierte Elemente einzelner Methoden soll vermieden werden.[854] Idealerweise wäre bei neugeschaffenen gesetzlichen Grundlagen eine „Überwachungs-Gesamtrechnung“ anzustellen, in der sämtliche Methoden, Technologien und Fusionsmöglichkeiten berücksichtigt und hinsichtlich ihrer „Gesamtbelastung“ der Grundfreiheiten überprüft würden.[855] Gerade im föderalen System der Schweiz mit vielen verschiedenen Akteuren auf vielen verschiedenen Ebenen scheint dieser Ansatz indes schwer zu realisieren. Es scheint aber zumindest bei einem Einsatz, der mehrere dieser Instrumente kombiniert, nicht angemessen, die Methoden einzeln, getrennt oder stufenweise – erst die Zulässigkeit der Datenquelle selbst, dann die Zulässigkeit des Datenabgleichs – zu beurteilen.[856] Vielmehr ist für jede *Kombination* der Methoden eine eigene, (einigermassen) spezielle, ausdrückliche, hinreichend klare, formell-gesetzliche Ermächtigungs-

---

850 SCHEFER, S. 62 ff. Ebenso STUDER, S. 69, WEICHERT, S. 73 f. und HORNUNG/DESOI, S. 154 f. zur Verknüpfung von Verdachtsregistern und Videokameras mit biometrischer Personenerkennung. Siehe dazu auch Drucksache 17/9003 vom 16. März 2012; NORRIS, S. 146. Denkbar wäre etwa auch, ein automatisiertes System die Stadionkameraaufnahmen nach bestimmten „Hooliganmerkmalen“ durchsuchen zu lassen. Die gewonnenen Aufnahmen führten zu einem Verdächtigenkreis, der in einem zweiten Schritt z. B. über Hooligandatenbanken identifiziert werden könnte. Zu Verknüpfungsmöglichkeiten der Vorratsdatenbanken, siehe auch KURZ/RIEGER, S. 11 ff.

851 ZSCHOCH, S. 200. Momentan ist aber die Unzuverlässigkeit dieser Kombination noch ein immanentes Problem, vgl. ZSCHOCH, S. 198.

852 NOWAK, S. 40 f.

853 AL-FAROUQ ABO YOUSSEF, S. 102. Siehe dazu auch KURZ/RIEGER, S. 19 ff.; HENSEL, S. 528 f.; MONROY/BUSCH, S. 6.

854 PETRI, G N. 69.

855 ROSSNAGEL, S. 1240 und 1242. Vgl. BVerfGE 125, 260 (323 f.); PETRI, G N. 33.

856 ZSCHOCH, S. 201 f.; BIER/SPIECKER GEN. DÖHMANN, S. 613.

grundlage zu verlangen.[857] Derartige gesetzliche Grundlagen existieren in der schweizerischen Rechtsordnung für die Verknüpfung insbesondere neuerer Technologien erst in sehr wenigen Bereichen. Sollten Überwachungstechnologien künftig öfter eingesetzt werden, ist ferner zu bedenken, dass sich geringfügige Eingriffe gegen Einzelne häufen können, sobald unkoordiniert und unabhängig voneinander verschiedene (verdachtsunabhängige) Massenmethoden betrieben werden. Diese können momentan nicht in ihrer Summe beurteilt werden, weil dafür kein Mittel zur Verfügung steht. Die Konsequenz ist, dass die Eingriffsqualität der einzelnen Massnahmen für sich genommen im Rahmen einer Einzelbetrachtung vielleicht nicht ausreichend schwer ist, um eine Person vor diesen Massnahmen zu schützen. Die Beurteilung der Gesamtsumme dieser vielen geringfügigen Eingriffe an einem Tag vielleicht aber schon. Neben der bereits angesprochenen Häufung von Informationen aus vielen Quellen bei einer Behörde, könnte also auch eine Häufung von vielen kleinen Eingriffen von verschiedenen Verursachern hinsichtlich *einer* Person im Ergebnis einen grösseren Eingriff bedeuten – ohnehin, wenn bedacht wird, dass diese einzeln gesammelten Informationsstücke möglicherweise später verknüpft werden könnten.

---

857 Siehe etwa MÜLLER L. 2011, S. 226; BARTSCH, S. 241; BÜLLESFELD 2002, S. 129; ROSSNAGEL/DESOI/HORNUNG 2011, S. 695 („recht spezielle Erlaubnisregelungen“); STUDER, S. 69.

DRITTER TEIL:
KRIMINOLOGISCHE ÜBERLEGUNGEN

Im vorangehenden Teil konnte aufgezeigt werden, dass rechtliche Institute nicht immer ausreichen, postmoderne Kriminalitätsbekämpfungstechnologien vor entgrenzenden Einsätzen zu bewahren. Neben der technischen Machbarkeit und rechtlichen Zulässigkeit ist als weiterer Faktor zu berücksichtigen, inwieweit postmoderne Technologien und Vorgehensweisen gesellschaftlich wünschenswert und tragbar sind.[858] Wie in diesem Teil festgestellt wird, ist auch diese Frage nicht leicht oder eindeutig zu beantworten.

I. Formationen, Wechselwirkungen und Synergien

Tiefgreifende Transformationsprozesse in allen Bereichen veränderten in den letzten fünfzig Jahren die Grundbedingungen der gesellschaftlichen Koexistenz stark.[859] In der Schweiz vollzog sich in der zweiten Hälfte des 20. Jahrhunderts, parallel zu vielen anderen Ländern, ein Wandel in der gesellschaftlichen Mentalität hinsichtlich Kriminalität:

Im Umfeld der Postmoderne verloren nach und nach mehr Mitglieder der Gesellschaft ihren Halt. Die solidarische Grundeinstellung und soziale Einrichtungen, welche dem Einzelnen vormals stabilisierend beistanden, zerfielen stetig.[860] Ehemals informelle Kontrollinstanzen der Gemeinschaften mit dörflichem Charakter wichen unpersönlichen und losen Nachbarschaften. Vormals beständige „Häfen“ und vorgegebene Referenzgruppen lösten sich auf.[861] Unterprivilegierten Personengruppen gegenüber setzte sich eine unnachgiebige Haltung durch. Ihr Scheitern wurde vermehrt durch Selbstverschulden, Leistungsdefizite oder

---

858 Siehe dazu SINGELNSTEIN/STOLLE 2012, S. 153 ff.

859 Siehe ausführlich zu den Transformationsprozessen: SINGELNSTEIN/STOLLE 2012, S. 17 ff.

860 Stabilisierend waren vormals das enge gesellschaftliche Gefüge der Kleinstädte und Dörfer eingebettete Leben, der gemeinschaftliche Zusammenhalt des wohlfahrtsstaatlichen Sozialgedankens oder die gute Wirtschaftslage.

861 Siehe GARLAND, S. 282 ff.; KUNZ 2011, S. 132 ff.; SINGELNSTEIN/STOLLE 2007, S. 108 f.; YOUNG 2004, S. 2 ff.; BAUMAN, S. 7.

kognitive Schwächen erklärt.[862] Vermittelte der Wohlfahrtsstaat noch das Gefühl eines wohlbehüteten Daseins, kehrte sich dieses in der postmodernen Zivilisation zu einer allgemeinen sozialen Verunsicherung um. Noch in den Siebziger- und Achtzigerjahren herrschte in der Schweiz das Bild vom eigenen Land in Harmonie vor: Sicher, ruhig und weitgehend verschont von Kriminalität. In den folgenden Jahren wurde die Perspektive hinsichtlich Kriminalität zunehmend pessimistischer und die Bevölkerung zunehmend verunsichert.[863] Diese Veränderung in der Wahrnehmung der Bevölkerung beruhte nicht zuletzt auf den neuen Kommunikationsformen, Informationstechnologien und Massenmedien, welche die Welt zusammenrücken liessen und die Gesellschaft fortan mit Meldungen zu globalen Bedrohungen, aber auch zu lokalen Geschehnissen aus fernen Regionen versorgte. Die Informationsflut indes ist selektiv: Berichtet wird über das, was sich gut verkauft. Oft sind dies dramatisierte Bilder von Kriminalität und kaum fassbaren Bedrohungen.[864] Durch all diese Faktoren wuchs in der Bevölkerung das Bewusstsein der „strukturellen Verletzlichkeit" der Gesellschaft, womit sich immer stärker ein „Angstklima" in der gesellschaftlichen Wirklichkeit etablierte und festigte.[865]

Für den vorliegenden Untersuchungsgegenstand ist zum einen relevant, dass die laufende Technisierung die Lebensgewohnheiten des Einzelnen und die Gesellschaft selbst in ihrer Struktur bedeutend, teilweise radikal, veränderte und weiterhin verändert.[866] Die Gesellschaft ist rund um die Uhr mit neuester Technologie, allgegenwärtiger Information und digitaler Kommunikation konfrontiert. Neue Technologien bringen viele Vorteile: Bequemlichkeit, Wissen, Reichtum,

---

862 KUNZ 2011, S. 327 f.; YOUNG 1999, S. 52.

863 Siehe dazu ALBRECHT H. J., S. 38 ff.; NIGGLI/PFISTER, S. 519. Ausführlich zum Rückzug des Wohlfahrtsstaats: KRASMANN, S. 177 ff.

864 Siehe dazu etwa TESCHNER, S. 42 ff. In diesem Zusammenhang interessant BUCKLER/SALINAS, S. 713 ff. mit weiteren Hinweisen, u. a. zu den marktbasierenden Kriterien der „Newsworthiness": Themen aus dem Bereich der letalen Kriminalität eignen sich für die Massenmedien je mehr, desto stärker die „statistical", „status", „cultural" und „normative deviance" im Vergleich mit dem gesellschaftlichen Durchschnitt ist. Zur „Macht der Bilder", siehe bspw. auch ULLRICH/LÊ.

865 Siehe zum Ganzen: KUNZ 2011, S. 328 ff. und 334 f.; DERS. 2006, S. 71 f.; GARLAND, S. 281 ff.; SINGELNSTEIN/STOLLE 2012, S. 25 ff.; BAUMAN, S. 17 ff.; BOERS, S. 10; HASSEMER 2000, S. 258 f.; VOLKMANN, S. 216; YOUNG 2004, S. 1-6; SCHMIDT-SEMISCH, S. 63 ff. ZIMRING, S. 175 beschreibt die Stimmung der 1990er Jahre in den USA wie folgt: „The predominant public mood was a mixture of fear, frustration, and anger." Ferner NORRIS/ARMSTRONG, S. 67 ff. Zur generellen Verängstigung vor dem Draussen, siehe SESSAR, S. 127 ff.

866 Siehe etwa NOGALA/SACK, S. 119 f.

um nur einige zu nennen. Aber sie verunsichern auch: Zeit rast, gewohnte Routinen stocken plötzlich, neue Technologien verursachen neue Risiken. Zum anderen wurde die Kriminalitätsbekämpfung als Vehikel der Kommunikation der Politik und der Medien mit der Bevölkerung entdeckt.[867] Das Aufbauschen der Kriminalitätsrate durch Politik und Medien schürt Missinterpretationen von Delinquenz und kriminologischen Erkenntnissen und letztlich die Angstkultur in der Gesellschaft.[868]

Angesichts dessen, dass eine umfassende und lückenlose Verbrechensverhinderung oder -verfolgung illusionär sein dürfte, wären dahingehende Anliegen zu ignorieren.[869] Trotzdem – die Verantwortung bezüglich der ausufernden Tendenzen in der Sicherheitspolitik ist leichthin an das Unsicherheitsgefühl der Bevölkerung abgeschoben; und über teilweise absurde prophylaktische Sicherheitsbemühungen kann man leicht den Kopf schütteln. Vergessen wird dabei hingegen, dass es sich beim Ruf nach Sicherheit durchaus um eine legitime Forderung handeln kann.[870] Diese Forderung wird jedenfalls in der Gesellschaft populärer denn je vertreten. Sie bedarf folglich einer Reaktion des Staates. KUNZ stellt treffend fest: „Die Sicherheitspolitik wird damit kommunikativ."[871] Indes sollte nicht verwundern, dass die übersteigerten Ansprüche der Gesellschaft und die vom Strafverfolgungsapparat präsentierten Ergebnisse weit auseinander klaffen. Die enttäuschte, misstrauische und emotionsgeladene gesellschaftliche Haltung gegenüber einer gemässigten Kriminalpolitik rührt vorwiegend daher, dass jegliches Scheitern der Behörden medienwirksam in Szene gesetzt wurde und die Bemühungen und Instrumente der mit der Kriminalitätseindämmung betrauten

---

867 KUNZ 2011, S. 328 ff.; HASSEMER 1995, S. 488; NIGGLI 2004, S. 40. Zur „Boulevardisierung" der Artikel in den Printmedien, siehe REUBAND 2007, S. 76 f.

868 Gl. A. wie KUNZ 2011, S. 331; NIGGLI 2004, S. 32 ff.; NIGGLI/PFISTER, S. 522 ff. insb. N. 55 S. 532; BOERS, S. 13 f.; DITTMANN 1997, S. 123. A. A. sind KILLIAS ET AL. 2003, S. 322 f. und KILLIAS ET AL. 2011b, die die Sorge um die öffentliche Sicherheit wegen steigender Kriminalitätsraten als begründet erachten. Vgl. auch das Streitgespräch KILLIAS/NIGGLI.

869 Siehe bspw. die geringe oder unklare Wirksamkeit der vorliegend besprochenen Technologien. Vgl. KUNZ 2011, S. 331 f.

870 Vgl. SZUBA, S. 23.

871 KUNZ 2011, S. 330. Ebenso ALBRECHT P. A. 2003, S. 169; DERS. 2010, S. 9; GARLAND, S. 262 f. Nach DELEUZE 1993a, S. 250 ist die „unmittelbare Kommunikation" ein wesentliches Element einer Kontrollgesellschaft. Siehe auch ERICSON/HAGGERTY, S. 257 für konkrete Beispiele, wie die Polizei mit Anwohnern interagiert.

Behörden als nicht funktionierend bewertet wurden.[872] Die kritische Kriminologie rechnete ab den 1960er Jahren dahingehend mit vielen unreflektierten beziehungsweise unüberprüften Thesen der damaligen, traditionell-konservativ ausgerichteten Kriminalpolitik ab. Spätere Zweige der kritischen Kriminologie, die sich im Ergebnis und den Empfehlungen stark davon unterschieden, entzogen danach aber auch vielen Lösungsansätzen der früheren kritischen Kriminologie (so zum Beispiel dem Resozialisierungsgedanken oder der sozialen Ursachenforschung) ihre Plausibilität. Schliesslich löste einhergehend mit der Prekarisierung ab den 1980iger Jahren der positivistisch-konservative Grundton denjenigen der kritischen Kriminologie wieder allmählich ab. Gemeinsam traten sie den Konzepten und der Ideologie des Wohlfahrtsstaats entgegen.[873] In den Ruinen des Streits fanden anschliessend vor allem rohe und weder zu verifizierende noch zu widerlegende Zweckgedanken des Strafrechts besondere Beachtung: Vergeltung, Sicherung und positive Generalprävention.[874] Die Theorien der verschiedenen Schulen bestehen seitdem in teilweise friedlicher, ja begünstigender, teilweise unverträglicher Koexistenz, wobei diejenigen Strategien die Öffentlichkeit zu überzeugen scheinen und damit die Kriminalpolitik dominieren, welche mit der neoliberalen Weltanschauung und deren Abwicklungsprozessen sowie Erklärungskomplexen kompatibel sind. Das Angstklima verursacht in der Gesellschaft den ernstgemeinten Ruf nach der Bekämpfung der Kriminalität, nötigenfalls über die Exklusion bestimmter dämonisierter Personen oder Personengruppen, die sie für das scheinbar überhandnehmende Übel „Kriminalität" verantwortlich sieht. Politik und Kriminalitätsforschung antworten darauf mit Legitimationsversuchen und Rechtfertigungsansätzen. Die Strömungen des Feindstrafrechts und des Risikomanagements liefern dazu in der Postmoderne wesentliche Bestandteile. In bestimmten Bereichen nähern sich somit auch Teile der schweizerischen Rechtsordnung einem „Bekämpfungsstrafrecht" immer mehr an.[875] Insbesondere hinsichtlich technischer Massnahmen scheint sich dieser Wandel allmählich zu vollziehen. Die sich daraus ergebenden, nachfolgend beschriebenen gesellschaftli-

---

872 Siehe KUNZ 2011, S. 331 f.; SINGELNSTEIN/STOLLE 2012, S. 28 ff. Langfristig oder unspektakulär wirkende Instrumente scheinen hingegen wenig medientauglich zu sein.

873 KRASMANN, S. 55 f.; SCHMIDT-SEMISCH, S. 58 ff. Zu den historischen Ursprüngen, Entwicklungen und zur Rezeption dieser kriminologischen Strömungen, siehe ausführlich KRASMANN, S. 15-66.

874 SINGELNSTEIN/STOLLE 2012, S. 28 ff.

875 ARNOLD 2006a, S. 304, schlägt diesen Überbegriff vor. Vgl. SINN, S. 117. Zur Dämonisierung von Personen(-gruppen), siehe YOUNG 1999, S. 110 ff. und 192; KRASMANN, S. 283 ff.

chen Formationen der Postmoderne bilden die Ausganglage für den Einsatz der in der vorliegenden Arbeit untersuchten Technologien.

A. Eine Welt der Pannen

Der Mensch in der (westlichen) Gesellschaft des 21. Jahrhunderts sieht sich einer veränderten Welt mit neuen Reizen gegenüber, aufgrund derer er zuweilen die Orientierung verliert.[876] Um die neue Welt zu (be-)greifen und seine Selbstsicherheit aus der alten Welt wieder zu erlangen, versucht er die neue Welt schematisch zu ordnen. Die postmoderne Verunsicherung verleitet ihn dazu, vom Staat Ordnung und Sicherheit als höchste Güter zu verlangen. Jedoch: „In Wirklichkeit war es die begehrte Ordnung selbst, die von vornherein alles, wofür sie keinen Raum und keine Zeit hatte, als kontingent und bodenlos konstruierte. Der Traum von der Ordnung und die Praxis des Ordnens konstituieren die Welt – ihr Objekt – als Chaos. Und natürlich als Herausforderung, als zwingenden Grund zu handeln.“, so ZYGMUNT BAUMAN.[877] Die Gesellschaft fordert Sicherheit jeglicher Form und Ausprägung in jedem Bereich: Finanzielle Sicherheit bis ins hohe Alter (und die Sicherheit des Arbeitsplatzes, bis es soweit ist), Sicherheit im Strassenverkehr, Sicherheit vor Umweltkatastrophen etc.[878] In den Medien werden täglich „Opfer von Kriminalität“ gezeigt. Die Mathematik rechnet vor, wie gefährlich es ist, zu leben. Wer den Tag unbeschadet übersteht, hat zahlreichen Wahrscheinlichkeiten getrotzt. Da die Welt und das Leben jedoch nicht gefährlich sein sollen, wird mithilfe von Vermeidungs- und Vorsorgestrategien versucht, das Pannenrisiko zu verkleinern.[879]

Die Kriminalitätsfurcht nimmt in der Angstkultur einen Ehrenplatz ein. Umfassende Sicherheit vor Kriminalität ist zwar nur ein Anliegen der Gesellschaft; indes eines mit zentraler Bedeutung. Dies ist vor allem unter dem Gesichtspunkt problematisch, als übermässige Sicherheitsbemühungen im Bereich der Kriminalität nicht nur diese betreffen, sondern zusätzlich weitreichende Fernwirkungen auf die Gesellschaft und die Freiheiten Einzelner haben können. Verlangt werden das Verbrechen bekämpfende Programme und Methoden, welche möglichst umfassenden Schutz vor Kriminalität gewährleisten. Scheinbar unerwünscht sind

---

876 Vgl. SCHMIDT-SEMISCH, S. 65 f.
877 BAUMAN, S. 10.
878 Siehe dazu KUNZ 2011, S. 330 f. Siehe auch SINGELNSTEIN/STOLLE 2012, S. 38 ff.
879 SCHMIDT-SEMISCH, S. 12 ff. und 19 ff.

hingegen Stimmen einer „rationalen Kriminalpolitik“.[880] Die Ansätze zum Risikostrafrecht und die Tendenz der Verwandlung des klassischen Strafrechts in ein Präventivstrafrecht verstärken die Problematik des Feindstrafrechts im Bekämpfungsstrafrecht, indem sie einerseits versicherungsmathematische, statistische Prognosen als empirische Wahrheit in die Beurteilung und Früherkennung von Kriminellen und andererseits eine Interventionsbasis für vorgelagerte Kriminalitätsbekämpfungstätigkeiten in die Kriminalpolitik beziehungsweise in die Rechtsordnung einführen.[881] Diese Entwicklung begünstigt die Annahme, das Vorausahnen und Eliminieren zukünftiger Gefahren und Bedrohungen sei möglich und praktikabel, indem sie als kalkulierbare Ereignisse betrachtet und behandelt werden. Kriminalität wird damit zum bereits im Vorfeld, proaktiv durch vorausschauende Massnahmen zu verhindernden Risikoereignis.[882]

Die neuen Informations- und Kommunikationstechnologien sollen dieses postmoderne Konzept verwirklichen, sie sollen Risiken regulieren – produzieren aber gleichzeitig selbst neue Risiken, nicht zuletzt, indem postmoderne Technologien diese erst sichtbar machen.[883] Wie noch zu erörtern sein wird, reflektiert die Bevölkerung durchaus auch im vorherrschenden gesellschaftlichen Klima die Konsequenzen von Raumüberwachungs-, Registrierungs- und Informationsverarbeitungstechnologien. Indes beherrschen oft klischeehafte, substanzlose Annahmen und intuitive „Weisheiten“ (in der Art von: „Kameraüberwachung hilft, die Kriminalität zu verringern!“ oder „Ich habe nichts zu verbergen!“[884]) die alltägliche Diskussion. Diese Entwicklung begünstigend, operieren einige Protagonisten der Kriminalitätsforschung mit ähnlich vereinfachenden Erklärungen der Kriminalität.

---

880 Siehe KUNZ 2011, S. 323 f. und 331; GARLAND, S. 275 ff.; LOADER/SPARKS, S. 10 ff.

881 PRITTWITZ, S. 364 ff.; KUNZ 2011, S. 339 f; KAMMERER 2008, S. 90.

882 KUNZ 2011, S. 340; SINGELNSTEIN/STOLLE 2012, S. 68 und 79 ff. Vorausgeahnte, nicht geduldete Handlungen, welche zum Beispiel durch die polizeiliche Intervention, basierend auf einer Raumüberwachungsmassnahme, verhindert werden konnten, können vom Strafrecht erfasst werden, indem alle Stadien einer Straftat, das heisst auch Vorbereitungshandlungen, mit einer ähnlich hohen Strafandrohung versehen werden. Vgl. PRITTWITZ, S. 371. Beispielhaft das Betäubungsmittelstrafrecht oder Art. 260^{ter} und $260^{quinquies}$ StGB.

883 Siehe dazu SINGELNSTEIN/STOLLE 2012, S. 32 ff.; ERICSON/HAGGERTY, S. 238.

884 Siehe SOLOVE 2007 für eine überzeugende Replik auf diesen Spruch und das Urteil des Bundesgerichts 1B.466/2012 vom 3. September 2012 E. 2.4 für eine etwas unglückliche Formulierung („Hätte sie [die Beschwerdeführerin] insoweit nichts zu verbergen gehabt, hätte sie dazu nähere Angaben machen können.“). Siehe auch MARX 2007 zu dieser und vielen anderen „techno-fallacies“. Vgl. auch CROSSMANN; TESCHNER, S. 116.

Dieses gesellschaftliche Klima, gekoppelt an die dargestellte Risikologik, begünstigt ein uferloses Verständnis des Begriffs „Sicherheit". Die „Sicherheit" wird gleichzeitig zum Wert, Rechts-/Schutzgut und öffentlichen Interesse. Dem weitgefassten Ideal soll gar Grundrechtsstatus zukommen. Die Sicherheitsbedürfnisse des Staats und der Gesellschaft bekommen dadurch eine Vorrangstellung gegenüber Grundrechten einzelner Individuen; geschweige denn derjenigen (mutmasslicher) Delinquenten.[885] Sicherheit wandelt sich zum „naturrechtlichen Gut […], das jedes Individuum für sich verlangen und verteidigen kann"[886], aber, und das ist die wichtigere Feststellung, in Befolgung des implizierten Imperativs der Eigenverantwortung und zum Schutze seiner Mitbürger zugleich verteidigen *muss*.[887]

B. Kriegsanalogien

Die Sicherheitsdebatte führte zu einer Denkweise des Vorgehens gegen die Kriminalität, welche oft mit dem stilisierten Ausdruck *war on crime* umschrieben wird. Der Terminus „war on crime" ist aber nicht nur eine Bezeichnung der Entwicklung, sondern zugleich ein von den Exponenten dieser Strömung bewusst gewählter Leitspruch, welcher die Dringlichkeit und Notwendigkeit des ausserordentlichen Handelns gegen die Kriminalität vermitteln soll. Mit den Worten SIMONS: „[…] the term «war» with the substantive issue transforms it from a question of policy to a model of how to govern."[888] Der Gebrauch des „Kriegs" als Leitbegriff für Strategien der Begegnung von Kriminalität drückt das Vorliegen einer Krisensituation aus, in der die sonst geltenden Grundsätze und Normen aufgrund der ansonsten nicht abwendbaren Gefahr ausser Kraft gesetzt sind.[889] Der andauernde Ausnahmezustand wird schliesslich zum Regelzu-

---

885 ALBRECHT P. A. 2003, S. 39 ff., welcher die Neuschöpfung des „Grundrechts auf Sicherheit" eine „juristische Kunstfigur" nennt. Ebenso skeptisch Winfried Hassemer und Attilio Nisco, siehe NISCO, S. 79 f. Ablehnend auch KUNZ 2000, S. 55 f.; MÜLLER L. 2011, S. 188 f.; RUDIN, S. 282; SIMON D., S. 40 und 72 f. Einen Überblick zum „Grundrecht auf Sicherheit" und dessen Problematik geben THIEL, S. 154 ff. und MIDDEL, S. 39 ff., der dieses für verzichtbar hält, die Befürchtungen ALBRECHTS aber nicht vollumfänglich teilt.

886 NISCO, S. 79.

887 Vgl. SCHMIDT-SEMISCH, S. 103. Die Verdachtsregister und die Raumüberwachung demonstrieren dieses Problem in eindrücklicher Art und Weise.

888 SIMON, S. 99 f. und 259 ff.

889 Vgl. CHESTERMAN, S. 39 ff., insb. S. 44; HEYMANN, S. 161; KUNZ 2010b, S. 20; SINN, S. 109 f.; TROTHA, S. 227 ff. und 231.

stand. Der Begriff der Kriminalitätsbekämpfung impliziert zudem das Postulat, dass es „die Kriminalität" gibt, sie ein Problem (mit neuen Herausforderungen) darstellt, das jederzeit eskalieren kann und ihr gegenüber von jedem entschlossenes Handeln verlangt wird. Damit wird mithin jedwede Kriminalitätsbekämpfungstechnologie gerechtfertigt, solange mit ihrer Hilfe drohende Gefahrenquellen antizipiert und möglichst proaktiv und effizient abgewendet werden sollen.[890]

Im Umfeld der Angstkultur wurde und wird diese Rhetorik benutzt, um eine harte Haltungen gegenüber Kriminalität und Kriminellen zu verbreiten. Ob die Methapher des Kriegs taugt, das tatsächlich vorherrschende Szenario zu erfassen, ist indes höchst fraglich.[891] Die Begrifflichkeiten und Taktiken des Kriegs helfen in der Kriminalitätskontrolle selten weiter, sondern lassen im Gegenteil viele neue Probleme entstehen, die dem eigentlichen Ziel entgegenwirken:

Erstens verschafft die Kriegsterminologie dem „Kriminellen" eine privilegierte Stellung, indem sie ihn auf die gleiche Stufe wie die Kriminalitätsbekämpfer des Staats hebt. Im Krieg begegnen sich zwei gleichgestellte Parteien auf gleicher Ebene mit gleichem Anspruch auf „Kriegshandlungen". Die kriminelle Handlung wird dadurch aus dem Kontext der rechtlichen Ordnung des Staats herausgerissen und quasi legitim. Der Staat anerkennt demnach den Kriminellen als Gegenspieler und rückt ihn in eine, diesem an sich nicht zustehende, besondere Position. Damit einher geht eine Verschlechterung der Stellung der Opfer und der zu Unrecht verdächtigten Betroffenen, denn Kriegsopfer und gelegentliche haltlose Verdächtigungen (in Kriegsterminologie: „Kollateralschäden") sind nach diesem Argumentationsmuster hinzunehmen.[892] Dieses Argumentationsmuster wird verwendet, obwohl die Strömung des Bekämpfungsstrafrechts als dringende Anliegen eigentlich die Wiedereinführung der opferzentrierten Haltung und die Stärkung der Opferstellung im Strafrechtskomplex fordert. Darin ist eine sehr ambivalente Wahl von Begrifflichkeiten zu erkennen.

---

890 ZERBES, S. 7, 35 f. und 312; NOGALA 1998, S. 283 f. Siehe auch SZUBA, S. 41 f. und 45. Das Strafrecht wird damit zum „gefügigen Diener", schliesslich zum „Kampfinstrument" (HASSEMER 2006, S. 132; vgl. NOGALA/SACK, S. 145 f.).

891 Siehe HEYMANN, S. 19-24; MARX 2007 (Fallacy 18); CHESTERMAN, S. 2 f. und 47; SIMON D., S. 3 und 127. A. A. sind etwa MINOW ET AL., S. 11-13, die den Terrorismus im 21. Jahrhundert als komplett neue Bedrohung in nie dagewesenem Ausmass sehen.

892 Siehe den Artikel von DYER in The Guardian vom 24. Januar 2007, in dem Sir Ken MacDonald im Sinn der hier vertretenen Meinung plädiert: „The fight against terrorism on the streets of Britain is not a war."; CHESTERMAN, S. 100 f.; HEYMANN, S. 19.

Zweitens dürfte die globale Kriegserklärung gegen „die Kriminalität" die Zahl solcher, die bereit sind, eine Straftat zu begehen oder Straftäter zu unterstützen, eher steigern als mindern. Eine derartige Blankoerklärung weckt Zugehörigkeits- und Solidaritätsgefühle.[893] Zudem kann sich daraus, neben anderen negativen Auswirkungen, ein ungerechtfertigt schlechter Ruf von gut funktionierenden Einsatzvarianten postmoderner Technologien ergeben.

Drittens verschleiert der Gebrauch von Kriegsanalogien die klare Sicht aller an der Kriminalitätsbekämpfung Beteiligten (inklusive der Bevölkerung). Vielmehr sollten anstatt dessen einzelne Probleme vertieft und zweckmässige Ansatzpunkte in transparenter Weise zur Diskussion gestellt werden.[894]

C. Bekämpfungsstrafrecht

Das Konzept des Feindstrafrechts ist einer der Hauptpfeiler des Bekämpfungsstrafrechts. Es stellt, deskriptiv verstanden, einen zunächst einigermassen einleuchtenden Erklärungsversuch der dargestellten Strategien zur Strafprävention und -verfolgung dar. Zudem trifft GÜNTHER JAKOBS, wenn er meint, allzu normatives und idealisierendes Kritisieren vorhandener Tatsachen sei müssig[895], einen angreifbaren Punkt der rechtsstaatsortienterten Kritik an der Kriminalitätsbekämpfung mittels postmoderner Techniken: Sind diese verfügbar und scheinen sie zu wirken, ist deren Einsatz nicht zwingend eine juristische Frage, die von Experten beurteilt und beantwortet wird, sondern ihre Anwendung wird basierend auf einer politisierten Agenda entschieden und getragen.

Davon abgesehen ist Feindstrafrecht ein Konzept, das Anlass zu Kritik gibt.[896] Im Sinne einer pragmatischen Herangehensweise wird zunächst der Frage nachgegangen, woran es liegt, dass die Ideologie des Bekämpfungsstrafrechts in der Gegenwart eine valable Option darzustellen scheint. Es ist nicht lange her, dass

---

893 Vgl. CHESTERMAN, S. 101; HEYMANN, S. 46. Zumindest werden mit dieser Vorgehensweise (gemachte) „Feinde" weiter entsozialisiert. Vgl. SIMON, S. 278.

894 HEYMANN, S. 87.

895 JAKOBS 2006, S. 291 f. und 297.

896 Neben den im Folgenden zitierten Beiträgen eignet sich zum kritischen Einstieg in das Thema „Feindstrafrecht" der Sammelband von THOMAS UWER.

einige der durch das Bekämpfungsstrafrecht entstandenen Methoden und Massnahmen als zur Verbrechensprävention unzulässig angesehen wurden.[897]

JAKOBS brachte seine Erklärungsvariante des Begriffs „Feindstrafrecht" Mitte der Achtzigerjahre im Rahmen einer Strafrechtstagung in Frankfurt am Main in den Strafrechtsdiskurs wieder ein – viele feindstrafrechtliche Überlegungen äusserte Franz von Liszt bereits Ende des 19. Jahrhunderts[898] – und er ist es, der den Begriff bis heute prägt.[899] Auf dieser Strafrechtstagung beschrieb JAKOBS vor allem die Probleme der Vorfeldkriminalisierung und sprach sich tendenziell (noch) für eine kritische Haltung gegenüber den sich abzeichnenden feindstrafrechtlichen Tendenzen im Recht aus. Während der folgenden Jahre indes entwickelte er seine Gedanken weiter und kreierte seine eigene Theorie des Feindstrafrechts, in welcher er immer stärker für die seines Erachtens für die Rettung des Strafrechts notwendige Unterteilung desselben in das Feindstrafrecht und das Bürgerstrafrecht argumentierte.[900]

JAKOBS konnte mit dieser Forderung in der Lehre, Praxis und Literatur wenig Unterstützung finden.[901] Festzustellen ist aber, dass heute in verschiedenen Bereichen des Strafrechts feindstrafrechtliche Einflüsse in die Gesetze und das Allgemeinverständnis von Strafrecht übernommen wurden. Vor dem Hintergrund der Anschläge am 11. September 2001 und eines immer grösser werdenden gesellschaftlichen Interesses an umfassender Sicherheit hat die Thematik um das Feindstrafrecht seit dem Jahr 1985 also keineswegs an Aktualität verloren.[902]

---

897 Siehe KUNZ 2006, S. 73; HASSEMER 1995, S. 484; ZERBES, S. 4 f.; REUBAND 2001, S. 6; SINGELNSTEIN/STOLLE 2012, S. 171 f.; SIEBER, S. 2; SIMON D., S. 1, 5 und 92; OBERHOLZER 2003, S. 330 f., denen Recht zu geben ist, dass sich diesbzgl. ein „Paradigmenwechsel" vollzogen hat. Ähnlich SINN, S. 107; CROSSMAN, S. 115.

898 LISZT, S. 163-174.

899 ARNOLD 2006a, S. 303 f.; DERS. 2006b, S. 13.

900 JAKOBS beharrt indes darauf, die im Strafrecht herrschenden Zustände lediglich deskriptiv aufzuzeigen (vgl. JAKOBS 2006, S. 290). Angesichts seiner klaren Meinung bezüglich der Notwendigkeit einer Unterteilung des Rechts in Feind- und Bürgerstrafrecht ist ihm nicht zu folgen. Gl. A. wie MELIA, S. 277 f. Zum Wandel JAKOBS Ansicht: NEUMANN, S. 299 ff.

901 Der überwiegende Teil der Lehre lehnt seine Theorie des Feindstrafrechts ab. Eine Aufstellung der herrschenden Lehre dazu findet sich bei HEINRICH, S. 101 Fn. 37 und NEUMANN, S. 299 Fn. 2. Die breite Auflehnung der Praxis gegen diese Theorie wird bei ARNOLD 2006b, S. 15 ff. ersichtlich.

902 Vgl. zum Ganzen: HEINREICH, S. 94 f.

Eine Kernthese seines Modells des Feindstrafrechts formuliert JAKOBS wie folgt: „Jeder, *der zumindest einigermassen verlässlich Rechtstreue verspricht*, hat den Anspruch, als Person im Recht behandelt zu werden. Wer dieses Versprechen nicht in glaubhafter Weise leistet, wird tendenziell fremdverwaltet; ihm werden Rechte genommen. Seine Pflichten bleiben ungeschmälert [...], sonst wäre er mangels Pflichtverletzung nicht Verbrecher. Soweit ihm Rechte genommen werden, wird er [...] nicht als Person im Recht behandelt."[903] JAKOBS teilt die Adressaten des Strafrechts in zwei Gruppen auf: Die Bürger und die Feinde. Die beiden Gruppen unterschieden sich in ihrer Einstellung zu ihren Pflichten gegenüber dem Staat beziehungsweise der Gesellschaft. Die Bürger achteten ihre Pflichten im Grossen und Ganzen. Die Feinde hingegen definiert Jakobs als notorische Rechtsbrecher oder nennt sie, mit Rückgriff auf Thomas Hobbes und Immanuel Kant, auch „prinzipielle Abweichler".[904] Die Bürger genössen im Austausch für ihre grundsätzlich eingehaltene Rechtstreue alle vom Staat garantierten Rechte, den Feinden jedoch spricht Jakobs diese (teilweise) ab. Sie werden „entpersonalisiert" – das heisst ihr Personenstatus wird angezweifelt oder aufgehoben, und sie werden „als rechtliche Unperson aus der Gesellschaft" ausgeschlossen.[905] JAKOBS bezeichnet sodann den (zu entpersonalisierenden) Feind als jemanden, der mangels einer „kognitiven Mindestgarantie" als Person behandelt zu werden, und dadurch, dass er eine „Gefahrenquelle" darstelle, „kaltgestellt" und wie ein „wildes Tier" gesichert werden müsse.[906] Abgrenzungskriterien des Feindes vom Bürger sieht Jakobs in der Haltung einer Person, in deren Erwerbsleben und in der Frage, ob sie in eine kriminelle Organisation eingebunden ist. Um als Feind zu gelten, muss sich die Person ausserdem dauerhaft vom Recht abgewandt haben.[907] Weil die Adressaten des bestehenden Strafrechts sich derart grundlegend in ihrer Rechtstreue unterschieden, hält JAKOBS die Aufteilung des Strafrechts in zwei auf die Adressaten zugeschnittene Bereiche, das Bürger- und das Feindstrafrecht, somit für unabwendbar.[908]

---

903 JAKOBS 2006, S. 293.

904 JAKOBS 2006, S. 292; DERS. 2004a, S. 90.

905 JAKOBS 2004a, S. 90; DERS. 2006, S. 292. Sehr ähnlich wie LISZT, S. 172 („Unschädlichmachung der Unverbesserlichen").

906 JAKOBS 2000, S. 52 f.; DERS. 2004, S. 41. Vgl. HEINRICH, S. 100.

907 JAKOBS 2004a, S. 92 mit Beispielen.

908 JAKOBS 2000, S. 53, hält zum heutigen Zeitpunkt Alternativen zu seinem Konstrukt des Feindstrafrechts für ausgeschlossen.

Die wichtigsten Kennzeichen und Folgen des implementierten Feindstrafrechts sind die Vorverlagerung der Strafbarkeit ohne proportionale Reduktion der Strafe (Vorfeldkriminalisierung), das Bekämpfungsvokabular sowie die Bekämpfungsgesetzgebung und der Abbau prozessualer Garantien.[909] Der erste Punkt bezeichnet Entwicklungen im Strafrecht, die in der vorliegenden Untersuchung lediglich erwähnt werden. Die letzten beiden Punkte weisen indes einen direkten Konnex zu den postmodernen Bekämpfungstechnologien auf. Der vermehrte Einsatz dieser Technologien ist sowohl im Strafprozessrecht als auch im Polizeirecht zu beobachten. In der Terminologie des Bekämpfungsstrafrechts wandelt sich die präventive Gefahrenabwehr der Polizei zur Bedrohungsbekämpfung und -elimination. Mit der ausgewechselten Bezeichnung der präventiven Aufgabe der Polizei steigt gleichzeitig der Anspruch an ihre Leistung. Was früher genügte, ist heute zu wenig. Die Mutation der *unpersönlichen* Gefahr (eines Unglücks), welche irgendwo und irgendwie da ist, zur persönlichen Bedrohung (durch ein Übel oder Unrecht), die sich gegen jeden richtet und jeden von uns auf Schritt und Tritt verfolgt, führt zu einer veränderten Sichtweise der Gesellschaft auf die polizeiliche Tätigkeit in der Gefahrenabwehr. Denn das Übel ist im Gegensatz zum Unglück identifizierbar und muss somit eingeschätzt und verhindert werden. Indem sich die Kriminalität in der Wahrnehmung durch die Gesellschaft in der jüngeren Zeit vom Unglück zum Übel wandelt, ändert sich auch die gesellschaftliche Haltung gegenüber dem einzelnen Kriminellen.[910] Die Postmoderne, die neoliberale Grundhaltung und die diffusen Unsicherheitsgefühle der westlichen Gesellschaft rufen in der Bevölkerung neue Bedürfnisse hervor: Einerseits sollen neue, formell-staatliche Sicherheitsmechanismen jegliches Übel verhindern oder eliminieren und zugleich die Normgeltung in der Gesellschaft erhalten.[911] Andererseits sollen die für trotzdem geschehenes Unrecht verantwortlichen Subjekte und Instanzen zur Rechenschaft gezogen werden.[912]

---

909 SINN, S. 108. Vgl. JAKOBS 2004a, S. 92 mit Beispielen zur Bekämpfungsgesetzgebung. Vgl. auch HASSEMER 2006 und ZERBES, S. 298 f. zum „modernen Präventionsparadigma".

910 BOERS, S. 12; PRITTWITZ, S. 378 ff.; SIMON, S. 259 ff. insb. 264; KUNZ 2011, S. 366 f.; VOLKMANN, S. 216. Das bevorstehende, voraussehbare Unglück nehme ich nicht persönlich; es ist etwas, das passiert. Das drohende Übel ist hingegen etwas, das zogeordnet und abgewendet werden kann. Insofern geht mit der Entwicklung zur *Entpersonifizierung des Kriminellen* eine *Subjektivierung des Unglücks* einher.

911 Vgl. SINGELNSTEIN/STOLLE 2007, S. 106 f.

912 KUNZ 2011, S. 134 f.

Gegen wen sind die postmodernen Bekämpfungsstrategien einzusetzen? JAKOBS ist der Ansicht, in der Sozialkontrolle der Postmoderne sei jeder „Person im Recht", solange „dieser «Jeder» seinerseits seinen Pflichten nachkommt, oder falls nicht, wenn man ihn im Griff hat, er also nicht gefährlich werden kann."[913] Worin unterscheidet sich der andere „Jeder" von uns, die wir „Jeder" sind? Wie erkennen wir denjenigen „Jeder", der keine „Person im Recht" sein soll? Mit diesen Fragen beschäftigen sich Feind- und Risikostrafrecht lediglich oberflächlich.

Den Hintergrund des Feindstrafrechts bilden insbesondere an Defiziten orientierte Theorien. Das Risikostrafrecht stützt sich wesentlich auf das Menschenbild der Theorie des „rationalen Wahlhandelns" ab.[914] Feind- und Risikostrafrecht werden wieder im Bekämpfungsstrafrecht benutzt: Zum einen, um die Merkmale des Feindes zu finden und definieren. Zum anderen um (vermeintliche) Möglichkeiten zu präsentieren, wie (potenzielle) Übeltäter behandelt werden sollen, damit sie ungefährlich bleiben.[915] Diese Ansätze schlagen indes meist keine Lösungen vor, sondern stellen vor allem Argumente für den Feindstatus einer Person oder Personengruppe bereit. Um das Bekämpfungsstrafrecht zu konstituieren und aufrechtzuerhalten, bedarf es diesbezüglich klar zuzuschreibender Merkmale der Nonkonformität. Die als *kanzeroid* bezeichneten Elemente der Gesellschaft muss man gemäss diesem Konzept in Extremform kennzeichnen und damit dem Bürger allgegenwärtig vorführen können.[916] Der Bürger muss und will die Bedrohung („das Böse") sehen, verorten und mit seinem „gesunden Menschenverstand" begreifen können.

Mittels der kriminologischen Hirnforschung und postmoderner Kriminalitätstheorien wird das Konzept des Bekämpfungsstrafrechts mit den dafür benötigten Feindbildern versorgt. Das Feindstrafrecht rechtfertigt die Exklusion der identifizierten Gefährlichen: Der potenzielle Feind soll frühzeitig, bevor er anfängt zu „wüten", oder die zum Feind verkommene Person, wenn sie gewütet hat, „in den Griff" bekommen werden.[917] Hinsichtlich einer anhaltenden und breitgefächerten Ausgrenzung im Sinne des Gesellschaftsschutzes (respektive des Bürgerschutzes) und der gestärkten „Integration" der Konformen mussten neue Methoden

---

913 JAKOBS 2006, S. 290.
914 PRITTWITZ, S. 367.
915 Vgl. KUNZ 2010a, S. 128 f.
916 CAMPBELL, S. 88.
917 So JAKOBS 2006, S. 290.

gefunden werden.[918] Die vorausahnende Wache und die eiserne Durchsetzung als Konzepte der Kriminalitätsbekämpfung beruhen auf einem Menschenbild, das anschaulich anhand der aktuellen kriminologischen Hirnforschung, der Theorie des ökonomischen Wahlhandelns von GARY S. BECKER und der „allgemeinen Kriminalitätstheorie" von MICHAEL R. GOTTFREDSON und TRAVIS HIRSCHI dargestellt werden kann.

D. Aktuelle Biokriminologien

Aktuelle Biokriminologien sehen für delinquente Verhaltensweisen, teils multifaktoriell bedingte, auf den menschlichen Körper einwirkende negative Einflüsse verantwortlich.[919] Ein Teil der aktuellen kriminologischen Hirnforschung erkennt in Gehirnschädigungen, Fehlfunktionen des Stoffwechsels und unbalancierten Botenstoffen „sehr eindeutige Zusammenhänge" zu einer erhöhten Vulnerabilität für Devianz.[920] Axel Honneth trifft den Kern dieser Strömung in seinem Vorwort zu LEMKE: „Was als Ursache einer organischen Erkrankung oder eines abweichenden Verhaltens gilt, ist dem menschlichen Sinnhorizont gänzlich entzogen, weil es nur noch als technisch beeinflussbarer Defekt des Körpers wahrgenommen wird. Blindes Schicksal der Natur scheint mithin allein Chancen und Gefährdungen des menschlichen Lebens zu bestimmen."[921] Dieser prosperierende Forschungszweig besinnt sich eines *anlagebetonten* Modells, das vor allem auf Überlegungen Cesare Lombrosos zurückzuführen ist. Lombroso studierte im Italien des 19. Jahrhunderts die äusserlichen Gesichtszüge von Gefängnisinsassen. Er kam zum Schluss, er könne menschliches Verhalten anhand angeborener und bleibenden, äusserlichen Merkmalen erklären. Deren Analyse erlaube es ihm, „l'uomo delinquente" vom konformen Mitbürger zu unterscheiden.[922]

---

[918] SINGELNSTEIN/STOLLE 2007, S. 107 und 109. DIES., S. 107, halten, m. E. zutreffend, auch die Sozialkontrolle für einen wichtigen Bestandteil des Bekämpfungsstrafrechts.

[919] Siehe für einige Varianten KUNZ 2011, S. 63 ff.; SCHWARZENEGGER, S. 116 ff.; ROSE, S. 81; die Biocrime-Website <http://www.crimetimes.org>.

[920] MARKOWITSCH/SIEFER, S. 11. Zu den bildgebenden Verfahren der funktionellen Magnetresonanz-Tomografie (fMRT) siehe HASLER, S. 42 ff.; SCHLEIM, S. 154 ff.

[921] LEMKE, S. 9.

[922] KUNZ 2011, S. 44 ff.; DERS. 2010a, S. 124 f.; KRÖBER, S. 74 ff.; SCHWARZENEGGER, S. 113 f.; RZEPKA, S. 120 f. Siehe dazu auch HOFINGER. Lombroso (1836-1909) schrieb seine Erkenntnisse erstmals in seinem Buch „L'uomo delinquente" (1876) nieder. Nur schon, weil er lediglich retrospektive Untersuchungen an einer Gefängnispopulation betrieb, ist die

Von Vertretern der aktuellen kriminologischen Hirnforschung wird behauptet, analog dazu eine Methode zur objektiven, neuro-medizinischen Identifizierung der Prädisposition eines Menschen zu bestimmten Verhaltensweisen gefunden zu haben. Das Kriterium für die Abgrenzung des delinquenzaffinen, vor allem des zu Gewalt neigenden, vom „normalen" Individuum sei (die äusserlichen Charaktermerkmale von Lombroso wurden aufgegeben) in strukturellen und funktionalen Auffälligkeiten des Stirnhirns, insbesondere des prä- und orbitofrontalen Cortex, zu finden.[923] Menschliches Verhalten ist nach Ansicht einiger Vertreter dieser kriminologischen Strömung durch die Beschaffenheit des Gehirns determiniert und durch *medizinische Fakten* erfassbar. Ähnliche Einflüsse dieses biologisch determinierenden Menschenbilds sind auch in der Kriminalpsychiatrie (defizitäre Persönlichkeit) und der Genmedizin auszumachen.[924] ROTH kommt stellvertretend für die Extremposition in der aktuellen kriminologischen Hirnforschung zum Schluss: „Das bewusste, denkende und wollende Ich ist nicht im moralischen Sinne verantwortlich für dasjenige, was das Gehirn tut […]".[925] MARKOWITSCH/SIEFER meinen, besonders bei Gewalt- und Gewohnheitsverbrechern finde sich fast immer ein „hirnbiologischer Hintergrund".[926]

Aussagekraft sehr gering. Ein Problem, das auch die folgenden, heutigen Theorien und Methoden oft haben. Siehe dazu etwa GMÜR, S. 1310 f.; SKILLICORN 2008b, S. 72.

923 ROTH ET AL. 2006, S 56; MERKEL/ROTH, S. 30 mit weiteren Hinweisen; ROTH 2012, S. 93 ff.; KUNZ 2011, S. 71; HASLER, S. 198 ff. DERS., S. 49 f. und 202, merkt kritisch an, dass die Hirnregion des sog. „anterioren cingulären Cortex" ohnehin notorisch aktiv sei, sobald Emotionen und Kognition involviert seien und der Befund dessen Aktivierung in Studien deshalb nicht mehr als eine „erkenntnistheoretische Trivialität" sei. Ähnlich skeptisch SCHLEIM, S. 84 und 88. Zur Vertiefung der Thematik siehe auch SPRANGER (Übersicht über den Einfluss der Neurowissenschaften auf das Recht in ausgewählten Ländern) und die Website der „kritischen Neurowissenschaften" <http://www.critical-neuroscience.org>. Für weitere anlagebetonte Ansätze, siehe SCHWARZENEGGER, S. 118 f. und 123.

924 Siehe SCHWARZENEGGER, S. 120 ff.; KUNZ 2011, S. 82; HOFINGER. Vgl. zum Beispiel MARKOWITSCH/SIEFER, S. 160 ff.

925 ROTH 2003a, S. 180 f. Dadurch erhebt er das Gehirn zu einem das Ich steuernden, aber von diesem unabhängigen Homunculus. Vgl. SCHNEIDER, S. 236; HASLER, S. 62.

926 MARKOWITSCH/SIEFER, S. 132, 140 und 170.

E. Postmoderne Kriminalitätstheorien

Im scheinbaren Gegensatz zu den deterministischer ausgeprägten biologischen Theorien verantwortet nach den postmodernen Kriminalitätstheorien[927] die Person alle eigenen Handlungen selbst: Jedes Individuum wählt „utilitaristisch-kalkulierend", wie es sich in einer bestimmten Situation verhält.[928]

So stellt GARY S. BECKER in seiner *ökonomischen Theorie des rationalen Wahlhandelns* („rational choice theory") die These auf, menschliches Verhalten beruhe allgemein auf einer Kosten-Nutzen-Rechnung. Der Mensch als „homo oeconomicus" folge in seinen Entscheidungen fortwährend einer subjektiven, aber rationalen Nutzenmaximierung. Das Individuum entscheidet sich gemäss dieser Theorie somit für kriminelles Verhalten, sobald dieses einen grösseren Gesamtnutzen verspricht als dessen gesetzeskonforme Alternativen. Um Entscheidungen zugunsten der Kriminalität zu verhindern, soll diese „besteuert" werden, indem unerwünschtes Verhalten durch Anreize legaler Handlungen oder durch Abschreckung ökonomisch unattraktiv gemacht werde. Die Abschreckung beruht auf zwei Elementen: Der Strafhärte und der Strafwahrscheinlichkeit, wobei Letztere wohl grössere Auswirkungen auf die rationale Kosten-Nutzen-Rechnung hat.[929]

Die *allgemeine Kriminalitätstheorie* von GOTTFREDSON/HIRSCHI betrachtet den Abweichler hingegen als hedonistischen, sprunghaft und impulsiv Handelnden, welcher zu keinem rationalen Kalkül der Kosten und Nutzen fähig sei, sondern seine Handlungsentscheidungen auf den raschen Gewinn ausrichte.[930] Das gewöhnliche Verbrechen geschehe ungeplant. Der Delinquent selbst sei in der Regel ungeschickt und unorganisiert. Die Theorie von GOTTFREDSON/HIRSCHI führt kriminelles Verhalten, basierend auf diesen Beobachtungen, ausschliesslich auf zwei Faktoren zurück: Vorhandene, objektive Tatgelegenheiten und die mangelhafte oder mangelnde Selbstkontrolle.[931] Die Fähigkeit zur Selbstkontrolle entwickle sich beim Menschen in den ersten sechs bis acht Lebensjahren und

---

927 Siehe ausführlich zu den postmodernen Kriminalitätstheorien KUNZ 2011, S. 131 ff.; KRASMANN, S. 286 ff.

928 KUNZ 2011, 136 f.

929 Siehe zum Ganzen: KUNZ 2011, S. 139 ff.; DERS., S. 738 ff.; SINGELNSTEIN/STOLLE 2012, S. 46 ff. Vgl. PRATT ET AL., S. 369; NIGGLI 1995, S. 98.

930 KUNZ 2011, S. 149.

931 GOTTFREDSON/HIRSCHI 1990, S. 269 und 119: „[…] complex, difficult crimes are so rare that they are an inadequate basis for theory and policy." Vgl. KUNZ 2011, S. 150 ff.

hänge wesentlich von der erziehenden Familienstruktur ab. Entwächst das Individuum diesem Kindesalter, bleibt die erlangte oder eben nicht erlangte Selbstkontrolle über das ganze Leben hinweg unveränderlich und konstant.[932] GOTTFREDSON/HIRSCHI meinen demnach im Defizit der Selbstkontrolle ein objektivierbares Kriterium der Devianz gefunden zu haben.[933]

F. Kriterien der Gesellschaftsuntauglichkeit

Mit seiner Entpersonalisierung des Feindes und mit dessen Degradierung „zum wilden Tier" findet sich JAKOBS nahe der von ihm angesprochenen Anschauung Fichtes wieder, welcher Mörder als „Vieh" bezeichnete.[934] Der Personenbegriff JAKOBS beruht, wie ausgeführt, auf einer von den Bürgerpflichten abhängigen Leistung der Normkonformität. Die Einteilung der Bürger und Feinde beruht alleine auf dieser Voraussetzung. Bei der Beurteilung, meint JAKOBS, sei nicht nur das Verhalten einer Person im Moment und in der Vergangenheit bei ihrer Etikettierung zu berücksichtigen, sondern auch eine Prognose zur zukünftigen Gefährlichkeit des zu erwartenden Verhaltens zu stellen und beizuziehen.[935] Eine *im Ergebnis* übereinstimmende Ideologie verkörpern die kriminologische Hirnforschung und die allgemeine Kriminalitätstheorie von GOTTFREDSON/HIRSCHI. Der Kriminelle begeht seine Taten aufgrund eines unüberwindbaren, (quasi-) anlagebedingten Defizits.[936] Ihr Erklärungsansatz verdammt den Delinquenten ebenso zum determinierten Roboter wie die Hirnforschung. Eine fehlende Selbstkontrolle lässt keine freien Entscheidungen zu. Das defizitäre Individuum kann sich nicht bewusst gegen seinen unkontrollierten Drang entscheiden, was autonome Willenshandlungen per se ausschliesst.[937]

---

932 GOTTFREDSON/HIRSCHI 1990, S. 272 f.; KUNZ 2011, S. 152 f.

933 KUNZ 2011, S. 153 f.

934 Siehe JAKOBS 2006, S. 293 oben; DERS. 2004, S. 41.

935 Sehr bezeichnendes Zitat JAKOBS 2006, S. 290: „Wenn er aber wütet, muss man ihn bekämpfen, und wenn er wüten könnte, muss man sich vorsehen." Die Wortwahl „wüten könnte" weist auf einen nicht sehr zurückhaltenden Umgang mit dem Positivbefund „Feind" hin. JAKOBS deutet damit an, dass bereits die *Möglichkeit*, nicht etwa eine grosse und individuell überprüfte Wahrscheinlichkeit, der Realisierung zukünftigen problematischen Verhaltens dafür ausreichen solle.

936 Siehe KUNZ 2011, S. 181 ff.

937 GOTTFREDSON/HIRSCHI 1990, S. 61 sind a. A. Auch ROTH 2003b, S. 531, wehrt sich gegen diesen Vergleich mit einer Maschine, indem er denselben Trick anwendet wie GOTTFREDSON/HIRSCHI: Er konstruiert die Verantwortlichkeit des Einzelnen über die „Autonomie

Die Theorie des rationalen Wahlhandelns erklärt abweichendes Verhalten zwar nicht mittels eines Defizits oder determinierten Verhaltens. Sie intensiviert indes die Zuweisung der Verantwortung für geschehenes Übel, indem sie annimmt, der Delinquent entscheide sich bewusst, nach reiflicher Überlegung und rational für das Unrecht. Da die ökonomische Theorie BECKERs die Impulse und Beweggründe *hinter* der Kosten-Nutzen-Abwägung nicht konkretisiert, können diese zudem in seine Theorie hinein interpretiert werden. Die Theorie ist demzufolge kompatibel mit Ansätzen der Erklärung des Ursprungs und der Genese von Willensentscheiden aus anderen Theorien.[938] Das rationale Wahlhandeln besitzt, unter Vorbehalt der beschriebenen Probleme, dort eine gewisse Plausibilität, wo die gewählte Handlung eine gesellschaftstaugliche (nicht zwingend legale) ist. Sie versagt, wo die gewählte Handlung aus der subjektiven Sicht und Werthaltung der Öffentlichkeit scheinbar unerklärlich ist. Die Öffentlichkeit äussert heute Kriminalität gegenüber schneller Unverständnis. Sie anerkennt kriminelle Handlungen weniger häufig als vernünftig. Der Bogen von dieser Theorie zu den Defizittheorien lässt sich somit über das Image des Kriminellen schlagen: Dieser ist eine personifizierte Bedrohung. Die Zuordnung des Abnormalen in der kriminologischen Hirnforschung ist absolut. Aber gerade bei besonders verabscheuungswürdigen, furchtbehafteten Delikten kümmert sich die Bevölkerung nicht um Kleinigkeiten, wie die Unterscheidung, ob die Untat willentlich und rational im Sinne der Theorie BECKERS oder aufgrund eines angeborenen oder anerzogenen, persistenten Defizits begangen wurde.[939] Der „gesunde Menschenverstand" mischt die Theorien nach Belieben und ermöglicht damit zum Beispiel, dass das Modell und die Erkenntnisse der Theorie des rationalen Wahlhandelns auch diejenigen Kriminellen erfassen kann, die er als zu vernünftigem Handeln unfähig einordnet. Das ist widersprüchlich. Dieses Schema spricht indes das Bedürfnis der heutigen Gesellschaft nach einfachen Erklärungen und Lösungen in der Kriminalität an.

menschlichen Handelns" (was seiner eigenen Theorie widerspricht, siehe KUNZ 2010a, S.132 f.). Siehe dazu RZEPKA, S. 127.

938 Siehe dazu PRATT ET AL., S. 370 ff. und 385. Der ökonomische Ansatz ist ohnehin für „jegliche praktische Kriminalpolitik instrumentalisierbar", siehe KUNZ 2011, S. 147. Vgl. ROTH 2003b, S. 533, der die Entscheidung zum Ergreifen von Handlungsoptionen für kalkulierbar, also deterministisch bestimmt, hält.

939 Eine Konsequenz der gesellschaftlichen Verunsicherung, siehe BOERS, S. 12 f.; SIMON, S. 260 f., welcher, m. E. zu Recht, meint, diese „alptraumhaften" Themen eigneten sich hervorragend für eine „Politik der Furcht".

In dieser Fiktion der Verantwortlichkeit zeigt sich ein innerer Widerspruch. Dem *entpersonifizierten* Feind – JAKOBS aberkennt dem Feind die „kognitive Mindestgarantie", als Person behandelt zu werden und bedient sich damit der Argumentation der vorgestellten Defizittheorien[940] – kann sein (deliktisches) Verhalten nicht zugerechnet werden.[941] Was für das Feindstrafrecht gilt, betrifft in analoger Weise auch die anderen Modelle: Sowohl eine unheilbar abnorme Hirnstruktur als auch die seit dem Kindesalter unveränderliche, fehlende Selbstkontrolle schliessen die Verantwortlichkeit für das eigene kriminelle Handeln (faktisch) aus.[942] Einerseits kann diese Betrachtungsweise (eine Täterzentrierung ohne zurechenbare Schuld) aber unerwünschte beziehungsweise problematische Folgeerscheinungen nach sich ziehen.[943] Andererseits schwächt die Unterstellung der Unverantwortlichkeit des Delinquenten die Rechtfertigung der harten Haltung ihm gegenüber, und der Anspruch auf Tilgung des Unrechts durch Sühne oder auf die Vereitelung des Geschehens von Unrecht durch extensive Massnahmen der Gefahrenabwehr verliert seine Berechtigung (was dem Bekämpfungsstrafrecht nicht entgegen kommt). Die Konstruktion der „Unperson der Gesellschaft" wird unterstützend herangezogen: Weil das Bekämpfungsstrafrecht ohne Begründung, *warum* die Feinde hart angefasst werden dürfen, nicht auskommt[944], muss diese aber an einem anderen Ort gesucht werden. Gefunden wird sie wiederum in den vorgestellten, dramatisierenden Modellen der Kriminalitätstheorien. Die „paradoxe Formel" der Zurechnung von strafrechtlicher Verantwortung an den determinierten Täter aus den Anfängen der Defizittheorien im 19. Jahrhundert[945] wird neu interpretiert. So kann die Anwendung jeglicher Ge-

---

940 Die Parallele und Kompatibilität des Feindstrafrechts zu den Defizittheorien wird offensichtlich, wenn Jakobs 2000, S. 53 festhält, der Feind demonstriere „dieses Defizit durch sein Verhalten".

941 NEUMANN, S. 311. Vgl. JAKOBS 2004b, S. 41.

942 ROTH 2003b, S. 544 hat nicht *grundsätzlich* Unrecht, wenn er meint, die Gesellschaft habe unabhängig von der Schuldfrage ein berechtigtes Anliegen der Abwesenheit von Delinquenz. Diese Ansicht ist zudem kompatibel mit derjenigen JAKOBS 2005, S. 265 f. Es ist indes stark anzuzweifeln, dass die Abwesenheit von Delinquenz je erreichbar und hartes Vorgehen, insb. gegen Kleinstkriminalität oder jegliches unkonforme Verhalten, wünschenswert ist.

943 Siehe RZEPKA, S. 126.

944 Gl. A. wie NEUMANN, S. 309. Der Personenbegriff Jakobs bietet lediglich eine Kategorie zur Kennzeichnung von Individuen.

945 KRASMANN, S. 27: „Je determinierter die Tat, also je eher sie zwingend aus der Persönlichkeit des Täters heraus folgte und je bestimmbarer diese als Individuum war, um so erklärba-

genmassnahmen gegen die Delinquenten doch noch über einen Umweg scheinbar überzeugend gerechtfertigt werden.[946] Die „quasi-wissenschaftliche Rationalität“[947], welche diese Allianz des Bekämpfungsstrafrechts formt und vermittelt, löst zudem entsprechende Handlungsweisen und Methoden von jeglicher Moral, wandelt sie vielleicht höchstens in Moralitäten oder in *Schauspiele über Moral*.

Allen vorgestellten Theorien ist gemein, dass sie vordergründig kaum Abstufungen in der Beurteilung des Menschen kennen. Sie bewerten und etikettieren sie nach einer dramatischen, binären Ordnung in (potenzielle) Opfer und (potenzielle) Täter.[948] Das vermittelte Bild der Abnormalität des Feindes wird zum wesentlichen Kriterium der Gesellschaftsuntauglichkeit. Wer versucht, den Feind zu resozialisieren, ist nach dieser Auffassung verantwortlich für Risiken, die von ihm ausgehen und macht sich mitschuldig an allen Folgen, sollte sich dieses Risiko verwirklichen.[949]

G. Agnostische Zwecksetzung und Artenvielfalt

Die ökonomische Theorie, die allgemeine Kriminalitätstheorie und die Biokriminologien unterscheiden sich in ihren Annahmen sehr wesentlich. Postmoderne Strategien zögern jedoch nicht, diese trotzdem nebeneinander und verknüpft zu verwenden. Im Bekämpfungsstrafrecht wird diesen Strategien gefolgt: zur Bekämpfung von Kriminalität werden mehrere unterschiedliche Taktiken

rer war folglich die Tat und um so eher war der Täter strafrechtlich zur Verantwortung zu ziehen.“

946 NEUMANN, S. 312. GOTTFREDSON/HIRSCHI, S. 272 schliessen, angesichts der faktischen Übertragungsmöglichkeiten ihres Modells ein wenig scheinheilig, alle Massnahmen, ausser der frühkindlichen Erziehung, aus.

947 SCHMIDT-SEMISCH, S. 94. Vgl. SLABY, S. 380.

948 KUNZ 2011, S. 72 ff.; DERS. 2010a, S. 128 f. Ebenso HARCOURT, S. 33. Freilich kennt z. B. das Feindstrafrecht die Kategorie des „straffälligen Bürgers“. In den Schlussfolgerungen oder spätestens im öffentlichen Dialog spielen derartige Abstufungen aber meist keine Rolle mehr. Die Erkenntnisse aus Theorien und Studien entfalten eine eigene Dynamik, die dafür sorgt, dass allfällige Relativierungen der Entwickler der Theorien rasch übersehen werden. Gl. A. wie SCHWARZENEGGER, S. 126 f.

949 Siehe als anschauliches Bsp. das Pamphlet der Kolumnistin DEBRA J. SAUNDERS zu den psychiatrischen Gutachten im Fall Anders Behring Breivik in Norwegen (SAUNDERS in SFGate vom 1. Dezember 2011). Zur „Entmenschlichung“ Krimineller in Italien, insb. illegaler Einwanderer, siehe FERRAJOLI 2009, S. 13; NISCO, S. 74.

genutzt, je nach Situation pragmatisch gemischt.[950] Alte Konzepte, Theoreme und Werte gehen nicht vergessen, sondern werden neben neuen weiter verwendet oder nutzbringend in neue Erklärungscluster integriert und „situations- und kontextabhängig" verwendet.[951] Postmoderne Kriminalitätsbekämpfungsstrategien bedienen sich eklektisch bei verschiedenen theoretischen Ansätzen. Sie verschmelzen unterschiedliche Taktiken und Technologien und verwenden diese opportun-agnostisch.[952] Sie folgen keinem bestimmten „Antwortmuster"[953].

Im Gegenteil werden gerne auch sich in Theorie und Praxis widersprechende Zugänge verwendet: Aus der allgemeinen Kriminalitätstheorie von GOTTFREDSON/HIRSCHI werden als Einsatzweck von Überwachungsmassnahmen die situative Prävention (objektive Tatgelegenheiten sollen durch mehr Fremdkontrolle und dadurch unerwünschtes Verhalten der Person mit mangelnder oder fehlender Selbstkontrolle vermindert oder unterbunden werden) und Taktiken des Gesellschaftsschutzes durch die Verbannung Auffälliger und Unerwünschter aus besonders heiklen Arealen beziehungsweise in Randgebiete abgeleitet.[954] Durch Biokriminologien werden diese Vorgehensweisen beeinflusst, indem unbelehrbare Abweichler konditioniert werden sollen[955]: Durch das Androhen von Strafe (manchmal auch durch die Strafe selbst), Belohnung sowie Lob und Tadel könne

---

950 Vgl. KUNZ 2000, S. 13; SINGELNSTEIN/STOLLE 2012, S. 96 f., 106 f. und 135; FOUCAULT 1994a, S. 260 f., der die Synergien und Wechselwirkungen zwischen „Machtverhältnis und Kampfstrategie" beschreibt.

951 COHEN, S. 127 f.; SCHMIDT-SEMISCH, S. 65; BARZ, S. 26 f.; KRASMANN, S. 54 f.; KUNZ 2000, S. 123; DERS. 2010b, S. 9 und 17; KAMMERER 2011, S. 20 f. Vgl. auch SCHMIDT-SEMISCH, S. 61; HOFFMANN/MUSOLFF, S. 269; BAUMAN, S. 7. Wohl a. A. ALBRECHT P. A. 2010, S. 7, der anmerkt, nicht „Vergeltung oder Prävention, nur noch flächendeckende Sicherheit" sei gefragt. Dem ist insofern nicht zuzustimmen, als zwar flächendeckende Sicherheit nachgefragt wird, aber ebenso alle möglichen Mittel, diese herzustellen.

952 Vgl. HITZLER, S.193 f.

953 GARLAND, S. 258 nennt zwei Antwortmuster der staatlichen Verbrechenskontrolle: Die „Anpassungsstrategie" (Prävention und Partnerschaft) und die „Strategie souveräner Staatlichkeit" (Kontrolle und ausdrucksstarke Bestrafung).

954 Vgl. SINGELNSTEIN/STOLLE 2007, S. 112 f. Bsp.: Bei den Verdachtsregistern soll dies durch die Warnung der Bevölkerung vor den eingetragenen Delinquenten erreicht werden oder indem Letzteren verboten wird, bestimmte Areale zu betreten (Bsp.: Stadionverbot) oder sich bestimmten Gebieten anzunähern (Bsp.: die nähere Umgebung von Spielplätzen). Bei der Videoüberwachung wird in dieser Hinsicht versucht Zonen zu schaffen, in denen das Begehen von Straftaten oder allgemein unerwünschtes Verhalten erschwert wird.

955 ROTH 2003b, S. 544. Siehe dazu RZEPKA, S. 125 f. Ein Praxisbeispiel wäre diesbzgl. die strengen Meldepflichten von Registrierten. Siehe auch HOFINGER, S. 19 für andere Bsp. entsprechender Interventionsvorschläge.

das „emotionale Erfahrungsgedächtnis“ von *einigen* Individuen beeinflusst und damit erreicht werden, dass sie ihre angeborenen Eigenschaften beziehungsweise Anlagen zu steuern (nicht: überwinden oder verändern) vermögen. Bei anderen sei dies jedoch zwecklos.[956] Auf diesem Gedanken basiert auch der Gesellschaftsschutz durch Sicherung des Täters.[957] Der ökonomischen Theorie des rationalen Wahlhandelns entnehmen die Massnahmen alsdann die Idee der „Besteuerung“ illegalen Verhaltens, indem eine hohe Kontrolldichte eine hohe Sanktionswahrscheinlichkeit garantieren soll. Der potenzielle Delinquent soll also gemäss dieser Theorie mittels Abschreckung von unerwünschten Handlungen abgehalten werden.[958]

Wechselwirkungen sind indes nicht nur zwischen den Massnahmen und Theorien untereinander zu erkennen, sondern auch zwischen gesellschaftlichen Bedingungen, Protagonisten, Mechanismen und Institutionen.[959] Aus diesen Synergien und Wechselwirkungen entstehen im Gegensatz zu konsequent auf isolierten Ansätzen beruhenden Strategien flexiblere Instrumente[960], was ein Vorteil sein mag. Gleichzeitig werden dadurch die untersuchten Kriminalitätsbekämpfungsmassnahmen aber undurchsichtig und teilweise rechtlich schwer einschätzbar. Diese Strategien können zudem für problematische Formen der Gefahrenabwehr oder der Ermittlung im Strafverfahren instrumentalisiert werden, indem sie zum Beispiel auf die diffusen Unsicherheitsgefühle und Sicherheitsbedürfnisse der Gesellschaft mit einer auf konstruierte, konturlose Bedrohungen konzentrierten Tätigkeit antworten.[961]

---

956 ROTH 2003a, S. 106 ff. und 181; DERS. 2003b, S. 530 f., 540 f. und 544; ROTH ET AL. 2006, S. 58. Ebenso MARKOWITSCH/SIEFER, S. 132 und 239; DIES., S. 218: „Die Erkenntnis lautet: Die allermeisten Verbrecher sind in ihrer Psyche und damit in ihrem Sozialverhalten gestört – sie sind Psychopathen, Soziopathen oder leiden an einer antisozialen Persönlichkeitsstörung.“ Vgl. KUNZ 2011, S. 70 f.

957 Eine derartige Variante des Gesellschaftsschutzes wären etwa die angesprochenen weiterentwickelten Kombinationen, beispielsweise von Register und Standortdatenabruf, die eine Live-Überwachung erlaubten. Der entstehende Effekt wäre demjenigen einer elektronischen Fussfessel sehr ähnlich. Siehe oben Erster Teil, Kapitel III.C.

958 Bsp.: Die sichtbare Installation von Kameras i. V. m. einer guten Aufklärungsquote (bedingt durch die Kameraaufnahmen des überwachten Raums) und dem Herumsprechen dieses hohen Entdeckungsrisikos in diesem Raum in „einschlägigen Kreisen“ (siehe ROGGAN 2001, S. 138).

959 SINGELNSTEIN/STOLLE 2012, S. 17 und 118 ff.

960 KAMMERER 2008, S. 95; KRASMANN, S. 241.

961 Vgl. HASSEMER 2000, S. 248 f.; SIMON, S. 280.

Die Ausgrenzung und verachtende Behandlung des „wilden Tiers" stört das ethische Bewusstsein der Bevölkerung weniger stark. Der Delinquent hat diese Behandlung entweder verdient, oder es ist die einzige Möglichkeit, seinem gesellschaftsschädlichen Verhalten beizukommen.[962] Dieses „einfache Denkmuster"[963] harmoniert mit den Menschenbildern der Postmoderne, denn es kann der Gesellschaft die Feinde vorführen, das „Böse" damit fassbar machen und „empirische" Voraussagekriterien für deviantes Verhalten beisteuern.[964] Der Beitrag der Opferzentrierung, das heisst die Erfindung der potenziellen Opfer und die Konzentration auf die Belange dieser fingierten Interessengruppe, in der Form eines treibenden Rechtfertigungsgrunds[965], darf dabei nicht unterschätzt werden.[966] Die Seilschaft des Feindstrafrechts, der neuro-medizinischen Kriminalitätsursachenforschung und der vorgestellten postmodernen Kriminalitätstheorien antwortet nicht nur auf diese Bedürfnisse, sondern unterstützt sie mit Schlagworten und leicht verständlichen, intuitiv einleuchtenden Erklärungskonzepten kriminellen Verhaltens und dementsprechenden Massnahmelösungen zum Vorgehen gegen Kriminalität.[967] Obwohl die Autoren oder Forscher auf den Gebieten ihrer krimi-

---

962 Siehe dazu kritisch YOUNG 1999, S. 112 f. Die m. E. stark zu kritisierende „Rechtfertigung" im Konzept des Feindstrafrechts: Einen tollwütigen Hund schläfert man ohne moralische Bedenken ein, obwohl er am durch die Tollwut bedingten Festbeissen nicht „schuld" ist. Die Determiniertheit des abnormalen menschlichen Verhaltens assoziiert das Vorhandensein des „Bösen" in bestimmten Individuen (vgl. HEINRICH, S. 121). Und das entmenschlichte Böse, der Dämon darf doch menschenverachtend behandelt werden (ja, er muss sogar!). Intensive Eingriffe in seine Grundrechte bzw. der Entzug von Grundrechten rechtfertigen sich über seinen persistierend verdorbenen Charakter.

963 SCHWARZENEGGER, S. 127.

964 Vgl. PRATT ET AL., S. 385; KUNZ 2010a, S. 128 f. Ihnen wohnt demgemäss eine Abnormalität inne. Sie werden in diesem Sinne zu unverbesserlichen Feinden der Gesellschaft.

965 Vgl. JAKOBS 2006, S. 291: Eine Rechtsordnung soll „mehr als nur eine abstrakte, nämlich für potenzielle Opfer nutzbare Orientierung leisten".

966 Es sei daran erinnert, dass sich mehrere medienwirksam und mit viel Pathos vermittelte Einzelfälle als massgebliche Katalysatoren für die Verbreitung und Verschärfung der Sexual Offender Register in den USA (Fall Megan Kanka, Fall Jessica Lunsford etc.) und die Videoüberwachung in Grossbritannien (Fall Jamie Bulger; vgl. GRAS, S. 33 und LINGG, S. 22 f.) erwiesen haben – obgleich weder Register noch Überwachungskameras die Auflösung dieser Fälle vorangetrieben hätten oder auf andere Weise nützlich gewesen wären. Vgl. auch TESCHNER, S. 46 mit weiteren Hinweisen.

967 Vgl. KUNZ 2010a, S. 125 f.; RZEPKA, S. 124 und 127 f. jeweils mit illustrierenden Beispielen zur Medienpräsenz der Hirnforschung; PRATT ET AL., S. 367. Ebenso TATTERSALL, S. 657 f.: „[human beings] appear to prefer simple, all-encompassing explanations of phenomena of whatever kind to the contemplation of the messy, contigent, and often inexplicable facts of human life".

nalätiologischen Theorien[968] meist Vorbehalte zu ihren Ergebnissen anbringen, werden deren Erkenntnisse teils zweckentfremdet, uminterpretiert oder aufgebauscht – zum Beispiel ohne Weiteres als absolute Fakten auf *andere* beziehungsweise *alle* Bereiche der Devianz übertragen.[969] Sicherlich will auch das Gros der Hirnforscher Forschungsergebnisse differenzierter betrachtet wissen und distanziert sich von zu deterministischen Sichtweisen oder absoluten Biokriminologien[970] – öffentliche Plattformen finden indes nicht zurückhaltend interpretierte Besprechungen, sondern plakative, aufregende Manifeste populärer Neurowissenschaftler.[971] Derartige Manifeste werden im Umfeld des postmodernen Bekämpfungsstrafrechts gerne übernommen und können als Rechtfertigung von rigoros eingesetzten technischen Massnahmen benutzt werden.[972]

Aus den Wechselwirkungen zwischen diesen (umstrittenen) Theorien und den konkreten Massnahmen entsteht ein Komplex, welcher scheinbar konsistent ist, der Bevölkerung anschaulich vermittelt und zudem, bei Bedarf, leicht an Emotionen und die gesellschaftliche Stimmung gekoppelt sowie mit Einzelfallbeispielen (zum Beispiel mit Schicksalsgeschichten von Opfern) wirksam dramatisiert vermarktet werden kann.[973] Gleichermassen plakativ sind die von Raumüberwachung und Registrierung generierten Bilder und bildhaften Nachrichten.[974] Das Gefäss „Massenmedium" lässt eine faszinierende Inszenierung (und damit

---

968 Bspw. sehen GOTTFREDSON/HIRSCHI in ihrer Theorie nur eine nachhaltige Erziehung als adäquate Massnahmen zur Festigung der Selbstkontrolle und damit zur Prävention von Kriminalität vor.

969 Siehe RZEPKA, S. 123 f.; KUNZ 2010a, S. 125 f.; MATHIESEN 1980, S. 160 f. Vgl. SCHMIDT-SEMISCH, S. 61.

970 Eine jeweils sehr umfassende Kritik mit vielen aktuellen Hinweisen findet sich bei HASLER und SCHLEIM. Vgl. MCCABE/CASTEL, S. 351; ELGER ET AL., S. 78 f.; KRÖBER, S. 64; ferner SCHWEIZER/BISCHOF, S. 270 f. Selbst MARKOWITSCH/SIEFER, S. 197 f. und ROTH ET AL. 2006, S. 55 sowie 58 relativieren teilweise allzu absolute Deutungen der Ergebnisse der Hirn- oder Genforschung.

971 Vgl. KRÖBER, S. 64; SCHLEIM, S. 48.

972 Siehe zum Ganzen KUNZ 2011, S. 181 ff. Vgl. BOERS, S. 13: Das Bild vom „Kriminellen" intensiviert die Kriminalitätsfurcht, diese wiederum die angesprochene Dynamik. Für ein Bsp. einer Ausgrenzung durch ein öffentliches Verdachtsregister, welches definitiv zu weit ginge, siehe Bericht HRW, S. 52.

973 Vgl. etwa KAMMERER 2008, S. 9 (ein Gemisch aus „Fakt und Fiktion"), 246 und 335.

974 Vgl. KAMMERER 2008, S. 10 und 224. Diese Entkoppelung der Nachricht vom ursprünglichen Kontext und die anschliessende Neukontextualisierung raubt dem Bild seine „Originalität und Authentizität", siehe BIDLO, S. 38. Ähnlich TINNEFELD/BUCHNER/PETRI, S. 50 zu Datenverknüpfungen, welche nach ihrer Ansicht soziale Realitäten verändern können.

gleichzeitig Interpretation) des zunächst meist unspektakulären Materials und die zeitnahe und weite Verbreitung dieser aufgearbeiteten, kontextentfremdeten Impressionen möglich werden.[975] Der Zuschauer erfährt dadurch Kriminalität (vermeintlich) aus erster Hand und quasi interaktiv, indem er beispielsweise Internetregister konsultiert oder verdächtige Vorkommnisse auf im Internet veröffentlichten Überwachungsaufnahmen meldet, was Nervenkitzel verspricht. Die konstruierte Authentizität der Information sorgt derweilen für die Illusion der unmittelbaren Erfahrung von „realer Kriminalität".[976] Von diesem Ausgangspunkt lässt sich dem Verunsicherten fast jede Vorgehensweise gegen Kriminalität, inkohärente Theorie oder unwirksame Massnahme verkaufen, solange diese einen gewissen Bezug zu oder Anteil an der beschriebenen Inszenierung hat.[977]

Die fachliche Rationalisierung der postmodernen Methoden nimmt in diesem Komplex oft nicht mehr als die Aufgabe des schmückenden Beiwerks für eine oberflächliche Proklamation ein, hingegen nicht diejenige einer Checkliste für einen strategisch klugen und tatsächlich lohnenden Einsatz. Den Bürger scheint der bunte Strauss an Zweckbestimmungen nicht argwöhnisch zu stimmen, sondern im Gegenteil zu begeistern. Werden Theorieansätze oder naturwissenschaftliche Ergebnisse indes ohne eingehende Beurteilung, vor allem auch durch die Fachleute der Disziplin, in der die Strategie schliesslich eingesetzt werden soll, in der Praxis verwendet, sind negative Auswirkungen häufig erst zu erkennen, wenn sie eintreten. Punktuell aus alten, vielleicht entlegitimierten Anleitungen herausgerissene Handlungsanweisungen und Protokolle vermögen neue Strategien über einen kommunikativen Nutzen hinaus häufig nicht verbessernd zu ergänzen. Gedanken zum Beispiel der positivistischen oder kritischen Kriminologie, wirken sich innerhalb eines Pluralismus von Zwecksetzungen und Rechtfertigungen selten so aus, wie ursprünglich beabsichtigt.[978] Neue Technologien mit (mehreren) unüberlegten neuen Rationalisierungen zu bestücken, birgt die Gefahr, bestehende Ordnungen mit widersprüchlichen und inkompatiblen Elementen zu schwächen. Das gilt insbesondere für Einflüsse aus Disziplinen, die mit den Konzepten, Prinzipien und Aushandlungsusanzen des Strafrechts und

---

975 Siehe SINGELNSTEIN/STOLLE 2007, S. 108; KAMMERER 2008, S. 305 f.; HILGENDORF, S. 827; BIDLO, S. 45.

976 Vgl. KAMMERER 2011, S. 25 f. mit Hinweisen auf DELEUZE.

977 Vgl. HILGENDORF, S. 827; HASSEMER 2006, S. 139.

978 SCHMIDT-SEMISCH, S. 61. Das soll freilich nicht heissen, dass Gedanken früherer Theorien nicht wertvoll sein können. Sie unsorgfältig in neue Strategien einzuspannen, kann aber sehr problematisch sein.

der Kriminologie weniger vertraut sind. Beispielsweise unterschätzen Protagonisten aus der Biokriminologie die Konsequenzen ihrer ins Strafrechtssystem adaptierten Schlussfolgerungen teilweise massiv. Nicht selten formulieren sie ihre naturwissenschaftlichen Einsichten als „rechtspolitische Folgerung“[979]. Sie verursachen damit nicht etwa einen nachsichtigeren Umgang mit abweichendem Verhalten, sondern befördern unter anderem ausgrenzende Konzepte.[980]

Langfristige oder tiefgreifende Lösungsstrategien präsentieren die genannten Kriminalitätsforschungszweige und -theorien nicht.[981] Das soll nicht heissen, dass die Kriminologie etwa neuen Erkenntnissen aus anderen Wissenschaften nicht grundsätzlich offen gegenübersteht oder stehen sollte. Der interdisziplinäre Austausch ist anzustreben.[982] Sicherlich verdankt die Kriminologie sowohl der Hirnforschung als auch den vorgestellten Kriminalitätstheorien gewisse Errungenschaften und einige interessante Erkenntnisse und Ansätze, welche bestimmte Teilbereiche stimmig erklären oder zumindest die Basis für weitere Forschung bilden können. Von Interesse ist für die vorliegende Arbeit aber vielmehr, dass die neueren Ansätze der Biokriminologien, postmoderne Kriminalitätstheorien und das Feindstrafrecht punkto Kriminalität bestimmte Strategien implizieren, die zu einem Bekämpfungsstrafrecht führen, wenig kompatibel mit dem heutigen Justizsystem sind und (teilweise plakativ) ein sehr spezielles Menschenbild vermitteln.

II. Risikoorientierte Vorgehensweisen

A. Versicherungsmathematische Gerechtigkeit

Hinter dem Kalkulieren mit Rückfallquoten und Tätergruppen steht eine relativ junge Strategie, die FEELEY/SIMON „actuarial justice“ und SCHMIDT-SEMISCH

---

979 LÜDERSSEN, S. 189.

980 BOMMER, S. 31 (bzgl. der kriminologischen Hirnforschung): „Was hier auf samtweichen Pfoten daherkommt, ist in Tat und Wahrheit eine harte Strategie der Exklusion, die handelnde Subjekte zu Gefahrenquellen degradiert, die es zu bekämpfen gilt.“

981 Abgesehen vielleicht vom Vorschlag von GOTTFREDSON/HIRSCHI, das Individuum im Kindesalter zur Selbstkontrolle zu erziehen.

982 Siehe aber unten Vierter Teil, Kapitel II.C.

„versicherungsmathematische Gerechtigkeit" nennen.[983] Diese Strategie antwortet in besonderer Weise auf die postmoderne Erkenntnis, dass Bedrohungen omnipräsent und deshalb nicht (mehr) endgültig und immer zu verhindern sind. Anstatt wenig erfolgversprechend zu versuchen, die jeweilige Gefahr zu bewältigen, sollen zu erwartende Risiken berechnet und reguliert werden.[984] Die Ambition der „actuarial justice" ist die „numerische Erfassung der Welt"[985], das oberste Gebot die Rationalität der „Effizienzlogik"[986] und das zentrale Dogma: „Es gibt kein risikofreies Verhalten, weil es nur riskante Entscheidungen gibt […]."[987] Die Bedeutung von Sicherheit ist bei dieser Betrachtungsweise der gesellschaftlichen Situation eine wesentlich veränderte. Um einzelne klar abgrenzbare Gefahren zu beseitigen, eignen sich einzelne, zielgerichtete Interventionen. Hingegen müssen, wenn jedes Verhalten riskant ist, Massnahmen und Regulierungsprozesse zur (Wieder-)Herstellung von Sicherheit allgegenwärtig sein. Die Risikologik vergrössert die Streuung der Bekämpfungsstrategie sowohl in ihrer Breite (Erfassen immer neuer riskanter Bereiche) als auch Weite (Früherkennung und Vorsorge).[988] Die versicherungsmathematische Gerechtigkeit mit ihrer Risikologik ist dabei *vordergründig* keine moralische Gerechtigkeit. Sie soll nicht werten. Ihre Rationalität sieht das Feld der Kriminalität vielmehr als einen regulierbaren Markt wie jeden anderen.[989] Die Leitidee dieser Strategie, das Risikomanagement, habe „mit dem Traum Lombrosos […] nichts mehr zu tun".[990] Die Strategie zielt darauf ab, Kriminalität zu kontrollieren, indem das Verhalten von Personen beeinflusst und nicht das Individuum selbst geändert wird. Der Defekt ist nicht mehr im Menschen, sondern in Situationen zu verorten.[991] Indes hält diese Leitidee der Praxis nicht stand. Die aktuarische Gerechtigkeit ist keine in

---

983 FEELEY/SIMON, S. 173 ff.; SCHMIDT-SEMISCH, S. 75. Ausführlich zu diesen Rationalitäten und zur „actuarial justice": KRASMANN, S. 71 ff. und 237-253; KUNZ 2011, S. 339 ff.; YOUNG 1999, S. 45 f. und 65 ff.; HARCOURT, S. 16 ff. Siehe auch HARCOURT, S. 1 ff. und 39 ff. zur Entstehungsgeschichte.

984 SCHMIDT-SEMISCH, S. 10, 15 und 45; KRASMANN, S. 242; SINGELNSTEIN/STOLLE 2012, S. 34 ff.

985 SCHMIDT-SEMISCH, S. 15.

986 KRASMANN, S. 249. Ebenso SCHMIDT-SEMISCH, S. 75.

987 SCHMIDT-SEMISCH, S. 13.

988 Vgl. SINGELNSTEIN/STOLLE 2012, S. 34 f.

989 Siehe dazu SCHMIDT-SEMISCH, S. 95.

990 SCHMIDT-SEMISCH, S. 95. Ähnlich KRASMANN, S. 243.

991 SCHMIDT-SEMISCH, S. 95; COHEN, S. 124. Ähnlich ALBRECHT P. A. 2010, S. 5. Vgl. auch SINGELNSTEIN/STOLLE 2012, S. 64 f.

sich geschlossene Theorie und ist nicht an eine bestimmte Theorie gebunden.[992] Sie ist eine Bezeichnung für eine bestimmte Strategie des Umgangs mit Kriminalität oder vielleicht treffender ein „Ordnungskalkül“[993]. Mit diesem Ordnungskalkül werden Risiken lokalisiert und ein allgemein-abstrakter Handlungsimperativ ausgesprochen. Wie das Verhalten gesteuert oder Situationen beeinflusst werden sollen, wird damit aber zunächst offengelassen.

Für die Praxis ist notwendigerweise zu klären, wessen Verhalten denn überhaupt gesteuert werden soll. Einzig absolut situative Ansätze, die ganze Verhaltenscluster für jedermann bezogen auf einen bestimmten Raum verunmöglichen (man denke zum Beispiel an die verschlossene Haustüre), kommen ohne weitere einschätzende, klassifizierende Rationalitäten aus. Mit den versicherungsmathematische Gerechtigkeit verfolgenden postmodernen Strategien soll aber mehr beigetragen werden, als bloss risikobehaftete Orte zu benennen, weshalb durch sie zudem Risikofaktoren eruiert werden. In dieser Hinsicht sind diese Strategien angewiesen auf entsprechende Erklärungsansätze. Das ist der Zeitpunkt, an dem unter anderem die Defizittheorien wieder ins Spiel kommen – Defizite sind (vermeintlich) einleuchtende Risikomerkmale. Faktisch moralisiert die versicherungsmathematische Gerechtigkeit also, auch wenn sie vorderhand als emotionslos präsentiert wird.[994] Der Einzug der versicherungsmathematischen Gerechtigkeit äussert sich im Endeffekt zum einen vor allem als grundsätzliches Misstrauen gegenüber der Besserung von Straffälligen (zukünftig konforme Lebensweise) oder des Wohlverhaltens einer als riskant eingestuften Person oder von Risikogruppen, basierend auf empirischen, eben versicherungsmathematischen Wahrscheinlichkeitsrechnungen, und zum anderen in projektiven Risikokalkülen des Sicherheitsdiskurses. Durch versicherungsmathematische Gerechtigkeit werden objektivierende und proaktive Instrumente gefördert, insbesondere technischer Art, die ermöglichen sollen, Risikogruppen und Risikoszenarien zu kategorisieren und zu managen.[995] Der Drang, den Kriminellen wissenschaftlich zu verstehen, und das Bedürfnis, ihn möglichst früh effizient zu bekämpfen, harmonieren dabei ausgezeichnet.[996] Die aktuarische Gerechtigkeit ist mithin keine in

---

992 Auf die agnostische Vermischung von Ideen im postmodernen Bekämpfungsstrafrecht wurde bereits andernorts hingewiesen, siehe Dritter Teil, Kapitel I.G.

993 NOGALA 1998, S. 314 gebraucht diesen Begriff.

994 Vgl. KRASMANN, S. 108 und 113.

995 LOGAN, S. 595; HARCOURT, S. 2, 31 f. und 174; KRASMANN, S. 241 f.; KUNZ 2011, S. 340 f.; KAMMERER 2008, S. 90; SINGELNSTEIN/STOLLE 2012, S. 66 ff. Vgl. dazu NEDOPIL, S. 287.

996 HARCOURT, S. 174.

sich kohärente Taktik, sondern auch sie verschmilzt Zwecke, Ideen und Ansätze opportun-agnostisch. So basieren postmoderne Kriminalitätsbekämpfungstechnologien einerseits auf Überlegungen der versicherungsmathematischen Gerechtigkeit und des situativen Risikos, agieren indes sowohl „täterabgewandt" als auch „täterzugewandt".[997] Die „actuarial justice" befördert, obschon dies ihrem Grundgedanken vielleicht zuwiderläuft, unter anderem Bilder von „gefährlichen Menschen", an welchen bestimmte Risiken haften. Die personifizierten Risiken gilt es zu meiden oder (möglichst präventiv-proaktiv) zu bekämpfen. Die postmodernen Überwachungs-, Massendatenverarbeitungs- und Registrierungstechnologien sind in dieser Hinsicht passende Vermittler. Sie entsprechen (theoretisch) diesen Vorgaben. Postmoderne Kriminalitätsbekämpfungstechnologien folgen dieser Strategie, „die Moral impliziert und produziert."[998]

B. Der Blick in die Zukunft

Der Nutzen von Identifizierungs- respektive Analysesystemen zur Kriminalitätsbekämpfung hängt wesentlich ab vom Umfang der Datenbanken mit Vergleichsmustern oder anderen Informationen, auf die zugegriffen werden kann. Bereits verdachtsunabhängige Datenbanken mit Einträgen zu einer grossen Anzahl Personen sind in dieser Hinsicht aber problematisch, wie im rechtlichen Teil dargestellt wurde.[999] Im sehr problematischen Extremfall stünden Register mit Vergleichsmustern der Gesamtbevölkerung zum Abgleich (z. B. mit Profilkriterien, Überwachungsaufnahmen etc.) bereit.[1000] Auf der anderen Seite sollten *Verdachtsregister* möglichst übersichtlich gehalten werden, um ihre gewünschte, hilfreiche Wirkung zu entfalten. Der Fokus müsste in erster Linie darauf liegen, möglichst *zuverlässige* Informationen zu archivieren, nicht möglichst viele.[1001]

Eine grosse Anzahl an personenbezogenen Daten ist bereits in zahlreichen staatlichen oder privaten Datenbanken vermerkt, die an sich keinen Bezug zur Kriminalitätsbekämpfung haben. Diese Dossiers stehen grundsätzlich bereit genutzt zu werden, sobald dies erlaubt wird. Teilweise beinhalten diese wenig verwertbare Informationen, teilweise Daten, die erst, wenn sie beispielsweise mit anderen

---

997 SCHMIDT-SEMISCH, S. 62 benutzt diese Begriffe.

998 KRASMANN, S. 249. Vgl. HARCOURT, S. 190 f.

999 Siehe oben Zweiter Teil, Kapitel I.B. und II.A.

1000 Vgl. KUNZ 2006, S. 74. Siehe oben Erster Teil, Kapitel I.G.5. zu verdachtsunabhängig geführten Datenbanken in der Schweiz.

1001 Siehe zum Ganzen MIDDEL, S. 113 und 333.

Daten verknüpft werden, sehr umfassende Rückschlüsse auf die betroffene Person ergeben können.[1002] Speziell für die Ziele der postmodernen Kriminalitätsbekämpfung eingeführte und auf deren Strategien zugeschnittene Datenbanken vermögen oft noch mehr zu leisten, unterstehen aber selbst strengeren Auflagen und der Aufsicht übergeordneter Instanzen. Das macht sie jedoch nicht weniger anfällig, Verhältnismässigkeiten zu verzerren. So ergibt sich aus der dargestellten Datenpool-Abhängigkeit der postmodernen Methoden ein Abwägungsproblem, welches OBERHOLZER anschaulich anhand der (damals noch in Entwicklung befindlichen) schweizerischen DNA-Datenbank erklärt. Er begreife zwar, dass die DNA-Analyse „geradezu phänomenale Erfolge" aufzuweisen vermöge; das ausschliessliche Abstellen auf die Tauglichkeit eines Strafverfolgungsinstruments bei dessen Einführungsprüfung, bereite ihm hingegen nach wie vor Sorgen.[1003] Er spricht hier ein bereits angeschnittenes Problem an: Ist die Anwendung einer Methode je legitimer, desto effizienter sie ist, rechtfertigt die Effizienz einer Methode also automatisch deren Einsatz?[1004] Und auch: Eignen sich anlagebetonte oder andere scheinbar objektive Messmethoden des Devianzpotenzials als unmittelbare Basis für das Taktieren in der Kriminalpolitik?

Ein Ethik-Bericht zum Projekt INDECT stimmt dem zu. Die Sondierung von Verdächtigen und Unverdächtigen über Kriterien bewerten die Verfasser als je zulässiger, desto stärker diese evidenzbasiert seien.[1005] Ähnlich wird teilweise in der biologisch-neurologischen Kriminalitätsforschung argumentiert: Durch kriminologische Hirnforschung soll ein wissenschaftlicher Nährboden für evidenzbasierte Kriterien zur Identifizierung von Kriminellen angelegt werden. Wo das „quasi-intuitive Profiling" und die ursprünglichen biologischen Kriminalitätstheorien noch zu stark auf Klischees und Vorurteile bauten, könne an der Wissenschaftlichkeit neuerer Ansätze, beispielsweise aus der kriminologischen Hirnforschung, kein Zweifel mehr bestehen, konstatieren deren Vertreter.[1006] Verfolgt man die Überlegungen von OBERHOLZER zu DNA-Datenbanken im Sinne von ROTH weiter und glaubt man den Projektberichten, handelt es sich bei den sich in Entwicklung befindlichen vorgestellten neuen Technologien um – sowohl in

---

1002 GILLIOM beschreibt bspw. die umfangreichen Dossiers sozialer Einrichtungen in den Vereinigten Staaten; WEBER-HASSEMER bspw. den für Polizei und Staatsanwaltschaften potenziell begehrenswerten Zugriff auf „Biodatenbanken".

1003 OBERHOLZER 2003, S. 328 f.

1004 Vgl. VAN DER HILST, S. 10; NOWAK, S. 10 f.

1005 SORELL, S. 19.

1006 Siehe dazu KUNZ 2011, S. 71 und 73 f.

präventiver als auch repressiver Hinsicht – höchst effiziente und effektive Methoden der Verbrechensbekämpfung. Konsequent zu Ende gedacht, würden zum Beispiel Biokriminologien in Verbindung mit einem, nach den Massstäben dieser neuen Generation der Technik geschaffenen, kombinierten Verdachtsregister eine fehlerlose, äusserst verlässliche „wissenschaftliche" Kategorisierungsmethode erlauben und damit das Führen eines Registers von (neuro-)medizinisch respektive biologisch Gefährlichen, also von Risikopersonen mit einer Prädisposition zur Delinquenz ermöglichen.[1007] Deren präventive Absonderung von normalen Personen und deren Kontrolle durch normale Personen, mit jeweils persistenten Anlagen zur Konformität, bedeutete – vertraut man diesen Erklärungsansätzen und der Wirksamkeit von Registern – eine Gesellschaft mit einer minimalen Kriminalitätsrate oder zumindest einer extrem effizienten Ermittlungsarbeit in den vom Register erfassten Delinquenzkategorien.

Zu eifrige Präventionsbemühungen und Risikologiken verleiteten sicherlich dazu, immer mehr „Krankheiten" und bereits Veranlagungen (Dispositionen) als Defizite zu erfassen, insofern der Ausbruch ausreichend wahrscheinlich ist.[1008] THOMAS LEMKE berichtet beispielsweise von zivilrechtlichen Fällen, bei denen Personen von Versicherungsgesellschaften abgelehnt wurden, weil sie hypothetisch die genetische Disposition zur Erbkrankheit Chorea-Huntington aufwiesen.[1009] Überträgt man diese vorverurteilende Risikologik, diese Versicherungsmentalität, analog auf die Kriminalitätsbekämpfung, weitet sich das traditionelle Einsatzgebiet zum Unterbinden riskanten Handelns und schliesslich zum Unschädlichhalten von Risikogruppen, Risikopersonen, Risikofaktoren usw., also zu Entitäten, die, versicherungsmathematisch berechnet, beunruhigend wahrscheinlich zu unerwünschten Ergebnissen führen.[1010] Alles kann mit dem Attribut „Risiko-" versehen und damit zum einen in Beziehung zu empirischen Tatsachen und zum anderen zu einer offensichtlichen Dringlichkeit gebracht werden. Die sprachliche Bezeichnung einer komplexen Beurteilung des Risikoobjekts oder -subjekts mit wenigen Worten dramatisiert und zementiert dessen Bedrohlichkeit. Ja, das Risiko wird teilweise sogar erst als solches wahrgenommen, wenn es übersteigert vermittelt wird. Die Zuordnung zum Risiko ist dabei eine extreme Vereinfachung, weil damit jegliche Hintergrundinformation über

---

1007 ROTH 2003b, S. 542 ff. Vgl. OBERHOLZER 2003, S. 300.
1008 LEMKE, S. 9, 27, 40 und 72 f.; SLABY, S. 383.
1009 LEMKE, S. 87 ff. Die Ausbruchswahrscheinlichkeit beträgt bei erkranktem Elternteil 50%.
1010 Vgl. KRASMANN, S. 241 f.

die Entität abhanden kommt. Dieses stark reduzierte Attribut enthält danach lediglich noch rudimentäre Informationen darüber, weshalb etwas riskant ist, aufgrund welcher Kriterien etwas als riskant eingestuft wurde oder wie wahrscheinlich das riskante Ereignis eintreffen wird. Die Wahrnehmung des Risikos verschwimmt.

Für die Glaubhaftigkeit der Zuschreibung von Risikoverhalten und der Benennung von Risikopersonen, mithin für Risikoprognosen als Erkenntnisquelle und Grundlagen für präventiv-polizeiliches Handeln im stark prophylaktischen Stadium, sorgen Wissenschaft und Statistik.[1011] Mit TOLMEIN ist indes festzustellen: „Die Humangenetiker wirken wie einstmals die Hohepriester des Orakels: Sie sagen ein Schicksal weis, enthüllen aber nicht, wie man sich darauf einstellen oder ob man ihm entgehen kann.“[1012] Als gravierend einzuschätzen ist demnach unter anderem, dass mittels derartiger Theorien zwar Werte zur Wahrscheinlichkeit des Ausbruchs einer Disposition geliefert, diese aber ohne die Konsequenzen zu bedenken unkommentiert in den Raum gestellt werden. Sie lassen die Justiz ziemlich ratlos Konstellationen gegenüberstehen, in denen körperliche Devianzdispositionen plötzlich eine grosse Rolle spielen.

Angenommen, die Hirnforschung oder ein Profilanalyse-Programm könnte potenzielle Brandstifter anhand von Hirnauffälligkeiten oder psychologischen Kriterien sehr akkurat identifizieren und gegenüber Nicht-Brandstiftern abgrenzen. Angenommen, das Programm ist in diesem Gedankenspiel in der Lage, einen potenziellen Brandstifter zu 85% zutreffend als solchen zu erkennen. Würde eine derart überzeugende Erkennungsquote und mit ihr die Verhinderung einer Grosszahl von Brandstiftungen es rechtfertigen, jeden Einzelnen in der Bevölkerung auf das Vorhandensein des „Brandstifter-Gens“ oder des „Brandstifter-Profils“ zu überprüfen (mithilfe einer umfassenden Profil- oder DNA-Datenbank und automatisierter Analysesysteme wäre dies an sich nicht besonders aufwendig)? Ab welcher Höhe wäre die Quote eine ausreichende Rechtfertigung?[1013] Ist die isolierte Suche nach dem einen Kriterium und die anschliessende Registrierung der „Positiven“, also von Personen, welche höchstwahrscheinlich eine konkrete Gefahr darstellen (werden), als grosser Eingriff in die Rechte des Einzelnen beziehungsweise des Registrierten zu werten? Immerhin wäre er bei einer tadel-

---

1011 Vgl. BOGARD, S. 59.

1012 TOLMEIN.

1013 ROTH 2003b, S. 543 sieht das „Dilemma“ bereits bei einer Wahrscheinlichkeit von 63%. Vgl. zu dieser Abwägung NEDOPIL, S. 363.

losen Überführungsquote (ohne Falsch-Positive, ohne Zweifel an der Richtigkeit der Diagnose) „zu Recht" eingetragen.[1014] Daraus ergäben sich weitere Fragen, zum Beispiel, ob sich (präventiv) sichernde Massnahmen bereits aufgrund einer Disposition, die mit hoher Wahrscheinlichkeit ausbrechen wird, rechtfertigen oder ob das Defizit im Beurteilungszeitpunkt vorliegen und wie sicher der Beleg eines Defizits oder der entsprechenden Anfälligkeit sein muss.

Es ginge wohl zu weit, darin die Anfänge einer „Genetokratie"[1015] zu vermuten – das Potenzial für eine kleine „genetische Inquisition", für eine „Polizei der Gene"[1016], ausgeführt durch die dargestellten Kriminalitätsbekämpfungsechnologien in Verbindung mit postmodernen Sicherheits- und Risikologiken, bestünde aber durchaus. Diese Strategien müssen freilich nicht an Gene geknüpft sein. Horst Herold, ehemaliger Präsident des deutschen Bundeskriminalamts, begeisterte sich bereits in den 1980er Jahren für die Idee, „die Polizei als gesellschaftliches Diagnoseinstrument" auszustatten und einzusetzen, durch Technologie und Wissenschaft ein „Gemälde der Gesellschaft" zu zeichnen und darauf beruhend eine (präventive) „Therapie" zu erdenken. Die wissenschaftlich-empirische, technisierte Polizei mache dabei den „Richter entbehrlich".[1017] Die derart verstandene empirisch-moralische Polizei legt Werturteile mittels eines objektiven Krankheitsbegriffs fest. Sie richtet selbst, quasi als Vollstrecker der empirischen Evidenz, der wissenschaftlichen Wahrheit.[1018] Die gekoppelten postmodernen Kriminalitätsbekämpfungstechnologien eröffnen in dieser Weise durchaus die Möglichkeit einer wissenschaftlich-empirischen, polizeilichen Inquisition. Auch heute steht diese Strategie durchaus noch (oder wieder) im Raum und büsste ihren Reiz, trotz vieler schlechter Konnotationen, scheinbar keineswegs ein.[1019]

1014 Vgl. HASSEMER 2000, S. 266.

1015 Jeremy Rifkin zitiert bei LEMKE, S. 15.

1016 Georges Canguilhem zitiert bei LEMKE, S. 14.

1017 Herold im Interview bei COBLER, S. 30 und 36. Zu demselben Schluss kommend, aber kritisch bewertend KRÖBER, S. 77. Vgl. GEHRING, S. 67 und ausführlich zu den damaligen Gedankengängen Herolds: NOGALA 1989, S. 15-25. Ferner GRAU, S. 167 ff., der darlegt, bildgebende Verfahren der Hirnforschung lieferten lediglich *Kunstwerke*.

1018 Vgl. LEMKE, S. 35 f.

1019 Vgl. KRASMANN, S. 252. Siehe bspw. das Manifest einiger Hirnforscher bei ELGER ET AL., S. 83 oder Hans Markowitsch im Spiegel-Interview vom 30. Juli 2007 bei LAKOTTA, S. 122, der meint, die Arbeit der Richter könnten auch Gutachter übernehmen. Siehe auch HASLER, S. 158 f. (Hirnscans von „Hoodies").

Das Ausgeführte gilt jedoch nur unter zahlreichen Vorbehalten. Derartig fehlerlose Analysesysteme und -methoden, wie sie Technologien einer funktionierenden empirischen Polizei erforderten, sind kaum je zu erwarten.[1020] Sie erlauben zwar durchaus Blicke in die Zukunft, aber lediglich in der Form von vagen Wahrscheinlichkeitsaussagen.[1021] Es ist dahingehend Acht zu geben, sich auch von vermeintlich hohen Trefferquoten nicht verführen zu lassen. Sie verleiten oft zu einem Trugschluss. Sie erwecken den Anschein, diese Technologien könnten eine beinahe zweifelsfreie Identifizierung anbieten, was deren Propagierung als sehr zuverlässige Instrumente erleichtert. Dadurch vertraut die Gesellschaft in das ordentliche und unproblematische Funktionieren dieser Systeme (also auf ein Zerrbild), was sie freilich dazu veranlasst, diese zu unterstützen.[1022] Es ist aber zu beachten, dass bereits eine sehr hohe Wahrscheinlichkeit und Voraussagequalität von über 99% noch nicht „fehlerlos" bedeutet. Bei grossen Populationen ist die Quantität der Falschmeldungen auch in diesem Fall noch unbefriedigend hoch.[1023] Zum Beispiel ergab das bereits erwähnte Forschungsprojekt Fotofahndung des BKA bezüglich der biometrischen Identifikation von Personen eine Falschakzeptanz-/Verwechslungsrate von 0.1%. Dieser zunächst gut klingende Wert führte jedoch zu 23 „Falscheinsätzen" pro Tag am Hauptbahnhof Mainz.[1024] Diese Anzahl an überflüssigen Interventionen wäre in der Praxis zum einen kaum zu bewältigen ohne die entsprechenden personellen Ressourcen, die zudem ständig einsatzbereit sein müssten. Zum anderen dürften 23 ungerechtfertigte Interventionen pro Tag gegen fälschlicherweise identifizierte Personen vom Publikum negativ aufgenommen werden: Unschuldige werden zu Unrecht behelligt, Kriminalitätsfürchtige zusätzlich verunsichert sein, weil sie den Hauptbahn-

---

1020 GMÜR, S. 1315 meint z. B. der heutige Stand der Forschung in der psychiatrischen Rückfallprognosestellung bei Gewalt sei von einer Treffsicherheit über 50-60% weit entfernt.

1021 RÖSLER, S. 85 f.; KRÖBER, S. 63. Zutreffende Prognosen seltener Ereignisse sind zudem wesentlich schwerer zu stellen, siehe HARCOURT, S. 231. Mittels proaktiver Polizeitätigkeit und spezieller postmoderner Kriminalitätsbekämpfungstechnologien sollen aber doch genau diese seltenen Ereignisse (schwere Delikte, Grossbedrohungen) verhindert werden.

1022 Ein Paradebeispiel dafür sind die öffentlichen Verdachtsregister. Vgl. EBNER ET AL., S. 71 f. zur Fehlerquote bei unseriöser Prognoseerstellung lediglich aufgrund von Persönlichkeitsmerkmalen.

1023 Siehe SKILLICORN 2008b, S. 69; TONDORF, S. 41; SCHNEIER in Blog vom 9. März 2006. Vgl. auch MARX 2007 (Fallacy 3).

1024 Siehe Bericht BKA Fotofahndung. Für ein sehr ähnliches Beispiel aus der Hirnforschung, bei dem mittels eines lernenden Computeralgorithmus und fMRT schizophrene von gesunden Personen unterschieden werden sollten, das angewendet auf grössere Populationen sehr unzuverlässige Resultate liefert, siehe HASLER, S. 204 f.

hof als gefährlich wahrnehmen, da an diesem Ort offenbar ständig Interventionen nötig sind. Der angesprochene „Paradigmenwechsel" in der Verbrechensbekämpfung[1025] kann zudem bewirken, dass auch relativ hohe Fehlermengen noch akzeptiert werden, also bereits tiefere, noch einigermassen gut aussehende und verkäufliche Quoten den Einsatz der angesprochenen Systeme zu rechtfertigen vermögen. Das ist nicht nur hinsichtlich der entstehenden Grundrechtseingriffe besonders zu vermerken, sondern in aller Regel kontraproduktiv, Straftaten zu verhindern und zu verfolgen. Die Falschpositiven-Rate muss dem tatsächlich zu erwartenden Nutzen gegenübergestellt werden, nicht einfach der Erkennungsrate. Beispielsweise muss hinsichtlich des Berichts BKA Fotofahndung auch relevant sein, wie viele Gesuchte denn pro Tag und Jahr an den Kameras überhaupt vorbeilaufen, wie viele davon erkannt werden und wie viele aufgrund der Identifikation durch die Kameras rechtzeitig gefasst werden können.[1026]

III. Verdächtige Klischees

A. Hindernisse der Praktikabilität

In der Strafrechtskonzeption JAKOBS werden mögliche Adressaten in drei Gruppen unterschieden: Die Feinde, die straffälligen Bürger und die nicht straffälligen Bürger. Das Feindstrafrecht ist gekennzeichnet durch hartes Vorgehen und eine früh ansetzende Gefahrenabwehr. Es soll deshalb theoretisch nur die Feinde belangen. Die Unzulänglichkeit dieses Modells zeigt sich in der Praxis: Das Feindstrafrecht in seiner praktischen Anwendung muss teilweise auch straffällige und gar nicht straffällige Bürger betreffen, damit sichergestellt ist, dass tatsächlich alle Feinde erfasst werden. Deshalb wird sicherheitshalber eine gewisse Streubreite in Kauf genommen, um die verschwindend kleine Zahl wirklicher Feinde möglichst lückenlos zu erkennen.[1027] Feind- und Bürgerstrafrecht vermischen sich wieder. Einen sinnvollen Ansatz für die Gefahrenabwehr oder Strafverfolgung liefert die Unterscheidung von JAKOBS zwischen den Adressaten Bürger und Feind somit nicht. Eine taugliche Grenze kann nicht gezogen werden, wes-

---

1025 Siehe oben Dritter Teil, Kapitel I.C.

1026 Gemäss Bericht BKA Fotofahndung, sind Personen nach Ablauf einer Minute nach der Identifikation per Kamera nurmehr schwer oder unmöglich aufzufinden. Siehe dazu auch HORNUNG/DESOI, S. 153 mit weiteren Hinweisen.

1027 Gl. M. wie NEUMANN, S. 307.

wegen das darauf beruhende Bekämpfungsstrafrecht die eigentlichen Adressaten öfters verfehlt.

Das Modell JAKOBS gründet auf der Annahme, die „Rechtlichkeit" einer Gesellschaft setze Gegenseitigkeit voraus. Nur wer seine gesellschaftlichen Pflichten achtet, kommt auch in den Genuss aller gesellschaftlichen Rechte. Das Verhalten des Gegenübers bestimmt das Verhalten *ihm* gegenüber.[1028] Im Endeffekt bestraft die Gesellschaft jedoch den Abweichler, nicht ein davon isoliertes Gebilde. Das Strafrecht im weiteren Sinn ist ein helfendes Konstrukt, das zum Zweck der Intervention bei ungewolltem Verhalten einer Person stellvertretend für die Gesellschaft einschreitet. So weist der Anspruch der Gegenseitigkeit, angewendet auf die Praxis der Massnahmen des Bekämpfungsstrafrechts, eine weitere Lücke auf. Die favorisierte Waffe des Feindstrafrechts ist die frühansetzende Gefahrenabwehr. Indes verpflichtet das Konstrukt der Gegenseitigkeit die Gefahrenabwehr zu einer äusserst präzisen Erfassung ausschliesslich „wahrer" Feinde. Dies vermag sie aber gerade nicht zu leisten.[1029] *Konsequent* in die praktische Wirklichkeit integriert, würde das Dogma der Gegenseitigkeit den Handlungsspielraum der Gefahrenabwehr auf ein Minimum einengen. Es würde voraussetzen, dass die Gefährlichkeit von Individuen zuverlässig ermittelt werden kann. Die Gefahrenprävention würde somit als Massnahme gegenstandslos, insoweit sie sich nicht auf eine perfekte Analyse und Erkennung von Gefahren abstützen kann (Methoden, die über einen Generalverdacht verwirklicht werden, fielen ohnehin aus dem von JAKOBS vorgegebenen Rahmen der Gegenseitigkeit). Um eine Gefahr abzuwehren, müsste sie erst identifiziert werden. Zur Identifikation der Gefahr dürfen aber keine feindstrafrechtlichen Mittel zur Anwendung gelangen, weil sie eben noch nicht (eindeutig) identifiziert ist. Wo feindstrafrechtliche Massnahmen *trotz* lediglich vager Verdächtigungen oder alternativ bereits bei an sich unerheblichen Abweichungen praktiziert werden, wird Gegenseitigkeit einseitig unterstellt. Zu Recht merken ARNOLD und HEINRICH deshalb an, das Feindstrafrecht verkomme im Extremfall zu einem ausgeprägten Willens- beziehungsweise Gesinnungsstrafrecht, welches nicht die Taten eines Individuums beurteile, sondern seine Absichten in den Vordergrund stelle. Dasselbe hat analog für die Modelle der in dieser Arbeit erwähnten Kriminalitätstheorien und

---

1028 JAKOBS 2006, S. 289 f.

1029 Diesen Punkt verkennt JAKOBS 2006, S. 294, insbesondere, wenn er feststellt, das Feindstrafrecht sei im „klug verwalteten Rechtsstaat" lediglich als ultima ratio zu gebrauchen. Vgl. NEUMANN, S. 304; KUNZ 2006, S. 77.

jede in die Zukunft gerichtete technische Massnahme, die eine Beurteilungs- respektive Prognosefehlerlosigkeit nicht garantieren kann, zu gelten.[1030] Das Ansetzen bereits bei den (gefährlichen) Absichten zur Bestimmung des Feindes ist aber schwerlich mit der Annahme der Gegenseitigkeit vereinbar. Nur wenn JAKOBS sich mit der „lombrosianisch" angehauchten Behauptung einiger der anlagebetonten Defizittheorien, sie könnten das Abnormale im kriminellen Menschen (dem Feind) einwandfrei identifizieren und voraussagen, einverstanden geben würde, verbliebe überhaupt noch ein plausibel vertretbarer Anwendungsbereich für das Feindstrafrecht.

Ein weiteres Problem der Gegenseitigkeit: Für die mutmassliche, aber tatsächlich „unschuldige", Risikoperson sollen alle Pflichten gelten, gleichzeitig werden ihr aber alle Rechte abgesprochen. In diesem Fall hat die Idee der Gegenseitigkeit wohl eine Art aufgezwungene Entsozialisierung von eigentlich konformwilligen Individuen oder Personengruppen zur Folge.[1031] An der Komponente der „Gegenseitigkeit" festzuhalten, wenn jene theoretische Fiktion sich im faktischen Gebrauch (teilweise) als sehr *einseitig* geprägt herausstellt, ist sehr zynisch.

Die grösste Schwierigkeit, abweichendes Verhalten und Bedrohungen zu erkennen, dürfte sich für die automatisierten Raumüberwachungssysteme demnach aus den immer höher angesetzten Präventions- und Sicherheitsansprüchen der Gesellschaft ergeben. Je weniger sich das inkriminierte vom „normalen" Verhalten unterscheidet und je früher sich die Gesellschaft von einer Handlung bedroht fühlt, desto differenziertere Kriterien müssen dem automatisierten System vorgegeben werden. Eine niedrige Schwelle bei der Definition von Gefahr verlangt dem Voraussagen von Geschehnissen eine Menge ab. Die Forderung der Erkennung kleinster Unterschiede im Verhalten von Personen ist für eine noch so ausgefeilte Technik schier unerfüllbar. Fehlalarme oder Falsch-Positiv-Meldungen dürften bei Kleinstdelikten die Regel sein.[1032] Jene führen dazu, dass diese Vorgehensweise ineffizient wird. Zum einen muss diesfalls der menschliche Kontrolleur zu oft eingreifen, zum anderen werden die Voraussagen unverläss-

---

1030 ARNOLD 2006a, S. 308; HEINRICH, S. 96. Vgl. STEGMANN A., S. 102 f. Zur Analogie bspw. ROTH 2003b, S. 531 ff. Sehr ähnlich ROTH 2003b, S. 512: „Keinen Willen zu haben oder «willensschwach» zu sein, ist ein Zustand, der bei Mitmenschen leicht zu erkennen ist."

1031 Vgl. zum Ganzen NEUMANN, S. 312 f.

1032 Siehe MOECHEL in futurezone vom 16. November 2009 und GMÜR, S. 1307 und 1317.

lich.[1033] Zwar ist eine Verringerung der Falsch-Positiven über ihr Ausbalancieren mit den Falsch-Negativen grundsätzlich möglich. Das Modell zu überdenken oder einen neuen Ansatz zu verfolgen, sei aber meistens sinnvoller, als diesen Trade-off vorzunehmen, meint etwa SKILLICORN.[1034] Das (automatisierte) Melden von Falsch-Positiven durch intelligente Programme und Systeme ist insbesondere dann bedenklich, wenn die Bedrohungsmeldungen als unfehlbar angesehen werden. Sie klagen in diesem Fall Unschuldige für eine Verfehlung an, welche diese zu begehen nicht vorhatten, und liefern zur Untermauerung der (falsch interpretierten) Verhaltensweise zugleich vermeintlich auf objektiven Kriterien basierende Beweise. Dies verschlechtert die Position des bezichtigten Unschuldigen vor und im Ermittlungsverfahren oder dem Strafprozess, vor allem, wenn jener einer ohnehin grundsätzlich verdächtigen Personengruppe angehört (beispielsweise als gewaltbereiter Störer registriert ist). Darauf kann eine sich zunehmend schneller drehende Spirale folgen: Durch das fälschlicherweise als verdächtig angezeigte Benehmen oder ein verdächtiges Umfeld wird eine Person als Abweichler gekennzeichnet. Diese Kennzeichnung veranlasst zur Aufnahme in das entsprechende Register. Der Registereintrag wiederum sorgt für eine zusätzliche Portion an Misstrauen gegenüber dieser Person, weswegen diese umso genauer beobachtet wird und andere Personen in ihrem Umfeld in den Kreis der „Verdächtigen" hineingezogen werden.[1035]

B. Entpersonifizierende Register und Subjektivierungsapparate

THOMAS MATHIESEN sah 1979 erste Anzeichen für eine veränderte Betrachtungsweise in Bezug auf Kriminalität in Europa. Das traditionelle Strafrecht habe die Rechtsbrecher als Individuen behandelt und „one by one" diszipliniert. Der

---

1033 In der Folge kann nicht nur der Mensch das Vertrauen in derartige Prädiktoren verlieren, sondern auch das System selbst. Es könnte in diesem Fall künftig die Anwendung dieser Prädiktoren selbstständig verweigern. Siehe SKILLICORN 2008b, S. 78 f.

1034 SKILLICORN 2008b, S. 79. Zumindest müssen diese Trade-offs aber erkannt und diskutiert werden, damit man sich auf eine vertretbare Variante einigen kann, siehe INTRONA/NISSENBAUM, S. 4.

1035 Bspw. meldet ein Stadionbesitzer (fälschlicherweise) einen nur abstrakt Verdächtigen. Dieser wird in das Register aufgenommen. Der Eintrag generiert einen verstärkten Vorverdacht bei zukünftigen Sportevents, weshalb an diesen auch sein soziales Umfeld bzw. seine Bekanntschaften und Kontakte genauer unter die Lupe genommen, beruhend auf dieser Verbindung von einem Stadionbesitzer gemeldet und in das Register aufgenommen werden. Vgl. die Ausführungen oben im Zweiten Teil, Kapitel I.F.

kriminelle Akt sei als zwar nicht akzeptierte, aber nachvollziehbare Reaktion auf das Umfeld verstanden worden. Demgegenüber manipulierten die neuen Kontrollstrategien die alltäglichen Lebensbedingungen von ganzen Gruppen und Kategorien.[1036] Die Genese der Entindividualisierung des Delinquenten beruht auf dieser von MATHIESEN dargestellten Ausgangslage: Die postmoderne Gesellschaft hält die Taten des Rechtsbrechers für unverständlich. Möglicherweise aus Enttäuschung der anscheinend misslungenen Kriminalitätsbekämpfung in der zweiten Hälfte des 20. Jahrhunderts oder vielleicht wegen der aufreibenden, beängstigenden Bilder der Abgründe menschlichen Handelns in den in dieser Zeit aufgekommenen Massenmedien. Die weiter oben besprochene Terminologie des Bekämpfungsstrafrechts veranschaulicht den Verlust des Einfühlungsvermögens in oder auch des Mitgefühls für den Rechtsbrecher sehr deutlich.

Die zur Kommunikation gedrängte Kriminalpolitik nimmt zur Kenntnis, dass die Öffentlichkeit naturwissenschaftliche, also (vermeintlich) zwingend evidenzgestützte, Erklärungsversuche der Kriminalität am besten aufnimmt.[1037] Wohl mitunter deshalb, weil diese „kalt" kalkulierenden Theorien einen Abstand zwischen konformem Bürger und „dem Kriminellen" schaffen und das schlechte Gewissen beruhigen. Die Auseinandersetzung mit ungelösten sozialen Problemen wird dadurch ausgeklammert.[1038]

Der Einsatz der untersuchten Kriminalitätsbekämpfungsmassnahmen ist eine Möglichkeit, wie Bekämpfungsstrafrecht im Strafrechtsalltag praktiziert werden kann. Das Modell der Verdachtsregister verlangt vom Rechtssystem dieselben strukturellen Änderungen wie das Feindstrafrecht. So fusst die Idee des Verdachtsregisters auf einem täterzentrierten Verständnis des Strafrechts. Verdachtsregister identifizieren und kennzeichnen Risikopersonen und geben sie damit zur intensivierten behördlichen oder öffentlichen Überwachung und Kontrolle frei. Sie bezwecken unter anderem, Gefahrenquellen dadurch zu beseitigen, dass ihre Nutzer Kenntnis von diesen Quellen drohenden Übels erlangen. Ausser Acht gelassen – oder ignoriert – wird dabei, dass die Register nicht nur Risikoperso-

---

1036 MATHIESEN 1980, S. 152 und 157. Ähnlich HARCOURT, S. 180.

1037 Vgl. HARCOURT, S. 3 und 174.

1038 Stattdessen zeigen sie Bilder über Risikopersonen (siehe unten Dritter Teil, Kapitel V.E.) und appellieren an die Selbstverantwortung und Selbstvorsorge der Bürger (siehe unten Dritter Teil, Kapitel IV.A).

nen auflisten, sondern zuweilen Risikopersonen *konstruieren*.[1039] Ob eine Person zu Recht als Risiko gilt, wird beim Eintrag in das Register nicht geprüft. Listet es mutmassliche, aber nicht tatsächliche Gefährder, festigt es ihren Risikostatus zu Unrecht. Hierin offenbart sich ein zusätzliches Problem von Teilungspraktiken: Wie wird entschieden, wer deviant, wer Feind ist? Das wiederholte oder gar notorische widerrechtliche Handeln einer Person ist allerhöchstens oberflächlich betrachtet ein hilfreiches und bezeichnendes Kriterium bei der Sondierung von Straftätern auf ihre Zugehörigkeit zu einer Risikogruppe. Postmoderne Technologien und insbesondere Verdachtsregister tendieren mithin dazu, der Gesellschaft Risikopersonen zu präsentieren, die vielleicht keine sind. Da die heute zur Verfügung stehenden Methoden, Instrumente und Kriterien zur Prognose zukünftiger Straffälligkeit wenig verlässlich sind, funktionieren auch Verdachtsregister nicht immer intentionsgemäss.[1040] Wesentlich bequemer und kosteneffizienter als etwa umfangreiche psychologische Abklärungen einer Person ist zudem die Klassifizerung von Risiken, indem beispielsweise Tätergruppen mit allgemein, folglich unspezifisch schlechter Rückfallprognose *Risikokategorien* zugeordnet werden. Die Zugehörigkeit zu einer bestimmten Tätergruppe führt in diesem Fall automatisch zum Risikoverdacht oder zur direkten Zuordnung in die Risikoklasse. Unvermeidbare Konsequenz eines derartigen Zuordnungssystems sind die dargestellten, teils gravierenden Schwachstellen der Verdachtsregister.[1041]

Das als gefährlich eingestufte Subjekt wird in diesen Registern entpersonifiziert. Die Person, von der eine bestimmte Gefahr ausgeht, wird zu einer Gefahr oder

---

1039 Das führt zudem zu einem „Sonderstrafrecht" für diese markierten Täter(-gruppen), siehe HEINRICH, S. 118. Vgl. KUNZ 2011, S. 75; ZERBES, S. 314.

1040 Siehe dazu die Ausführungen im Ersten Teil. Rückfallprognosen bestehen bspw. immer aus ungewissen Komponenten, und die Ergebnisse ihrer Interpretation hängen auch vom Verhältnis ab, in dem sie beurteilt werden, siehe NEDOPIL, S. 362 ff.

1041 Zwar zeichnen sich manche Tätergruppen tatsächlich durch höhere Rückfallquoten aus. Diese sind aber unter anderem bei Weitem nicht hoch genug, um ganze Tätergruppen über einen Kamm zu scheren und zu Risikopersonen zu erklären. Ein nach heutigen Erkenntnissen geführtes Sexualstraftäterregister läuft aber genau darauf hinaus, wie bereits im Ersten Teil dargestellt wurde. Vgl. zu den Rückfallraten: Bericht HRW, S. 25 ff. und 31 f.; GODERBAUER, S. 118; KUNZ 2011, S. 298 ff. Zu beachten ist dabei die Feststellung von NEDOPIL, S. 290, dass, je niedriger die Basisrückfallrate sei, desto höher die Zahl der Falsch-Positiven werde. Bei sehr tiefen oder überschätzten Basisrückfallraten führen statistische Gefährlichkeitsprognosen deshalb zu unbefriedigenden Ergebnissen. Irrtümer in der Gefährlichkeitsprognose sind somit systemimmanent häufig.

Bedrohung *an sich* reduziert. Personen werden objektiviert.[1042] Sie werden mit Etiketten versehen (zum Beispiel „Terrorist", „Hooligan" oder „Sexualstraftäter"). Es scheint den Bedürfnissen des postmodernen Durchschnittsbürgers zu entsprechen, Bedrohungen und gefährliche Subjekte möglichst durch (leicht erkennbare) Merkmale zu identifizieren und dadurch zu meiden oder paralysieren zu können.[1043] Gleichzeitig dienen Verdachtsregister, Erkenntnisse aus den Biokriminologien und die von den Technologien produzierten Bilder als Subjektivierungsapparate. „Teilungspraktiken" im Sinne FOUCAULTS erstellen Ordnungsmuster.[1044] Der konforme Teil der Gesellschaft bestätigt sich über die Abgrenzung zum Kriminellen, zum Risikoträger.[1045] Indem dem Bürger nahegelegt wird, sich möglichst von charakterlichen, biologischen oder anerzogenen Defiziten Krimineller zu distanzieren, wird er in Kontrollstrategien eingebunden.[1046] Der Bürger fühlt sich nicht betroffen und sieht seine Freiheiten durch schärfere Überwachungsmassnahmen nicht bedroht, da diese in Verbindung mit besonders dramatisierten Täter- und Risikokategorien gebracht werden.[1047]

IV. Regulierende Kontrolle

A. Selbstregulierung und Wiedergeburt der bürgerlichen Selbsthilfe

Responsabilisierende Strategien machen ein wesentliches Element postmoderner Sozialkontrolle aus.[1048] Es sind verschiedene „Aktivierungs- und Selbstführungsprozesse des Bürgers" auszumachen.[1049] Die Besinnung auf das Selbst in

---

1042 FOUCAULT 1994a, S. 243; NEUMANN, S. 308; KUNZ 2006, S. 77. Vgl. auch ZERBES, S. 8.

1043 Vgl. SLABY, S. 383.

1044 FOUCAULT 1994a, S. 243 und 249; BUBLITZ, S. 145. Ausführlich KRASMANN, S. 141 ff.

1045 KUNZ 2010a, S. 125 f.; DERS. 2011, S. 332 und 358 f.; SINGELNSTEIN/STOLLE 2007, S. 107, 109 und 114; LEGNARO 2010, S. 63.

1046 KRASMANN, S. 143; BUBLITZ, S. 133 und 145; SLABY, S. 383 f.

1047 Vgl. ZERBES, S. 314; KREISSL/STEINERT, S. 967.

1048 Den Begriff „Responsabilisierung" verwenden in diesem Zusammenhang etwa SCHMIDT-SEMISCH, S. 97; KRASMANN, S. 183; SINGELNSTEIN/STOLLE 2012, S. 76; KAMMERER 2008, S. 94. Vgl. auch HAGGERTY/ERICSON, S. 262.

1049 BIDLO, S. 40 f. Diese Selbstaktivierungstendenzen sind in Westeuropa sicherlich noch nicht so ausgeprägt wie in Grossbritannien und den USA, noch scheinen die Bürger in Westeuropa das Vorgehen gegen Kriminalität mehrheitlich als Aufgabe des Staats zu erachten, siehe NOGALA 1998, S. 273; SCHLEPPER/PETER/LÜDEMANN. DIES., S. 95 halten wohl zutreffend fest, dass Bürger aktivierende Strategien noch oftmals auf der „programmatischen Ebene

der postmodernen Gesellschaft äussert sich zunächst darin, dass fehlende Selbstkontrolle in irgendeiner Form jeder postmodernen Kriminalitätstheorie, und ebenso dem Feindstrafrecht, als eine Ursache von Kriminalität hinterlegt ist. Mit postmodernen Technologien werden Bürger in die Kriminalitätsbekämpfung miteingebunden. Anknüpfend an den Gedanken des Risikomanagements und der Sicherheitsrationalitäten soll der Staatsbürger selbst fähig sein, Risiken zu kalkulieren, sie zu minimieren, ihnen zu entgehen oder sie abzuwenden und sich und die Gesellschaft dadurch vor Übel zu schützen: „Die Vorsorge wird zur liberalen Tugend schlechthin und das Übel zu einer Art Lektion, das die Konsequenz mangelnder Vorsorge demonstriert."[1050] Das eintretende Delikt ist gleichermassen Versagen des Täters, der sich nicht unter Kontrolle hat, wie auch des Opfers, das dem drohenden Risiko nicht ausreichend Bedeutung zugemessen und nicht mit entsprechenden Massnahmen vorgesorgt hat. Der Bürger hat Eigenverantwortlichkeit zu gewährleisten und ergänzend zur staatlichen Grundversorgung das erwartete, alltägliche Mass an sicherheits- und risikobezogener Eigenleistung zu erbringen.[1051] Bürger sollen sich nicht nur konform verhalten, sondern anderen Personen gut sichtbar zeigen, dass sie sich konform verhalten. Personen müssen, im Sinne einer Risikoeinschätzung, ein Urteil über die Bedrohlichkeit anderer Personen fällen können. Straffällig gewordene Personen haben speziell dafür Sorge zu tragen, ihren aktuellen Status zu melden und ihr Handeln offenzulegen.[1052] Folge der dargestellten Entwicklungen ist ein Rückschritt im Verständnis der Aufgabe des Staats hinsichtlich des Vorgehens gegen Kriminalität – ein Rückschritt deshalb, weil die Zuweisung des Strafmonopols an den Staat eigent-

der politischen Akteure stecken" bleiben würden. Hinsichtlich postmoderner Kriminalitätsbekämpfungstechnologien scheinen sich hingegen auch in der Schweiz Trends in diese Richtigung abzuzeichnen, die bereits an mehreren Stellen der vorliegenden Arbeit angesprochen wurden, etwa bezüglich der Selbstregulierung im virtuellen Raum, der Meldung von Personen zur Aufnahme in Verdachtsregister oder der Videoüberwachung.

1050 SCHMIDT-SEMISCH, S. 20. Siehe auch KAMMERER 2008, S. 241; KRASMANN, S. 64.

1051 SCHMIDT-SEMISCH, S. 64; SCHLEPPER/PETER/LÜDEMANN, S. 83; GATES, S. 71; KUNZ 2011, S. 353; DERS. 2010b, S. 20 f.; DERS. 2002, S. 733; LEMKE, S. 20 und 131 f.; SINGELNSTEIN/STOLLE 2012, S. 78 f.

1052 Sehr anschaulich dafür Sachsens Innenminister Albrecht Buttolo im Jahr 2007 gegenüber Spiegel Online: „Der Bürger sollte die Chance bekommen, Gefahren zu erkennen und diese auch durch Eigenverhalten zu minimieren.", siehe MEIRITZ in Spiegel Online vom 7. März 2007. Sehr ähnlich Tony Blair zitiert bei HESSDÖRFER/BACHMANN, S. 170: „To all should be given opportunity; from all responsability demanded." und die „Readiness Campaign" in den USA, siehe dazu ANDREJEVIC, S. 161 ff. oder bspw. <www.ready.gov> und <www.citizencorps.gov>.

lich gerade die Selbsthilfe bzw. die Selbstjustiz zu verhindern gedachte.[1053] Der Staat kann die umfassende Versorgung mit Sicherheit unter den Voraussetzungen der postmodernen Risikologik zwar versprechen, aber nicht oder zumindest nicht überall in gleichem Mass wahrnehmen. Ergänzend oder substituierend werden mit der Erwartung auf Selbstverantwortlichkeit Aufgaben an den Bürger zurückdelegiert.[1054]

Der vorbildliche Bürger hat sich erstens über Risikozonen zu informieren. Der postmoderne Staat leistet in den unüberwachten Gebieten nur die Grundversorgung an Gefahrenabwehr. Er hat schliesslich eigens dafür gesorgt, dass bestimmte Bereiche sicher sind, also soll man sich tunlichst auch in diesen bewegen. Durch diese Auffassung staatlicher Gefahrenabwehr wird nicht nur der Straftäter, sondern auch der Bürger wesentlich in seiner Bewegungsfreiheit beschnitten. Beiden ist vorgeschrieben, in welchen Kreisen sie sich zu bewegen haben.[1055] Ähnliches gilt für das Konzept der öffentlichen Verdachtsregister: Für den Einzelnen bedeuten sie nicht nur ein Stückchen mehr (scheinbare) Sicherheit[1056], sondern insbesondere eine Verpflichtung zu grösserer Aufmerksamkeit.[1057] Die Kontrolle der Eingetragenen obliegt seit der breiten Verfügbarkeit der Register über das Internet dem einzelnen Bürger beziehungsweise der Bevölkerung als solcher und nicht mehr nur der früher mit dem Vorgehen gegen Kriminalität betrauten Dienststelle oder Behörde. Die Logik hinter dieser Abwälzung der Kontrolle von Risken ergibt sich aus der Überlegung, dass, wenn schon ein umfassend öffentliches Register bereitgestellt werde, dann jeder dieses zu konsultieren und dementsprechende Eigenvorsorge zu treffen habe.[1058]

Eigenverantwortung in diesem Sinne auszuüben heisst aber nicht nur sich selbst passiv vor Bedrohungen zu schützen, also etwa sich dagegen zu wappnen, mit

---

1053 Vgl. KUNZ 2006, S. 72; HITZLER, S. 196 f.

1054 Vgl. KRASMANN, S. 64; SCHMIDT-SEMISCH, S. 80 f.; SCHLEPPER/PETER/LÜDEMANN, S. 84.

1055 Siehe analog das „System individueller Lichtpflicht" während den Nächten in europäischen Grossstädten ab dem 15. Jahrhundert, das später durch das „Lichtmonopol" des Staats im 17. Jahrhundert abgelöst wurde. Siehe dazu KAMMERER 2008, S. 19 ff.

1056 Man kann darin auch die Befriedigung von Neugier oder ein positives „Sich-Abgrenzen" von „den anderen" sehen.

1057 Vgl. Bericht HRW, S. 52 f. mit Beispiel; SCHMIDT-SEMISCH, S. 80. Das ist dem subjektiven Sicherheitsempfinden der Anwohner wiederum nicht zuträglich.

1058 Siehe zum Ganzen: KUNZ 2011, S. 363 f. und SIMON, S. 280 („[…] victims are active subjects who must be mobilized to fight their cancer."). Vgl. KAMMERER 2008, S. 94. Die interaktive Teilnahme der Bürger ist auch als wesentliches Element des öffentlich zugänglichen Portals des INDECT geplant, siehe oben Erster Teil, Kapitel III.A.2.

Gefährlichen zusammenzutreffen, oder gefährliche Orte zu meiden, sondern zweitens auch, Bedrohungen in Eigeninitiative aktiv zu bekämpfen. Der „neue Vigilantismus“[1059] floriert, wenn die Bevölkerung sich in ihren kriminalpolitischen Anliegen, seien diese noch so absurd, vom Staat, der Polizei und anderen im Strafrechtsbereich tätigen Behörden nicht ernst genommen fühlt, sie der „Befriedungspotenz“ staatlicher Institutionen nicht mehr traut[1060] oder wenn sie vom Staat zur Eigenvorsorge ermutigt wird.[1061] Anschaulich sieht man dies an den prosperierenden Nachbarschaftswachen und ähnlichen Selbsthilfe leistenden Laienprojekten der Kriminalitätsbekämpfung in Quartieren im anglo-amerikanischen Raum. Ein gutes Beispiel eines derartigen englischen Nachbarschaftsprojekts ist die „St Peters Neighbourhood Monitoring“. Mithilfe hochauflösender Kameras filmt die Anwohnerschaft den Raum ihres Quartiers St Peters in Leicester. Findet sie auf einer der Aufnahmen unerwünschtes Verhalten vor, stellt sie die entsprechende Aufnahme auf ihrer Website ins Internet und offenbart damit der ganzen Welt das Aussehen der Abweichler in ihrem Quartier.[1062] Letztere sind in den veröffentlichten Aufnahmen nicht etwa unkenntlich gemacht. Vielmehr wird mit dieser nachbarschaftlichen Massnahme bewusst bezweckt, die ertappten Täter durch Hinweise aus der Bevölkerung oder durch „Selbstanzeige“ (man verlässt sich in diesem Fall auf die demütigende Wirkung der Anprangerung im Internet) zu identifizieren und darauf gestützt zur Rechenschaft zu ziehen.[1063]

Drittens drängt die postmoderne Eigenverantwortung jeden Einzelnen dazu, selbst für seine eigene Unverdächtigkeit (unverdächtiges Erscheinungsbild, unverdächtiges Verhalten etc.) zu sorgen. Wer sich nicht darum kümmert, unver-

---

1059 HITZLER, S. 192.

1060 HITZLER, S. 195.

1061 Vgl. SCHLEPPER/PETER/LÜDEMANN, S. 83 f. und 90; KAMMERER 2008, S. 94.

1062 Siehe dazu <http://stpetersnm.com/>. Siehe bspw. auch <http://www.interneteyes.co.uk/viewer-how-to-view-cctv-online>.

1063 Die Massnahme weist Ähnlichkeiten mit der öffentlichen Internetfahndung auf (siehe dazu oben Zweiter Teil, Kapitel I.G.). Ein Erfolg dieser privaten Massnahme ist aber zu bezweifeln. Mit Stand 23. Januar 2012 konnten erst drei Täter identifiziert werden. Die Quote 3:81 ist nun aber nicht besonders überzeugend und wird dem getätigten Aufwand – jemand muss die Aufnahmen auf abweichendes Verhalten hin durchsuchen, die Kameras warten etc. – wohl nicht gerecht. Problematisch daran ist insbesondere, dass bereits relativ harmlose Verfehlungen (z. B. sog. „Littering“) mit dieser Massnahme bekämpft werden und dass kaum angemessene Kontroll- und Aufsichtsmechanismen, denen im Gegensatz dazu staatliche Akteure unterworfen sind, bestehen.

dächtig zu wirken, ist selbst schuld, wenn er als verdächtig angesehen, dementsprechend näher überprüft oder weiteren Massnahmen unterzogen wird.[1064] Zudem wird dazu aufgefordert, verdächtige Vorkommnisse oder Personen in der Nachbarschaft zu melden.[1065] Die Selbstvorsorge macht den Bürger rastlos, unruhig, paranoid. Da ein jeder als potenziell gefährlich gilt, der staatliche Kriminalitätsbekämpfungsapparat aber nicht fähig ist, diesen Generalverdacht gesamthaft zu behandeln, sieht sich der Bürger genötigt, zu folgern: „Es muss kontrolliert werden und ich bin Teil dieser Kontrolle; ich bin Kontrolleur wie auch Kontrollierter."[1066] Wer sich nicht an diese selbstregulierende Strategie hält, läuft Gefahr, zum Aussenseiter zu werden, der intensiver fremd überwacht werden muss.

Die Eigenvorsorge spielt mit der Verunsicherung und den Sicherheitsbedürfnissen in der Bevölkerung.[1067] Sie beschäftigt die Bürger unmittelbar mit dem Kampf um Sicherheit. Das klassische Verständnis des staatlichen Gewaltmonopols im Bereich der Kriminalität hatte den Bürger noch von dieser Last befreit. Die skizzierte eigenverantwortliche Selbstregulierung in der Gesellschaft, speziell im näheren sozialen Umfeld (Nachbarschaft etc.), schafft über verschiedene Anreize unter anderem ökonomisch produktive – weil fügsam, gesetzestreu, kooperativ, risikolos und gesund handelnde – Mitglieder der Gesellschaft.[1068] Straftäter und Abweichler hingegen werden zunehmend einer bürokratisch-administrativen Überwachung unterzogen, die im Zeitalter der Informationsgesellschaft darauf hinausläuft, bekannte Straftäter oder Verdächtige engmaschigen Monitorings zu unterziehen oder Eingetragene in Registern durch die zeiteffiziente Arbeitsweise computergestützter Register zur Selbstregulation zu zwingen.[1069] Die Behörde, die ihre Geschäfte schneller abwickeln kann (durch automatisierte Datenbanken) und Verstösse gegen Auflagen oder Fristen sofort entdeckt (durch automatische Alarme der Systeme), verlangt diese neue administrative Effizienz auch von den Registrierten. Fristen sind unbedingt einzuhal-

---

1064 Vgl. den Blog von SIMON zum Thema „Whose Public Safety? Trayvon Martin and Neighborhood Watch" vom 24. März 2012: „[…] African American young men wearing hoodies are presumed to be cruising for criminal opportunities and should be prepared to perform their innocence visibly at all times […]."

1065 GILLIOM, S. 88 f.

1066 BIDLO, S. 41.

1067 Vgl. HESSDÖRFER/BACHMANN, S. 171.

1068 Siehe LEE, S. 86; CAMPBELL, S. 79 ff.; KAWASHIMA, S. 167 f.; KRASMANN, S. 196 ff.

1069 Vgl. LEGNARO 2010, S. 64; GILLIOM, S. 9; HESSDÖRFER/BACHMANN, S. 168 f.

ten, potenziell dienliche Angaben sind nicht zu vergessen und der Behörde unverzüglich mitzuteilen. Das aufgezwungene Selbstmanagement drangsaliert diejenigen, die willig sind (fortan) gesetzestreu zu leben und lässt überforderte Eingetragene davor flüchten.[1070]

B. Die fingierte Selbstexklusion

Das Modell des Wohlfahrtsstaats sah vor, dass sich jeder um jeden sorgte und für alle Verantwortung übernahm. Lagert der Staat nun Verantwortung an den Bürger aus[1071], ändert er gleichzeitig die Quantität und Qualität der Gesamtverantwortung. Der Bürger ist nicht zu mehr anzuhalten, als zuallererst für sich selbst zu schauen. Die Gesellschaft kann eine Verantwortung der Gesellschaft für die Gesellschaft und die Kriminalität in der Gesellschaft verleugnen. Die Gesellschaft und der Einzelne entziehen sich damit ihrer Verantwortung gegenüber Auszugrenzenden.

Die Rückbesinnung auf das Selbst, darauf selbst aktiv an der Kriminalitätsvermeidung und Sicherheitsvorsorge teilzunehmen, so könnte man meinen, lehre den zur Eigenverantwortung angehaltenen Menschen gleichzeitig mehr Selbstkontrolle, lasse ihn sich in Selbstdisziplin üben. Dem ist nicht so: Die Selbstbestimmung wird zum einen liberal als „unabdingbare Voraussetzung für ein gelungenes Leben“ verstanden.[1072] Zum anderen forciert das heutige Verständnis von Selbstverwirklichung die Selbstperfektion zugunsten des Gemeinwohls.[1073] Selbstkontrolle, auch im Sinne guten Betragens, des Willens zur Integration etc., kennzeichnet die erste Bedingung der Gesellschaftsfähigkeit. Sie zu erlangen, das heisst das vorgegebene Ideal zu erreichen, liegt aber in seiner eigenen Verantwortung. Sein Scheitern hat er selbst zu verantworten und auf Vorschussvertrauen kann er selten hoffen. Die Aktivierungsstrategien und entsprechende postmoderne Technologien vermitteln, wie die Eigenverantwortung im hier beschriebenen Verständnis, keine Selbstkontrolle. Vielmehr gehen sie von der Annahme aus, selbstkontrollierte Bürger seien rar geworden, weshalb als Ersatz eine, in extremis omnipräsente, (situative) Fremdkontrolle einspringen müsse. Es stellt sich indes die Frage, ob das Individuum nicht tendenziell verlernt, Selbst-

1070 Vgl. dazu bspw. GILLIOM und die OPPAGA-Berichte.
1071 KRASMANN, S. 186.
1072 ROTHE, S. 68.
1073 Siehe HESSDÖRFER/BACHMANN, insb. S. 170.

kontrolle zu entwickeln, wenn diese in immer grösseren Teilen ersetzt wird durch Fremdkontrolle, und es jene deswegen nicht üben muss.[1074]

Die Ansicht, dass „Exklusion in einer freiheitlichen Gesellschaft […] immer Selbstexklusion" sei[1075], kann in dieser Hinsicht streng genommen zutreffend sein, zeigt jedoch eine sehr zynische Haltung. Natürlich kann einer theoretisch selbst entscheiden, ob er sich so verhält, wie es die Gesellschaft von ihm verlangt, oder eben nicht. Die Gleichung „gesellschaftliche Exklusion bedeutet immer Selbstexklusion" ist aber viel zu simpel.[1076] Unhaltbar wird diese Gleichung, sobald ein Aussortierungssystem für Risikpersonen in der Praxis nicht dem Ideal entsprechend umgesetzt werden kann. Können Fehler bei der Beurteilung in der Praxis nicht ausgeschlossen werden, führen sie zu unzutreffenden Risikobefunden bei Menschen, die sich eigentlich gesellschaftskonform verhalten haben, demnach trotz Verdacht oder Verurteilung „unschuldig" sind, oder zu unfairen und kontraproduktiven Risikobefunden bei denjenigen, welche ernsthaft beteuern, sich in Zukunft konform zu benehmen, denen man dieses Versprechen (zu Unrecht) aber nicht abnimmt. Die zweite Gruppe hat sich zumindest nicht unmittelbar selbst aus der Gesellschaft exkludiert, die erste Gruppe konnte nun wirklich nichts für ihre Ausgrenzung als Risikoträger. Sie wurde vielmehr von der Gesellschaft aktiv, zum Beispiel aufgrund vager Verdachtsmomente oder klischeehafter (automatisierter beziehungsweise objektivierter) Merkmale, ausgesondert. Die Annahme, deren Einteilung in eine Risikokategorie habe von ihrer auffälligen, verdächtigen Verhaltensweise oder Haltung abgehangen, weswegen sie sich damit selbst ausgeschlossen hätten, ist wenig überzeugend. Insbesondere, sobald biologische Kriminalitätstheorien herangezogen werden, werden körperliche Dispositionen des Menschen, die das Handeln oder Leistungsvermögen beeinflussen, zu Risikofaktoren erhoben. Ganz im Sinne der postmodernen Eigenverantwortung und Selbstvorsorge hat der Mensch mit kriminellen Körperdispositionen oder anderen Defiziten sich danach letztlich als (sein eigener) Feind, mit wenig Aussicht auf Erfolg, selbst zu bekämpfen.[1077] Das harte, exkludierende Vorgehen der Gesellschaft gegen Abweichler und Kriminelle scheint dabei vermeintlich nicht ganz so hart, wenn deren Abweichungen und Verbre-

---

1074 Siehe HEMPEL/TÖPFER, S. 50.

1075 JAKOBS 2006, S. 293.

1076 Gesellschaftliche Vorschriften einzuhalten, die jemand für ungerecht, unethisch oder aus anderen veritablen Gründen zu verachten hält, kann für diesen, jedenfalls faktisch, Zwang bedeuten, sich zu beugen.

1077 Vgl. TOLMEIN.

chen selbstverschuldet oder natürlich-defizitär bedingt sind, sondern im Gegenteil legitim.

Hinzu kommt, dass Feindbilder der Gesellschaft in der Realität stark fluktuieren können und etwa die unbestimmten Abgrenzungskriterien von JAKOBS in dieser Hinsicht keineswegs eine nützliche Hilfe bieten.[1078] JAKOBS anerkennt diese argumentative Schwachstelle immerhin insoweit, als er die Beliebigkeit der Feindbilder ausdrücklich zugesteht.[1079] Die Gesellschaft bestimmt, wer Risikoträger ist; *sie* ist es, die Risikoklassifizierungen in diesem Sinne konstruiert.[1080] Zynisch ist jene Erkenntnis JAKOBS insbesondere deshalb, weil er dennoch ein „leistungsorientiertes Modell der Person" vertritt.[1081] Das kognitive Defizit determiniert folglich zur Zuordnung in eine Risikokategorie. Neben der Exklusion und Sicherung bleiben in diesem Konzept kaum Alternativen mit dem unbelehrbaren Merkmalsträger umzugehen.[1082] Die Schwachstelle dabei ist indes, dass der Merkmalsträger als Unperson ohne die kognitive Mindestgarantie zur Normbefolgung in diesem Sinne keine freie Entscheidung bezüglich seines Wohlbetragens treffen kann. Er ist somit nicht befähigt, sich durch normwidriges Verhalten *willentlich* selbst zu exkludieren. Aus dem Gebiet der Biokriminologien wird daher als Alternative etwa vorgeschlagen, dem defizitären Wesen wegen einer „Fehlsteuerung ohne Fehler des Steuermanns"[1083] ein „Gefühl der Verantwortung für das eigene Tun einzupflanzen"[1084].

C. Inklusion und Exklusion

Die angesprochenen Teilungspraktiken und Strategien der Selbstaktivierung können in letzter Instanz zu einer Ordnung führen, die Inklusion und Exklusion als Instrumente des Regierens einsetzt und die C. D. SHEARING und P. C. STENNING anschaulich anhand eines Berichts ihres Besuchs von „Disney-World" be-

---

1078 Vgl. ARNOLD 2006a, S. 307; NEUMANN, S. 311; KUNZ 2006, S. 77.

1079 JAKOBS 2006, S. 294

1080 Gl. A. wie APONTE, S. 300. Vgl. NIGGLI 2004, S. 37; SCHWARZENEGGER, S. 125.

1081 Das Konzept, den Personenstatus über das Pflichtbewusstsein der Bürger zu bestimmen, verschärft die Problematik. Siehe NEUMANN, S. 310 f.: „Das Modell von Jakobs verbindet somit hohe Anforderungen, die an den Erwerb und Besitz des Personenstatus gestellt werden, mit der Konsequenz der fast völligen Rechtslosigkeit dessen, der diesen Anforderungen nicht gerecht wird."

1082 Vgl. SINGELNSTEIN/STOLLE 2012, S. 88 f.

1083 Georges Canguilhem zitiert bei LEMKE, S. 14.

1084 ROTH 2003b, S. 544.

schreiben.[1085] „Disney-World" setzt den Traum postmoderner Teilungspraktiken um: Das Souveränitätsgebiet wird in verschiedene Lebensräume eingeteilt. Die einzelnen Lebensräume sind abgeschlossene und relativ autarke Systeme, in denen sich nur diejenigen Leute bewegen dürfen, welche sich den dort herrschenden Regeln und Verhaltensnormen unterwerfen. Einzige Strafe ist die (permanente) Wegweisung aus dem Lebensraum. Das Kontrollinstrument ist der allgegenwärtige Hinweis auf den jederzeit möglichen Ausschluss aus dem Lebensraum bei Missachtung der geltenden Regeln. Omnipräsente technische Überwachungsmethoden und situative Prävention gewährleisten, dass Abweichungen leicht erkannt werden, und ermöglichen sofortiges Eingreifen seitens der Ordnungskräfte. Sowohl präventive Belehrungen als auch repressive Interventionen werden stets mit dem Hinweis auf Eigenverantwortung und Selbstvorsorge verknüpft – es ist nur zum eigenen Besten und eine Gefahr für andere will man ja auch nicht darstellen –, was, wie selbstverständlich, eifrige Kooperation hervorruft.[1086] Die drohende Wegweisung ist hart, da der nämliche Lebensraum attraktiv und der alternative Lebensraum im Vergleich dazu unattraktiv ist. Diese Teilungspraktiken betreiben nicht den erzieherischen Aufwand eines Überwachungsstaats, sie dulden nur bereits erzogene Personen. Wer sich nicht an die im Voraus verkündeten und immer wiederholten, jedoch oft vage formulierten, Regeln hält, bekommt keinen Lehrgang in Anpassung, sondern wird schlicht aus dem attraktiven Lebensraum verbannt. Der treue Bürger nimmt diese strikten Ordnungsvorschriften – die Regeln können vom Bürger auch nicht beeinflusst werden[1087] – und die sich daraus ergebenden Unannehmlichkeiten deshalb in Kauf, weil die Alternative, im „Draussen", im unkontrollierten Gebiet zu sein, schlechter (mit anderen Worten gefährlicher, unbequemer oder weniger verlockend etc.) ist oder scheint (wichtig ist die Inszenierung). Draussen herrscht das Chaos unklarer Zuordnungsmerkmale, facettenreicher Erklärungen von Delinquenz und allgemeiner Unsicherheit, drinnen die integrierende Garantie klarer, dichotomer Abgrenzungen vom Anderen und allgegenwärtig einzuhaltender, risikominimierender Verhaltenskodizes.[1088] Freilich sind alle Vorschriften nur

---

1085 SHEARING/STENNING, S. 51 ff. Passenderweise publizierten sie den Artikel im Jahr 1984.

1086 Vgl. LEGNARO 2000, S. 291 f.

1087 Sie nehmen eine ähnliche Stellung wie die von SARAT, S. 345 f., beobachteten Bedürftigen im Wohlfahrtssystem der USA ein: „They are «caught» inside law's rules, but are, at the same time, excluded from its interpretive community."

1088 Vgl. SINGELNSTEIN/STOLLE 2012, S. 43 f.; KUNZ 2000, S. 48; KRASMANN, S. 222 f.; YOUNG 1999, S. 20.

zum Besten des Bürgers da. Das Leben darin ist ein Privileg. Einen Ausschluss hat der Bürger daher immer selbst zu verantworten[1089]:

1. Dem Bürger wird empfohlen, sich den Vorschriften auszuliefern. Dass die drohende Exklusion ständig über den Köpfen der Bürger schwebt, verleiht dieser Empfehlung Nachdruck. Darin zeigt sich die Logik der fingierten Selbstexklusion. Die impliziten Drohungen „aus gesellschaftlicher Teilhabe oder Anerkennung herauszufallen, lassen es dabei so aussehen, als wäre diese Selbstmobilisierung ein originär individueller Wunsch."[1090]
2. Der Bürger hat die entsprechenden umfassenden „gesellschaftlichen Spielregeln"[1091] in Eigenleistung zu erkennen oder vielmehr zu erahnen.[1092] Der unsichere, treue Bürger verhält sich dadurch im Zweifelsfall folgsamer und konformer als über Vorschriften gefordert werden könnte.
3. Die Teilungspraktiken reizen das „Ich habe nichts zu verbergen"-Argument bis auf das Letzte aus: Zugang zu Dienstleistungen und Konsumgütern hat, wer seine Alltagsdaten offenlegt. Wer konsumiert, legt seine Alltagsdaten freiwillig offen.[1093] Es besteht keine staatliche Anordnung, sich der Gesellschaft zu öffnen, aber faktisch eine Notwendigkeit, ein indirekter Zwang. Die Unannehmlichkeiten, die entstehen, wenn dies nicht getan wird, sind zu gross.[1094]

Das dargestellte System funktioniert in „Disney-World" offensichtlich.[1095] Nun ist die Gesellschaft in der Welt ausserhalb dieses Traums noch weit entfernt von

---

1089 Vgl. SCHMIDT-SEMISCH, S. 67.

1090 KRASMANN, S. 224 f.

1091 KRASMANN, S. 225. Spontanität wird in diesem Ordnungssystem kein Platz eingeräumt, siehe LEGNARO 2000, S. 291 ff.

1092 SINGELNSTEIN/STOLLE 2012, S. 75 und 84 f.

1093 Vgl. SOLOVE 2007, S. 770; STALDER, S. 120; LEGNARO 2010, S. 63.

1094 Vgl. SINGELNSTEIN/STOLLE 2012, S. 85.

1095 SHEARING/STENNING, S. 53 zum strikt choreographierten Ablauf in „Disney-World": „[…] beauty *is* created, safety *is* protected, employees *are* helpful." Das rührt sicherlich auch daher, weil es von einem privaten Unternehmen als machtausübende Instanz geführt wird. Der finanzielle Aufwand dürfte immens sein. Die situativ-präventive Bauweise, die Überwachungstechniken, die angestellten Sicherheitsleute und all die anderen Vorkehrungen in „Disney-World" müssen überall in ausreichend grosser Zahl vorhanden sein. Finanziell tragbar ist ein in dieser Art künstlich attraktiv gehaltener Lebensraum nur, wenn dessen Gebiet verhältnismässig klein und überschaubar bleibt und wenn die Kaufkraft der zugelassenen Bürger ausreichend gross ist.

einer derartig ausgeprägten Sozialkontrolle. Die Überlegungen zum „Disney-World-Effekt“ und zu den Teilungspraktiken können jedoch, das kann den Ausführungen zu den postmodernen Formationen entnommen werden, auf Tendenzen, die in diese Richtung zeigen, übertragen werden. Diese sind nicht nur in anglo-amerikanischen, sondern auch in westeuropäischen Ländern zu beobachten, unter anderem auch im virtuellen Raum: Das Internet oder andere moderne Kommunikationsmittel nicht zu gebrauchen ist für den Durchschnittsbürger in der heutigen, entwickelten Welt sehr umständlich. Er nimmt deshalb gewisse Kontrollmechanismen oder Überwachungstätigkeiten in Kauf, um Zugang dazu zu er- und behalten.[1096]

Der Preis, das Konzept von der Fantasie-Welt im Vergnügungspark in die alltäglichen Lebensräume zu überführen, wäre wohl in vielerlei Hinsicht hoch.[1097] Erstens bedeutet der Bürger in einer derart teilenden Gesellschaft wenig. Bedeutung wird ihm lediglich vorgegaukelt. Er wird zwar behandelt, als wenn sich alles um ihn drehen würde, in Wahrheit ist er jedoch nicht mehr als eine Milchkuh in einer Herde von Milchkühen. Eine Beteiligung des Volks an der Willensbildung der Staatsordnung ist darin inexistent, fingiert oder moderiert. Das Regime bestimmt die Regeln, das Leitbild, die Ideologie und die künftige Entwicklung. Letztlich ist darin auch die Kriminalität konstruiert und dient unter anderem dazu, über andere Probleme hinweg zu täuschen.[1098] Die entstehenden Entfremdungseffekte[1099] zwischen den ausgeschlossenen Personengruppen und den Bürgern dürften abgesehen davon kontroproduktiv sein, da in sozialer Isolation ein

---

1096 Vgl. CHESTERMAN, S. 226. Die Umgebungen sozialer Netzwerke, wie „Facebook“, ähneln zudem „Disney-World“ stark. Gestützt auf einen relativ vagen „code of conduct“ (siehe bspw. <http://www.facebook.com/legal/terms>) werden abweichlerische Inhalte angedeutet, die nicht toleriert werden. Zuwiderhandlungen können mit (permanenten) Kontosperren geahndet werden.

1097 Was vor allem in Amerika immer häufiger der Fall ist. Beobachten lässt sich der Trend zum Beispiel an den spriessenden postmodernen Burgstädten, den „gated communities“ oder „gated new towns“ in den USA, vgl. dazu SCHMIDT-SEMISCH, S. 90 f.; KUNZ 2000, S. 26; HEYMANN, S. 93; NOGALA 1998, S. 316.

1098 Vgl. BOGARD, S. 60 f.; BAUDRILLARD, S. 31.

1099 ZEHNDER M., S. 28 nennt diese „mikroregionale Entmischung“. Siehe auch GILLIOM, S. 90 ff. zu den Folgen. Teilungspraktiken können dazu führen, dass auch die Ausgeschlossenen kaum Groll gegen das System an sich hegen, sondern im selben Schema denken und sich daher zum einen schämen und zum anderen untereinander misstrauisch begegnen, siehe die Interviews bei GILLIOM, insb. S. 93 ff. und 105; SCHMIDT-SEMISCH, S. 73. Dieser Effekt erinnert an den Behandlungsansatz der Neurokriminologien, den Defizitären ein „Gefühl der Verantwortung für das eigene Tun einzupflanzen“ (ROTH 2003b, S. 544).

Risikofaktor für höhere Kriminalitätsaufkommen in bestimmten Räumen liegen kann.[1100]

D. Protagonisten, Transparenz und altruistische Motive

Aus der skizzierten Selbstaktivierung des Bürgers ziehen vor allem die Politik und der Staat Nutzen, indem Verantwortung für die Sicherheit sowie für Misserfolge und Fehler mit den Bürgergemeinschaften geteilt und Kosten für Projekte und (technische) Massnahmen auf sie abgewälzt werden.[1101] Vom Staat ist dabei sicherlich ein grosses Mass an Transparenz aller erörterten Massnahmen gegenüber der Bevölkerung zu erwarten. Sie soll einerseits nicht Teile ihrer Freiheit zugunsten der Illusion der von ihr gewünschten, aber in der Praxis nicht realisierbaren Fantasiewirkungen dieser Massnahmen aufgeben. Werden die Funktionsweise der besprochenen Instrumente und deren Problematik von staatlicher Seite offen angesprochen, sodass sich idealerweise die drängenden illusionären Ansprüche aus der Gesellschaft auflösen, kann möglicherweise einem allzu symbolischen und extensiven Einsatz vorgebeugt werden.[1102] Andererseits kann so die Enttäuschung der Bevölkerung über die Kriminalitätsverhinderungskapazitäten dieser Massnahmen schon früh in Grenzen gehalten werden, was dazu führt, dass deren Vertrauen in den Staat, die Polizei und das Justizsystem nicht in Mitleidenschaft gezogen wird. Staatliche Behörden haben folglich ein Interesse daran, offen und ehrlich mit den Bürgern zu kommunizieren und angewendete Techniken zum Vorgehen gegen Kriminalität zu diskutieren.

Den postmoderne Technologien einsetzenden Staat undifferenziert als Überwachungsstaat zu diffamieren, ist verfehlt und verkennt zum einen, dass dem Staat oder staatlichen Behörden mehr die Rolle eines, zuweilen durchaus parteiischen, Mittlers zwischen den gesellschaftlichen Sicherheitsbedürfnissen und den angebotenen Technologien zukommt. Weder ist der Staat der einzige Akteur noch darf sich die Gesellschaft und damit die Bevölkerung aus dem Kreis der mitmischenden und beitragenden Protagonisten herausnehmen. Dem hinzuzufügen ist freilich, dass staatliche Behörden dazu neigen, ihre Kompetenzen und Eingriffsbefugnisse kontinuierlich zu erweitern.[1103] Zum anderen divergiert der Einsatz

---

1100 Siehe ZIMRING, S. 216; YOUNG 1999, S. 21.
1101 SCHLEPPER/PETER/LÜDEMANN, S. 96; GRAS, S. 220.
1102 BARTSCH, S. 235; HILGENDORF, S. 82; SINGELNSTEIN/STOLLE 2012, S. 142 und 147 f.
1103 SINGELNSTEIN/STOLLE 2012, S. 53 ff. Siehe dazu oben Zweiter Teil, Kapitel I.

der postmodernen Kriminalitätsbekämpfungstechnologien, auch wenn diese als bekämpfungsstrafrechtliche Strategien teils kritisch zu betrachten sind, zumindest in der Schweiz stark von denen eines die Bevölkerung unterdrückenden Regimes. Den massgeblichen Unterschied zwischen einem dystopischen Regierungsmodell und den heute praktisch angewendeten postmodernen Strategien charakterisieren SHEARING/STENNING folgendermassen: „Surveillance is pervasive but it is the antithesis of the blatent control of the Orwellian State: its source is not government and its vehicle is not Big Brother.“[1104] Die Teilungspraktiken anwendende Rationalität regiert durch ein umgebendes Gefüge aus Faszination und Furcht, aus Emotionen und unsicherem Glück, aus plakativen Schranken und versteckten Prozessen sowie Dynamiken. Es gilt daher analog, was FOUCAULT zum Panoptikum bemerkte: „[Es hat] wenig Bedeutung, wer die Macht ausübt“. Die Macht ist „automatisiert und entindividualisiert“.[1105] Der entindividualisierte Machtapparat steht jedermann zur Verfügung. Im Sinne des neuen Verständnisses der Eigenvorsorge benutzen die Bürger dieses Instrument nicht zuletzt untereinander.[1106]

In Anlehnung an GILLES DELEUZE, der das Unternehmen, welches die Fabrik der Disziplinärgesellschaft in der Kontrollgesellschaft ablöse, als „kein Körper, sondern eine Seele, ein Gas“ versinnbildlicht[1107], könnte man die dargestellte Eigendynamik als Energie von Machtprozessen verstehen, die die postmoderne, technisierte Kontrollmaschinerie antreibt: Die Abläufe und Hierarchien in der Fabrik sind klar geordnet, die Angestellten kennen sich untereinander und an der Spitze steht der Patron, der den Betrieb im Interesse einer gesund laufenden Fabrik leitet und klare Anweisungen erteilt. Die Fabrik ist ein Körper mit vielen Gliedern, die das Gehirn dirigiert. Die Gestalt des Unternehmens hingegen ist undurchschaubar und diffus. Es kennt keine richtigen Chefs, sondern Gremien,

---

1104 SHEARING/STENNING, S. 56. Sehr ähnlich KRASMANN, S. 93 f. und 332; SINGELNSTEIN/STOLLE 2012, S. 158. Vgl. auch BORNEWASSER, S. 135 f. und STRÖM, S. 253, der meint: „Nur die misstrauischsten Personen dürften dahinter [hinter der Informationsbeschaffung durch staatliche und kommunale Stellen] einen bösen Plan, eine böse Absicht vermuten.“ Ebenso ZURAWSKI, S. 11, der aber m. E. nicht ganz zutreffend darauf hinweist, diese Strategien würden genau deshalb nicht als Überwachung oder Kontrolle wahrgenommen. Das Überwachungselement zumindest dürfte vom Durchschnittsbürger durchaus wahrgenommen werden, aber wohl zuweilen als im Allgemeinwohl liegend oder aus Bequemlichkeit hinzunehmend eingeschätzt werden.

1105 FOUCAULT 1994c, S. 259.

1106 SINGELNSTEIN/STOLLE 2012, S. 158.

1107 DELEUZE 1993b, S. 256.

Abteilungsleiter und Verantwortliche. Das Unternehmen ist ein Gas mit vielen einzelnen, aber gleichartigen Partikeln, geordnet nach Kategorien. Hinter dem Kontrollapparat stehen letztlich Viele.[1108] Der Ursprung, der Kopf oder die Verantwortlichkeit des Konglomerats von postmodernen Überwachungsstrategien sind nicht einer einzelnen Quelle klar zuzuordnen. Sehr ähnlich beschreibt FOUCAULT diese postmoderne Formation und nennt sie „gouvernementalité“: „Unter Gouvernementalität verstehe ich die Gesamtheit, gebildet aus den Institutionen, den Verfahren, Analysen und Reflexionen, den Berechnungen und Taktiken, die es gestatten, diese recht spezifische und doch komplexe Form der Macht auszuüben, die als Hauptzielscheibe die Bevölkerung, als Hauptwissensform die politische Ökonomie und als wesentliches technisches Instrument die Sicherheitsdispositive hat.“[1109] KRASMANN folgert aus den Überlegungen Foucaults zur Gouvernementalität: „[Die Macht] ist nicht im Besitz einer zentralen Instanz oder einer Person, sondern zerstreut; eine Frage von Positionen und Relationen.“[1110] Und, wie ROTHE sicherlich zutreffend bemerkt, werden die entstehenden Machtgefälle und Asymmetrien „nicht selten von *allen* Beteiligten eingerichtet, unterhalten, genutzt und ausgenutzt.“[1111]

Eine „Staatszentrierung des Protests“ verfehlt somit, die postmodernen Formationen angemessen zu beschreiben, führt vielmehr auf Irrwege.[1112] In diesem Sinne inszenieren auch fundamentalistische Überwachungsgegner überstilisierte Geschichten und bewegen leidlich wenig, ausser Panik hervorzurufen und (positive sowie negative) „Ikonen des Protestes“ zu erschaffen, was kaum Konkretes oder Konstruktives zur Lösung der Problematik beiträgt.[1113] Nun profitieren aber durchaus verschiedene Protagonisten von den postmodernen Sicherheitsrationalitäten und vom Einsatz postmoderner Kriminalitätsbekämpfungstechnologien:

Zum einen halten technisierte Massnahmen einen ganzen Wirtschaftszweig, die Sicherheitsindustrie, am Leben und fördern dessen Wachstum.[1114] Die kommer-

---

1108 Vgl. KAMMERER 2011, S. 30 f.

1109 FOUCAULT 2000, S. 64.

1110 KRASMANN, S. 68 mit zahlreichen Hinweisen auf Schriften FOUCAULTS. Ausführlich zur Gouvernementalität DIES., S. 67 ff.

1111 ROTHE, S. 70. Ebenso ULLRICH/LÊ, S. 120 f.

1112 ULLRICH/LÊ, S. 117 f.

1113 Siehe ULLRICH/LÊ; GROEBNER, S. 176. Im Gegenteil können derartige Protestikonen der gouvernementalen Strategie auch als Material für Skandalisierungstaktiken dienen.

1114 Vgl. etwa ZURAWSKI, S. 11; GRAS, S. 218; VOREGGER in Spiegel Online vom 23. September 2009.

ziellen Interessen hinter der Kriminalitätsbekämpfung blühen in Krisen erst richtig auf.[1115] Kriminalität kann als „positives Gut" im Sinne eines „Produktionsfaktors" benutzt werden.[1116] Dasselbe gilt für die Politik und die Medien, indem die Einführung von neuen, möglichst aufsehenerregenden Massnahmen gegen die Kriminalität willkommene Ansatzpunkte für Wahlkampfkampagnen und auflagenstarke Leitartikel verheisst. Das führt mitunter im Nachhinein auch dazu, dass schlechte Ergebnisse hinsichtlich der Wirkung der besprochenen Massnahmen überspielt oder auf andere Anwendungsgebiete angepasst werden, um zum Beispiel die für die Entwicklung, Installation oder den Betrieb ausgegebenen Mittel zu rechtfertigen.[1117] An die Stelle von wissenschaftlicher und praktischer Erkenntnis, die durchaus vorhanden wäre, aber sich häufig nicht durchzusetzen vermag, treten „wahlkampftaugliche Alltagstheorien".[1118] Die (Massen-)Medien sind ein zweischneidiges Schwert: Zwar versorgen sie die Öffentlichkeit mit Wissen und Informationen über die Kriminalität und die entsprechenden postmodernen Bekämpfungsmethoden. Da hinter den (Massen-)Medien jedoch profitorientierte Unternehmen stehen, folgt die Auswahl und Aufmachung der Artikel ökonomischen Kriterien.[1119] Anstatt die Öffentlichkeit aufzuklären, zu informieren und damit im positiven Sinne aufzurütteln oder zu beruhigen, festigen (Massen-)Medien zuweilen mit effektheischender Berichterstattung Furchtzustände und dämonisierte Menschenbilder.[1120] Dahinter muss kein böser Plan stehen, um trotzdem Schaden an und in der Gesellschaft anzurichten. Wenn zum Beispiel Politiker oder eine politische Fraktion ihren Machterhalt anstreben und diesen mithilfe einer populistischen Jagd auf Kriminelle und Abweichler erreichen können, werden Ethik und Moral schnell unterbewertet oder gar unerheblich. Partnerschaften zwischen diesen profitierenden Akteuren sind zudem nur logisch. Machen sie sich doch dieselben Prozesse und Dynamiken zu Nutze, um zwar verschiedene, aber *nicht gegenläufige* Ziele zu erreichen.[1121]

1115 Vgl. KUNZ 2011, S. 353 f.

1116 SCHMID-SEMISCH, S. 96.

1117 Siehe NORRIS/ARMSTRONG, S. 65 ff. und 69 f.; SINGELNSTEIN/STOLLE 2012, S. 57 ff.; TEMME, S. 167. Vgl. LOADER/SPARKS, S. 62.

1118 SINGELNSTEIN/STOLLE 2012, S. 58. Ebenso ALBRECHT P. A. 2010, S. 10.

1119 Vgl. BUCKLER/SALINAS, S. 712.

1120 YOUNG 1999, S. 69, 115 und 128 f.; BUCKLER/SALINAS, S. 717 f.

1121 KUNZ 2011, S. 336 f. Siehe dazu auch SINGELNSTEIN/STOLLE 2012, S. 45 ff. HAYES 2009, S. 50, beschreibt diese Partnerschaften wie folgt: „[…] a simple *quid pro quo*: profit for companies and power for states […]".

Zum anderen erlaubt die fortschreitende Technisierung privaten Unternehmen, ihre an sich öffentlich zugänglichen Räume (Einkaufszentren, Parks etc.) frei von unerwünschten Personen zu halten. Wer sich der Kontrolle nicht unterwerfen will, der soll woanders einkaufen gehen oder sich um ein anderes Fortbewegungsmittel bemühen. Und wer die Ästhetik oder die Kauflust anderer Personen stört, wird mithilfe „organisatorischer Formen der Kontrolle", also abgeschwächten Spielarten polizeilicher oder strafrechtlicher Folgeinterventionen (Listen mit Hausverboten, per Videoüberwachung angeleitete Putzkolonnen etc.), vom Areal verscheucht.[1122] In diesem Zusammenhang können Ansätze zur engen Zusammenarbeit der Akteure der Wirtschaft mit den Akteuren staatlicher Behörden sehr fruchtbar (und sehr problematisch) sein. Die staatlichen Kriminalitätsbekämpfungsbehörden haben ein starkes Eigeninteresse an umfassenden Datenbanken über Personen, an grossen Datensätzen zu menschlichen Verhaltensweisen, an der Entlastung durch ausgelagerte Überwachung von gefährlichen Subjekten usw. Kooperieren sie deshalb mit den wirtschaftlichen Akteuren, fördern sie deren Regulierung und Management öffentlicher Sphären, indem sie teils heikle, ökonomisch motivierte Eingriffe unterstützen.[1123] Je stärker abdeckend und vernetzter sich die private Raumüberwachung ausbreitet, desto unmittelbarer ist der Zwang, sich einer Überwachung auszusetzen. Dem Bürger gehen schlicht die Alternativen aus, insbesondere, wenn auch der virtuelle Raum zunehmend überwacht wird. Als besonders gravierend könnte sich diese Entwicklung für randständige Personengruppen herausstellen. Im Extremfall vermischen sich staatliche und zivile Kontrollmassnahmen zu einem ganzheitlichen Exklusionsapparat.[1124] Dies ist auch ein Kernproblem der öffentlichen Zugänglichkeit von Registern, verbunden mit staatlicher oder privater Überwachungstechnik: Wer will schon einen (mutmasslichen) Hooligan, Pädophilen oder Terroristen in seinem Kaufhaus, in seinem Büro oder im Umfeld seiner Kinder?[1125]

1122 KAMMERER 2008, S. 99 f. mit Beispielen; YOUNG 1999, S. 18 f.

1123 Vgl. ANDREJEVIC, S. 126 f. mit weiteren Beispielen aus dem digitalen Bereich.

1124 Gl. A. wie NORRIS/ARMSTRONG, S. 8 f.; KUNZ 2011, S. 369 und 376; ROGGAN 2001, S. 139. Vgl. auch TROTHA, S. 223.

1125 Siehe KUNZ 2011, S. 332 ff. Die Anforderungen an den Grad der Verdächtigkeit oder Bedrohlichkeit einer Person dürften in diesen Fällen wohl kaum hoch angesetzt sein. Vgl. NORRIS/MORAN/ARMSTRONG, S. 510 und 513; GRAS, S. 111 f. und 203 f.; KUNZ 2011, S. 270 f.; SINGELNSTEIN/STOLLE 2012, S. 36; SCHMIDT-SEMISCH, S. 90 f. Weniger bedrohliche, aber trotzdem unerwünschte Personengruppen wird ein automatisches Erkennungsprogramm womöglich in privaten Registern auffinden oder über auffällige Einträge in sozialen

V. Konstruierte Sicherheit, konstruierte Realität

A. Situative Präventionsansätze

Situative Präventionsansätze der „Alltagskriminologien" stützen sich tendenziell auf ein „fatalistisches Prinzip instrumentell-pragmatischer Regulierung".[1126] Das ist zugleich ihre Schwachstelle: „Harte" Ansätze der situativen Prävention versuchen bestimmtes Verhalten an bestimmten Orten (nahezu) zu *verunmöglichen*. „Weiche" Ansätze hingegen versuchen Verhalten zu steuern, indem Tatgelegenheiten im Sinne der ökonomischen Theorien *verteuert* und dadurch reduziert werden sollen. Methoden des weichen Wegs können versuchen, Verhalten durch Symbolkraft zu beeinflussen. Rein symbolische Methoden wirken aber nur dann, wenn die Adressaten an ihre Wirkung glauben. Bei situativen Präventionsansätzen helfen handfeste Veränderungen, beispielsweise bei der Strassenbeleuchtung, der Vorteil, dass man den Angreifer frühzeitig sieht und sich dementsprechend auf Gegenwehr oder zur Flucht vorbereiten kann.[1127] Indes ist auch hinsichtlich harter Ansätze zu vermuten, dass *wirksame* situative Massnahmen den Delinquenten meist nicht zu legalem Handeln zwingen, sondern ihn eher gemässigt zur Verlagerung seines kriminellen Waltens verleiten, vor allem aber zum kreativeren Ausarbeiten seiner Vorgehensweise im Einsatzraum der situativen Prävention, wodurch zudem Eskalationseffekte entstehen können.[1128]

Netzwerken im Internet identifizieren. Kooperationen zwischen Staat und Privaten scheinen diesbzgl. grundsätzlich aussichtsreich, wenn auch sehr problematisch.

1126 KRASMANN, S. 299. Siehe allgemein zur situativen Prävention und zu den Alltagskriminologien („criminologies of everyday life" von David Garland): KRASMANN, S. 292 ff. Zur situativen Prävention bzgl. Videoüberwachung, siehe etwa LINGG, S. 33 ff.

1127 Zu Studien zur situativen Prävention über verbesserte Strassenbeleuchtung ist anzumerken, dass deren Erkenntnisse über Effekte nicht eindeutiger sind als diejenigen aus den Videoüberwachungsstudien, mithin nicht besonders aussagekräftig. Zudem halten die Autoren einer Meta-Studie zu diesem Untersuchungsgegenstand Erklärungen der Wirkungsweise über den ansteigenden Gemeindestolz oder die informelle Sozialkontrolle für plausibler als über die gesteigerte Überwachung oder Abschreckung. Siehe die Meta-Studie des Home Office von FARRINGTON/WELSH, S. 39.

1128 KUNZ 1987, S. 38; GRAS, S. 210; NIGGLI 1995, S. 106 mit illustrierenden Beispielen. Siehe auch oben Erster Teil, Kapitel III.G. zu den vielfältigen Umgehungstaktiken, insbesondere auch im virtuellen Raum. KAMMERER 2008, S. 304, beschreibt das unter britischen Jugendlichen verbreitete „Versteckspiel" vor den Videokameras. Siehe auch ausführlich DERS. 2008, S. 323 ff. zu Widerstandstaktiken. Vgl. die Straftäter-Befragung von SHORT/DITTON, S. 135 ff. Teils a. A. sind KILLIAS ET AL. 2011a, S. 303. GOTTFREDSON/HIRSCHI, bspw. S.

Eine situativ-präventiv die Kriminalität verhindernde Wirkung der postmodernen Kriminalitätsbekämpfungstechnologien ist somit zweifelhaft. Die verbleibenden Verlagerungseffekte – welche fast ausschliesslich dann wirksam werden, wenn die jeweiligen Massnahmen sehr einschneidend konzipiert sind oder kombiniert angewendet werden – können lediglich im Sinne einer défense sociale mittels Exklusion von Abweichlern erwünscht sein. Ziele des Gesellschaftsschutzes über die postmodernen Methoden durchzusetzen, könnte erfolgreich sein: „No-fly"-Listen, Stadionsperren oder Bewegungsprofile von Registrierten könnten die betroffenen Personen theoretisch, insofern die zur Durchsetzung erforderlichen Ressourcen vorhanden sind und die dargestellten Schwachstellen (Unübersichtlichkeit und Fehleranfälligkeit von grossen Datenbanken etc.) überwunden werden können, effektiv daran hindern, bestimmte Orte zu betreten oder verlassen. Risikopersonen und Risikogruppen könnte der Zugang zu Räumen oder freie Beweglichkeit verwehrt werden.

B. Inszenierungen

Im letzten Kapitel wurde ausgeführt, dass die postmoderne Überwachungsstrategie in westlich geprägten Demokratien kein Instrument der Unterdrückung des Einzelnen durch den Staat ist. Die Bevölkerung auferlegt sich die Überwachung selbst, wird vielleicht von verschiedenen Protagonisten dazu verführt, sich selbst zu überwachen und zu kontrollieren.[1129] Dafür müssen zwar nicht zwingend die Techniken der Überwachung selbst perfekt sein, jedoch muss zumindest ihre *Inszenierung* stimmig sein. Postmoderne Kriminalitätsbekämpfungstechnologien leben von ihrer Glaubwürdigkeit und der Reputation ihres reibungslosen Funktionierens. Das Mittel dieser Methoden ist ihr Prestige, der Schein ihrer Mächtigkeit, ihrer Wirksamkeit. Ohne (konstruierte) Erfolgsgeschichten erlischt das Interesse an ihnen.[1130]

Die Abschreckung nimmt einen hohen Stellenwert in den Kriminalitätsverhinderungsbemühungen der Verdachtsregister, Informationsverarbeitungstechniken und der Raumüberwachung ein. Die neuere juristisch-kriminologische Lehre indes entlegitimierte in den letzten Jahren eine potenziell abschreckende Wirk-

272, würden dieser Ansicht wohl widersprechen, auch wenn ihre Theorie der Selbstkontrolle für einmal im Kindesalter „falsch" geprägte Individuen, neben der Wegsperrung bzw. der Sicherung, keine andere Methode der Kriminalitätsprävention übrig lässt.

1129 SHEARING/STENNING, S. 56. Siehe oben Dritter Teil, Kapitel IV.D.

1130 KAMMERER 2008, S. 224 f., TEMME, S. 167 und sehr anschaulich GATES, S. 86.

komponente nach der anderen. So werden der negativen Generalprävention mittlerweile kaum noch positive Präventionseffekte zugestanden.[1131] Allenfalls geringfügig durch sie beeinflusst würden höchstens gewisse Deliktskategorien, wie zum Beispiel kleinere Vermögensdelikte oder bestimmte Personengruppen, wie beispielsweise Studenten oder Jugendliche.[1132] Die negative Spezialprävention scheitert unter anderem daran, dass sie von der Rationalität menschlicher Entscheidungen ausgeht. Gerade Straftäter besitzen wohl im Allgemeinen eine verzerrte Wahrnehmung der bestimmenden Faktoren der Theorie rationellen Wahlhandelns (zum Beispiel impulsives Handeln, Anstreben des augenblicklichen, anstatt des weit entfernten langfristigen Nutzens, verzerrte wirklichkeitsbezogene Risikoeinschätzung, andere Überzeugung etc.).[1133]

Die Abschreckung als präventive Zweckvorstellung soll hingegen in vielen Bereichen postmoderner Techniken als wesentliches Wirkelement fungieren. Der Glaube an Abschreckungseffekte scheint in weiten Teilen der Praxis und im Verständnis der Öffentlichkeit ungetrübt, denn in ihrer Vorstellung scheinen postmoderne Technologien mit eingebautem Verbrecherschreck ausgeliefert zu werden. Der Glaube an die Abschreckungswirkung reicht indes nicht aus, um eine solche auszulösen. Vielmehr müssen die Adressaten an die Wirkungen der *postmodernen Technologien* glauben.[1134]

Nicht, dass es schwer wäre, diese Technologien mit einer symbolischen Fassade zu versehen. Viele Personen durchschauen aber möglicherweise spätestens vor Ort das Blendwerk. Zum Beispiel wurde im Laufe der Arbeit bereits mehrfach gezeigt, dass Einstellungen und Aussagen zu den untersuchten postmodernen Technologien vor allem oberflächlich sind – sie stimmen nicht immer mit dem tatsächlichen Verhalten überein. Ohne zumindest gelegentliche, einigermassen erfolgreiche Rückmeldung beziehungsweise Reaktion verbleibt der Respekt vor der postmodernen Technologie auf der theoretischen, symbolischen Ebene, verwirklicht sich aber nicht im Verhalten der Adressaten.[1135] Die reine Wahrnehmung der Präsenz einer Kamera (ob nun funktionsfähig oder lediglich Attrappe)

1131 Anstatt vieler: NIGGLI 1995, S. 97 mit Hinweisen auf diesbzgl. Studien sowie DERS., S. 107; PRATT ET AL., S. 370 und 383 f.; MAZZUCCHELLI, S. 1337; KUNZ 2011, S. 286 f. und 291.

1132 PRATT ET AL., S. 380 f. (insb. Table 13.2) und 384; MAZZUCCHELLI, S. 1337.

1133 NIGGLI 1995, S. 99 ff.; KUNZ 2011, S. 304. Darauf weisen auch die Antworten der Delinquenten in der Befragung von SHORT/DITTON hin.

1134 KAMMERER 2008, S. 268.

1135 BORNEWASSER, S. 137 und 140 f.

durch eine erfasste Person, ohne daraus tatsächlich resultierende Beeinflussung dieser Person, legitimiert das Dasein der Kamera in diesem Sinne nicht.[1136] Der Placebo-Effekt ist unzureichend für eine wirksame Kriminalprävention, auch wenn gewisse Verhaltensänderungen beim gläubigen Betroffenen herbeigeführt werden können.[1137] Es genügt nicht, dass tatwillige Personen überzeugt sind, überwacht zu werden. Sie müssen auch davon überzeugt sein, dass ihr Tun unmittelbar danach geahndet wird oder sonstige negative Folgen nach sich zieht. Beobachteten Verstössen müssen, zumindest ab und zu, (erfolgreiche) Interventionen folgen, ansonsten wird die Überwachungsmassnahme über kurz oder lang nicht ernst genommen.[1138] Weder Register noch Raumüberwachungsmassnahmen kommen ohne handfeste Auswirkungen im Sichtbaren aus. Es reicht nicht aus, wenn der Beobachtete davon überzeugt ist, überwacht zu werden. Der Beobachter muss auf die eine oder andere Art in Erscheinung treten, obgleich es sein Prestige ruinieren kann, wenn er seine Fehler offenbart (beispielsweise, dass er eben nicht an jedem Ort eingreifen kann).[1139] Der panoptische Trick des verborgenen Beobachters beruht auf der Annahme, dass die Beobachteten vernünftig handeln. Es wird vorausgesetzt, dass diese überzeugt sind, sie würden immer beobachtet und sich deswegen wie vorgeschrieben benehmen. Sie wollen dem Beobachter daher nicht negativ auffallen, auch wenn keine Sanktionen drohen oder Vergünstigungen winken. Beide Annahmen dürfen aber nicht vorschnell als gegeben erachtet werden. Sie sind zu vereinfacht, denn Menschen treffen irrationale Entscheidungen, und der Vorgang des reinen Beobachtens oder Feststellens einer Tat, vor allem wenn dieser Vorgang lediglich durch eine Maschine verarbeitet wird, ohne irgendeine sichtbare Konsequenz, dürfte kaum die gewünschte Regung beim *Delinquenten* bewirken. Ständige Überwachung ohne Feedback lässt den beobachteten Abweichler höchstens gleichgültig gegenüber der Überwachung werden.[1140]

1136 Siehe GATES, S. 71 und 86. Damit sei KAMMERER 2008, S. 10 und NOGALA 1989, S. 166 zumindest im Grundsatz widersprochen.

1137 So KAMMERER 2008, S. 268 und 347; MARX 1985, S. 59.

1138 KRASMANN, S. 341. Keiner verneigt sich vor dem Hut Gesslers, stehen nicht eingriffsbereit dessen Häscher in der Nähe.

1139 KAWASHIMA, S. 160; BORNEWASSER, S. 137 und 140 f.

1140 Vgl. KAMMERER 2008, S. 270. Sie kann möglicherweise aber Auswirkungen auf konforme Personen haben, siehe dazu unten Vierter Teil, Kapitel IV.D.

C. Dynamiken der Technik

Postmoderne Kriminalitätsbekämpfungstechnologien entfalten zudem eine spezielle Eigendynamik. Die zugrundeliegenden Programmierungen, aber auch die zugehörige Interpretation und gesetzliche Regelung, übersteigen das Verständnis von Fachunkundigen. Nur Spezialisten vermögen die inneren Prozesse nachzuvollziehen, können indes häufig nicht so genau nachvollziehen, was ein Algorithmus im Endeffekt macht und können deshalb nicht alle Konsequenzen benennen und voraussehen, die er mit sich bringt.[1141] Als Folge operieren automatisierte Systeme mit einer Form von Eigenständigkeit, welche nicht vorgesehen ist, indem sie zum Beispiel bestimmte Personengruppen entgegen der Intention der Programmierer benachteiligen. Fehler, Verzerrungen und ungewollte Nebeneffekte führen so mitunter zu verstärkter beziehungsweise häufiger Beurteilung oder zur „unautorisierten Exklusion" von Personengruppen, die niemand erwartet hätte und die eigentlich niemand angeordnet hat oder anordnen hätte wollen.[1142] Es wurde bereits festgestellt, dass diese Technologie keine Urteilskraft für moralische Bewertungen besitzt. Dieser Mangel führt gelegentlich jedoch gerade dazu, dass diese Systeme versehentlich für moralische Urteile verantwortlich sein können.

Den Effekt verstärkend kommt hinzu, dass hochtechnisierte Systeme, Statistiken und automatisierte Methoden öfters als nahezu unfehlbar angesehen werden, insofern sie durch möglichst komplexe und undurchschaubare Prozesse gesteuert werden, hingegen im Resultat eine Situation oder Information *visuell* nachvollziehbar darstellen können (macht den Output greifbar und quasi direkt, „mit den eigenen Augen", erfahrbar). Videoaufnahmen, Analyseresultate von Computern, elektronische Datenbanken, Statistiken usw. bilden die Wirklichkeit scheinbar authentisch ab. Sie „suggerieren [dem Alltagsmenschen] Objektivität" und dieser nimmt sie in der Folge fälschlicherweise als „reine und unverstellte Fenster zur

---

1141 INTRONA/WOOD, S. 183: „In short, *software algorithms are operationally obscure*". Ebenso STEINBOCK, S. 42 f. mit weiteren Hinweisen. Vgl. COUDERT, S. 379; GILLIOM, S. 86; TOLMEIN.

1142 INTRONA/WOOD, S. 179 und 183 mit weiteren Hinweisen; STRASSER, S. 243. Vgl. INTRONA/NISSENBAUM, S. 41; COUDERT, S. 383; NOGALA 1998, S. 137. Siehe bspw. oben Erster Teil, Kapitel III.D.: Das intelligente System trifft eine Auswahl (etwa, wer dem menschlichen Überwacher als Bedrohung weitergemeldet wird), die durchaus diskriminierend sein kann, insofern der entsprechende Algorithmus nicht stimmig ist. Automatisierte Systeme können nur so neutral sein wie die vorgegebenen Kriterien etc., siehe INTRONA/NISSENBAUM, S. 41.

Welt“ wahr.[1143] Daraus folgt beispielsweise, dass andere an sich gleichwertige, glaubwürdigere oder aussagekräftigere Indizien unbeachtet bleiben oder als unstimmig beurteilt werden, weil sie als weniger objektiv gelten und weil die möglichst mathematische oder statistische „Objektivität“ zunehmend als Messlatte für die Beweiskraft dient.[1144] Darin werden erneut die Parallelen zwischen den postmodernen, technisierten Methoden und den postmodernen und neurobiologischen Kriminalitätstheorien ersichtlich. Letztere sind genau so kompliziert und letztlich einer exakten Erfassung nicht komplett zugänglich, die darauf beruhenden Dynamiken entgleiten der Kontrolle der Analysten und verselbständigen sich ausserhalb des Labors – sie präsentieren ihre Ergebnisse hingegen in verständlicher und authentisch scheinender Form.

D. Evidenzerlebnisse

Ergebnisse aus den postmodernen Methoden sind nicht evident, nicht selbsterklärend. Ihre Analyse und Einschätzung durch einen Laien oder Experten bringt einen Befund hervor, der Interpretationen, Beobachtungen und Wahrnehmungen umfasst, die nicht objektiv-wirklich sein müssen (oder überhaupt sein können). „Evidenzerlebnisse“ bei „Tatsachenurteilen“ sollten nicht mit Tatsachen verwechselt werden.[1145] Auch scheinbar „etablierte, standardisierte“ und „internen und externen Qualitätskontrollen“ unterliegende Technologien sind zu hinterfragen, desto mehr solche, zu denen noch wenig gefestigtes und wenig überprüftes Erfahrungswissen vorliegt.[1146] Ergebnisse postmoderner Kriminalitätsbekämpfungstechnologien brauchen einen Mediator, der sie in einen Kontext verortet, der übersetzt und umsetzt.

1143 BIDLO, S. 38 und 41 f. Ebenso KUNZ 2011, S. 60 f.; KAMMERER 2008, S. 175 ff.; NEUHAUS, S. 537 f.; BYGRAVE, S. 4; STEINBOCK, S. 42; HASLER, S. 44 („Hirnscanner sind Evidenzmaschinen.“). Ferner TEMME, S. 165 f.; WEBSTER, S. 18.

1144 Vgl. das illustrierende Beispiel bei MONAHAN/FISHER, S. 373: In der von ihnen beschriebenen Situation divergieren die Angaben eines Patienten und die Informationen auf seinem implantierten Identifikationschip. Das Krankenhaus vertraut den Daten auf dem Chip („the most accurate information“), anstatt den Angaben des Patienten, denn Letzterer könnte ja verwirrt sein.

1145 BENDER/NACK, S. 246. Ebenso KAMMERER 2008, S. 187 f.; BIEDERMANN/VUILLE, S. 280 f. und 294 (mit weiteren Hinweisen): „Materielle Indizien verfügen über keinen absoluten intrinsischen Beweiswert, […]“. Siehe auch TONDORF, S. 43 ff.

1146 BIEDERMANN/VUILLE, S. 279.

Die Frage ist, wem diese Aufgabe zufallen soll.[1147] Das latent Unexakte der Verbrechenslehre mittels naturwissenschaftlicher Vorgehen und Ansätze überspielen zu wollen, scheitert jedenfalls an der Komplexität sozialer Triebkräfte.[1148] Erschliessen sich uns heute schwer erklärliche, wahrscheinlich multimodal beeinflusste kriminologische Phänomene – wie beispielsweise der regelrechte Sturz der Kriminalitätsraten von ausgewählten schweren Straftaten um über 80 % in den letzten 20 Jahren in New York[1149] – nicht sofort, soll dies nicht dazu verleiten, abenteuerliche Mutmassungen mittels Schützenhilfe aus anderen wissenschaftlichen Disziplinen als Fakten auszugeben. Ratlosigkeit mit vereinfachenden Parolen zu überspielen, kann keine Lösung sein.[1150] Insbesondere dann nicht, wenn mit naturwissenschaftlicher Methodik produzierte Erkenntnisse selbst auf spekulativen Grundannahmen beruhen. Wir dürfen nicht erwarten, eine „fake scientificity" oder „Voodoo Criminology" helfe, die postmodernen Herausforderungen der Verbrechenskontrolle zu lösen.[1151] Die sicheren Patentlösungen, die Öffentlichkeit und Politik verlangen, wird eine rationale Kriminologie zwar kaum je liefern können, sie kann jedoch potenziell brauchbare Ansätze überprüfen und Problemstellen nüchtern aufzeigen. Auch wenn daraus zumeist keine eindeutigen Handlungsanweisungen zum Vorgehen gegen Delinquenten resultieren mögen, bringen relativierte Zugänge der Gesellschaft im Endeffekt einen grösseren Nutzen.

1147 Vgl. LEWONTIN 1995b, S. 43; YOUNG 2004, S. 12.

1148 Siehe LEWONTIN 1995a, S. 29: „Biology is not physics, because organisms are such complex physical objects, and sociology is not biology because human societies are made by self-conscious organisms. By pretending to a kind of knowledge that it cannot achieve, social science can only engender the scorn of natural scientists and the cynicism of humanists". Ähnlich HARCOURT, S. 239; KUNZ 2000, S. 145 f.

1149 Siehe dazu ZIMRING, S. 162 ff. M. E. spricht ein derartiger Rückgang nebenbei bemerkt gegen die Plausibilität allgemeiner Defizittheorien der Kriminalität. Plötzlich stark sinkende Kriminalitätsraten bei gleichzeitig sinkender Gefängnispopulation sind mit Theorien, die die Ursache von Kriminalität in einem persistierenden, determinierenden Defizit des Kriminellen sehen, kaum vereinbar. Im Gegenteil scheinen „kriminelle Karrieren" durchaus abwendbar, siehe ZIMRING, S. 167-170 und 185.

1150 Wird aber gerne gemacht. Dazu RANCIÈRE, S. 116: „Jeder Streit wird in diesem System zum Namen eines Problems. Und jedes Problem lässt sich auf den einfachen Mangel […] der Mittel seiner Lösungen zurückführen." Vgl. die Kritik bei KUNZ 2011, S. 182 ff.; SENN, S. 11 („trivialer Reduktionismus"); MCCABE/CASTEL, S. 343 („…people's affinity for reductionistic explanations of cognitive phenomena.").

1151 YOUNG 2004, S. 1 und 23. Vgl. sehr ähnlich HASLER, S. 22 f.; LÜDERSSEN, S. 195.

Die postmoderne Gesellschaft will hingegen oftmals nichts über sich selbst erfahren[1152], sondern einleuchtende Lösungen präsentiert bekommen, wie kriminelles Verhalten unterbunden und Sicherheit (wieder-)hergestellt werden können. Sie will leicht verständliche Ergebnisse, nicht unverständliche Theorien und Erklärungsversuche aus den akademischen Kreisen des entsprechenden Fachgebiets. Das Gewünschte kann jedoch, bei ehrlicher Betrachtung, niemand liefern. Die gesellschaftlichen Forderungen in Bezug auf Belange der Sicherheit stellen sich meist als unrealistisch und unrealisierbar heraus. Nicht selten driften deshalb postmoderne Strategien dann ins Metaphysische ab, wenn sie beginnen, bruchstückhaft und inkonzis Theorie und Praxis zu durchdringen.[1153] Oft fungieren fantasierte Schnittstellen zwischen Kriminologie und exakteren Wissenschaften als bequemes Mittel zur Kommunikation zwischen Kriminalpolitik und Öffentlichkeit, insbesondere mit der Werbung für postmoderne Technologien entsteht eine Symbiose. Die Situation wird im Besonderen dann problematisch, wenn Ergebnisse den wissenschaftlichen Diskurs verlassen und in eine populistische Kriminalpolitik dergestalt Einzug halten, dass obskure Gefahrenvorhersagen mit empirischer Präskription der Wirklichkeit verwechselt werden.[1154] Spätestens in diesem Stadium der Zweckverwendung entgleiten die gewonnenen Einsichten der Obhut der Fachgemeinschaft und geraten in einen unkontrollierbaren Strom von Mutmassungen und schablonenhaften Interpretationen.

Daraus entsteht auch der Reflex, durch objektiv individualisierende, vergleichende Klischees auf Täter schliessen zu wollen.[1155] Gerade heute dürstet es viele der biologischen Kriminalitätsätiologen in der Wüste von „nothing works" nach den kleinsten Fortschritten auf dem Gebiet des biologischen Profiling. Das Gleiche gilt für die umfassende Sicherheit fordernde postmoderne Gesell-

---

1152 Vgl. LOADER/SPARKS, S. 11.

1153 SENN, S. 6 und 8; SCHNEIDER, S. 236 f. Vgl. SLABY, S. 379; HASLER (Titel seines Buches: „Neuromythologie"). Lesenswert dazu auch MORSE, welcher übermütigen Hirnforschern sarkastisch den pathologischen Zustand des „Brain Overclaim Syndrome" diagnostiziert.

1154 Vgl. CAMPBELL, S. 79; KREISSL/STEINERT, S. 969. Vgl. zum Ganzen: HASSEMER 2000, S. 249. Derart umstrittene Ansätze können eventuell auf einer wissenschaftlichen Ebene diskutiert werden, können indessen auf einer politisierten und emotionalisierten Ebene schnell zu Feindbildern und harten Vorgehensweisen führen. Die Öffentlichkeit besitzt eine leicht beeinflussbare Meinung in furchtgeladenen Themen, vgl. NORRIS/ARMSTRONG, S. 60 ff.

1155 Vgl. zu diesem „Reflex" SCHWARZENEGGER, S. 114. Michael Hagner, Professor an der ETH Zürich, nennt diesen Reflex in der Hirnforschung im Interview bei BREDEKAMP/WERNER, S. 104, „Cyber-Phrenologie".

schaft.[1156] Es scheint aber vielmehr, als würde es sich bei der immer am Horizont sichtbaren Oase der ganzheitlichen Erklärung von Kriminalität über ein stark deterministisch geprägtes Verständnis der menschlichen Natur (unveränderliche Typisierung der Persönlichkeit oder anderer Eigenschaften), wie bei der Gewähr einer lückenlosen Kriminalitätsprävention, um einen Glückseligkeit verheissenden, aber unerreichbaren, Zustand handeln.[1157] Die postmoderne öffentliche Kriminalpolitik orientiert sich häufiger an den farbenfrohen, prächtigen oder näher scheinenden Fata Morganas anstatt an den vielleicht unscheinbareren, kargeren oder weiter entfernt liegenden realen Oasen. Mehr noch: RANCIÈRE bemerkt zutreffend, dass das Subjekt heute dazu „aufgefordert ist, alles über seine Phantasmen zu sagen und sie gänzlich zu befriedigen" und „seine Phantasmen in der Welt der vollständigen Ausstellung und der asymptotischen Annäherung der Körper in Gänze auszuleben".[1158]

E. Hyperrealität

„Disney-World" ist gleichzeitig imaginäre Wunschwelt und akzentuiertes Abbild der Wirklichkeit[1159]: Eine „Hyperrealität".[1160] Die hyperreale Komponente der postmodernen Kriminalitätsbekämpfungsinstrumente und allgemeiner der postmodernen Sicherheitsmaschinerie zeigt sich darin, dass sie gelobt und gefürchtet werden, etwas zu bewirken, das sie nicht zu bewirken im Stande sind und eingesetzt werden, um Scheinrealitäten zu beeinflussen, die (noch) nicht wirklich sind.[1161] RANCIÈRE beobachtet unter Rückgriff auf BAUDRILLARDS Überlegungen zur Simulation die „Verabschiedung eines Wirklichen, das sich nicht mehr ereignen muss, da es immer von seinem Trugbild vorweggenommen wird".[1162] Übertragen in das Gebiet der Kriminalpolitik beschreibt dieses Zitat die postmodernen Bemühungen zur immer früher ansetzenden Prävention sehr treffend. Die aktuelle Tat, der Schaden, darf nicht mehr geschehen. Entscheidend ist das

---

1156 Vgl. BAUMAN, S. 7.

1157 Vgl. auch das Sinnbild des „war on cancer" von SIMON, S. 264. Vgl. KUNZ 2011, S. 372; DERS. 1997, S. 17; KAMMERER 2008, S. 33.

1158 RANCIÈRE, S. 129.

1159 Vgl. dazu BAUDRILLARD, S. 24 ff. Das zeigt sich u. a. in der Struktur der Abläufe, der Ordnungssucht, der vermittelten Unternehmensideologie, der kindlichen Freude der Parkbesucher etc.

1160 BAUDRILLARD, S. 10. Vgl. auch BOGARD, S. 70.

1161 Siehe dazu BOGARD, S. 70.

1162 RANCIÈRE, S. 113.

Trugbild, das aus subjektiven Einschätzungen, Inszenierungen, Wunschvorstellungen etc. entstehende Konstrukt „Kriminalität". Die Polizei soll vor potenziellen, ja virtuellen Gefahren schützen. Sie soll vorausberechnen, wo Probleme entstehen werden und die antizipierten Bedrohungen bereits im potenziellen, ja virtuellen Stadium an ihrer Manifestierung hindern.[1163] Das Bild, das sich dabei als Gesellschaftsidentität ausgibt, hingegen lediglich eine Projektion von Phantasmen der Gesellschaft ist oder aus pseudo-wissenschaftlichen Mutmassungen besteht, erwacht, weil es der Gesellschaft als Identität vorgehalten wird.[1164] Das Reale wird ersetzt durch seine Simulation, das Risiko.[1165]

Postmoderne Kriminalitätsbekämpfungsstrategien äussern sich in einem Bewältigungskonzept, das man „hyperpräventiv" nennen könnte. Postmoderne Kriminalitätsbekämpfung bedeutet nicht Ursachenbehebung, was eine konsequent vorgelagerte Strategie ja bedeuten müsste, sondern *Symptombekämpfung* im möglichst früh ansetzenden Stadium.[1166] Hyperrealität in der Kriminalitätsvorsorge bedeutet demnach auch, dass sich die Devianz, das Symptom, zum Primärziel und alleinig zu bekämpfenden Problem wandelt und die (gesellschaftlichen) Ursachen hinter einem Schleier verschwinden. Positive wie negative *Vorstellungen* über Sicherheit, über postmoderne Strategien und Technologien rücken in den Vordergrund, praktische Erkenntnisse über deren Effekte und tatsächliche Möglichkeiten in den Hintergrund. Interventionen zielen auf das antizipierte Risiko in der Zukunft, eine Reaktion in der Gegenwart wird bereits als Misserfolg bewertet. Umgekehrt werden Misserfolge von postmodernen Technologien als vorübergehende, überwindbare Nebensächlichkeiten gedeutet – zukünftige Technologien werden das bereits bei der letzten Technikgeneration Versprochene sicherlich erbringen können. Das Ideal der perfekten Kriminalitätskontrolle durch diese Technologien bleibt daher scheinbar immer möglich, immer erreichbar.

Hyperpräventive Vorgehensweisen verströmen Ungewissheit[1167]: War es die biometrische Kamera, die die Risikoperson davon abhielt, ein Delikt zu begehen? Bestand überhaupt ein Risiko? Wäre auch ohne die Überwachungstechnologie nichts geschehen? Hätte das verwirklichte Risiko durch ein Mehr an technisierten Massnahmen verhindert werden können? Das hyperpräventive Vorgehen

---

1163 Vgl. BOGARD, S. 60.
1164 Vgl. RANCIERE, S. 115.
1165 Vgl. BOGARD, S. 59 f.
1166 KAMMERER 2008, S. 92.
1167 BOGARD, S. 60 f.

findet somit auf einer losgelösten Ebene statt, jenseits vom Bestehen einer echten Bedrohung, auch wenn es zuweilen echte Bedrohungen verhindern kann. Es basiert nicht auf Sicherheits*erfordernissen*, sondern auf Sicherheits*bedürfnissen*.[1168]

Die dargestellten Technologien entfesseln zudem Echos und Rückkoppelungen. Entwickeln, verändern oder bedienen wir diese Techniken, entwickeln, verändern und bedienen sie gleichsam uns. Risikologiken und Effizienzrationalitäten übertragen sich auf die Bediener.[1169] Funktionieren technisierte Massnahmen nicht, werden die Gegebenheiten so angepasst, dass sie es tun, anstatt die Technologien in Frage zu stellen[1170]: Videoüberwachung profitiert von einer freien Sicht auf die überwachten Plätze, also werden die Plätze baulich offen gestaltet. Rasterfahndungsähnliche Methoden profitieren von umfassenden Datenbanken über möglichst jeden Lebenssachverhalt, also lassen wir es zu, immer neue und grössere Datenbanken zu betreiben oder bestehende zu durchsuchen. Wir verhelfen den postmodernen Technologien somit *künstlich* zu mehr Wirksamkeit, indem wir Situationen an sie beziehungsweise ihre Arbeitsweise anpassen. Kurz: Die postmodernen Kriminalitätsbekämpfungstechnologien evozieren Vorstellungen über sich selbst.[1171] Durch Rationalitäten der Sicherheit wird ihre zukünftige Daseinsberechtigung gesichert, indem Gegebenheiten zu ihren Gunsten zurechtgebogen werden. Die Bewegungen und Verhaltensweisen des Menschen sind am einfachsten zu erfassen, wenn sie gleich Datenströmen „synchronised, serialized, and standardized“[1172] gelenkt werden. Schliesslich führen diese Technologien zu einer Art Invokation: Sie ersetzen die bestehende Denkstruktur des Anrufers (des Staats, der Gesellschaft etc.) allmählich durch ihre eigene. Die Gesetzmässigkeiten der Technologie werden mehr und mehr bestimmend für das Vorgehen gegen Kriminalität, Sozialkontrolle und das Rechtssystem insgesamt. Nicht im Sinne einer Herrschaft der Technik, sondern im Sinne einer durch die Technik geleiteten Lebensgestaltung und der Aneignung technikbesetzter Denkmuster und Strategien.[1173]

1168 Vgl. BOGARD, S. 61.

1169 NOGALA 1989, S. 5; DERS. 1998, S. 264 und 284; NOGALA/SACK, S. 146; KRASMANN, S. 329. Vgl. HARCOURT, S. 3, 32, 36 und 173; TINNEFELD/BUCHNER/PETRI, S. 50.

1170 Vgl. dazu KAMMERER 2008, S. 350; NOGALA 1998, S. 138 f.; NOGALA 1989, S. 88 und 137 mit weiteren Hinweisen.

1171 Gl. A. wie NOGALA 1998, S. 137.

1172 BOGARD, S. 59.

1173 Siehe STRASSER, S. 243; NOGALA 1998, S. 137 f. und 264; KRASMANN, S. 322; FÜRNKÄS, S. 206 und 214.

VI. Schlussfolgerungen

Viele der in der Literatur vorgeschlagenen Bezeichnungen verfehlen, die Situation in allen Dimensionen zu erfassen oder beschreiben eine Extremsituation, die zumindest auf die Lage in der Schweiz nicht zutrifft. Der Versuch einer exakten Typisierung setzt Schwerpunkte und ruft oftmals falsche Assoziationen hervor.[1174] Gerade die eklektische Wandelbarkeit und Anpassungsfähigkeit postmoderner Überwachnungstechnologien zeichnen diese aus, im positiven wie im negativen Sinn.

Für die und mittels der vorgestellten Technologien der Kriminalitätsbekämpfung werden Risikokategorien geformt. Durch ihren Einsatz werden in erster Linie Risikogruppen und -personen fokussiert, indem diese unter anderem durch situative Prävention von bestimmten Räumen ferngehalten, ohne konkrete Verdachtsmomente eingehender beobachtet und beurteilt sowie, wenn sie die erforderliche Eigenleistung an Normbefolgung und Unverdächtigkeit nicht erbringen, an den Rand der Gesellschaft gedrängt werden. Dadurch entstehen Vorgehensweisen, die gleichzeitig versicherungsmathematisch kalkulierend als auch gestützt auf Kriterien objektivierend arbeiten. Einer der wesentlichen Mechanismen ist somit der Ausschluss von unerwünschten Personen[1175], ein anderer die Inszenierung der einzelnen Massnahmen unter anderem zur Kommunikation mit der Bevölkerung.[1176] Diese Mechanismen üben indirekt Sozialkontrolle aus. Freiheit und Freiwilligkeit werden suggeriert, anstatt offen Zwang ausgeübt.[1177] Der Effizienzgedanke, der ihnen innewohnt und zugleich erste Priorität hat, ist auf Strategien der Selbstaktivierung und Eigenverantwortung sowie auf (scheinbar) wissenschaftlich objektivierte Kriterien angewiesen. Denn zum einen kann der Staat die Sicherheit, die das Prestige dieser Technologien verspricht, nicht alleine leis-

---

1174 M. E. überzeugend nähern sich SIMONS „Zugangsgesellschaft", YOUNGS „Exklusionsgesellschaft", DELEUZES „Kontrollgesellschaft" oder SINGELNSTEIN/STOLLES „Sicherheitsgesellschaft" der Richtung, in welche die gesellschaftlichen Entwicklungen weisen. Siehe dazu etwa KRASMANN, S. 63 und 252; SCHMIDT-SEMISCH, S. 86 ff. und 217 Fn. 89; SINGELNSTEIN/STOLLE 2012, S. 121-123; YOUNG 1999.

1175 SINGELNSTEIN/STOLLE 2012, S. 133, sprechen von einer „Renaissance des Ausschlusses als Technik sozialer Kontrolle".

1176 Vgl. etwa VOLKMANN, S. 216 f.

1177 SINGELNSTEIN/STOLLE 2012, S. 136 und 138 f. Vgl. auch FOUCAULT 2005, S. 233: „Die Existenz dieser permanenten kleinen inneren Gefahr gehört zu den Voraussetzungen für die Akzeptanz des Kontrollsystems. Deshalb räumt man der Kriminalität in Presse, Radio und Fernsehen aller Länder der Erde so viel Platz ein, als wäre sie jeden Tag eine Neuigkeit."

ten und zum anderen können die Technologien Effizienz oft nur dann erbringen, wenn die zu erfassende oder zu analysierende Welt an ihre Arbeitsweise angeglichen oder in ihre Sprache übersetzt wird.

Der Grossteil der Varianten wird in Szene gesetzt, sowohl von Unterstützern (hinsichtlich grosser Wirksamkeit) als auch von Gegnern (hinsichtlich dramatischer Konsequenzen).[1178] Die dargestellten postmodernen Technologien ermöglichen wohl weder eine utopische Gemeinschaft ohne Kriminalität noch vermögen sie, ein dystopisches Orwellsches Szenario zu errichten.[1179] Jedoch lenken derartige Stories – dramatisierte Nachrichten, propagandistische Berichte und romantische Zukunftsvisionen – den Dialog von den tatsächlichen Möglichkeiten und Konsequenzen der Überwachungstechnologien in der Gegenwart ab.[1180] Durch die Debatte um diese Extreme gehen vielleicht kleinere, jedoch hilfreiche Erleichterungen unter, welche die postmodernen Technologien in die Kriminalitätskontrolle mit einbringen; ebenso werden aber oftmals auch die vielen einzelnen, zunächst unspektakulären, jedoch nicht unproblematischen Zugeständnisse und Unbilligkeiten übersehen.[1181] Als Beispiele aufzuführen sind die Fälle des aus Einkaufszentren vertriebenen Bettlers, des auf einem Areal nicht genehmen Jugendlichen oder des aus Städten verbannten Pädophilen.[1182]

Die Öffentlichkeit scheint Aufsehen erregende, grossangelegte Überwachungsaktivitäten zwar zu skandalisieren, derartige Vorgehensweisen im kleineren Rahmen aber zu akzeptieren. Problematisch sind nicht in erster Linie die sensationsträchtigen Einzelfälle, sondern die vielleicht unspektakulär scheinenden Reformen, die schleichend zu prägenden Veränderungen führen.[1183] Diese Reformen werden vermehrt in verschiedenen Bereichen durchgeführt. Durch sie wird stetig ein Komplex modelliert, durch den der Einsatz anlassloser, heimlicher Überwachungstaktiken als eine übliche Strategie des Vorgehens gegen Krimina-

---

1178 Vgl. KLEIN, S. 93 f.; NOGALA 1998, S. 320.

1179 Die dafür erforderliche Perfektion der Überwachung ist „nicht *erreichbar*" (POPITZ, S. 10).

1180 Vgl. GROEBNER, S. 176. Auch „düstere Sozialgemälde" der Zukunft in Literatur und Film evozieren vermutlich durchaus normalisierende Einstellungen gegenüber den an sich negativ beschriebenen „totalitären Lösungsmustern", siehe STRASSER, S. 244.

1181 Vgl. SOLOVE 2007, S. 768 f.: „At the end of the day, privacy is not a horror movie […]."

1182 Siehe etwa YOUNG 1999, S. 19 f.

1183 So bspw. der allmähliche Bedeutungsverlust von rechtlichen Instituten wie dem Verhältnismässigkeitsprinzip oder von Grundrechten (siehe dazu unten Vierter Teil, Kapitel IV.C. und V.D.).

lität etabliert wird[1184] und durch den Risikopersonen von der Teilnahme am gesellschaftlichen Leben ausgeschlossen werden.[1185] Das hauptsächliche Problem dieser postmodernen Massnahmen der Kriminalitätsbekämpfung stellt also, zumindest in den westlichen Demokratien, nicht die Entstehung eines totalen Überwachungsstaats dar, sondern vielmehr die Konsequenzen derselben für bestimmte, zu gesellschaftsuntauglichen oder störenden Elementen hochstilisierte Personengruppen.

Nicht der (böswilliger) Staat[1186] ist für diese Entwicklungen (alleine) verantwortlich, sondern auch wir, die Mitglieder der Gesellschaft. Die postmodernen Überwachungs- und Registrierungstechnologien dienen den Sicherheitsbedürfnissen der Bevölkerung, nicht Unterdrückungsfantasien des Staates.[1187] Der überwachende Staat in der postmodernen Gesellschaft ist ein Akteur unter vielen. Er überlässt Kompetenzen einerseits anderen Akteuren und distribuiert sie andererseits zurück an die Gesellschaft. Die Gesellschaft wird wieder aktiver Protagonist der Kriminalitätsbekämpfung. Der Staat tritt nicht mehr alleine als handelnder, ausführender, agierender Stellvertreter der, wie auch immer verstandenen, „volonté générale" auf. Die Gesellschaft beteiligt sich nicht mehr nur aus dem Hintergrund mit Debatten, Vorschlägen usw. am Vorgehen gegen Kriminelle, sondern soll oder will direkten Einfluss auf das entsprechende Tagesgeschäft nehmen. Die sich daraus ergebenden vigilanten Taktiken und Methoden sind unter anderem wenig eingeschränkt durch rechtsstaatliche Prinzipien, die staatliche Behörden zur Zurückhaltung anweisen. Den Überwachungstaktiken Grenzen zu setzen, bedeutete einen Preis zu bezahlen (der möglicherweise direkter sichtbar ist und deshalb lieber vermieden wird). Die offensichtliche Bequemlichkeit, die eine Gesellschaft der Teilungspraktiken für uns Inkludierte und die beispielsweise auch viele der modernen Kommunikationsgeräte und Computersysteme mit ihren automatisierten Datenbanken im Alltagsleben mit sich bringen, ist jedoch zu verlockend.[1188] Die postmodernen Rationalitäten versprechen also ein bequemeres Leben und Geborgenheit. Im Gegenzug verlangen sie unter anderem

---

1184 Vgl. etwa HASSEMER 1995, S. 483.

1185 Siehe SCHMIDT-SEMISCH, S. 86 ff. und 195. Das gilt natürlich ebenso für virtuelle Räume, vgl. etwa BECKER K. B., S. 203 f.

1186 ZURAWSKI, S. 11.

1187 Vgl. SZUBA, S. 23; SINGELNSTEIN/STOLLE 2012, S. 158; YOUNG 1999, S. 78. Die „Duldung und Akzeptanz vielfältiger Kontrolle im Alltag" (BIDLO, S. 45) beruht insofern auf unseren Begehrlichkeiten.

1188 ROTHE, S. 70; CHESTERMAN, S. 251. Vgl. GILLIOM, S. 124.

Kooperation und Unterordnung unter bestimmte, dem Strafrecht locker angegliederte Verhaltensvorschriften. Unterstützung und Verständnis kommt jenen zuteil, die kooperieren.[1189]

Der Einzug der Postmoderne hatte eine starke Heterogenisierung der Gesellschaften zur Folge, sie brachte Unordnung in das zuvor relativ klar geordnete Leben.[1190] Die Ordnung soll, unter anderem durch technische Massnahmen, wiederhergestellt werden. Die Postmoderne machte das Leben weniger vorhersehbar. Die verlorene Zukunftssicherheit soll daher durch vorausschauende Technik kompensiert werden. Die Gegentaktik besteht mithin darin, die Gesellschaft (neu) zu kartieren, um sie zu regieren: „Die Bevölkerung wird zum Objekt des Wissens, der Beobachtung und zugleich zum Gegenstand der Regierung."[1191] Vielleicht kann ein an YOUNGS „loosening of the moorings" der Postmoderne angelehntes Sinnbild die folgenden Gedankengänge veranschaulichen[1192]: Wo das Leben früher in einer Gemeinschaft auf einem Passagierschiff stattfand, das zu klar vorgegeben Zeiten klar vorgegebene Häfen ansteuerte, scheinen die heutigen Menschen alleine oder in kleinen Gruppen auf mehr oder weniger grossen Segelbooten dahinzutreiben; dem Wind ausgeliefert und ohne klare Zielhäfen. Die Segelboote stehen in ständigem Kontakt zu anderen Segelbooten und werden ständig darüber informiert, was auf anderen Segelbooten (Schreckliches) geschieht (zum Beispiel Überfälle durch Piraten). Die Segelboote können zwar, anscheinend frei, überall hinfahren, sind aber doch stark abhängig von gewissen Notwendigkeiten und bedroht von unkontrollierbaren Naturgewalten. Die Bürger sehnen sich daher nach dem Leben auf (luxuriösen und sicheren) Kreuzfahrtschiffen.[1193]

Angestrebt wird aber nicht Homogenität. Angestrebt werden klare, abschätzbare, berechenbare Verhältnisse. Zugeschriebene Unterschiede und alternative Lebensstile dienen im Gegenteil als Orientierungspunkte. Ohne abgrenzbare Merkmale funktionieren Risikologiken und Strategien des Sicherheitsmanagements nicht. Die Referenz auf „das Andere" ist essentiell für die Projektionen

---

1189 Siehe dazu KRASMANN, S. 139 f. mit weiteren Hinweisen. Wer sich nicht selbst reguliert, disqualifiziert sich selbst.

1190 Siehe etwa SINGELNSTEIN/STOLLE 2012, S. 22.

1191 KRASMANN, S. 79.

1192 YOUNG 2004, S. 2 ff.

1193 Kreuzfahrtschiffe für Bürger und Privilegierte, Galeeren für unerwünschte und gefährliche Personen, für Risikoträger.

des Bürgers, für dessen Selbstbestätigung und letztlich, um postmoderne Logiken aufrechtzuerhalten.[1194] Die Fronten im postmodernen Staat sind aber zunächst nicht klar, weswegen sie klar gemacht werden müssen. Auch hier hilft das DELEUZEsche Sinnbild des Unternehmens im Vergleich zur Fabrik, die daraus folgende Entwicklung zu verstehen. Wo früher der Staat (also die Fabrik) dem Individuum gegenüberstand und Letzteres vor dem Ersteren beschützt werden musste, fiel der Staat über die Zeit aus dieser Konstellation beinahe ganz weg (an dessen Stelle trat das körperlose Unternehmen). Sicher ist heute nur, *dass* der Bürger beschützt werden *will* und daher *muss*; vor wem, steht zunächst nicht fest. Das Unternehmen fördert „Rivalität als heilsamen Wetteifer und ausgezeichnete Motivation, die die Individuen zueinander in Gegensatz bringt, jedes von ihnen durchläuft und in sich selbst spaltet."[1195] Die vormalige Abgrenzung des „wir" (der Bevölkerung, der Bürger) vom (obrigkeitlichen, hoheitlichen) Staat löst sich auf und ist fortan „unter uns" zu suchen. Um diese Ordnung wirkungsvoll am Laufen zu halten (und nicht zuletzt, um allenfalls opponierendes Reflektieren müssig zu machen), beliefert die Maschinerie die Bürger mit sich verändernden und vagen Feindbildern zur Differenzierung[1196] sowie einleuchtenden Legitimationsargumenten für das eigene Handeln und unterhaltsamen, bildlichen Wirksamkeitsnarrativen postmoderner Technologien[1197]. Die Kommunikation richtet sie an die Herde. Jeder versteht die harmonisierten Botschaften; diese sind aber nicht auf Individuen abgestimmt.[1198]

Durch postmoderne Strategien wird kommuniziert, mit ihnen wird abgelenkt und werden zufriedenstellende Geschichten erzählt. Direkte Kontrolle kann und muss

---

1194 Vgl. YOUNG 1999, S. 104 f.; SCHMIDT-SEMISCH, S. 67 f. und 71 ff.; KUNZ 2002, S. 734; HESSDÖRFER/BACHMANN, S. 173; GROEBNER, S. 180 und 182; BOGARD, S. 68 f.: „They are the «engineering» schemas that separate normal from abnormal populations, truth from falsity, reality from illusion, sanity from madness. In all cases, the code organizes a territory of control and divides one population from another, or compounds forces to produce integrated functions."

1195 DELEUZE 1993b, S. 257.

1196 BOGARD, S. 64: „Empire no longer functions, in other words, to suppress differences, but to produce and micro-manage differences at both the level of content and expression." Der neue Gegner darf indes keiner sein, der mir gleicht, der gar im selben Boot wie ich sitzt oder denselben Anspruch auf einen guten Lebensstandard hat wie ich, sondern muss sich von mir, bestenfalls selbstverschuldet, durch negative Eigenschaften unterscheiden lassen.

1197 Vgl. FÜRNKÄS, S. 204 f.

1198 Siehe SHEARING/STENNING, S. 55, zu den Botschaften („messages") an die Besucher von „Disney-World". Die kommunizierten Klassifizierungen sind, wie dargestellt, oft konstruiert, oft in diesem Sinne *hyperreal*.

durch sie hingegen nicht erreicht werden. Die indirekte Bürgerlenkung über die Angst vor dem anderen und dem drohenden Risiko[1199] bezweckt vor allem, die Gesellschaft und den Einzelnen zu ermutigen, ökonomisch-effiziente Tugenden, beispielsweise den Erhalt von Arbeitskraft, das Sauberhalten des kauffördernden Kitschs in den Innenstädten, die Anregung der Politik durch brisante Themen, Arbeit für die Sicherheitsindustrie, die Beruhigung subjektiver Sicherheitsfantasien besorgter Bürger etc., auszuformen und zu verinnerlichen. Die „schreckliche permanente Fortbildung" in DELEUZES Konzept der Kontrollgesellschaft[1200] zielt in der Teilungspraktiken anwendenden Gemeinschaft nicht auf die charakterliche Kultivierung der Gesellschaft, des sozialen Gefüges oder der Individuen in der Gesellschaft, sondern auf die Konstituierung von nützlichen Verhaltenskonventionen. Sie bedient sich der Moral als Mittel dafür, die Effizienz gesellschaftlicher Abläufe zu fördern und hinderliche Schranken abzubauen.

Mittels Teilungspraktiken der postmodernen Technologien werden dadurch diejenigen ausgegrenzt, die einerseits vom Richtmass in störender Manier abweichen und andererseits leicht zu fassen und/oder leicht zu dämonisieren sind. Eine Scharade ist dabei die geschickte Verschiebung der Methoden der Bekämpfung von Grossbedrohungen auf das Vorgehen gegen unerwünschtes Verhalten und Kleinstkriminalität und letztlich auf Sozialkontrolle.[1201] Dort nämlich zeigen die Methoden gewisse Wirkungen, vergebens können sie ja keineswegs entwickelt worden sein.

1199 An das monströse Andere und die allgegenwärtigen Risiken erinnern uns etwa die Medienberichte und sichtbar platzierte Kamerainstallationen.

1200 DELEUZE 1993a, S. 251.

1201 NOGALA 1998, S. 81. Siehe auch KRASMANN, S. 315 ff.

VIERTER TEIL:
ZUSAMMENFÜHRUNG DER ERGEBNISSE

I. Rekapitulation der Leistungspotenziale postmoderner Kriminalitätsbekämpfungstechnologien

Die vorliegend untersuchten postmodernen Kriminalitätsbekämpfungstechnologien, das konnte im Teil zum Stand der Technik festgestellt werden, zeigen häufig geringe oder ambivalente Wirkungen, weisen grosse Schwachstellen auf und enttäuschen damit oftmals die in sie gesetzten Hoffnungen und die an sie gestellten Ansprüche. Zuweilen ist schwer einzuschätzen, ob und gegebenenfalls welche Wirkungen sie zeitigen: Ihnen kommt höchstens eine geringe abschreckende Wirkung zu. Tatgelegenheiten werden durch sie in der Regel ebenfalls nicht verhindert oder ansonsten vor allem verlagert. Durch Verlagerungseffekte oder bewusst angeordnete Verdrängungs- oder Sicherungsmassnahmen (so etwa die Sexualstraftäterregister in den USA) werden schwer kontrollierbare Ballungsräume generiert. Durch Konzepte der postmodernen Kriminalitätsbekämpfung werden zudem Bürger direkt oder indirekt zur Selbstvorsorge aufgerufen.[1202] Schwachstellen der Verdachtsregister sind vor allem in den Folgen früh ansetzender Verdächtigungen und auf möglichst hohe Sicherheit ausgelegter Gefährlichkeitsprognosen auszumachen. Akute und konkrete Gefährder gehen in der Masse miteingetragener vermeintlicher, abstrakter Gefährder unter und werden dadurch für die Behörden unsichtbar. Da die Beurteilung der Gefährlichkeit, aufgrund derer Personen eingetragen werden, häufig zu wünschen übrig lässt, enttäuschen sowohl öffentliche als auch nicht-öffentliche Register oft das in sie gesetzte Vertrauen und das Anliegen, den staatlichen Behörden und der Öffentlichkeit ein verlässliches Instrument zur Prävention und Verfolgung von Straftaten in die Hand zu geben. Allgemein häufen postmoderne Technologien regelmässig grosse Datenberge an, die schwer zu bewältigen sind. Massenverarbeitungstechniken könnten theoretisch Abhilfe leisten, setzen aber präzise Hypothesen und gut umgesetzte Algorithmen voraus. Die neuen, sich in Entwicklung befindlichen Technologien der kriteriengestützten, automatisierten Erkennung von gesuchten Personen oder gar des Vorausahnens von Bedrohungen oder ab-

[1202] Vgl. etwa KUNZ 2002, S. 733.

weichendem Verhalten scheinen von ihrem verlässlichen Einsatz zumindest noch weit entfernt. Für komplexere Vorkommnisse scheinen sie nicht ausreichend zuverlässig programmiert werden zu können, da die zugrunde liegenden Profil-Kriterien beziehungsweise Merkmale wohl nicht im erforderlichen Masse objektivierbar sind. Die neuesten Techniken und Systeme sind nach wie vor zu überlisten (teils durch einfachste Taktiken). Lücken und Personen, welche diese entdecken, wird es immer geben. Die proaktiv-präventive Identifikation von gefährlichen Menschen mittels Werkzeugen und Vorgehensweisen, die auf dem Boden biologischer Kriminalitätstheorien entwickelt wurden, weist ähnliche, gravierende und ihrem Konzept inhärente Schwachstellen auf.[1203]

Aus rechtlicher Perspektive sind Kombinationen und Synergien zwischen verschiedenen postmodernen Technologien vor allem problematisch, weil sie die Grenzen zwischen Strafverfolgung und Prävention, zwischen reaktiven, aktiven und proaktiven Tätigkeitsbereichen und zwischen zielgerichteten, breitstreuenden und anlasslosen Massnahmen aufweichen und verschwimmen lassen.[1204] In der Praxis werden sich dahingehend viele schwer qualifizierbare Mischformen ergeben, was nicht nur die Beurteilung der gerichtlichen oder genehmigenden Behörde, sondern auch die Arbeit der anwendenden Behörden mit derartigen Instrumenten erschweren wird. Es dürfte eine gewisse Rechtsunsicherheit herrschen; der Anwender kann sich nicht sicher sein, dass getroffene Massnahmen einer (nachträglichen) Überprüfung durch eine übergeordnete Instanz standhalten. Und zeigten automatisierte Technologien keine zusätzlichen positiven Wirkungen, ist der Unterschied zum Status quo der Sicherheitslage in der Schweiz marginal oder reine Augenwischerei, brächten sie lediglich auf verschiedenen Ebenen negative Einschränkungen mit sich.[1205]

Viele der gestellten Ansprüche können durch die dargestellten Technologien der postmodernen Kriminalitätsbekämpfung nicht erfüllt werden. Lediglich in bestimmten Bereichen kann deren Nutzen festgestellt werden:

- Die Videoüberwachung zeitigt wahrscheinlich *irgendwelche* Effekte. Etwa in Parkhäusern beziehungsweise auf Parkplätzen scheint sie die gewünschten Wirkungen entfalten zu können. In den meisten Bereichen können hingegen nur vage Vermutungen zu ihrer Wirksamkeit geäussert werden. Eine gewisse

[1203] Siehe oben Erster Teil, Kapitel III.; Dritter Teil, Kapitel II.B.; Dritter Teil, Kapitel V.D.
[1204] Siehe oben Zweiter Teil.
[1205] Vgl. oben Dritter Teil.

präventive Wirkung auf Kleinkriminelle sowie auf grundsätzlich unerhebliche Abweichungen und Einflüsse auf die konforme Bevölkerung (einige davon ungewollt und sich nachteilig bemerkbar machend) sowie teilweise Verlagerungseffekte konnten festgestellt werden.[1206] Die Videoüberwachung kann die gefahrenabwehrende Behörde unterstützen, insoweit die Aufnahme unmittelbar an eine Intervention gekoppelt ist. Dies kann namentlich bei der Live-Überwachung und bei der Einsatzleitung über Kameras der Fall sein. Voraussetzung ist dabei immer, dass entweder die menschlichen Bediener oder die entsprechenden Programme die auf die Bildschirme projizierten Bedrohungen sofort erkennen und sofort eingreifen oder die Informationen an Einsatzkräfte vor Ort weiterleiten. Diese Bedingungen überfordern die meisten heutigen Videoüberwachungssysteme, insbesondere, weil ihnen nicht genügend Personal zugeteilt werden kann. Automatisierte Systeme der nächsten Generation versuchen dieses Problem zu überbrücken, liefern aber (noch) kaum verlässliche Analysen, die für den Einsatz im Umfeld der Kriminalitätsbekämpfung nutzbar sind.[1207]

- Virtuelle Überwachungsmassnahmen teilen diese Problempunkte analog. Hinzu kommen technisch bedingte Schwierigkeiten, welche zu kaum begrenzbaren überschiessenden Funktionalitäten und Problemen der Systemsicherheit und des Missbrauchs dieser Technologien führen.[1208]
- Eine nahezu flächendeckende Raumüberwachung, sollte sie dereinst möglich sein, erlaubte es eventuell im Nachhinein, Tatvorgänge Schritt für Schritt zu rekonstruieren.[1209] Das Überwachungsnetz müsste aber lückenlos jeden Ort überwachen.[1210] Allerdings ist dieser Anspruch, insbesondere aus Ressourcegründen, faktisch an wenigen Orten zu verwirklichen. Es bleiben des-

---

1206 Sie wirkt wohl in denjenigen begrenzten Bereichen, in denen Abschreckung wirkt. Vgl. GILL/SPRIGGS, S. 60; KUBERA, S. 132 ff.; Erster Teil, Kapitel III.J. und Dritter Teil, Kapitel V.A. Siehe aber auch GILL/SPRIGGS, S. 61.

1207 Siehe oben Erster Teil, Kapitel III.

1208 Siehe oben Erster Teil, Kapitel III.I. und Zweiter Teil, Kapitel I.D.

1209 Vgl. etwa KAMMERER 2008, S. 35 f.

1210 Vgl. KAMMERER 2008, S. 342 f. Bsp. Monaco, wo nicht die Gebiete *mit* Videoüberwachung ausgeschildert sind, sondern diejenigen *ohne*. Die Schilder warnen vor dem Eintreten in ein *nicht-überwachtes* Gebiet – und damit vor einer Umgebung, in der sich eine Person Bedrohungen jeglicher Art quasi schutzlos ausliefert. Die monegassische Haltung in der Prävention durch fast umfassende Videoüberwachung drängt den Bürger zur Selbstverantwortung in den Zonen, die nicht überwacht sind (also in den Lücken des Überwachungsnetzes).

wegen Räume übrig, welche nicht durch eine Überwachungsanlage geschützt sind – und in welche sich die Kriminalität verlagert, sollten die Überwachungssysteme zweckgemäss wirken. Zudem wünscht sich die Gesellschaft momentan noch Rückzugsorte ohne ständige Überwachung. Abgesehen davon ist eine flächendeckende Überwachung in der Schweiz rechtlich unzulässig. Weiter ist zu bezweifeln, dass dadurch ein genereller Mehrwert für die Ermittlungstätigkeit der Polizei entstünde. Die Tatrekonstruktion mittels Material aus Raumüberwachungsinstrumenten bedeutet hohen Aufwand. In der Regel dürften die wesentlichen Tathandlungen und Tatzusammenhänge für die Ermittlungsbehörden auch ohne dieses Material über „herkömmliche" Quellen nachzuvollziehen sein. Die lückenlose, bildliche Dokumentation des Tatablaufs scheint meist keine unabdingbare Voraussetzung. Freilich könnte ein derart dokumentierter Tatablauf als Studienobjekt dienen und so der Ausbildung und Forschung dienlich sein.

- Umfangreiche Verdachtsregister und Datenbanken mit personenbezogenen Informationen eignen sich grundsätzlich zu Ermittlungszwecken, insofern sie übersichtlich und verlässlich geführt werden. Neue Methoden der automatisierten Datensondierung und -analyse (wie diejenigen von INDECT) haben, abgesehen von den angesprochenen praktischen Hürden, das Potenzial, den Nutzen derartiger Datensammlungen enorm zu steigern. Die Anwendung dieser Methode kann aber, insbesondere in einer vorgelagerten Gefahrenabwehr, mit denkbar intensiven Eingriffen in die Grundfreiheiten Einzelner oder ganzer Personengruppen einhergehen.[1211]

- Die Technologien und Methoden der automatisierten Informationsverarbeitung (Data Mining, Knowledge Discovery und Rasterfahndung beziehungsweise Massendatenverarbeitung) sind teilweise ähnlich einzuschätzen wie die Videoüberwachung. Zur Sondierung simpler, objektivierbarer Vorgänge beziehungsweise Verhaltensweisen oder von sehr typischen Merkmalen eines gesuchten Subjekts können sie, stets eingedenk, dass sie keine perfekten Schlussergebnisse liefern und diesen Methoden immer Trade-offs innewohnen[1212], teilweise nutzbringend und sinnvoll eingesetzt werden. Demzufolge können derartige Ansätze und Verfahren, um Ermittlungen in eine bestimmte

[1211] Siehe oben Erster Teil, Kapitel IV.A. und Zweiter Teil.
[1212] MARX 2007 (Fallacy 10).

Richtung zu lenken (im Sinne von Hypothesen), in bestimmten Fällen grundsätzlich hilfreich, in anderen Fällen jedoch schlicht nutzlos sein.[1213]

- Die UN-Terrorliste und die Sexualstraftäterregister in den USA dienen hauptsächlich als Sicherungsinstrumente. Diesen Sicherungszweck können sie teilweise erfüllen. Sie leisten aber wohl höchstens einen kleinen Beitrag, die Kriminalitätsrate zu verringern. Die Auflistung von *vielen* Menschen ist ineffizient. Sollen derartige Register funktionieren, dann können sie dies nur bezogen auf eine sehr begrenzte „Klientel" und beruhend auf sorgfältigen, überprüfbaren Gefährlichkeits- und Prognosebeurteilungen.[1214]

Angesichts dieser wenig optimistischen Wirksamkeitseinschätzung stellt sich die Frage, worin denn die Problematik der dargestellten postmodernen Technologien liegt:

1. Die postmodernen Technologien funktionieren (noch) nicht immer so, wie eigentlich vorgesehen, sollen aber trotzdem eingesetzt werden. Nebeneffekte, überschiessende Funktionalitäten und Missbrauchsgefahren werden teils notwendigerweise, teils als nicht ungenehme Nebenzwecke bewusst in Kauf genommen. Wirkungen auf Drittpersonen durch eine hohe Streubreite, (ausgrenzende) Stigmatisierungen oder grundlose Verdächtigungen, allenfalls inklusive zu Unrecht getroffener Folgemassnahmen, sind nur einige Beispiele für mögliche (aber im Eintrittsfall sehr reale) Konsequenzen.[1215]
2. Die Technisierung und Digitaliserung unserer Lebenswelt schreitet fort. Immer stärker vernetzbare postmoderne Technologien erlauben es unter anderem, Informationen fast beliebig aus verschiedenen Lebensbereichen (auf Vorrat) zu sammeln und bei Bedarf weiterzuverwenden.[1216] Entgegnen liesse sich, dass Technologien, die auf einem Generalverdacht beruhen, uns Normalbürger höchstens leicht betreffen und nur Verdächtige einer tiefergehenden Sondierung unterziehen. Dieses Argument leuchtet einerseits grundsätzlich ein. Andererseits ist der Generalverdacht nach der hier vertretenen

---

1213 Siehe VAN DER HILST, S. 15; SCHNEIER in Blog vom 9. März 2006; SKILLICORN 2008b, S. 68 und 72 f.; GMÜR, S. 1308 Ziff. 3.1 und S. 1318. Siehe auch oben Erster Teil, Kapitel I.F.2. Optimistischer zum Kosten-Nutzen-Verhältnis der Profilerstellung im virtuellen Raum ist NOWAK, S. 33 f.

1214 Siehe oben Erster Teil, Kapitel IV.A.

1215 Vgl. etwa VOLKMANN, S. 219. Siehe oben Zweiter Teil, Kapitel I.

1216 Vgl. etwa LSE Briefing, S. 36; THIEL, S. 75.

Ansicht nicht das wesentliche Problem der postmodernen Methoden. Ein wesentlicher Einwand liegt darin, dass automatisierte postmoderne Technologien – da das Konzept des Generalverdachts alleine nicht ausreicht, um sie effizient arbeiten zu lassen – modifiziert auf einen generalisiert-kriterienbasierten Verdacht zum Einsatz kommen.[1217] Im Klima steigender Sicherheitsbedürfnisse geraten dadurch unter anderem immer häufiger, immer abstrakter Verdächtige in den Fokus weitergehender Überwachungstätigkeit. Der Einsatz postmoderner Kriminalitätsbekämpfungstechnologien bedeutet, isoliert und selektiv betrachtet, manchmal fast unspektakulär geringfügige Opfer und Einschränkungen des Normalbürger. Werden die Technologien einzeln eingesetzt, ist der Bediener zudem nicht immer in der Lage, etwa umfassendere Profile zu erstellen.[1218] Beispielsweise zeigt sich ROGALL skeptisch gegenüber der Meinung, Rasterfahndungen erstellten Persönlichkeits-, Verhaltens- oder Bewegungsprofile.[1219] Das Problem ist, dass die dabei gesammelten Daten hingegen ohne Weiteres *ermöglichen*, Profile zu erstellen, insofern sie nicht umgehend vernichtet werden. Problematisch sind somit vielfach und insbesondere die mannigfaltigen Kombinationsvariationen und Synergien zwischen den einzelnen Technologien – zum Beispiel die Daten, die auf Vorrat gespeichert werden, um effiziente Massendatenverarbeitung zu unterstützen oder die umfangreichen Informationsgeflechte, die sich gegenseitig durch Datenverknüpfungen ergänzen, und die daraus entstehenden, vielfältig und umfassend nutzbaren Informationsbestände. Möglicherweise ergeben sich daraus negative Effekte, die sich auf die gesamte Bevölkerung auswirken.[1220]

3. Postmoderne Strategien und Technologien arbeiten mit Risikokategorien, Risikogruppen und Risikopersonen. Sie formen Bilder von riskanten Menschen und klagen Personengruppen abstrakt-universell an. Diese Wertvorstellungen werden der Bevölkerung mitgeteilt.[1221] Die Folge sind Exklusionsneigungen: Überwachungs- und Registrierungstechnologien können Strategien der défense sociale hervorrufen. Zugänge *können* durch sie ver-

---

1217 Selbst die *anlasslose* Gefahren- bzw. Verdachtsforschung muss sich, soll sie automatisiert ablaufen, an bestimmten Kriterien orientieren.

1218 Vgl. etwa ALBRECHT H. J. ET AL., S. 221: „Verkehrsdaten spielen in der Regel nur in Kombination mit anderen Ermittlungsmassnahmen eine Rolle."

1219 ROGALL, S. 625. Ebenso ZSCHOCH, S. 208.

1220 Vgl. etwa CHESTERMAN, S. 251. Siehe dazu unten Vierter Teil, Kapitel IV.

1221 MARX 2007 (Fallacy 22); STRASSER, S. 244. Vgl. auch SIEBER, S. 29.

weigert werden, insofern die entsprechenden Ressourcen vorhanden sind.[1222] Theoretisch ermöglichen postmoderne Überwachungs- und Registrierungstechnologien die Exklusion vieler als gefährlich wahrgenommener oder unerwünschter Personen(-gruppen). Die Gesellschaft, beeinflusst durch die vermittelten Ergebnisse und Verfahrenspraktiken der postmodernen Technologien, folgt diesen ausschliessenden Strategien über eine verstärkte Selbstvorsorge und Eigenverantwortung.[1223]

II. Technisierung der Kriminalitätskontrolle

A. Technologielawinen und Sicherheitsfantasien

Aus der zunehmenden Einführung und Weiterentwicklung von Raumüberwachungs-, Informationsverarbeitungs- und Registrierungstechnologien entsteht eine schwer aufzuhaltende, aber nicht unbeeinflussbare Eigendynamik.[1224] Technische Potenziale beginnen sich weiten Teilen der Polizeiarbeit aufzudrängen.[1225] Automatisierte Werkzeuge diktieren und provozieren Vorgehensweisen der staatlichen Behörden, Rahmen der Konformität und formen nicht zuletzt die Einsatzumgebung nach ihren Logiken.[1226] An technisierte Instrumente und Strategien angepasste Verfahrensweisen befördern beispielsweise Effizienzlogiken, Raumüberwachungsmassnahmen die offene und einer Überwachung leicht zugängliche Architektur.[1227] Die verstärkte internationale Kooperation führt ferner

---

1222 Vgl. GROEBNER, S. 176.

1223 Siehe etwa KRASMANN, S. 297; oben Dritter Teil, Kapitel IV.A.

1224 Vgl. NOWAK, S. 47; HILGENDORF, S. 826 und 827.

1225 NOGALA/SACK, 143 ff.; VOLKMANN, S. 222. Siehe oben Dritter Teil, Kapitel V.E.

1226 Siehe NOGALA 1989, S. 76 f. mit weiteren Hinweisen. Diese Technisierung hat auch an der im Dritten Teil, Kapitel III.B. besprochenen Entsubjektivierung einen nicht unerheblichen Anteil, vgl. BOGARD, S. 63.

1227 Vgl. etwa KUNZ 2011, S. 152. Insofern verursachen sie so etwas wie einen Anpassungsdruck auf die zu überwachende (reale oder virtuelle) Umgebung. Bspw. fördern sie freie Plätze mit klaren, offenen Strukturen, da Plätze mit vielen die Sicht verstellenden Objekten der Videoüberwachung schwerer zugänglich sind. Ein indirekter Effekt davon könnte sein, dass diese (eintönige, unkreative) Umstrukturierung von Räumen auch die Menschen prägt, die sich darin bewegen, die darin leben. Allgemein neigen situative Ansätze dazu, den Lebensstil aller im Einsatzraum zu beeinflussen und einzuschränken, siehe KUNZ 2002, S. 732.

dazu, dass Datenbanken zu Ermittlungs- und Gefahrenabwehrzwecken ausgeweitet werden.[1228]

Nicht alle dieser Technologien und Systeme, die an sich realisierbar, profitabel und/oder besonders wirksam wären, sind im Sinne der Rechtsstaatlichkeit und der Zielvorstellung einer soliden und gemeinschaftlichen Gesellschaft wünschenswert.[1229] Zudem ist, wie im Zweiten Teil der vorliegenden Arbeit dargestellt, vielen Versprechen aus der Forschung zu den Fähigkeiten ihrer neuen Technologien skeptisch gegenüberzutreten. Texte sowohl über bestehende als auch über noch zu entwickelnde Technologien der Kriminalitätsbekämpfung arbeiten vielfach mit rhetorischen Extremen. Seit den ersten Anfängen des Einzugs des Computers in die Büros der staatlichen Behörden, seit man die Potenziale automatisierter Prozesse erahnen konnte, sprachen sich Befürworter dafür aus, möglichst alle technischen Potenziale auszuschöpfen. Im Gegensatz dazu warnten Kritiker vor den möglichen Gefahren, diese Technologien zur Bekämpfung von Kriminalität einzusetzen: DETLEF NOGALA stellte vor ungefähr 25 Jahren die damaligen Argumentationsfiguren der Befürworter und Kritiker dar und bemerkte, dass viele Diskussionen auf einer unsachlichen Ebene stattfanden und auf beiden Seiten übertrieben wurde.[1230] Die Technik schritt seitdem rasch fort, die Rechtsfertigungsfiguren haben sich indes kaum geändert: Unterstützer loben heute wie damals die jeweils neuen Technologien mit häufig substanzlosen Argumenten in den Himmel, Gegner kritisieren sie in bester Endzeitmanier auf einer fiktionalen Ebene. Gemein ist beiden Begründungsmustern, dass sie von einem hohen Wirksamkeitspotenzial dieser Technologien ausgehen und den Technologien übertriebene Attribute zuschreiben. Daraus entstehende, zuweilen irreführende Utopien oder Dystopien können in einem wissenschaftlichen Umfeld nicht (alleine) Ausgangspunkt für einen konstruktiven Diskurs sein.[1231]

1228 Vgl. ALBRECHT P. A. 2003, S. 42; HEINE, S. 41 ff.; KUTSCHA, S. 1044; THÜR, S. 113; GLESS 2012, S. 5 und 18.

1229 Vgl. HASSEMER 2000, S. 265; HAYES 2009, S. 80; Marx 2007(Fallacy 1); ZERBES, S. 42.

1230 Dazu ausführlich NOGALA 1989, S. 15-40 und 71-99; ebenso DERS. 1998, S. 143 f. jeweils mit zahlreichen Hinweisen. NOGALA bezeichnet den Schlagabtausch zwischen den beiden Extrempositionen als „Abwiegler vs. Paranoide", die „Euphorie" oder „Schock und Empörung" verbreiten (NOGALA 1989, S. 96; DERS. 1998, S. 320).

1231 MARX 2003, S. 371; GROEBNER, S. 175 f. Allzu schnell beruft man sich auf Seiten der Überwachungsgegner auf vermittelte Bildnisse eines skrupellosen Überwachungsstaats. Utopien und Dystopien zeichnen Bilder von Zuständen, die nicht sind und so auch nie sein

NOGALA brachte die bescheidene Bilanz der technisierten postmodernen Methoden im Jahr 1998 bestens zum Ausdruck: „Die *«technical fixes»* für Probleme sozialer Kontrolle erweisen sich angesichts einer vielschichtigen, dynamischen und anpassungserfahrenen sozialen Praxis oftmals schlicht als *zu teuer, dysfunktional, mit unerwünschten Nebenfolgen behaftet oder aus politischen beziehungsweise kulturellen Gründen unakzeptabel*.“[1232] Auch Jahre später und in Hinsicht auf die zu erwartenden Entwicklungen aus Projekten wie dem INDECT müssen diese Beschreibung hinsichtlich der Leistungspotenziale postmoderner Kriminalitätsbekämpfungstechnologien nicht wesentlich revidiert werden. Zwar werden Technologien regelmässig verbessert (etwa hinsichtlich ihrer Speicherkapazität) und um immer neue Funktionen erweitert. Viele der wesentlichen (technischen) Schwachstellen und Hindernisse konnten aber noch immer nicht gelöst werden.[1233] Die Öffentlichkeit nimmt das Leistungspotenzial dieser Technologien jedoch völlig anders wahr. Oftmals beruht die Daseinsberechtigung dieser Technologien lediglich auf einer oberflächlich symbolischen oder (populär) politischen Ebene. Ihre zunehmende Ausbreitung im Bereich der Kriminalitätsvorsorge ist daher bedenklich.

Neben dem Herstellen objektiver Sicherheit zielen postmoderne Kriminalitätsbekämpfungstechnologien vordergründig zudem darauf hin, die subjektive Sicherheit, das heisst das Sicherheitsempfinden der Gesellschaft, positiv zu beeinflussen.[1234] Es ist aber zu bezweifeln, dass *darin* die Stärke dieser Instrumente liegt. Die Modelle des Kriminalitätsmanagements, auf denen diese Instrumente basieren, halten dafür keine Lösungen bereit. Im Gegenteil: Die postmodernen Konzepte sollen das Phänomen Kriminalität *regulieren*. Es ist nicht vorgesehen, durch sie Unsicherheitsgefühle zu beseitigen, sondern beabsichtigt, mit diesen zu

müssen. Jene erfinden Verknüpfungen und Folgen dort, wo sie in der Zukunft *vermutet* werden. Vgl. NIGGLI/PFISTER, N. 5 S. 519 f.

1232 NOGALA 1998, S. 270.

1233 Siehe etwa oben Erster Teil, Kapitel III.F.-J.

1234 Vgl. KUNZ 2011, S. 328 ff.; ALBRECHT P. A. 2010, S. 9; NIGGLI 1995, S. 90; GRAS, S. 212 mit weiteren Hinweisen. Die rein auf eine allfällige Stärkung des subjektiven Sicherheitsgefühls abzielende, das heisst die rein symbolisch eingesetzte postmoderne Überwachungstechnologie kann aber wohl kein hinreichendes öffentliches Interesse begründen, siehe MÜLLER L. 2011, S. 236, BÜLLESFELD 2002, S. 190 und BARTSCH, S. 186 f. bzgl. Videoüberwachung.

feilschen, über sie zu verwalten. Letztlich begünstigen sie die Nachfrage nach immer neuen Kriminalitätsbekämpfungstechnologien.[1235]

Postmodernen Kriminalitätsbekämpfungstrategien *antworten* zwar auf gesteigerte Sicherheitsbedürfnisse der Gesellschaft, *lösen* die Probleme, die sich aus diesen Sicherheitsbedürfnissen ergeben, aber nicht: Zum einen zeigen dahingehende Präventionsbemühungen oft höchstens geringe oder ambivalente Effekte auf die Kriminalitätsfurcht in der Bevölkerung.[1236] Zum anderen führen sowohl die Überwachung eines Raums als auch die Ballung von Meldungen über eine grosse Anzahl von Tätern auf einem Gebiet dazu, dass die den Raum Durchquerenden oder die Anwohner diesen Raum beziehungsweise die Nachbarschaft, für welche Personen im Verdachtsregister verzeichnet sind, als gefährlich wahrnehmen (was die Massnahmen eigentlich verhindern sollten). Dies führt vermehrt zu Unsicherheitsgefühlen. Die Unsicherheitsgefühle wiederum führen zum Ruf nach einem Mehr dieser Massnahmen.[1237] Beschäftigt sich die Gesellschaft mit ihren Unsicherheitsgefühlen, verstärken sich diese. Erfolgsgeschichten und Versprechungen von Agenturen der Risikoverwaltungen rufen hinsichtlich immer besser funktionierender Kriminalitätsbekämpfungstechnologien „Sicherheitsfantasien“[1238] bei den Bürgern hervor. Diese Fantasien werden auch bei augenscheinlichen Fehlschlägen dieser Technologien nicht nach unten angepasst. Die Kluft zwischen erfüllbaren Ansprüchen und unerreichbarer Wohlfühl-Sicherheit

---

1235 Siehe SINGELNSTEIN/STOLLE 2012, S. 43 f., 123 und 138; TROTHA, S. 231; KRASMANN, S. 110 f. und 239; KUNZ 2002, S. 730 f.; HASSEMER 1995, S. 483; ERICSON/HAGGERTY, S. 269.

1236 Siehe BOERS, S. 14; LINGG, S. 81; GILL/SPRIGGS, S. 48 und 60, welche eine Steigerung der Kriminalitätsfurcht im überwachten Raum bei Personen, die von den Kameras wussten, beobachteten. Vgl. BÜLLESFELD 2002, S. 57 f.; SCHRÖDER, S. 48. Ähnlich skeptisch sind GRAS, S. 189-196 und 212; KAMMERER 2008, S. 78 ff. A. A. ist KRABBENBORG, S. 56 und wohl auch BORNEWASSER, S. 153 ff. Auch in einer Passantenbefragung von KUBERA, S. 137 scheinen sich die Unsicherheitsgefühle im Raum vermindert zu haben.

1237 KUNZ 2011, N. 329 f.; SINGELNSTEIN/STOLLE 2012, S. 167; TROTHA, S. 231; KAMMERER 2008, S. 69 f.; Bericht HRW, S. 61 f.; Stellungnahme des Bundesrats vom 7. Mai 2008 i. S. Natalie Simone Rickli. Interessanterweise stand man exakt diesem Dilemma bereits im 19. Jahrhundert gegenüber, als die damals als quälend grell empfundene Beleuchtung der Städte und Strassen allmählich flächendeckend verwirklicht werden konnte, aber trotzdem nicht zu den damit angestrebten, die Kriminalität verringernden Zielen führte. Siehe dazu KAMMERER 2008, S. 22.

1238 ROSE, S. 87 benutzt diesen Begriff.

wächst somit ständig. Das vermeintliche Versagen wird dabei dem Justizsystem angelastet.[1239]

Die Opferzentrierung unterstützt diese Dynamiken: Übertrieben wird die Opferfürsorge, wenn der Gesetzgeber, wie in Italien, die subjektive Befindlichkeit des Opfers und die Gefährlichkeit des Umfelds dem potenziellen Täter negativ anlastet, indem er dem subjektiven Unsicherheitsgefühl und dem „urbanen Verfall" in Strafnormen den Rang von Tatbestandsmerkmalen verleiht.[1240] Diese und ähnliche postmoderne Entwicklungen ziehen die beschriebene Verkettung von Konsequenzen nach sich: Das Angstklima führt zu nebulösen Unsicherheitsgefühlen. Die verunsicherte Gesellschaft fantasiert von potenziellen Tätern, die potenziellen Opfern auflauern. Letztlich wird virtuelle anstatt potenzielle Delinquenz bekämpft, also Delinquenz die denk- oder vorstellbar ist, die aber noch nicht einmal abstrakt droht.[1241] Die subjektiven Befindlichkeiten der durch diese Fantasmen verängstigten, zu virtuellen Opfern geformten Bürger dienen als Massstab für den Umgang mit virtuellen Tätern und deren Bestrafung. Die Szenarien, Theorien und Erklärungsmuster des Bekämpfungsstrafrechts werden willkommen geheissen, denn sie passen ausgezeichnet in gesellschaftliche Fantastereien. Sie transportieren *Vorstellungen* über Sicherheit, Kriminalität etc. und manifestieren dadurch in der Wirklichkeit entsprechende Verständnisse und Bedürfnisse.[1242]

Die „Welt der Pannen" wurde als Sinnbild für die lähmende Furcht vor dem schädigenden Ereignis verwendet. Es soll aber zugleich Mahnung vor zu lautem Jubel über technische Errungenschaften sein. Technische Pannen substituieren menschliches Versagen, wo technische Errungenschaften menschliches Handeln ersetzen.[1243] Eine Analyse wird nicht automatisch präziser oder glaubwürdiger, nur, weil sie computergestützt erfolgt.

Nun kann aber nicht ausgeschlossen werden, dass Entwicklungen im technologischen Fortschritt – aus der Perspektive der Wirksamkeit – neue Voraussetzungen für sehr überzeugende Lösungen hervorbringen könnten. Es scheint deshalb

---

1239 Vgl. LOADER/SPARKS, S. 78. Auch dieser Punkt führt zu einer sich verstärkenden Spirale, wenn die Justiz darauf mit der Entschuldigung und Forderung antwortet: „Wir brauchen mehr und/oder neuere technische Mittel."

1240 Siehe NISCO, S. 76 f. mit weiteren Hinweisen.

1241 BOGARD, S. 60.

1242 Siehe dazu oben Dritter Teil, Kapitel V.E.

1243 KAMMERER 2008, S. 204.

nicht verkehrt, sich frühzeitig über eine Konstellation Gedanken zu machen, in welcher zum Beispiel automatisierte Systeme bezüglich des Delinquenzaufkommens tatsächlich bedeutende Wirkungen entfalten. Es wurde festgestellt, dass die heutige Gesellschaft vom Staat augenscheinlich verlangt, seine Bürger mit einem Geborgenheit verströmenden Kokon aus Sicherheit vor Lebensrisiken zu umhüllen. Kann er das? Soll er das? Je vernetzter und flächendeckender eine Kontrolltechnologie in den Alltag eingepasst wird, desto unverhältnismässig stärker bemisst sich aus der Gesamtperspektive die Eingriffsintensität in die Rechte aller. Es ist demnach auch das *Gesamtpaket* der eingesetzten Überwachungstechnologien zu beurteilen.[1244] Diesbezüglich könnten sich die in Entwicklung befindlichen, stark vernetzten und kombinierten Systeme voraussichtlich, sollten sie tatsächlich im geplanten Umfang realisiert werden, eine sehr hohe Eingriffsstärke aufweisen.[1245]

Ohne vorbereitete Entgegnungen könnten rechtsstaatliche oder freiheitsrechtliche Bedenken gegenüber dem Argument der Effizienz untergewichtet werden. Die Anbieter neuer Technologien haben in derartigen Diskussionen einen Kommunikationsvorsprung. Sie entscheiden weitgehend über deren Namen, Konnotationen und Zukunftsvorstellungen. Die Replik der Kritiker vermag ein derart geprägtes Image und die damit assoziierten Hoffnungen oft nicht mehr zu verändern. Da das Vermögen und die Opportunität der neuen Technologie wie selbstverständlich als Prämisse gesetzt werden, müssen Kritiker zudem regelmässig aus einer defensiv-rechtfertigenden Position argumentieren.[1246]

Fest steht, dass sich die Gesellschaft mit den einzelnen neuen Technologien befassen muss. Der technologische Fortschritt bringt tatsächlich viele Bequemlichkeiten mit sich, und er ist weder aufzuhalten noch rückgängig zu machen, allenfalls zu lenken. Unreflektierte Technophilie in der Kriminalitätskontrolle entfesselt jedoch Technologielawinen, indem ineffiziente Technik ein Synonym für veraltete oder vom Rechtssystem zu stark eingeschränkte Technik bedeutet und präventive Gefahrenabwehr scheinbar immer zu spät ansetzt, um Bedrohungen zu verhindern.[1247] Nutzlose, unwirksame Techniken sollten jedoch nicht au-

---

1244 Siehe oben Zweiter Teil, Kapitel II.C.

1245 Siehe NORRIS/ARMSTRONG, S. 221 ff. Zu den Voraussetzungen einer „total surveillance society“: DIES., S. 6 ff. mit weiteren Hinweisen.

1246 GEHRING, S. 57 ff.

1247 KAMMERER 2008, S. 67; DERS. 2011, S. 32. Vgl. MATHIESEN 1980, S. 158; NOGALA/SACK, S. 130 f.; DELEUZE 1993b, S. 257.

tomatisch ihre Nachfolgetechniken legitimieren. Antizipierte Durchbrüche in naher oder ferner Zukunft sind keine Erfolge, auf die alleine sich der Einsatz dieser Technologien stützen darf.[1248]

B. Die Problematik technisierter Sachbeweise

Technisierte Sachbeweise wie beispielsweise Videoüberwachungsaufnahmen, über Govware sichergestellte Computerdaten, herausverlangte Verbindungsdaten digitaler Kommunikation oder DNA-Proben werden zunehmend beliebter. Eine zentrale Zielsetzung, die mit technisierten Sachbeweisen verfolgt wird, ist es, „strafrechtlich relevantes Geschehen beweiskräftiger und gerichtsfester als bisher" zu machen.[1249] Technisierte Sachbeweise scheinen Abläufe und Sachverhalte gut nachvollziehen zu lassen. Sie sind nützlich, gar von „überragender Bedeutung" für die Polizeiarbeit.[1250] Teils haben sie die Kriminalistik und Forensik revolutioniert.

Es drängen sich aber einige kritische Anmerkungen auf: Technisierte Sachbeweise können das richterliche Ermessen reduzieren, indem sie Ergebnisse präsentieren, die scheinbar für sich selbst sprechen und einen Sachverhalt gewissermassen unumstösslich aufzeigen.[1251] Diese ihnen inhärente Überzeugungskraft, dieses „Gütesiegel robuster Objektivität, technischer Neuheit und wissenschaftlicher Autorität"[1252] steht im Konflikt mit dem heutigen Strafverfahren, das dem Angeschuldigten ein schützendes Gebäude von Verfahrensgarantien zugesteht. Technisierte Sachbeweise unterminieren dieses Gebäude, indem sie zum einen asymmetrische Situationen einrichten (betrifft das Gebot der Fairness und der Waffengleichheit) und zum anderen die Unschuldsvermutung auflösen sowie das Recht, das Zeugnis beziehungsweise die Aussage zu verweigern, umgehen können.[1253] Technisierte Sachbeweise drängen die Funktion richterlicher Behör-

---

1248 SLABY, S. 378; WOOD jeweils mit weiteren Hinweisen. Vgl. GATES, S. 72.

1249 NOGALA 1998, S. 61.

1250 NOGALA/SACK, S. 144.

1251 Vgl. etwa SLABY, S. 379 f., welcher diesen Überzeugungseffekt der„Macht der Bilder" zuschreibt. Teilweise a. A. hinsichtlich des Einflusses von Hirnbildern auf Laienrichter sind SCHWEITZER/SAKS.

1252 SLABY, S. 380 zu fMRT-Bildern. Ebenso kritisch zu Ergebnissen von Überwachungstechnologien MARX 2007 (Fallacy 2-4).

1253 Siehe dazu NOGALA 1998, S. 159-162 und 174; SCHWEIZER/BISCHOF, S. 282; ZERBES, S. 273 f. jeweils mit weiteren Hinweisen.

den in Richtung „Rechtsautomaten“.[1254] Herrscht zudem eine Situation vor, in der das Vorliegen bestimmter technisierter Sachbeweise zu erwarten ist (beispielsweise in Grossbritannien eine Videoüberwachungsaufnahme des Geschehens), so kann es sein, dass die beurteilenden Instanzen misstrauisch werden, falls einmal *kein* derartiger Sachbeweis vorgelegt wird. Auch dadurch rufen bereits entgrenzt angewendete postmoderne Kriminalitätsbekämpfungstechnologien eine noch stärkere eigene Ausweitung hervor, indem mehr oder zuviele Sachbeweise immer besser zu sein scheinen, als einen Sachbeweis zu wenig zu haben.[1255]

Die technisierten Sachbeweise geniessen aber ein zu gutes Ansehen. Das Gütesiegel verdanken sie in erster Linie ihrem Ruf, Abläufe und Sachverhalte *authentisch* zu konservieren. Postmoderne Technologien sammeln keine Sachbeweise, sie stellen Sachbeweise her.[1256] Es können beispielsweise beim Kopieren Fehler geschehen. Auch nehmen intelligente Überwachungssysteme immer direkt Änderungen unter anderem am Informationsgehalt vor.[1257] Durch die automatisierte Verarbeitung von Daten können wesentliche Aspekte verloren gehen, oder es können sich etwa durch das Verknüpfen von Daten aus sozialen Netzwerken verzerrte Bilder einer Person („Fremdbilder“) ergeben.[1258] Weiter zeigen derartige, technisierte Sachbeweise oft Momentaufnahmen und selektive Ausschnitte, was insbesondere Auswirkungen auf ihre Aussagekraft haben kann.[1259] Die Technologien sind zudem zuweilen „stör- und irrtumsanfällig“ und deren Ergebnisse „interpretationsbedürftig“.[1260] Der resultierende technisierte Sachbeweis ist ein vermitteltes, ein interpretiertes Ergebnis.[1261] Er ist weder so etwas wie genuin objektiv noch unwiderlegbar überzeugend.

Hinsichtlich des virtuellen Raums besitzen technisierte Sachbeweise eine besondere Ausdehnung. Ausgesprochene Gedanken oder ausgeführte Handlungen im realen Raum sind vergleichsweise flüchtig. Informationen über Sachverhalte ergeben sich sehr häufig bestenfalls aus sekundären Quellen (Polizist, der die Aus-

---

1254 NOGALA/SACK, S. 145; NOGALA 1998, S. 291 f. Ähnlich SCHWEIZER/BISCHOF, S. 282.
1255 KAMMERER 2008, S. 173 f. mit weiteren Hinweisen.
1256 KAMMERER 2008, S. 184 f.
1257 BIER/SPIECKER GEN. DÖHMANN, S. 615.
1258 TINNEFELD/BUCHNER/PETRI, S. 50 und 52.
1259 TONDORF, S. 40 f.
1260 HASLER, S. 10, 43 ff. und 59 f. Ebenso SCHLEIM, S. 151; NEUHAUS, S. 538 und 559 ff.; KAMMERER 2008, S. 177 ff. Siehe auch BIEDERMANN/VUILLE.
1261 Siehe zum Ganzen oben Erster Teil, Kapitel III.I. und IV.B.1.

sage von Zeugen aufnimmt etc.). Gesagtes ist, wird es nicht mittels technischer Mittel aufgezeichnet, nach kurzer Zeit kaum noch zu rekonstruieren, weil Menschen vergessen, falsch einschätzen, ungenau oder verzerrt wiedergeben, Dinge nicht akkurat wahrnehmen etc. Über Hilfsmittel, wie die Videoüberwachung wird versucht, Geschehnisse als quasi-primäre Aufzeichnungen digitalisiert zu konservieren. Im virtuellen Raum hingegen produziert jede Aktion, jedes Wort direkt Daten. Handeln, Kommunizieren im virtuellen Raum heisst Daten austauschen. Die Vermutung, der virtuelle Raum ermögliche, „Gedankenverbrechen" (öfters) zu verfolgen, ginge wohl zu weit.[1262] Das Problem, dass in Daten gefasste Gedanken eine ungemein längere Zeit vorhanden sind als ausgesprochene Gedanken, besteht indes durchaus.[1263]

Abschliessende Antworten zu diesen Problembereichen technisierter Sachbeweise können im Rahmen der vorliegenden Arbeit nicht gegeben werden. Vielleicht konnte aber zu einer differenzierteren, relativierten Sichtweise auf Erzeugnisse aus postmodernen Technologien angeregt werden. Viele technisierte Sachbeweise sind hilfreich und einem in alle Richtungen ausbalancierten Strafverfahren förderlich. Um sie angemessen in den Prozess einzubringen, anzuwenden, anzuzweifeln und zu würdigen, müssen die Akteure der Justiz (Verteidiger, Staatsanwalt, Richter) aber das entsprechende Know-how besitzen.[1264] Sie müssen die Grundzüge ihrer Funktionsweise und deren Grenzen kennen, über Konsequenzen und bestehende Unklarheiten informiert sein. Die Nützlichkeit, Aussagekraft und Glaubwürdigkeit technisierter Sachbeweise können und müssen wohl letztlich einzelfallweise beurteilt werden.

C. Interdisziplinarität: Chance oder Problem?

An den Kriminalitätsbekämpfungstechnologien wirken verschiedene Disziplinen mit. Über mehrere Phasen verteilt, beteiligen sich verschiedene technische Berufsgattungen, Geistes- und Naturwissenschaftler, Politiker sowie Praktiker aus dem Polizei- und Justizbereich. Diese Interdisziplinarität bereichert die kriminologische Forschung, lässt gesellschaftliche Zusammenhänge besser erfassen und multivariate Erklärungen begründen. Interdisziplinarität hat aber in dieser Hin-

---

1262 So etwa Denis Simonet im Artikel „Trojaner passen nicht zu einem Rechtsstaat" in Tages-Anzeiger Online vom 14. Oktober 2011.

1263 Siehe etwa Bericht BJ inter net, Anhang 1, S. 5.

1264 Vgl. TONDORF, S. 39 ff.

sicht auch ihre Schattenseiten: In der Kriminalpolitik mischen viele Akteure und Interessengruppen mit. Die entstehenden Debatten erschweren der Bevölkerung, die Situation zu durchblicken. Ihr werden viele (vermeintlich einfache) Lösungen für verschiedene proklamierte Probleme präsentiert, wobei die grösste öffentliche Präsenz diejenigen Stimmen einnehmen, deren Programme für die Medien und die Politik am besten nutzbar sind.

Die Theorienvielfalt und Uneinigkeiten in kriminalpolitischen Themen, die sich über die letzten Jahre manifestierten, begünstigen das festgestellte mehrspurige Vorgehen gegen Kriminalität und die Neigung, postmoderne Kriminalitätsbekämpfungstechnologien opportun-agnostisch zu verwenden.[1265] Die postmoderne Kriminalpolitik erschafft dadurch keine *kohärente Ordnung*, sondern verschiedene, locker zusammenhängende und bedarfsgerecht zu verwendende Formationen. Das führt zu vielen schwer einzuschätzenden und unkontrollierbaren Wechselwirkungen und dazu, dass viele Strategien und Technologien der Kriminalitätsbekämpfung nicht oder nicht in der Weise, wie eigentlich angedacht, funktionieren.

Die Kommunikation zwischen den Disziplinen birgt ein weiteres Problem der Interdisziplinarität. Die Kommunikation ist nicht immer einfach, auch, da zuweilen die gemeinsame Sprache fehlt oder sich Denkkategorien stark unterscheiden. Der Trend weist auf einen Kurs vereinheitlichender Anpassung an empirisch-naturwissenschaftliche Erklärungsmuster und technisch-ökonomische Praktiken hin.[1266] Anschaulich dafür ist die, sicherlich nur von einer kleinen, aber dafür in den Medien desto prominenteren Minderheit der Hirnforschung vertretene Ambition, die Hirnforschung vermöge *überdisziplinär* absolute Wahrheit festzustellen und anderen Wissenschaften als Naturgesetze vorzugeben.[1267] Vertreter der

---

1265 Siehe dazu und zu entsprechenden Lösungsansätzen KUNZ 2011, S. 177 ff. Vgl. etwa SCHMIDT-SEMISCH, S. 65. Siehe oben Dritter Teil, Kapitel I.G.

1266 Siehe oben Dritter Teil. Vgl. etwa KUNZ 2011, S. 181 ff.; SCHMIDT-SEMISCH, S. 68.

1267 Siehe Phillip Reemtsma im Spiegel-Interview vom 30. Juli 2007 bei LAKOTTA, S. 122: Er sehe in Äusserungen der Neurobiologen zu philosophischen Fragen „Ambitionen, eine neue Fundamentaldisziplin zu erfinden". Das sei aber für die juristische Praxis „völlig bedeutungslos". Ähnlich stellt KUNZ 2011, S. 183 die Frage, ob denn Defizittheorien „mehr und anderes leisten können als Alltagsvorstellungen über Kriminalität zu bestärken". Ähnlich auch LEMKE, S. 108 f. mit Hinweisen. Vgl. zur unsicheren Datenbasis dieser Ansätze: RZEPKA, S. 125. Im Gegensatz dazu bspw. MARKOWITSCH/SIEFER, S. 218: „Natürlich kann man naturwissenschaftliche Erkenntnisse ignorieren und Recht und Hirnforschung als nicht interaktionsfähige Disziplinen ansehen. Rechtsprechung existiert auf der Basis des Volksglaubens und damit allenfalls der Alltagspsychologie."

Neurokriminologie mischen sich auf diese Weise in andere Wissenschaftsgebiete ein, ohne die unterschiedlichen Zugänge, Annahmen, Hilfsmittel und Terminologien dieser Wissenschaftsgebiete zu (be)achten.[1268]

III. Stereotypen, Risikoklassements und Chiffren

A. Generalverdacht, Eigenschaftsrasterung und Stichproben

Ein zentraler Zweck postmoderner Überwachungstechnologien ist das Erfassen potenzieller Bedrohungen und mutmasslicher Täter sowie Störer in Stadien, in welchen erst vage Anhaltspunkte für eine künftige Tat oder Bedrohung bestehen. Diese Aufgabe kann vorderhand auf drei Arten angegangen werden – mittels Generalverdacht, Eigenschaftsrasterung und Stichproben: Sind unter dem Regime des Generalverdachts alle Personen und Aktivitäten gleichermassen verdächtig, fokussieren die kriterienbasierenden (automatisierten) Überwachungssysteme, Massendatenverarbeitungssysteme und Register auf bestimmte Risikogruppen oder auf bestimmte verdächtige Verhaltensweisen.

Zum einen kann also generell jeder verdächtigt und es können bei Gelegenheit (Beispiel: Videoaufnahmen von Personen, die einen überwachten Park durchqueren) oder gezielt (Beispiel: Archivieren biometrischer Daten bei der Ausfertigung des Schweizer Passes) über jedermann Daten auf Vorrat gesammelt werden, mit dem Ziel, gute Muster zum Abgleich bei einem Zwischenfall und genügend Datenbestände für verschiedene (proaktive) Auswertungzwecke und -abläufe bereitzustellen. Idealerweise ergeben sich aus den gesammelten Daten selbst bereits veritable Verdachtsmomente. Zum anderen kann sich die einsetzende Behörde zu Beginn der Fahndung nach (potenziell) Verdächtigen oder einer (potenziell) drohenden Gefahr auf Eigenschaften und Kriterien einigen, welche wahrscheinlicher Verdächtige von weniger wahrscheinlich Verdächtigen und Bedrohungen von harmlosen Situationen abheben (Eigenschaftsrasterung). Die Behörde trifft demnach eine Auswahl von beschreibenden Kriterien, deren Kombination eine bestimmte Risikokategorie möglichst genau abbildet. Gelingt dies, ergibt die kriteriengeleitete Suche eine hoffentlich hilfreiche und möglichst

[1268] Siehe dazu HASSEMER 2012, S. 11 f. und 14; KRÖBER, S. 66 ff.; SCHWEIZER/BISCHOF, S. 275. Eine sehr umfassende Kritik dieses überall sich einmischenden „Neuro-Enthusiasmus" findet sich bei HASLER, insb. S. 195 ff.

zutreffende Erkenntnis. Am Beispiel der Rasterfahndung: Die Ausgangslage der negativen Variante der Rasterfahndung ist ein Generalverdacht gegen eine grosse Anzahl Personen, die mit jedem Verarbeitungsschritt kleiner wird. In der Schnittmenge verbleiben nicht Verdächtige, sondern Personen, die das Programm nicht als „unverdächtig" aussortieren konnte.[1269] Bei der positiven Variante steht direkt die Skizze eines hypothetischen Eigenschaftsträgers am Anfang des Prozesses.

Oft werden die Ansätze des Generalverdachts und der Eigenschaftsrasterung gestaffelt verknüpft. Zuerst werden möglichst viele Daten gesammelt, welche in einem zweiten Schritt kriteriengeleitet ausgewertet oder mit Daten aus anderen Quellen abgeglichen werden. Mithilfe automatisierter Systeme können theoretisch beide Varianten gleichzeitig vorangetrieben werden, das heisst, im gleichen Durchlauf auf Vorrat Daten gesammelt, gesichtet und nach Kriterien durchsucht und kategorisiert werden.[1270] Mittels nicht-automatisierter Überwachung vermag der Benutzer erst einmal Daten anzuhäufen. Diese können manuell auf relativ präzise Verdachtsmomente, auf nachträgliche Anzeigen hin oder stichprobenweise überprüft werden. Zudem kann der menschliche Überwacher während des Überwachungsvorgangs punktuell Sachverhalte oder Personen einer näheren Analyse unterziehen. Arbeitet er über den Ansatz genereller Verdächtigung, wird er sich aber ressourcenbedingt auf ausgewählte neuralgische Ballungspunkte beschränken müssen. Meistens wird er auch kaum umhin kommen, seine Überwachungstätigkeit auf den Weg der stereotypisierten Eingrenzung der Datenflut auszurichten, will er sie nicht völlig ineffizient betreiben: Menschliche Überwacher müssen vielfach gezwungenermassen stichprobenweise kontrollieren oder alternativ kategorisieren. Sie müssen sich auf einige wenige Risikogruppen, Risikoräume oder auf Risikoverhalten konzentrieren, können sich jedoch bei der Beobachtung von Ereignissen oder Personen auf ihre Erfahrungen und ihre Intuition verlassen.[1271] Sie können vorgegebene Abweichungsmerkmale selbst an

---

1269 Siehe PEHL, S. 13 ff.

1270 MARX 2005, sieht darin ein bezeichnendes Element neuer Überwachungstechnologien: „The new social surveillance can be defined as, «scrutinity through the use of technical means to extract or create personal or group data, wether from individuals or context.»". Fraglich ist dahingehend, wie gut, wie zuverlässig und wie autonom sie Analyseprozesse abarbeiten können. Ähnlich auch CROSSMAN, S. 117.

1271 Siehe etwa ZEHNDER M., S. 32. Selbstverständlich ist eine Einschätzung des Geschehens auf dem Monitor auf der Grundlage von Vor- und Einstellungen der menschlichen Beobachter

veränderte Verhältnisse adaptieren. Wohingegen die automatisierten Systeme durch ihre grösseren Kapazitäten differenzierter und ohne Ablenkung vorgehen können, aber auf im Voraus formulierte, distinguierte und zutreffende Kriterienvorgaben angewiesen und beschränkt sind.[1272] Die manuelle kategorische Überwachung ist somit weniger klar abgegrenzt, aber flexibler. Die automatisierte hingegen folgt starr den vorgegebenen Regeln, sollte daher *theoretisch* frei von verzerrenden subjektiven Faktoren sein und allgemein effizienter arbeiten.

Der Generalverdacht ist konzeptionell sehr inakkurat und damit erst einmal wenig effizient. Er ist einer effektiven Kriminalitätsbekämpfung zunächst grundsätzlich hinderlich: Je stärker eine Verdächtigengruppe eingegrenzt werden kann (idealerweise auf eine einzige Person), desto kleiner ist der Aufwand, nach diesen Personen zu fahnden, desto schneller können sie gefasst werden und desto solider wird das Fundament der Anklage sein. Zwar nutzen auch viele manuell bediente Systeme die Methode des Generalverdachts. Ohne die Effizienz automatisierter Systeme, zumindest im Zeitpunkt, in dem die gesammelten Informationen ausgewertet oder in anderen Zusammenhängen verwendet werden sollen, endet diese Methode jedoch lediglich im simplen Anhäufen von Datensammlungen, aus denen oftmals höchstens in einem sehr späten Stadium Hinweise gewonnen werden können, dann, wenn das Verbrechen ohnehin praktisch aufgeklärt ist.

In aller Regel kann aber auch die kriteriengeleitete Vorgehensweise ihre Effizienzversprechen nicht halten, und es ist zu bezweifeln, dass sich das (in absehbarer Zeit) ändern wird.[1273] Das Kernproblem liegt in ihrer Treffsicherheit und ihrer Verlässlichkeit.[1274] Indem durch statistische Prognosen, objektivierte Verhaltenskriterien, stereotypisierte Kategorisierungen oder vage Hypothesen die ins Schema passenden Nonkonformen von den vermeintlich Unverdächtigen in einem ersten Schritt aussortiert werden, verkleinert sich der Verdächtigtenpool. Entspricht diese Auswahl nicht der Wirklichkeit, können also beispielsweise die

sehr subjektiv, wie KAMMERER 2008, S. 165, m. E. richtig festhält. Vgl. auch HARCOURT, S. 237 f.; CROSSMAN, S. 117.

1272 NORRIS/ARMSTRONG, S. 119, 150 f. und 196 f.

1273 Siehe KUNZ 2011, S. 108; HARCOURT, S. 2 f.; DITTMANN 1997, S. 126 und 128 f.; NEDOPIL, S. 297 und 361. Selbst ROTH 2003b, S. 543, stellt fest, es werde „niemals zu präzisen Prognosen kommen".

1274 Vgl. etwa ROGALL, S. 618 zur Rasterfahndung: „[Sie] ist stets nur so gut, wie die Suchkriterien, die man der Massnahme als bekannt zugrunde legt." Ebenso STEINBOCK, S. 42 zu den Methoden des Data Mining.

aussortierten und die verleibenden Subjekte nicht Kategorien zugeordnet werden, die homogene oder annähernd vollständige Populationen Krimineller enthalten, schlüpfen einige tatsächliche Täter respektive Tatwillige durch die Maschen. Ihre Verdächtigkeit wird fälschlich als unwahrscheinlich bewertet, und sie fallen aus dem Raster, womit sie den folgenden Ermittlungsschritten entgehen.[1275] Die Systeme und Register erfüllen in diesem Fall die an sie gestellten Hauptansprüche nicht: dem Herstellen einer möglichst hundertprozentig fehlerlosen Verbrechensverhinderungs- oder Aufklärungsrate. Gerade auch bei konkreteren Verdachtsermittlungen oder Fahndungen nach wenigen Personen kann diese Schwachstelle fatal für den Nutzen derartiger Überwachungstätigkeit sein: Der Einsatz verursacht viel Aufwand, da aber die Verdachtshypothese beziehungsweise das Merkmalsprofil unzureichend präzise ist, befindet sich der gesuchte (unbekannte) Täter, die gesuchte Risikogruppe etc. nicht im Pool der verbliebenen Verdächtigen.

B. Versicherungsmathematische Ungerechtigkeit

Was theoretisch gut klingt, ist in der praktischen Anwendung somit ein schier unerreichbares Ideal. Brauchbare Eigenschaftsprofile und Algorithmen zu finden, die nicht auf die eine oder andere Art diskriminieren, scheint ein schwieriges Unterfangen zu sein.[1276] Es ist illusionär, jeden Unterschied zwischen Personengruppen über Algorithmen von einer fälschlichen Erfassung als Risiko auszuschliessen. Weiter drängen anlasslose Überwachungen, insbesondere auch des virtuellen Raums, sich widersetzende oder sich bewusst unkonform verhaltende Personen in dieselbe „Anonymitätsmenge" wie verdächtige, gefährliche Personen.[1277] Diese Undifferenziertheit erschwert die effiziente Arbeit der Behörden, da die vielen miterfassten harmlosen Personen Leerläufe verursachen.[1278] Angehörige von Minderheiten oder Personengruppen, die sich bewusst von der Masse abheben wollen, sind zudem durch ihre stärkeren Abweichungen vom Standard wahrscheinlich leichter zu identifizieren. Die Chance, einen minder-

---

1275 Vgl. HARCOURT, S. 28 f.

1276 Gl. M. wie KAMMERER 2008, S. 199 ff. Dies hat zur Folge, dass die mithilfe von automatisierten Prozessen als potenziell verdächtig eingestufte Person im Wesentlichen nichts anderes ist als ein Stereotyp, der *bestenfalls* in einer bestimmten Situation statistisch gesehen am ehesten als Täter bzw. Störer in Betracht kommt.

1277 PFITZMANN/KÖPSELL 2009a, S. 546.

1278 ZERBES, S. 333.

heitsangehörigen Straftäter aufgrund einer automatisierten Überwachungsaufnahme zu fassen, ist demnach höher.[1279] Es erstaunt ferner nicht, dass, wenn staatliche Behörden ihre Mittel auf bestimmte Risikogruppen konzentrieren, in dieser Population häufiger Kriminelle entdeckt werden als in Populationen, mit denen sich jene weniger intensiv beschäftigen. Angehörige der fokussierten Risikogruppe werden durch diese Dynamik somit statistisch überrepräsentiert. Das ist problematisch, insofern einige Risikogruppen per se als verdächtiger als andere angesehen werden, diese Annahme aber nicht (immer) zutrifft, also der prozentuale Anteil an tatsächlich Verdächtigen in allen Gruppen gleich hoch wäre. Trotzdem wird nicht selten dieses verzerrt wahrgenommene Kriminalitätsaufkommen als Rechtfertigung herangezogen, sich verstärkt auf die bereits fokussierte Risikogruppe zu konzentrieren.[1280]

Straftäter, die dem Standard nahe kommen, entwischen hingegen häufiger, da es schwerer ist, sie automatisch aus der Masse herauszufiltern und zu identifizieren. Dieser Schwachpunkt kann von Kriminellen ausgenutzt werden, indem sie ihre wesentlichen Merkmale und Verhaltensweisen an die grosse Masse anpassen und als riskant geltende Profileigenschaften vermeiden oder tarnen. Diese Gegenmassnahmen des Kriminellen lassen ihn die kriterienbasierten Sondierungsmethoden umgehen.[1281] Staatliche Ermittlungsbehörden können darauf wohl mit angepassten Kriterien, mit neuen Erkennungsstrategien und Merkmalshypothesen reagieren. Diejenigen Attribute zu erahnen, die etwa den sich konform verhaltenden Gefährder (beispielsweise den Terroristen) vom sich konform verhaltenden Durchschnittsbürger zuverlässig zu differenzieren vermögen, dürfte aber (bis zur Realisierung der Gefahr) sehr schwierig sein. Können keine geeigneten Hervorhebungsmerkmale gegenüber der konformen Bevölkerung mehr gefunden werden, können Anstrengungen wie die Schläferfahndung nur scheitern.

Kriterienunabhängige Stichproben und der reine Generalverdacht sind immun gegen diese Täuschungen. Überhaupt ist eine „Randomisierung" der Überwa-

---

1279 INTRONA/WOOD, S. 186, 190 und 192; HARCOURT, S. 223: So benachteiligt bereits die Verwendung von Standard- und Risikomustern Minderheiten, indem diese per se von der Mehrheit abweichen, denn würden keine unterscheidenden Merkmale zwischen Mehrheit und Minderheit bestehen, gäbe es diese Unterscheidung nicht und lägen keine Unterschiede zwischen den Kriminalitätsraten vor, wären Risikokategorien ohne jegliche Rechtfertigung.

1280 Siehe dazu HARCOURT, S. 27, 147 ff. und 163; SINGELNSTEIN/STOLLE 2012, S. 132 f.; ZEHNDER M., S. 32 f.

1281 Siehe HARCOURT, S. 5 und 228 f., der daher m. E. zutreffend feststellt, dass diese versicherungsmathematischen Mechanismen dazu neigen, fehlzuzünden. Vgl. ZEHNDER M., S. 33.

chungstätigkeit, das heisst die Taktik, Stichproben völlig zufällig zu überprüfen anstatt sich auf bestimmte Merkmalsträger zu konzentrieren und zu versuchen, Bedrohungen prognostisch an Kriterien festzumachen, eine durchaus bedenkenswerte und keineswegs neue Alternativtaktik.[1282] Auch ist sicherlich zuzugestehen, dass aufgrund der Taktik des Generalverdachts in seiner Reinform niemand diskriminiert wird.[1283] Die handelsübliche Videoüberwachungskamera im Kiosk mag den unbescholtenen Bürger in seinem Stolz, etwa kein Kaugummi-Dieb zu sein, kränken. Stereotype Vorurteile werden über sie nicht transportiert.[1284] Der zwölfjährige Rumtreiber wird für ebenso verdächtig eingestuft, einen Kaugummi von der Kioskauslage zu stehlen, wie die pensionierte Richterin oder die Kioskangestellten. Generell verdächtigende Überwachungsmethoden kennen Nebenfolgen wie beispielsweise stigmatisierende Effekte nicht[1285], sie können aber freilich Basis sein für möglicherweise stigmatisierende Folgemassnahmen oder eingriffsintensivere Folgeermittlungen. Auf der anderen Seite liesse auch die automatisierte Sondierung, beruhend auf ordentlich funktionierenden Profilen, tatsächlich Unverdächtige nahezu unberührt und könnte für diese sogar eine entlastende Wirkung haben.[1286] Smarte, automatisierte Systeme könnten menschliche Bediener solange vom Überwachungsprozess ausschliessen, bis sie Auffälligkeiten entdecken.[1287] Das Argument, die anlasslose Sichtung, Sondierung und Analyse von Personendaten durch einen Computer, durch ein automatisiertes System, bedeute höchstens leichte Eingriffe in Grundfreiheiten betroffener Personen, leuchtet dann durchaus ein.[1288] Der Grossteil der Menschen, der in

---

1282 Siehe dazu HARCOURT, S. 237 ff.

1283 Dieser Punkt wird von Kritikern teilweise übersehen, etwa von ROGGAN 2001, S. 140. Vgl. MIDDEL, S. 343. Inkludiert der Generalverdacht gar, indem er alle Personen gleichermassen denselben Überwachungsmassnahmen aussetzt und sie daher in dieser Situation vereint?

1284 Vgl. SORELL, S. 19 und 22; NORRIS/ARMSTRONG, S. 225; RUDIN, S. 278. Zur Missbrauchsanfälligkeit durch diskriminierende Kriterien und voyeuristische Motive der Überwacher, siehe BARTSCH, S. 46 f.; MÜLLER L. 2011, S. 138 f. und 144 f.

1285 Vgl. etwa MÖSTL, S. 226 zur Vorratsdatenspeicherung.

1286 NOWAK, S. 34; POSNER in The Washington Post vom 21. Dezember 2005; BIER/SPIECKER GEN. DÖHMANN, S. 614. Vgl. auch KAMMERER 2008, S. 199. Nicht ganz einleuchtend ist aber das Argument von BIER/SPIECKER GEN. DÖHMANN, S. 617, die „anlasslose Totalüberwachung" könne durch smarte Überwachungssysteme verhindert werden. Auch smarte, kriteriengeleitete Systeme und Methoden operieren zunächst anlasslos, *vertiefen* jedoch Analyseprozesse nur anlassgebunden.

1287 Siehe oben Zweiter Teil, Kapitel II.C.

1288 So etwa NOWAK, S. 34; POSNER in The Washington Post vom 21. Dezember 2005: „[M]achine collection and processing of data cannot, as such, invade privacy. Because of

die (Streu-)Wirkungen der verdachtsunabhängigen Massnahme einbezogen wird, wird lediglich von ihr gestreift, oberflächlich gescannt.[1289] Diese Personen haben keine Folgeeingriffe zu befürchten, da sie dem Raster nicht entsprechen, das heisst die gesuchten Eigenschaften nicht aufweisen. Dies gilt indes nur, wenn irrelevante Daten derjenigen Personen, die nicht den Kriterien entsprechen, umgehend gelöscht werden, diese also nicht für weitere Abgleiche oder Verwendungszwecke zur Verfügung stehen und demnach nicht in anderen Zusammenhängen wiederzuverwenden sind. Das Argument der Regierung im vor dem EGMR verhandelten Fall S. und Marper gg. Vereinigtes Königreich, die Aufbewahrung von (Personen-)Daten alleine habe keinen direkten oder signifikanten Effekt auf betroffene Personen, solange keine Treffer beziehungsweise Übereinstimmungen sie in ein Verfahren ziehen würden, überzeugte den EGMR jedenfalls nicht.[1290] Zudem ist daran zu erinnern, dass die Prozesse (automatisierter) Systeme auch für Experten nicht immer durchschaubar und daher Manipulationen, Programmierfehler oder technisch bedingte Irrtümer nicht leicht nachzuprüfen und zu berichtigen sind. Ihre Ergebnisse sind durchaus hinterfragbar.[1291]

Ein weiterer, verbreiteter Einwand gegen die dargestellte Argumentation und auch den Generalverdacht sind die vermuteten Aggregations- und Einschüchterungseffekte sowie der Konformitätsdruck, welche durch anlasslose Überwachungstätigkeiten bei der Bevölkerung entstehen könnten. Bereits die Möglichkeit, dass man einer tiefergreifenden Überprüfung unterzogen werden könnte, könnte zu Verhaltensänderungen führen. Bereits die Möglichkeit, dass der Staat bei Bedarf (heimlich und ohne Einwilligung der betroffenen Person) in die Lage versetzt wird, viele Informationen und damit ein Gesamtbild einer Person zusammenzutragen, könnte Machtasymmetrien entstehen lassen. Bereits die Möglichkeit, dass der Staat diese (anlasslosen) Instrumente missbrauchen könnte, könnte Misstrauen und Widerstand in der Bevölkerung erzeugen.[1292]

their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer." Kritisch indes LSE Briefing, S. 22.

1289 Bspw. bei der Rasterfahndung nur eine „logistische Sekunde" lang, siehe ZSCHOCH, S. 221. Siehe auch die abweichende Meinung der Richterin Haas im BVerfGE 115, 320 (371 ff.).

1290 Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04, § 121. Siehe dazu oben Fn. 550.

1291 Siehe oben Dritter Teil, Kapitel V.C. und V.D.

1292 Siehe dazu unten Vierter Teil, Kapitel IV.A. und IV.D.

C. Die Chiffrierung des Menschen

Proaktive Technologien und Strategien versuchen, Risikofaktoren aus weiter Ferne zu erkennen.[1293] Die Tendenz zum Gesinnungsstrafrecht äussert sich dabei im Anspruch an die Überwachungs- und Informationsverarbeitungstechnologien, unerwünschtes Verhalten vorauszuahnen. Um diesen Anspruch zu erfüllen, werden Kompromisse eingegangen, indem beispielsweise Verdachtsrregister sicherheitshalber auch prognostisch lediglich abstrakt Gefährliche – in dem Sinne etwa „mutmasslich Auffällige" – auflisten. Das führt in der Praxis dazu, dass „Normalbürger" mit erfasst werden.[1294] Desgleichen ist die versicherungsmathematische Denkweise im Forschen nach objektivierbaren Merkmalen des Risikoträgers zu beobachten. Das kommt dem Zweck der kriterienbasierenden, auf empirisch-statistischen Prognoseinstrumenten oder auf Verdachtshypothesen beruhenden Technologien entgegen. Die Annahme der allgemeinen Anfälligkeit und Empfindlichkeit der Menschen für Defizite[1295], die Sensibilisierung durch Präventionskampagnen für die Gewissheit mannigfaltiger Tatgelegenheiten in der Postmoderne und entsprechend der Aufruf zu selbstverantwortlichem Handeln formieren einen modifizierten Generalverdacht, der einerseits die Komponente der anlasslosen, möglichst früh ansetzenden Kriminalitätsvorsorge und andererseits die Komponente der typisch kriminellen Eigenschaften und der wissenschaftlich feststellbaren Defizite als Anknüpfungspunkte[1296] für tieferreichende Überwachungsmassnahmen heranzieht. Dieser „generalisierte Verdacht" proaktiver Überwachungs- und Registrierungstechnologien dient dem Zweck, objektivierte Risikomerkmale zuzuordnen und die identifizierten riskanten Elemente letztlich über ihren Ausschluss zu managen.[1297] Diese Überwachungstechnologien zielen, wie auch ihr Vehikel, das versicherungsmathematische Risikokalkül, trotz ihres vermeintlich anlasslosen Charakters auf Riskopersonen und -gruppen ab.[1298] Der überschwängliche Optimismus, der diese angestrebten Zielvorstellungen begleitet, vermittelt der Bevölkerung indes die trügerische Hoffnung, Kriminalität lasse sich mit smarten, kriterienbasierten Technologien ziel-

---

1293 COUDERT, S. 377; KRASMANN, S. 243; SCHMIDT-SEMISCH, S. 61.
1294 Vgl. GANDY 1989, S. 71; INTRONA, S. 85; NOGALA 1989, S. 84 mit weiteren Hinweisen.
1295 Vgl. ROSE, S. 96.
1296 ROSE, S. 96 nennt diese „biomarker".
1297 SCHMIDT-SEMISCH, S. 15 f.; KRASMANN, S. 242 ff.
1298 HARCOURT, S. 22.

gerichtet verhindern, weswegen sie in dieser Hinsicht problematischen Instrumenten gegenüber meist positiv eingestellt ist.[1299]

Die Gefährlichkeit einer Person äussert sich dabei nicht erst mit beobachteten Vorbereitungshandlungen oder akuten Anzeichen eines Ausbruchs ihrer kriminellen Energie. Die Gefährlichkeit wird an einem über Merkmale zugeschriebenen „Zustand" festgemacht.[1300] Nicht nur derjenige wird als potenziell akut gefährlich diagnostiziert, der einen konkreten Anlass für diesen Verdacht schafft, sondern ebenso derjenige, der keine Gewähr bieten kann, ungefährlich zu sein.[1301] Der gefährliche Zustand ist ein Behelf, eine bequeme Fiktion. Es gilt eine Gefährlichkeitsvermutung – wer sich nicht in diesem Sinne „exkulpiert", wird aus sicherheitspolitischen Gründen als Risiko eingestuft.

Die effiziente Überwachung oder Kontrolle einer Vielzahl von „Körpern" über diese Methoden kann nur gelingen, wenn die Masse möglichst gesamthaft erfasst ist, aber die einzelnen Teile unterscheidbar und einer Zuordnung zugänglich bleiben beziehungsweise gemacht werden. Die Zuordnung zu Kategorien vereinfacht die Abwicklungsprozesse erheblich. Sie wird in einer Art „Chiffre" ausgedrückt, mit welcher jeder Einzelne gekennzeichnet und zu der schliesslich jeder wird.[1302] Die Chiffre in dem Sinne muss keine Zahl sein, sondern ist allgemeiner eine Zuschreibung in Kurzfassung, die grundsätzlich auch als Zahl ausgedrückt werden könnte. Sie stellt eine stark reduzierte und abstrahierte Zusammenfassung von Merkmalen (zum Beispiel der Vorgeschichte, des bisherigen Lebensstils, von Charakterzügen etc.) dar.[1303] Der Unterschied der Chiffre zum Namen oder zur blanken Nummer liegt darin, dass jene nicht eine Person identifizieren, sondern Personen verkürzt beschreiben soll. Der Name steht für das Individuum, wohingegen die Chiffre in diesem Sinne Personen mittels Abgrenzungsmerkmalen beschreibt. Der Name ist Teil der Identität der Person. Indes können mehrere

---

1299 Vgl. unten Vierter Teil, Kapitel IV.C.

1300 Vgl. ZERBES, S. 332; VOLKMANN, S. 218; KUNZ 2000, S. 146.

1301 Vgl. oben Dritter Teil, Kapitel IV.B.

1302 DELEUZE 1993b, S. 258: „Die Individuen sind *«dividuell»* geworden, und die Massen Stichproben, Daten, Märkte oder *«Banken»*." Das Subjekt wird zum reinen „Merkmalsträger" (KUNZ 2000, S. 146). Auch die Merkmale selbst sind dabei „dividuell": Biometrische Kennzeichen, erfassbare Abweichungen vom Standard, wissenschaftlich erfahrbare Defizite oder hypothetische Kriterien (vgl. BOGARD, S. 66). Bsp.: Der Eintrag in einem Verdachtsregister reduziert die Person auf eine für das Register zu handhabende, auf das Register zugepasste Merkmalsliste, eben auf eine Chiffre.

1303 Vgl. BOGARD, S. 62; KLEIN, S. 96 f.

Personen dieselbe Chiffre zugewiesen bekommen. Die Chiffre in diesem Sinne ist ein stark verkürztes Narrativ, ein Abriss der (Risiko-)Eigenschaften einer Person.[1304]

Nennt man eine derartige Chiffre, weiss man, welche *Kategorie von Individuum* gemeint ist. Freilich gibt die Chiffre nur vor, ein exaktes Abbild dessen zu sein, was eine Person tatsächlich ist. Vielmehr handelt es sich bei ihr aber um eine mehr oder weniger oberflächliche und mehr oder weniger stimmige Zuschreibung von abgeleiteten Merkmalen, Wesenszügen und interpretierten Meilensteinen des Lebens der Person durch jemand anderen oder etwas anderes. Da in der Praxis die Chiffre aus Gründen der Übersichtlichkeit, effizienter Abläufe und anderer Rationalitäten zudem nicht besonders ausführlich sein darf, kommen eindeutig nur einer Person zuzuordnende Chiffren in der Regel nicht vor. Beispielsweise listet das Register den Terroristen oder den Sexual Offender höchstens mit kurzen, wenig aussagekräftigen Hinweisen auf[1305] und die smarte Videoüberwachung meldet Personen dann, wenn diese mit einem vorgegebenen, riskanten Muster übereinstimmen.

Das beschriebene Amalgam aus Stereotyp und Generalverdacht treibt jede der vorgestellten postmodernen Methoden voran. Es ist für sie unabdingbar.[1306] Die Chiffrierung, das heisst, die Übersetzung von Hypothesen in Kriterien und schliesslich in Algorithmen, macht die maschinell-automatisierte Suche nach Risiken (vermeintlich) effizienter. Technisiert-automatisierte Überwachungstechnologien fördern demnach Kategorisierungsansinnen, treiben dadurch die Forschung nach verbesserten Kategorisierungsmethoden an und bestätigen sie gleichsam mit dem symbolischen Fokus auf bestimmte Risikogruppen.[1307] Mit derartigen Kategorisierungsapparaten können sowohl Differenzen und Abweichungen vom Durchschnitt aufgezeigt und proklamiert als auch die Gefahr „virtuell" gehalten werden, indem durch sie jedermann zum überwachungsbedürftigen Kandidaten mit Delinquenzpotenzial erklärt wird.[1308] Über Kategorien werden Kriminelle als Risikopersonen entindividualisiert. Gleichzeitig werden Risiken geknüpft an täterzugewandte Erklärungsmuster und Rationalitäten der

---

1304 Vgl. YOUNG 2004, S. 18.
1305 Vgl. etwa oben Erster Teil, Kapitel IV.A.
1306 Vgl. SCHMIDT-SEMISCH, S. 61.
1307 Vgl. KREISSL/STEINERT, S. 964; STAPEL, S. 47; ERICSON/HAGGERTY, S. 238 und 254 f.
1308 Vgl. BOGARD, S. 64.

Selbstverantwortung und Selbstvorsorge dem Einzelnen aufgebürdet, sowohl dem Träger riskanter Eigenschaften als auch dessen potenziellem Opfer.[1309]

D. Konsequenzen

Die versicherungsmathematisch verwaltenden Strategien gehen davon aus, jedes menschliche Wesen sei eindeutig zu klassifizieren und dessen Handeln schematisch zu erfassen, zu beurteilen und zu sanktionieren. Sie engen mit dieser Verfahrensweise vor allem die Handlungsspielräume der betrauten Behörden und der Justiz ein. Die Besonderheiten einer Fallkonstellation sind für diese Strategien irrelevant. Sie neigen dazu, die richterliche Beurteilung in die gleichen administrativ-geordneten Bahnen zu manövrieren. Das lässt sie nicht selten mit dem den urteilenden Instanzen in der Schweiz zukommenden grossen Ermessen kollidieren.[1310]

Die Berechnung von Risiken mag zuweilen hilfreich sein.[1311] Die Versicherungsmentalität und postmoderne Risikokalküle sind jedoch im Feld des Straf- und Polizeirechts oftmals schlechte Ratgeber. Sie sind in der Kriminalitätsbekämpfung für jeden ein Damokles-Schwert[1312]: Sie machen die Bürger zu potenziellen Opfern, sie mahnen die Justiz-, Polizei- und Strafverfolgungsbehörden ständig vor Fehlern und sie treiben damit unter anderem Keile zwischen Öffentlichkeit und Behörden.

Durch Risikokalküle wird die Wahrscheinlichtkeit des Eintritts drohender Ereignisse berechnet. Das Risiko verwirklicht sich oder nicht, bis zum Ende aber *weiss* niemand, was tatsächlich eintreten wird. Die Voraussage von Ereignissen mittels Wahrscheinlichkeitsrechnungen gaukelt den Blick in die Zukunft in diesem Sinne nur vor. Auch das ausformulierte Risiko bleibt in letzter Instanz unbeherrschbar, das berechnete Ereignis unterliegt nicht zwingend dem durch die Risikoprognose vorgezeichneten Schicksal. Das führt dazu, dass einige der po-

---

1309 Siehe HARCOURT, S. 185; KRASMANN, S. 249. Vgl. auch BAKER/SIMON, S. 1; COHEN, 123.

1310 Diese Tendenz wurde bereits bzgl. der technisierten Sachbeweise aufgezeigt.

1311 Vgl. etwa SIMON D., S. 102 f.

1312 Dies gilt nicht für den tatsächlichen Straftäter, der sich von Abschreckungsversuchen nicht beeindrucken lässt.

tenziellen Opfer immer zu aktuellen Opfern werden und den Behörden trotz professionellem Handeln immer Fehler unterlaufen werden.[1313]

Das auf dem Generalverdacht beruhende Vorgehen schränkt zwar die Freiheiten aller ein, die Konsequenzen für den Einzelnen sind jedoch geringfügiger als bei stereotypisierenden Methoden. Umgekehrt greifen Letztere je nachdem sehr intensiv in die Grundrechte des mutmasslichen Abweichlers ein. Das Generalverdachtsmodell führt grundsätzlich zu einer Ausweitung sozialer Kontrolle[1314], die Stereotypisierung hingegen zur Benachteiligung bestimmter Personengruppen (zum Beispiel zu einer Verschlimmerung bestehender sozialer Ungleichheiten[1315]) und letztlich zur Exklusion von als potenzielle Delinquenten eingeschätzten Personen. Scheinlegitimierend für ausschliessende Taktiken und für proaktive Vorgehensweisen gegen bestimmte Personenkategorien wirkt, dass jene als – „quasi-wissenschaftlich" und somit scheinbar ohne moralische Bewertung – identifizierte Merkmalsträger Risikofaktoren in sich bergen, denen nicht erlaubt werden darf, auszubrechen.[1316]

Hervorzuheben ist in dieser Hinsicht, dass alle Varianten der Verdachtsforschung/-ermittlung, unabhängig, ob manuell oder automatisiert, in der Regel dann besonders diskriminierend sind, wenn sie (im Einzelfall) nicht die Wirklichkeit widerspiegeln, also Gruppen mit vermeintlich hohem Tatpotenzial generell verdächtigt werden. Mit anderen Worten: Wenn Überwachungsmethoden Prozesse implementieren, welche anhand von bestimmten Kriterien Objekte und Subjekte sondieren und aussortieren, wenn diese Kriterien aber nicht nur wirklich Verdächtige erfassen, sondern eine wiederum generalverdächtige Risikokategorie beschreiben. Kriterienbasierte Methode und Generalverdacht verflechten sich in diesem Fall zu einer prekären Verfahrensweise des kategorisierenden Verdachts, meist aufgrund von pseudo-wissenschaftlichen Klischees.[1317]

Wie bereits ausgeführt, verspricht diese Kombination für die praktische Realität der postmodernen Systeme einen Nutzen. Dieser darf aber angezweifelt werden.

1313 Anschauliches Bsp. bei GATES, S. 82 f. Vgl. auch SIMON D., S. 103 und 106 f.; ZERBES, S. 243.

1314 Vgl. SINGELNSTEIN/STOLLE 2007, S. 110 und 113.

1315 Vgl. etwa HARCOURT, S. 237.

1316 Vgl. SCHMIDT-SEMISCH, S. 31 f. und 94.

1317 Vgl. HAYES 2009, S. 50; NOWAK, S. 37 f.; KAMMERER 2008, S. 93; STAPEL, S. 47 f.; CAMPBELL, S. 79; SORELL, S. 22, welcher indes Massnahmen, gestützt auf Täterprofile, nicht als zwingend diskriminierend ansieht.

Jedenfalls müssen postmoderne mit herkömmlichen Methoden und Strategien verglichen werden. Kann durch postmoderne Überwachungsmassnahmen eine (nahezu) perfekte Quote, wie sie häufig versprochen wird, nicht garantiert oder durch sie keine (qualifiziert) bessere Quote als mit den herkömmlichen Alternativen erreicht werden, verlieren sie an Legitimität. Etablierten, weniger problematischen Methoden gebührte der Vorzug.[1318] Zu verlangen ist sicherlich auch, dass Personen, auf die ein System mittels automatisierten Alarms (sie entsprechen den vorgegebenen Risikokriterien) aufmerksam macht oder die nach einer Rasterfahndung in der Schnittmenge verbleiben, als Falsch-Positive zu behandeln sind (auch im Sinne der Unschuldsvermutung) bis andere Beweise oder Indizien den Verdacht erhärten.[1319] Mittels Gefahren- beziehungsweise Verdachtsforschung sollen mögliche Bedrohungen beziehungsweise mutmasslich Verdächtige sichtbar gemacht werden. Deren Ergebnisse alleine sollten aber nicht genügende Basis für Verurteilungen sein. Übersichtsaufnahmen, Rasterfahndungen, Massendatenverarbeitungstechnologien, Datensammlungen sowie Register und Online-Überwachungsmassnahmen können in der Regel nur Ausgangspunkt sein für weitergehende Ermittlungen oder Anregungen respektive neue Ermittlungsansätze oder Indizien liefern (wohingegen etwa Videoaufnahmen einer erfolgreichen Observation den Schlusspunkt einer Ermittlung darstellen können).[1320]

IV. Transparenz, Bluffs und Versteckspiele

A. Stille Unsichtbarkeit

Der mit einer persönlichen Überprüfung verbundene Aufwand veranlasst die Polizeipatrouille, die Lage zu erfassen und eine Gefährlichkeitsanalyse und Interessenabwägung vorzunehmen. Diese Interpretation des konkreten Einzelfalls beruht auf der Erfahrung oder Intuition des Beamten und ist vielleicht rudimentär oder sogar fehlerhaft, geschieht aber jedenfalls sichtbar und nachvollziehbar für den Betroffenen. Wird dieser kontrolliert und seine Identität überprüft, so hat er in der Regel Kenntnis davon. Für automatisierte Überwachungssysteme hinge-

---

1318 Vgl. NORRIS/ARMSTRONG, S. 225 f.; KUNZ 2011, S. 357 f. Siehe ausführlich am Beispiel der Videoüberwachung: MÜLLER L. 2011, S. 133 f. und 248 ff.

1319 INTRONA/NISSENBAUM, S. 44; HARCOURT, S. 227.

1320 Vgl. PETRI, G N. 528; ROGALL, S. 617; ZSCHOCH, S. 107; HOFFMANN/MUSOLFF, S. 155; HANSEN/PFITZMANN; PFITZMANN/KÖPSELL 2009b, S. 154.

gen bedeutet beispielsweise ein biometrischer Abgleich *aller* Subjekte in einem bestimmten Raum keinen nennenswerten Mehraufwand. Postmoderne Kriminalitätsbekämpfungstechnologien laufen in der Regel verborgen vor den Betroffenen und der Öffentlichkeit ab.[1321] Die Betroffenen werden eventuell durch Hinweistafeln darauf aufmerksam gemacht, dass Videokameras einen öffentlichen Raum überwachen[1322], sie wissen aber nicht, ob, wann und wie allenfalls ein biometrischer Abgleich oder ein virtueller Kriterienabgleich stattfindet, und es ist für sie unabsehbar, ob die gesammelten Informationen allenfalls zukünftig und/oder in anderen Zusammenhängen verwendet werden. Insbesondere sind den Betroffenen dadurch die Hintergründe der Analyse und allfällige Datenverknüpfungen nicht ersichtlich.[1323] Speziell virtuelle Überwachungstechnologien wie die DPI eröffnen Möglichkeiten, Aktivitäten einer Person ohne deren Wissen zu beobachten und analysieren.[1324] Heimliche technische Überwachungsmethoden (insbesondere heimliche Informationsverarbeitungs-, Identifizierungs- oder Analysetätigkeiten) hindern die Betroffenen folglich oftmals daran, sich der Überwachung bewusst zu entziehen, sich über Rechtsschutzmöglichkeiten zu informieren oder an entsprechenden Verfahren mitzuwirken und die Beendigung der Überwachung zu beantragen.[1325]

Dessen ungeachtet verschliesst sich im Einzelfall der automatische Identifizierungs- oder Analyseprozess vielfach selbst weitgehend der Kontrolle und der nachträglichen Überprüfung durch die zuständigen Behörden. Weshalb ein Algorithmus genau diese oder jene Person erfasste, kann ohne umfassende Untersu-

---

1321 NOGALA 1989, S. 165; INTRONA/WOOD, S. 183, bezeichnen diesen für den Betroffenen unsichtbaren Prozess als „silent" im Gegensatz zu offenen Prozessen, die sie „salient" nennen. MATHIESEN 1980, S. 158 und DERS. 2012, S. xvii f., sieht in der Anwendung derart verborgener Kontrolltechniken ein weiteres Merkmal des Wandels in der Kriminalpolitik („a change *from open to hidden discipline*"). ZERBES, S. 8 und 44, sieht in der geheimen Polizeiarbeit einen „Fremdkörper" im traditionell offenen „Konzept des Strafverfahrens". Vgl. auch oben Zweiter Teil, Kapitel I.E. und I.F.

1322 Vgl. etwa MÜLLER L. 2011, S. 119 und kritisch DERS., S. 24 f.; KAMMERER 2008, S. 237 ff., insb. 239.

1323 Anstatt vieler ZSCHOCH, S. 200; BIER/SPIECKER GEN. DÖHMANN, S. 615; PETRI, G N. 48; HORNUNG/DESOI, S. 157; NOGALA 1998, S. 153 f. mit weiteren Hinweisen. Bzgl. der Videoüberwachung könnten vielleicht entsprechende Piktogramme auf die Art des Systems (herkömmlich, smart etc.) hinweisen, siehe BIER/SPIECKER GEN. DÖHMANN, S. 614. Kritisch dazu aber HORNUNG/DESOI, S. 157. Diese Option besteht bei den anderen postmodernen Technologien ohnehin zumeist nicht.

1324 Vgl. etwa COOPER, S. 149.

1325 PETRI, G N. 48; SÖLLNER, S. 157; ZERBES, S. 64.

chung und *Interpretation* eines Experten höchstens vermutet werden.[1326] Die ständige und rasche Weiterentwicklung auf dem Gebiet dieser Technologien (über-)fordert die Instanzen des Justizapparats zunehmend.[1327] Das ist wohlverstanden ein festgestelltes Problem, nicht etwa eine Kritik an der Ausbildung der staatlichen Behörden oder Strafgerichte.[1328] Der Einsatz immer neuer Technologien der Kriminalitätsbekämpfung leitet sie in eine Zwickmühle: Eine Möglichkeit besteht darin, dass sie sich in jedem Fall umfassend über die entsprechenden Technologien und deren Einsatzweise sowie deren Relevanz für den ihnen vorliegenden Einzelfall kundig machen. Dieses Vorgehen wäre sehr wünschenswert, bauschte das Verfahren jedoch stark auf, was mit der Forderung nach rascheren Verfahren und den häufig sehr begrenzten Ressourcen der Behörden kollidierte.[1329] Die andere Möglichkeit wäre, dass die einsetzende Behörde, der Staatsanwalt oder Richter lediglich ihr Vertrauen in die neue Technik kundtun und annehmen, dass die verwendeten Technologien schon intentionsgemäss funktionierten. Freilich stellt sich für jede neu eingesetzte Technik über die Zeit eine ständige Rechtsprechung ein, die auch technische Probleme erfasst und beurteilt. Zu diesem Zeitpunkt liegt jedoch meist bereits eine Nachfolgetechnologie auf dem Tisch, deren offene Fragen diese Rechtsprechung nicht mehr hundertprozentig beantworten kann. Ernsthafte, auf die Effekte, Schwierigkeiten und Expertenmeinungen der einzelnen Techniken und Massnahmen fokussierte Studien schlagen zudem, sofern überhaupt vorhanden, meist nicht den Bogen zu den rechtlichen Aspekten, sondern verweilen bei Bemerkungen innerhalb des eigenen Fachgebiets.[1330] Eine gute und insbesondere offene Zusammenarbeit zwischen erstens Fachexperten (zum Beispiel Polizeitechnikern), die über Schwachstellen der Technologien informieren, zweitens Anwendungsbehörden,

---

1326 Vgl. INTRONA/WOOD, S. 183; KAMMERER 2008, S. 40.

1327 So etwa Thomas Hansjakob im Interview bei STÖCKLI, S. 16, bzgl. der „Wissenskluft" zwischen Polizeitechnikern und „altgedienten Staatsanwälten" beim Einsatz von Govware. Vgl. auch ROTERT, S. 439.

1328 Richter, Staatsanwälte etc. sind nun einmal keine IT-Experten. Insofern scheint es m. E. nicht fair, die Ursache dieses Problems (alleine) dem unkundigen Justizbeamten unterzuschieben, wie dies MALEK, S. 561 ff., tendenziell tut.

1329 Eine einfache Lösung wäre in dieser Hinsicht eine Aufstockung der personellen Ressourcen. Gerade diesen zusätzlichen Ausgaben sollen postmoderne Technologien und Strategien indes entgegenwirken: Sie sollen eine effizientere Abwicklung (mit weniger Personal) ermöglichen. Dass sie dies nicht immer leisten können, wurde im Ersten Teil, Kapitel III.F. und Zweiten Teil, Kapitel I.F. ausgeführt und etwa konkreter am Bsp. ISIS aufgezeigt.

1330 Die Ausnahmen, von denen die eine oder andere in dieser Arbeit Erwähnung fand, sind desto wertvoller.

die technische Massnahmen nur, wo nötig und tatsächlich hilfreich beantragen, und drittens Aufsichtsbehörden, die im Voraus klare Grenzen vorgeben, ist somit anzustreben.[1331]

Ein wesentliches Merkmal der postmodernen Präventionsmethoden ist, dass einige ihrer Prozesse für Betroffene nicht sichtbar sind. Abgesehen vom schwer vermeidbaren Problem, dass sich dem Justizapparat die für einen lückenlosen und schlüssigen Urteilsspruch eigentlich notwendige, genaue Funktionsweise der einzelnen Systeme nicht in jedem Fall erschliesst, entsteht durch den Einsatz dieser Methoden ein Ungleichgewicht zwischen Überwacher und Überwachtem.[1332] Die postmodernen Kriminalitätsbekämpfungstechnologien verlangen in der Regel eine vollumfängliche Transparenz auf Seiten der mutmasslich Verdächtigen, leisten diese aber oft nicht gegenüber den Betroffenen, ja führen im Gegenteil zu immer geheimeren Tätigkeiten der staatlichen Behörden.[1333]

Der Analyst weiss dank datenverknüpfenden Instrumenten und Aggregationstaktiken nicht nur quantitativ und qualitativ viel über die überwachte Person[1334], sondern darüber hinaus mehr über die Funktion und den Einsatz des Instruments selbst. Dieses Ungleichgewicht kann ein Abhängigkeitsverhältnis zwischen Überwachtem und Überwacher bewirken. Letzterer kann gesetzeskonform, gerecht, willkürlich, diskriminierend oder unbedacht analysieren, beurteilen und handeln – all das entzieht sich der Kenntnis des Überwachten. Es sind viele

---

1331 Thomas Hansjakob im Interview bei STÖCKLI, S. 16 f. Siehe auch HILGENDORF, S. 826 f.; LSE BRIEFING, S. 40 ff. Vgl. oben Zweiter Teil, Kapitel II.B. Zudem: Wie den Juristen die komplexen Hintergründe der Technik nicht immer geläufig sind, kann von Entwicklern nicht immer erwartet werden, dass sie die komplexen rechtlichen Konstellationen, Problematiken und Auswirkungen, die ihre Techniken verursachen, vollständig zu erfassen imstande sind.

1332 MÜLLER L. 2011, S. 133.

1333 Vgl. KREISSL/STEINERT, S. 968; CHESTERMAN, S. 9. Das ist vor allem ein Problem heimlicher, breit streuender, ungezielter und verdachtsunabhängiger Massnahmen. Bei gezielten Massnahmen kann in der Regel durch umfassenden nachträglichen Rechtsschutz ein Ausgleich geschaffen werden. Wo möglich, sollten dem Betroffenen auch Datenverarbeitungsaktivitäten angezeigt werden und die Möglichkeiten automatisierter oder kombinierter Anlagen offengelegt oder zumindest verschiedene Kategorien von Überwachungssystemen etwa am Eingang zu einem überwachten Gebiet unterschiedlich gekennzeichnet werden (gl. A. wie BIER/SPIECKER GEN. DÖHMANN, S. 615 f.; MÜLLER L. 2011, S. 201 f.). Siehe oben Zweiter Teil, Kapitel I.F.

1334 NOGALA 1989, S. 147. Vgl. etwa PROBST, S. 30 f.; KAESER in NZZ Online vom 8. August 2013.

Gründe ersichtlich, weshalb dieser die Analyse oder Beurteilung nicht auf ihre Rechtmässigkeit hin überprüfen kann: weil die Überwachung für ihn nicht sichtbar ist, er den Vorgang nicht versteht, Drohgebärden dafür sorgen, dass er sich vor einer Überprüfung fürchtet oder er die Überprüfung unterlässt, weil er dem Staat weiterhin vertraut oder für ihn eine Überprüfung zu aufwendig wäre, oder auch, weil eine Überprüfung durch den Überwachten explizit untersagt ist.[1335]

Es versteht sich von selbst, dass staatliche Behörden ihre Ermittlungstaktiken und -techniken nicht vor der Öffentlichkeit ausbreiten wollen. Tatverdächtige oder potenziell gefährliche Personen und Organisationen sollen über die entsprechenden Vorgänge und benutzten Technologien keine Kenntnis erhalten.[1336] Auch wenn dieses Argument grundsätzlich einleuchtet, ist zweierlei kritisch zu entgegnen: Zum einen, das wurde bereits mehrmals angesprochen, dürften sich Personen aus dem gehobenen (insbesondere dem organisierten) Delinquenzbereich ohne Weiteres über zahlreiche andere Kanäle mit diesen technischen Vorgängen bekannt machen können. Wozu eine Behörde heute grundsätzlich in der Lage ist, lässt sich leicht erahnen und mit ein wenig Mehraufwand genauer recherchieren. Die Geheimhaltung der Überwachungsmethoden und -technologien dürfte in diesem Fall nicht das erstrangige Ziel sein. Zum anderen will der Bürger im Rechtsstaat informiert sein und nicht erahnen müssen, welche Massnahmen der Staat gegen ihn ergreifen kann und darf, unter anderem, um demokratisch entscheiden zu können, welche Vorgehensweisen er zulassen will und welche nicht. Klar ist, dass nicht jedes eingesetzte Programm von der Behörde im Detail zu bezeichnen und nach aussen zu kommunizieren ist. Die Öffentlichkeit hat indes Anspruch darauf, in den Grundzügen über Kriminalitätsbekämpfungstechnologien, insbesondere, wenn auch sie davon betroffen sein kann, informiert zu sein, das gebieten schon das Legalitäts- und Demokratieprinzip.[1337] Daher kann das Gesetz nicht einfach „die Wahl der technischen Mittel bewusst und völlig zu Recht den Strafverfolgungsbehörden" oder sicherheitspolizeilichen Behörden überlassen, auch wenn sich technische Mittel laufend verändern.[1338]

1335 Siehe dazu GILLIOM, S. 85 ff., 142 und 149; PETRI, G N. 48.

1336 Vgl. die Mediensprecherin der Bundesanwaltschaft im Fall Stauffacher bei SCHMID/BAUMGARTNER in NZZ Online vom 15. Oktober 2011.

1337 MOHLER 2012, S. 88.

1338 So aber die Mediensprecherin der Bundesanwaltschaft im Fall Stauffacher bei STÖCKLI, S. 17.

B. Persönlicher Kontakt und Vertrauen

Wie das Bedürfnis der Öffentlichkeit nach mehr Sicherheit vor Kriminalität und nach Effizienz des Kriminalitätsbekämpfungsapparats oftmals falsche Anreize zu entgrenzenden Einsätzen von Kriminalitätsbekämpfungstechnologien setzt, werden durch postmoderne Strategien oftmals falsche Signale an die Öffentlichkeit ausgesendet. Zum einen wird vorgegeben, die öffentlichen Bedürfnisse – zukünftig – durch Überwachungstechnologien erfüllen zu können. Zum anderen werden Bürger zu Selbstvorsorge und Eigenverantwortung angehalten. Diese rückverlegte Verantwortung lässt den Bürger nicht zur Ruhe kommen, hetzt ihn.[1339]

Überwachungs- und Registrierungsmassnahmen, die anlass- oder verdachtsunabhängig arbeiten und weite Bevölkerungsteile miteinbeziehen, streifen deren Grundfreiheiten möglicherweise nur leicht oder gar nicht.[1340] Wird aber publik, dass der Staat breit streuende Technologien einsetzt, führt dies zu Misstrauen und schadet dem Ansehen anwendender Behörden und der technischen Kriminalitätsbekämpfungsmethoden insgesamt, also auch den wesentlich zielgerichteteren und durchaus zweckmässigen Varianten.[1341] Durch technisierte Überwachungsmethoden und bürgerferne polizeiliche Aktivitäten entstehen Entfremdungseffekte, Vorurteile und Misstrauen zwischen Kontrolleur und Kontrollierten.[1342] Auch wenn die Polizeipräsenz das subjektive Sicherheitsgefühl in der Anwohnerschaft vielleicht nicht zu stärken vermag[1343], hat sie einen entscheidenden Vorteil: Der Polizist vor Ort ist „mittendrin“ und in seinem Revier. Er kann die Lage und die sich entwickelnde Dynamik einer Situation besser beurteilen als ein Überwachungsangestellter vor seinem Monitor, der vielleicht physisch nie vor Ort war und durch die Kameras nur einen sehr limitierten

---

1339 Vgl. TESCHNER, S. 117. Persönliche Polizeipräsenz signalisiert dem Bürger möglicherweise im Gegenteil, dass sich jemand um die Sicherheit kümmert und vermittelt dadurch vielleicht Gelassenheit. Überwachungs- und Registrierungstechnologien, insbesondere heimliche, können diesen beruhigenden Effekt nach der hier vertretenen Ansicht kaum je leisten.

1340 Vgl. oben Zweiter Teil.

1341 Vgl. PFITZMANN/KÖPSELL, S. 157; ALBRECHT P. A., S. 171; oben Vierter Teil, Kapitel III.A.

1342 HEMPEL/TÖPFER, S. 50; NOGALA 1989, S. 165 f.; DERS. 1998, S. 155. DERS. 1998, S. 295 und NOGALA/SACK, S. 149, sehen dadurch die „sozialen Kohäsionskräfte“ der Gesellschaft bedroht.

1343 Vgl. etwa BOERS, S. 14. Interessanterweise scheint die Polizeipräsenz von der Bevölkerung aber gut akzeptiert zu sein, siehe SZVIRCSEV TRESCH/WENGER 2012, S. 108 (83% der befragten Personen sprachen sich für eine Erhöhung der Polizeipräsenz in Wohngebieten aus).

Ausschnitt des überwachten Raums und der Geschehnisse darin erfasst. Der Polizeibeamte auf Patrouille kann die Situation „fühlen" und sich ihr flexibel anpassen: Er kann auf verschiedene Szenarien adäquat reagieren und (potenziellen) Unruhestiftern in Person entgegentreten. Schon dadurch kann er die Situation womöglich spontan, bestenfalls präventiv, entschärfen.[1344] Idealerweise kennt der Polizist die Beteiligten und kann ihnen direkt ins Gewissen reden. Umgekehrt können diese mit dem „menschlichen Kontrolleur […] diskutieren, verhandeln, streiten".[1345] Gerade der Kontakt der Polizei mit den Abweichlern und Delinquenten („auf der Strasse") kann eine wichtige Komponente der Prävention sein. Wenn ein Polizist beispielsweise auf seiner abendlichen Patrouille beim Vorbeigehen mit einer Gruppe von potenziellen Abweichlern unverfänglich einige Worte spricht, kann er späterem Radau vielleicht vorbeugen. Nicht durch Abschreckung, sondern durch Vertrauensbildung. Die simple Abschreckung durch Polizeipräsenz wird in diesem Sinne ergänzt oder gar ersetzt durch eine Form der Wohlgesinnung und des (gegenseitigen) Respekts.[1346] Dieser Effekt mag nicht schon nach der ersten Begegnung eintreten, dafür ist er, einmal Routine geworden, wohl nachhaltiger, versucht das Problem an der Wurzel zu packen und tritt allen Teilen der Bevölkerung mit weniger Misstrauen als die Raumüberwachung gegenüber.[1347] Die persönliche Begegnung ist vielleicht kein ge-

---

1344 NORRIS/ARMSTRONG, S. 117 f. und 168 ff.; GRAS, S. 202 und 219; KAMMERER 2008, S. 146 und 160 f.

1345 NOGALA 1989, S. 165.

1346 Vgl. BOERS, S. 14; GRAS, S. 220. Indem sich die Gruppe respektiert oder ernst genommen fühlt, bringt sie auch dem Polizisten ein gewisses Verständnis entgegen und verhält sich dementsprechend (bei einem Zwischenfall) ruhiger. Ein *kombinierter* Vorteil, welchen BARTSCH, S. 193 f. bei ihrer Bewertung der Polizeipräsenz und Sozialkontrolle gegenüber der Raumüberwachung nicht erwähnt. Dieses Vorgehen setzt einen gewissen Ermessenspielraum des Polizisten voraus, der von Kameras teilweise eingeschränkt wird, siehe KAMMERER 2008, S. 153.

1347 Vgl. zum Ganzen: MOHLER 2000, S. 212 f. Kritisch gegenüber der Polizeipräsenz als Alternative zur Raumüberwachung steht BÜLLESFELD 2002, S. 196 f. Zur Frage, ob Polizeipräsenz eine mildere Massnahme darstellt, siehe MÜLLER L. 2011, S. 250 f. Zu weiteren alternativen Massnahmen BARTSCH, S. 194, BÜLLESFELD 2002, S. 197 ff. (kritisch), KUNZ 2011, S. 374 f. und für alternative gefahrenabwehrende Strategien im virtuellen Raum, PERREY, S. 186 ff. Wenn den wirklich gefährlichen Subjekten durch unsere Freiheiten arg beschneidende bekämpfungsstrafrechtliche Massnahmen, aus welchen im Gegenzug kaum mehr Sicherheit resultiert, nicht besser beizukommen ist als mit herkömmlichen oder alternativen Massnahmen und wenn mit (verhältnismässig) billigen Aufklärungskampagnen oder Ähnlichem ein mindestens gleichwertiger Effekt erzielt werden kann, ohne die Freiheit eines jeden einzuschränken, dann erübrigen sich die in Entwicklung befindlichen Überwachungs- und

eignetes Mittel für Grossbedrohungen und Schwerstverbrecher, aber wie bereits mehrmals festgestellt, scheint sich die polizeiliche Tätigkeit besser auf alltägliche Situationen auszurichten als sich primär an (hypothetischen) Ausnahmesituationen zu messen.

Die Auswirkungen der Raumüberwachung, der Informationsverarbeitungstechniken und der Registrierungsmethoden auf die präventive oder repressive Kriminalitätsbekämpfung sind wenig eindeutig. Trotzdem kann ihnen die Daseinsberechtigung nicht ohne Weiteres abgesprochen werden. Denn: *irgendwie* scheint beispielsweise die Videoüberwachung Kriminalität, wenn auch nur in geringem Masse oder in gewissen Bereichen, zu beeinflussen. Fraglich ist gleichwohl, ob nicht mildere Mittel zu finden sind, um dieselben oder gar bessere Effekte zu erzielen. Der Einsatz von (heimlichen) Überwachungs- und Registrierungstechnologien muss wohlüberlegt sein.

Mit der Allokation von grossen finanziellen Beträgen, die in die Installations- und laufenden Betriebskosten, welche bei allen hier vorgestellten postmodernen Überwachungs- und Registrierungsmethoden nicht gerade günstig sind[1348], und in die Erforschung automatisierter Überwachungssysteme fliessen, fehlt Geld in den klassischen Bereichen der Polizeiarbeit und der Strafverfolgung.[1349] Zu überlegen ist auch, ob diese Gelder nicht sinnvoller in *nachhaltigere* Mittel investiert wären, wie beispielsweise das Bildungssystem, soziale Auffanginstitutionen oder „weichere" Präventionsprogramme. Weshalb sollten Reintegrations- oder „weiche" Präventionsprogramme Verdachtsregistern und anderem „hartem" Vorge-

Kontrollinstrumente. Analog sehr anschaulich auch das von GILLIOM beschriebene Wohlfahrtssystem in Amerika: Mit einem riesigen (administrativen) Aufwand und einer peniblen Überwachung jedes Wohlfahrtsempfängers wird versucht, einige „Wohlfahrtsbetrüger" zu überführen, anstatt die finanziellen Mittel direkt in die Wohlfahrt zu investieren und dafür weniger Empfänger, die mit dem empfangenen Geld nicht über die Runden kommen, zum „Betrug" zu animieren. Das System soll dem Wohlfahrtsempfänger dienen und ihn nicht zusätzlich drangsalieren; es soll Wohltat sein, ihn entlasten, nicht ihn noch schlechter dastehen lassen. Die Wohlfahrt sollte Instrument zur (Re-)Inklusion sein, nicht zur endgültigen und bleibenden Exklusion.

1348 Vgl. etwa Erster Teil, Kapitel III.F.; ZGOBA ET AL., S. 35 f. Sogar kleine Videoüberwachungssysteme mit verhältnismässig geringen Kosten, wie dasjenige in Bielefeld, rentieren nur in Räumen mit einem Kriminalitätsbrennpunkt, und die Rentabilität hängt auch dort von vielen Faktoren ab, siehe KUBERA, S. 145 f.

1349 Vgl. etwa HARCOURT, S. 28.

hen gegen bestimmte Delinquentenkategorien weichen[1350], wenn diese Alternativen hinsichtlich einer Kosten-Nutzenrechnung den postmodernen Überwachungstechnologien nicht unterliegen?[1351]

C. Nichts zu verbergen – Sicherheit und Freiheit

Soziale Netzwerke im Internet boomen. Facebook und Co. erfreuen sich trotz bekannter Sicherheitslücken und dem Wissen, dass es durchaus wahrscheinlich ist, als Bewerber für eine Arbeitsstelle auf seine Auftritte in derartigen Netzwerken durchleuchtet zu werden, steigender Beliebtheit. Offenbar misst zumindest die jüngere Generation der eigenen Privatsphäre keine grosse Bedeutung zu. Es stellt sich damit die Frage, ob es sich beim Gut „Privatsphäre" nicht um eine veraltete Idee handelt, um ein überholtes Konzept aus vergangenen Tagen, welches immer mehr an Bedeutung verliert.[1352] Hat der Durchschnittsbürger (gegenüber dem Staat) nichts zu verbergen?[1353] Auf den Punkt gebracht: Greift die Überwachung nur in die Privatsphäre ein und besteht die Bereitschaft der Gesellschaft, dieses Gut aufzugeben (da sie dieses als überflüssig ansieht), worin liegt dann das Problem?[1354] Ist es mithin zu einem „common sense" geworden, dass eine permanente Überwachung des E-Mail-Verkehrs oder von öffentlichen Parks keinen unzulässigen respektive unangemessenen Eingriff in die Privatsphäre darstellt, *ist* es dann faktisch auch keiner?[1355] Aus den jährlich vom Center for

---

1350 Siehe THIRIET in BAZ Online vom 17. Juli 2010; Bericht HRW, S. 9 f. und 11. Siehe auch HASSEMER 1995, S. 488. Von sehr wenigen Ausnahmen abgesehen, besteht letztlich kein plausibler Grund, weshalb irgendjemand permanent aus dem gesellschaftlichen Leben ausgeschlossen werden sollte, siehe GODERBAUER, S. 116; DITTMANN 1997, S. 138.

1351 ZIMRING, S. 184, 190 und 194 f. Das Beispiel New York zeigte in den letzten Jahren, dass wohl zumindest das Mantra „nothing works" widerlegt sein dürfte, vgl. ZIMRING, S. 195.

1352 So etwa STALDER, S. 121; ähnlich KREISSL/STEINERT, 966; CHESTERMAN, S. 4; WESTIN, S. 450; ZIMMER, S. 213. Skeptisch aber etwa MARX 2007 (Fallacy 31).

1353 „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht gar nicht erst tun." So sprach Eric Schmidt, CEO von Google, anlässlich eines Interviews des Fernsehsenders CNBC im Dezember 2009, zitiert im Artikel „Lauschangriff von Google" in NZZ am Sonntag vom 23. Mai 2010. Dieses Argument wird häufig ins Feld geführt. Es ist bspw. mit SOLOVE 2007, MARX 2007, KREISSL/STEINERT, S. 966 f. und TINNEFELD/BUCHNER/PETRI, S. 52 f., zurückzuweisen. Vgl. auch oben Dritter Teil, Kapitel I.A.

1354 Vgl. VAN DER HILST, S. 5. Das, was die Gesellschaft dem Begriff „Freiheit" zuschreibt, ist, was diese ausmacht. Vgl. MASTRONARDI, N. 37 zu Art. 7 BV.

1355 Die Studie von GILL/SPRIGGS, S. 56 bspw. ergab, dass die befragten Personen die Videoüberwachung nicht als massgebenden Gegner der Privatsphäre betrachtet hatten.

Security Studies (CSS) der ETH Zürich durchgeführten Meinungsumfragen in der schweizerischen Bevölkerung scheint hervorzugehen, dass postmoderne Kriminalitätsbekämpfungsmethoden von der Bevölkerung nicht nur geduldet werden, sondern teilweise mit hohen Werten befürwortet wird, sie auszudehnen.[1356] Nun handelt es sich bei Meinungskundgaben in Umfragen kaum um gründlich durchdachte Stellungnahmen. Aber womöglich äussert sich gerade darin das Kernproblem des heutigen Verständnisses von Freiheit in der Öffentlichkeit: Sie wird oft lediglich oberflächlich wahrgenommen und eindimensional begriffen – als Gegengewicht zur Sicherheit und zum Gemeinwohl sowie als Hilfsmittel zum Verbergen von Geheimnissen.

Privatsphäre zu haben, bedeutet nicht einfach nur, der Öffentlichkeit oder der Obrigkeit möglichst wenig von sich preiszugeben, sondern, essentieller, einen Ort des Rückzugs zu besitzen, welcher unbedingt zu achten ist.[1357] Spezieller auf das Thema dieser Arbeit bezogen, beinhaltet diese Sphäre insbesondere ein „eingriffsfreies Feld".[1358] Überwachungsprozeduren, die als „unacceptable or illegitimate, untrustworthy or invalid, demeaning, unnecessary, or irrelevant" wahrgenommen werden, produzieren geradezu die Bereitschaft zu Abweichungen und Auflehnung.[1359] Unter Gleichgesinnten rechtfertigt die Nicht-Anerkennung der Autorität der Systeme, schuldlos gegen sie vorzugehen. An sich hilfreiche und wirksame, aber nicht akzeptierte respektive als unfair empfundene Bekämpfungsinstrumente können unter dem Strich folglich mehr unerwünschtes Verhalten produzieren als solches verhindern, abweichlerische Äusserungen immer

---

1356 Es ist auf die durchgängig hohen Akzeptanzwerte (jeweils ca. 80% Zustimmung) hinsichtlich Videoüberwachung öffentlicher Plätze, Datensammlungen verdächtiger Personen und Massnahmen gegen Hooligans hinzuweisen, siehe SZVIRCSEV TRESCH/WENGER 2012, S. 107 ff. und DIES. 2013, S. 107 ff. Lediglich Computer- und Telefonüberwachungsmassnahmen werden ambivalent wahrgenommen (ca. 45-50% Zustimmung).

1357 SOLOVE 2008, S. 80; TINNEFELD/BUCHNER/PETRI, S. 52 ff.; VAN DER HILST, S. 4.

1358 Siehe ZERBES, S. 243 und 323 f. In dieser Sphäre der Unantastbarkeit kann ferner offen Kritik an der Obrigkeit geübt werden und Meinungen können offen (und gegebenenfalls politisch unkorrekt) kundgetan werden. Das ist vom Staat bis zu einem gewissen Grad zu dulden. Vgl. HEINRICH, S. 96; SOLOVE 2008, S. 99; KLEY/TOPHINKE, N. 10 f. zu Art. 16 BV.

1359 MARX 2003, S. 372 f. Beispiel: Hinweisschilder der Videoüberwachung werden wohl letztlich vielfach, wie der Hut des Gessler, als Zeichen der Unterjochung wahrgenommen werden. Sie führen wohl hauptsächlich zu Verdruss und Widerstand, nicht zu gesteigerten subjektiven Sicherheitsgefühlen oder sichereren Strassen durch Abschreckungseffekte. Dieser Verdruss vereitelt die Nützlichkeit der symbolischen Überzeugungskraft der postmodernen technischen Instrumente als Kanal der Kommunikation mit der Gesellschaft.

weiter in den Geheimbereich verlagern oder angespannte Situationen eskalieren lassen.[1360]

In diesen Zusammenhängen wird oft ein Spannungsverhältnis zwischen Freiheit und Sicherheit diskutiert.[1361] Hinsichtlich der dargestellten technisierten Massnahmen und Methoden überzeugen Ausgleichsmodelle, die einen Konflikt zwischen Freiheit und Sicherheit lösen wollen, nicht immer.[1362] Freiheit und Sicherheit werden in der Debatte um den Einsatz dieser Technologien regelmässig als Kontrahenten auf einer Waage gegenübergestellt. Dieses duale, vereinfachte Konzept klammert konstruktivere Überlegungen aus.[1363] Weniger Freiheit(en) muss beziehungsweise müssen keineswegs mehr Sicherheit oder weniger Sicherheit mehr Freiheit(en) bedeuten. Aus einer stärkeren Gewichtung der Freiheit(en) können positive Wirkungen auf die Sicherheit der Gesellschaft oder des Einzelnen folgen.[1364] Oder jene lässt Sicherheitsbelange komplett unberührt. Massnahmen, die im Namen der Sicherheit getroffen werden, verringern vielleicht sogar die subjektive oder objektive Sicherheit in der Gesellschaft.[1365] Und ein Plus an Sicherheit kann für eine Bevölkerungsgruppe oder die Gesellschaft genauso gut ein Minus an Sicherheit für eine andere Bevölkerungsgruppe oder Einzelne bedeuten.[1366] Zudem versieht beispielsweise die Privatsphäre nicht einzig das Individuum mit einem Schild zur Verteidigung *gegen* staatliche Eingriffe. Privatsphäre ist ein soziales Anliegen, das der Gesellschaft grossen Nutzen bringen kann. Die gegenseitige Balancierung von Freiheiten als individuellem

---

1360 Siehe dazu MARX 2003, S. 372 f.; HEYMANN, S. 59 f. und 174; GILLIOM, S. 93 ff. und 99 ff. Zu berücksichtigen ist diesbzgl. auch, dass, je weniger diskret bspw. Pläne zur Begehung von Straftaten geäussert werden, desto leichter die Polizei davon Kenntnis erlangen kann. Im Gegensatz dazu werden sie schwerer zugänglich, je öfters intensive und grossflächige Überwachungstechnologien dazu führen, dass die Pläne verborgener geäussert werden.

1361 COUDERT, S. 380; HAYES 2005, S. 1; THIEL, S. 138. Siehe bspw. BARTMANN, S. 271 ff.; SIMON D., S. 91 ff.; ZIMMER, S. 37 ff. Zu den staatstheoretischen Grundlagen von Freiheit und Sicherheit, siehe etwa ALBRECHT P. A. 2003; CALLIESS; SIMON D., S. 9 ff.; THIEL, S. 138 ff.

1362 COUDERT, S. 380; HAYES 2005, S. 1 ff.; SINGELNSTEIN/STOLLE 2012, S. 166; THIEL, S. 476.

1363 CALLIESS, S. 5 f.; SIMON D., S. 263. Diesbzgl. stellt MIDDEL, S. 323 f. fest, die angenommene Konstellation einer prinzipiellen Vereinbarkeit von Freiheit und Sicherheit beschreibe lediglich den Idealfall, in welchem Störer und Opfer sowie der Kausalverlauf in den wesentlichen Zügen bekannt seien und das staatliche Handeln den Übergriff auch tatsächlich verhindern oder beenden könne. Wie bereits dargelegt, trifft dies indes bei den vorgestellten Massnahmen und bei der stark vorgelagerten Gefahrenabwehr oft gerade nicht zu.

1364 CHESTERMAN, S. 257.

1365 Vgl. THIEL, S. 180 ff.; oben Vierter Teil, Kapitel II.A.

1366 Vgl. SOLOVE 2008, S. 261 f.; CHESTERMAN, S. 257 ff.; GILLIOM, S. 129.

Abwehrmechanismus und dem öffentlichen Interesse an mehr Sicherheit als gesellschaftlichem Belang ist demnach nicht immer legitim oder sinnvoll, da beide Interessen Streiter im gleichen Team oder sogar identisch sein können.[1367] Hier wird nicht die Meinung vertreten, dass Zugeständnisse an bestimmte Werte niemals den Einfluss anderer Werte kosten. Der Punkt ist, dass sie das nicht immer tun und vor allem eine Veränderung verschiedene positive Auswirkungen auf verschiedene Bereiche haben kann. Weder das triviale Verständnis noch die streng rechtliche Definition dieser Werte lösen den Diskurs über postmoderne Technologien. Kurz: Eine bipolare Sichtweise (Freiheit gegen Sicherheit) kann diesen Komplex nur sehr oberflächlich erfassen.[1368] Die Begriffe Freiheit, Sicherheit und Privatsphäre sind unter anderem auch instrumentalisierbar und ohnehin anfällig für ständige Bedeutungswandel, wie demjenigen, der sich etwa vollzieht, wenn die postmoderne Risikologik zur Grundlage des Verwaltens von Kriminalität wird.[1369] Das Kalkül mit dem „Preis der Freiheit" stellt sich als profitabel heraus, um die Bevölkerung zu regieren.[1370]

Die streng rechtliche Definition der Freiheiten hilft im kriminalpolitischen Diskurs über die postmodernen Kriminalpräventions- und Strafverfolgungsmethoden nicht immer weiter, weil sie zuweilen nur inhaltsleere Argumente beizutragen vermag. Soll etwa „Privatsphäre" indes nicht lediglich über eine Terminologie, sondern in einem sozialen Zusammenhang erfasst werden, entzieht sich die Bedeutung dieses Werts aus verschiedenen Gründen erst einmal einer sinnvollen, universalen und objektiven Definition.[1371] Der annähernde Zugang von SOLOVE überzeugt deshalb mehr, als der Versuch einer exakten Definition.[1372] Die Missachtung des Konzepts der „Privatsphäre" oder damit vernetzter Teilgehalte verursacht bestimmte Probleme, die bestimmte Konsequenzen nach sich ziehen. Wichtig ist somit nicht an erster Stelle, was unter „Privatsphäre", „Freiheit" oder „Sicherheit" verstanden wird, sondern welche Situationen auf indivi-

---

1367 SOLOVE 2007, S. 763; WESTIN, S, 434.

1368 Gl A. wie THIEL, S. 137 und 180 ff.

1369 Vgl. SINGELNSTEIN/STOLLE 2012, S. 43 f.: Sicherheit *vor* dem Staat und Sicherheit *durch* den Staat bezeichnen bspw. sehr unterschiedliche Forderungen mit vielen Interpretationsvarianten.

1370 KRASMANN, S. 85 f. mit weiteren Hinweisen. Siehe auch HASSEMER 2006, S. 135; ALBRECHT P. A. 2010, S. 5; KUNZ 2011, S. 331; SCHMIDT-SEMISCH, S. 68 ff.; KREISSL/STEINERT, S. 963.

1371 SOLOVE 2007, S. 754; STALDER, S. 121 f.; MINOW ET AL., S. 21.

1372 SOLOVE 2007, S. 759.

dueller und gesellschaftlicher Ebene entstehen, sobald diese „Zertifikate" involviert sind, jene überbewertet oder vernachlässigt werden. „Privatsphäre" (ebenso „Freiheit" und „Sicherheit") in diesem Sinne hat keinen Wert an sich, sie teilt eine Idee oder ein Ziel mit, sie ist Mittel zum Zweck. Sie weist auf eine Problematik hin und sorgt dafür, „dass nicht…" oder hilft dabei, „dass…".[1373] Diese Begriffe sind in einer kriminalpolitischen Debatte als Feldstecher zum Betrachten der „neuen Landschaft"[1374] postmoderner Kontrolltechniken zu gebrauchen – als ein künstliches Gebilde beziehungsweise als Sammelbegriffe zur Umschreibung eines Komplexes von Konsequenzen und Dynamiken.

Gut veranschaulichen lassen sich die dargestellten Probleme am Beispiel der Videoüberwachung des öffentlichen Raums. Viele Studien stellen fest, dass diese die an sie gestellten Ansprüche im Bereich der Kriminalitätskontrolle selten erfüllt. Trotzdem: Vielfach dreht sich die Debatte in der Öffentlichkeit und im Fazit derselben Studien um die immerzu wiederholte Mahnung, Freiheit dürfe nicht zugunsten von Sicherheit aufgegeben werden.[1375] Die Debatte sollte sich von dieser uralten Waagemetapher mit Sicherheit und Freiheit auf je entgegengesetzten Seiten lösen, ansonsten können Gespräche über die postmodernen Kriminalitätsbekämpfungstechnologien ungeachtet deren festgestellter Unwirksamkeit in vielen Bereichen nur viel zu allgemein und schein-systematisch geführt werden. In der oberflächlichen Diskussion anhand dieser abstrakten, kaum fassbaren Begriffe werden zu viele der wichtigen, wichtigeren Punkte ausgeklammert: Die (technische) Machbarkeit (im Rahmen bestehender Schranken), Differenzen zwischen Theorie und Praxis, tatsächliche Wirkungen auf die Zielkriminalität, unvorhergesehene (Neben-)Folgen etc.[1376] Die Reduktion auf zwei sehr schwer einschätzbare, oftmals nur schwer zu gewichtende, symbolbehaftete Extreme, die derart entkoppelt und abstrahiert von der eigentlichen Fragestellung sind, hebt die Beurteilung dieser Fragestellung auf eine andere Ebene und wandelt sie zu einer Glaubensfrage.[1377] Eine sorgfältige, angemessene Beurteilung scheint nur auf dem Boden einer Gesamtbetrachtung möglich. Hingegen spuren Gespräche in der Öffentlichkeit über das Spannungsverhältnis zwischen Sicher-

---

1373 SOLOVE 2007, S. 763: „Privacy is a set of protections against a related set of problems."

1374 STALDER, S. 123.

1375 HEMPEL/TÖPFER, S. 58: „The debate is focusing on how to balance public safety and national security on the one hand and individual privacy on the other."

1376 Vgl. auch BOWYER, S. 18.

1377 Und Glaubensfragen ist nur schwer mit Argumenten der Vernunft zu begegnen, vgl. NIGGLI 1995, S. 96.

heit und Freiheit die Beurteilung der Verhältnismässigkeit in zuweilen wenig konstruktive Richtungen vor. Die Abwägung gegen die Sicherheit kann die Freiheit in einem Klima der Unsicherheit nur verlieren. Oberflächliche Debatten auf öffentlicher Ebene können daher Verhältnismässigkeitsprüfungen massgeblich vorbelasten.[1378]

Vor allem auf die „alltägliche Verbrechensbekämpfung" übertragen, wird ersichtlich, dass derartige Überlegungen es wert sind, gemacht zu werden[1379]: Neben der Makrokriminalität und dem absolut konformen Verhalten existiert eine reichhaltige Auswahl an Handlungsformen (wiederum handelt es sich dabei eben nicht um ein zweiteiliges Wertesystem). Wer demnach nicht absolut konform handelt, befindet sich bereits in einem Graubereich, was angesichts des wandelbaren und unbestimmten Begriffs der Konformität nicht unbedenkliche Konsequenzen auf die Bekämpfung sozial-inadäquaten Verhaltens haben kann. Sozial nicht adäquates Verhalten sollte zum Erhalt der Vielfalt von Denk- sowie Lebensweisen und Meinungen erlaubt und geduldet bleiben, solange es eine gewisse (nicht zu tief anzusetzende) Schwelle nicht überschreitet, auch wenn es von Teilen der Bevölkerung nicht erwünscht ist oder weggewünscht wird.[1380]

D. Aggregation und Konformitätsdruck

Täglich werden in verschiedenen Datenbanken Informationen über uns angehäuft. Zumeist geben wir diese Informationen preis, ohne darüber nachzudenken.[1381] Isoliert betrachtet sagen sie ohnehin wenig über uns aus. Sobald jedoch mehrere dieser an sich unerheblichen Informationen kombiniert werden, manifestiert sich ein Mosaik, ein Gesamtbild, das mehr über uns aussagt als die einzelnen Teile. Diese Datenverknüpfungsmethode wird häufig „Aggregation" genannt.[1382] Sie ermöglicht Rückschlüsse auf unser Verhalten, unsere Persönlichkeit, Beziehungen zu Drittpersonen oder Bewegungen und kann je nachdem auch einzelne zukünftige Handlungen antizipieren lassen. Die Aggregationsme-

---

1378 Vgl. ALBRECHT P. A. 2003, S. 84 f. Siehe dazu weiter unten Vierter Teil, Kapitel V.D.

1379 Siehe auch unten Vierter Teil, Kapitel V.B.

1380 Vgl. SOLOVE 2008, S. 94.

1381 BISCHOF/SCHWEIZER, S. 152; BELSER, S. 2 N. 4 f.; MEIER, N. 304.

1382 SOLOVE 2007, S. 766; MINOW ET AL., S. 35-37; CHESTERMAN, S. 229 f. Vgl. Bericht BJ inter net, Anhang 1, S. 5; COOPER, S. 149. POPITZ, S. 7 hielt es 1968 für unwahrscheinlich, dass „die jeweils begrenzten Kenntnisse anderer über unser Verhalten [sich] akkumulieren" und „in einer Hand" zusammenfliessen. Genau darauf zielen Aggregationsprozesse jedoch ab.

thode kann dazu benutzt werden, ansonsten schwer zugängliche respektive gut gehütete persönliche Informationen aus mehreren leichter verfügbaren Datenquellen oder einzeln gesehen unproblematischen Personendaten abzuleiten.[1383]

Dieses Gesamtbild oder Profil wollen wir vielleicht jedem oder jemand Bestimmtem verheimlichen. Rückschlüsse auf sich selbst lassen Menschen nur selektiv zu. Die Aggregation zeigt damit anschaulich das Problem zu enger Definitionen der Privatsphäre: Das Sammeln und Archivieren dieser alltäglichen Daten, beispielsweise vom Ort und Zeitpunkt einer Geldtransaktion am Geldautomaten, betrifft die Privatsphäre im klassischen Sinn nicht. Jeder kann einen dabei beobachten. Diese Information kann indes in Verbindung mit anderen Informationen, bereits zum Beispiel mit dem Wissen um mehrere derartige Transaktionen, sehr rasch sehr aufschlussreich werden, beispielsweise Rückschlüsse über Gewohnheiten erlauben. Das kann problematisch sein.[1384] Einerseits, weil die einzelnen Informationen für sich gesehen als a priori harmlos, deren Kundgabe als freiwillig und eine mögliche Erhebung nicht als Eingriffe qualifiziert werden und der Betroffene somit nachträglich nicht kontrollieren kann, ob diese Informationen irgendjemandem weitergegeben oder (wofür auch immer) verwendet werden. Andererseits bleiben dem Betroffenen die Aggregationsvorgänge verborgen. Der Zugang zu seinen Profilen, zu den darauf gestützt getroffenen Entscheidungsprozessen ist ihm damit verschlossen und Korrekturmöglichkeiten werden allenfalls verwehrt.[1385] Um das Machtgefälle zu überwinden, ist somit die Reziprozität, die Wiederherstellung der Informationssymmetrie wichtig.[1386] Je mehr der Bürger offenlegt, desto mehr ist die Datensammel- oder Datenanalysestelle zu verpflichten, ihrerseits Daten offenzulegen. Der Bürger soll die über ihn gesammelten Daten und abgeleiteten Profile kennen und deren Löschung oder Berichtigung, zumindest im Rahmen einer (nachträglichen) richterlichen Beurteilung, beantragen können.

Die Aggregation führt demnach zu Informationsasymmetrien, schafft ein Machtgefälle und stört letztlich das Vertrauensverhältnis zwischen dem Staat und dem

---

1383 PROBST, S. 26 und 33 f. Die Aussagekraft der gesammelten Personendaten ist ein wichtiges Indiz für die Eingriffsschwere. Zu beurteilen ist dabei die Aussagekraft des Gesamtbilds, welches durch die Verknüpfungen entsteht.

1384 Vgl. etwa PROBST, S. 30 f. und 35 ff.; ROSSNAGEL/DESOI/HORNUNG 2011, S. 698. Eben auch das Sammeln, Analysieren und Verknüpfen von im virtuellen Raum frei verfügbaren Daten.

1385 BISCHOF/SCHWEIZER, S. 152; MEIER, N. 12; ROSSNAGEL/DESOI/HORNUNG 2011, S. 698.

1386 Vgl. MARX 2005.

Einzelnen. Der analysierende Staat ist gegenüber dem Betroffenen ungerechtfertigt im Vorteil. Betroffene haben sich dem Analysten preiszugeben, was diesem erlaubt, sie über die entstehenden Informationsgefälle zu manipulieren und letztlich zu kontrollieren.[1387] Die Betroffenen sind dem Analysten ausgeliefert und können dadurch in auswegslose Positionen, mit denen sie sich vielleicht irgendwann abfinden müssen, gedrängt werden.[1388] Die Aggregation begünstigt damit unter anderem Einschüchterungseffekte, indem potenziell betroffene Personen befürchten, sie legten mit ihren Einzelhandlungen ungewollt Lebenssachverhalte offen, die sie lieber nicht offenbarten. Teilt die Behörde dem Betroffenen den getätigten Sammel- und Analysevorgang und den Grund dafür mit, zeigt sie ihm, dass sie ihn für verdächtig hält oder hielt und würdigt ihn somit in der Regel zudem herab. Die für den Betroffenen sichtbar gemachte Etikette lässt ihn von diesem Zeitpunkt an stets spüren, dass er einer Risikokategorie angehört und insofern jederzeit erneut einer Überprüfung unterzogen werden könnte.[1389]

Die Aggregation kann daher Konformitätsdruck auslösen. Bürger könnten sich „übervorsichtig" verhalten, sich zu Verhaltensänderungen in eigentlich unproblematischen Bereichen veranlasst sehen, um etwa nicht auf einer Liste zu landen oder den Fokus der Raumüberwachung, zum Beispiel eines intelligenten Videoüberwachungssystems, auf sich zu ziehen.[1390] Kritiker von Überwachungsmassnahmen meinen, schon in kleinem Rahmen seien Verhaltensänderungen – vor allem bei an sich konformen Personen, die fürchten, sie könnten auffallen oder unangepasstes Verhalten zeigen – zu beobachten. BIDLO merkt zu diesem Verhaltensmuster an: „Konformitäts- und Kontrolldruck entsteht durch Überwachung, aber vor allem durch die befürchtete Überwachung."[1391] Diese „Konfor-

---

1387 Siehe etwa NOGALA 1989, S. 104; ROTHE, S. 71; LSE Briefing, S. 56; INTRONA/NISSENBAUM, S. 46; STALDER, S. 121; SPINNER, S. 262. Wobei bereits Sachverhalte, die dem Betroffenen gegenüber dem Analysten, der Behörde etc. peinlich sind, ausreichen, die Position zu verändern, in denen sich die beiden Parteien gegenübertreten.

1388 Siehe GILLIOM, S. 84.

1389 Die vermittelte Etikette muss dazu nicht einmal besonders weit gehen (verdächtiger als der Durchschnitt, weil „jung" oder „arm", reicht bereits). Zum Ganzen SOLOVE 2007, S. 766 f. und 770; STALDER, S. 120 f.; LSE Briefing, S. 56 f.; ausführlich GILLIOM.

1390 Vgl. SIMON, S. 272; HORNUNG/DESOI, S. 156.

1391 BIDLO, S. 40. Ebenso FISAHN, S. 37. So auch in zwei Experimenten von BATESON/NETTLE/ROBERTS und ERNEST-JONES/NETTLE/BATESON, bei welchen sich Personen kooperativer verhielten (in Form einer grösseren Spende bzw. der Abfallbeseitung), wenn über der „Kaffeekasse" in der Cafeteria Poster von Augen hingen (welche das Gefühl des Überwachtwerdens simulieren sollten).

misierung“ zu *überangepasstem* Verhalten im überwachten Raum nennt sich auch „Einschüchterungseffekt“ oder „chilling effect (on human behaviour)“.[1392] Wo die Überwachung kleinräumig eingesetzt bleibt, könnten Einschüchterungseffekte insbesondere dazu führen, dass die Leute beispielsweise einen überwachten Park meiden. An die Stelle des Unsicherheitsgefühls im Park tritt das unangenehme Gefühl der Überwachung, insofern wird der Park wohl nicht unbedingt für eine grössere Anzahl Personen nutzbar gemacht, jedoch *möglicherweise* für Personen mit positiver Einstellung gegenüber Videoüberwachung. Solange den verdrängten Parkbesuchern nicht nachgejagt wird, indem *jeder* für sie in Frage kommende Aufenthaltsort derart versiegelt wird, kann diese Wirkung mancherorts anstrebenswert sein.[1393] Andernorts könnten verdrängende Einschüchterungseffekte den gemeinsamen öffentlichen Raum in getrennte Lebensräume für vielerlei Publikum aufteilen oder immer mehr private Lebensräume entstehen lassen. Eine Balance mit freien Räumen für verschiedene Personengruppen, einerseits für sehr sittliche, hochkonforme und andererseits für weniger angepasste, die vielleicht eine von der Mehrheitsmeinung abweichende Lebensweise zelebrieren (es geht hier aber um grundsätzlich *nicht* strafrechtsrelevant Agierende)[1394], scheint noch wenig problematisch. In der Praxis, bedingt durch ein aufgewühltes Klima des Misstrauens und der abnehmenden Solidarität für das Anderssein und bereits geringfügig abweichendes Verhalten, ist es aber keine leichte Aufgabe, diese Balance zu halten. Ohne gemeinsame Begegnungsräume oder -projekte, welche unterschiedliche Menschen näher zusammenbringen, sind zudem allmähliche Entfremdungseffekte und steigendes gegenseitiges Misstrau-

---

1392 Siehe zu Einschüchterungseffekten durch die verschiedenen Technologien und Methoden: BARTSCH, S. 79 f.; MÜLLER L. 2011, S. 4; HENSEL, S. 527; BELSER, S. 2 f. N. 5; PETRI, G N. 54 und 532; THIEL, S. 249 ff.; ZSCHOCH, S. 200; ROSSNAGEL, S. 1240; TSCHENTSCHER, S. 392; ZERBES, S. 43; CHESTERMAN, S. 251; SOLOVE 2008, S. 193 f.; NOWAK, S. 38 und 40 f.; VAN DER HILST, S. 20 f.; LSE Briefing, S. 56 f.; BVerfGE 65, 1 (42); 115, 320 (354 f.); 120, 378 (402 und 430); 125, 260 (319 f.). Dieser Effekt kann faktische Eingriffe z. B. in die Versammlungs- bzw. Meinungsäusserungsfreiheit bedeuten, siehe ROHNER, N. 18 zu Art. 22 BV; TSCHENTSCHER, S. 392; BARTSCH, S. 80, jeweils mit Hinweisen.

1393 Im Sinne einer „Rückeroberung“ des öffentlichen Raums für die Bürger, siehe KUNZ 2011, S. 347. Vgl. KAMMERER 2008, S. 96 und 101 sowie anschaulich GATES, S. 73 und 76 f. Allerdings fanden z. B. GILL/SPRIGGS, S. 53 ff. *keine* Änderung der Angewohnheiten der Bürger. Die videoüberwachten Räume wurden von den Bürgern nicht reger benutzt als vor der Installation der Kameras. Ob derartige Wiederherstellungsbemühungen über Überwachungstechnologien zweckmässig sind, ist also zweifelhaft.

1394 SCHMIDT-SEMISCH, S. 88 nennt diese Räume „Orte der Andersheit“.

en zu vermuten.[1395] Mit einer zunehmenden Entfremdung der Gruppen steuert die Gesellschaft auf Kontrollstrategien zu, durch die begonnen wird, mittels Teilungspraktiken unerwünschte Risikogruppen auszuschliessen und ihnen Zugänge zu verwehren oder Risikopersonen mittels sichernden Konzepten zu paralysieren.[1396]

Einschüchterungseffekte grossräumiger und breit streuender Methoden könnten theoretisch zu konformem Verhalten drängen, bestimmte Räume oder Risikopersonen und -gruppen meiden lassen oder auch Selbstzensur fördern.[1397] Einschüchterungseffekte sind diesbezüglich einerseits wohl vor allem bei kombiniert angewendeten Methoden und Aggregationstätigkeiten (zum Beispiel Datenverknüpfungen von Informationen aus frei verfügbaren Internetquellen) zu vermuten. Andererseits dürfte der Grossteil der technischen Massnahmen lediglich in Ausnahmefällen einen starken Konformitätsdruck ausüben.[1398] Analog der präventiven Wirkungen auf deviante Personen beruhen Einschüchterungswirkungen auf konforme Personen darauf, dass den Technologien bestimmte Effekte zugeschrieben werden. Damit präventive Wirkungen eintreten, müssen die Technologien als effizient funktionierend wahrgenommen werden.[1399] Einschüchterungseffekte hingegen setzen zusätzlich voraus, dass konforme Personen vermuten, die Technologien würden missbräuchlich verwendet oder funktionierten unzuverlässig: Sie ziehen beispielsweise die Möglichkeit in Betracht,

---

1395 Vgl. dazu KUNZ 2011, S. 374 f.; KAMMERER 2008, S. 101; SINGELNSTEIN/STOLLE 2012, S. 143. Man kann durchaus noch argumentieren, dass beispielsweise Drogensüchtigen keine Rückzugsorte in Stadtzentren und Personen mit bestimmten extremistischen Ansichten keine Austauschplattformen wie etwa Internetforen zugestanden werden sollten. Schwieriger wird die Verweigerung von Rückzugsorten sicher, sobald Personengruppen (bspw. Jugendliche) betroffen sind, die diese Orte innerhalb der Gesellschaft für ihre Entwicklung oder einen Ausgleich benötigen und die (quantitativ wie qualitativ) einen wesentlichen Teil unserer Gesellschaft ausmachen.

1396 Siehe zum Ganzen die Ausführungen im Dritten Teil. Damit einher geht möglicherweise eine fortschreitende Entsensibilisierung der Mehrheit für die Probleme und Anliegen der Andersartigen, Andersdenkenden und der Unerwünschten.

1397 Anstatt vieler: BELSER, S. 2 f. N. 5; COOPER, S. 147; TSCHENTSCHER, S. 392.

1398 Wohl zu Recht skeptisch hinsichtlich des Konformitätsdrucks der Rasterfahndung, ROGALL, S. 625 und ZSCHOCH, S. 51, sowie der Vorratsdatenspeicherung, ZIMMER, S. 212 ff. Viele Vorstufen zum Konformitätsdruck dürften zu vernachlässigen sein. Im realen Raum äussern sie sich vielleicht als Hemmung von urprivaten Verhaltensweisen, im virtuellen Raum vielleicht mehr in einer milden Selbstzensur – Menschen machen sich nun einmal Gedanken darüber, was sie in Anwesenheit anderer tun und sagen. Vgl. COOPER, S. 147.

1399 Siehe oben Dritter Teil, Kapitel V.B.

durch die Technologien ungerechtfertigt verdächtigt zu werden und dadurch Folgemassnahmen ausgesetzt zu sein oder gedemütigt zu werden, dass die Informationen über die eigene Person die Kontrolleure belustigt oder dass möglicherweise kompromittierende, persönliche Informationen an die Öffentlichkeit gelangen.[1400] Insofern begünstigen nicht zuletzt (über)dramatisierte Warnungen vor den Gefahren postmoderner Technologien, vor der Allgegenwärtigkeit von Überwachung und vor dem Überwachungsstaat die allenfalls mit diesen Technologien verbundenen Einschüchterungseffekte.

Jedoch ist es auch sehr wahrscheinlich, dass als Antwort auf die Überwachungsmassnahmen aktive und widersetzende Verhaltensänderungen folgen.[1401] Dazu könnten etwa Umgehungstaktiken gehören.[1402] Zudem könnten Überwachungstechnologien anstatt zu angepasstem Verhalten auch zu entgrenztem Verhalten führen.[1403]

Zum Beispiel ist es im Falle einer flächendeckenden Überwachung und alle Lebensbereiche betreffenden Datensammlung, wie sie sich etwa in England abzeichnet, durchaus vorstellbar, dass die Anpassung zuletzt in einer breiten Gleichgültigkeit mündet oder die Autorität der Systeme in weiten Bevölkerungsteilen nicht mehr anerkannt wird.[1404] Die neue Generation von Menschen, welche mit der Raumüberwachung aufwächst, muss den psychischen Stress des „chilling effect" nicht mehr zwingend verspüren.[1405] Die Überwachung und wahrscheinlich auch die *Erwartungen der Überwacher* könnten schlicht ignoriert werden. Das ist umso wahrscheinlicher, je stärker die Erwartungen von Überwachern und die Überzeugungen der Überwachten auseinanderfallen. Man kann dieses Verhalten ein Aufbegehren nennen, vielmehr dürfte es aber einfach Ausdruck einer Abstumpfung und Gleichgültigkeit gegenüber dem Überwachtwer-

---

1400 Vgl. MÜLLER L. 2011, S. 133, 138 f. und 144 f. („voyeuristisch motivierte Datenbeschaffung"). Auch die sichtbare Präsenz einer Kameraattrappe kann theoretisch unterdrücken, Grundfreiheiten auszuüben, wenn diese nicht als Attrappe wahrgenommen wird, siehe PETRI, G N. 197.

1401 Vgl. den Artikel „Das Ende des Vergessens" in NZZ am Sonntag vom 10. Oktober 2010. Zum Beispiel könnten im Internet, das einer Überwachung grundsätzlich leicht zugänglich ist, immer mehr Räume und Inhalte mit Passwörtern geschützt werden.

1402 Vgl. etwa POPITZ, S. 8 f.; oben Dritter Teil, Kapitel V.A.

1403 PETRI, G N. 50; TINNEFELD/BUCHNER/PETRI, S. 51 ff. mit weiteren Hinweisen.

1404 Bei britischen Jugendlichen scheint dies bzgl. der Videoüberwachung bereits der Fall zu sein, siehe Erster Teil, Kapitel II. A. und auch NOGALA/SACK, S. 156.

1405 NOGALA 1998, S. 322.

den sein, welcher unter anderem gerade auf den angesprochenen Wertverlust der Privatsphäre folgt. Insofern lenken (staatliche) Überwachungsmassnahmen vielleicht nur diejenigen, welche mit ihnen nicht vertraut sind, zu konformen Verhalten, die anderen hingegen, bewusst oder unbewusst, beispielsweise zur schamlosen Übertragung des im privaten Bereich gewöhnten und gebilligten Verhaltens auch in die Öffentlichkeit. Vielleicht lernt der Mensch durch die neuen Medien (soziale Online-Netzwerke, Blogs etc.) sich nicht so schnell zu schämen, sich unter dem Auge eines Beobachters so zu verhalten wie immer. Vielleicht kümmert sich die mit diesen Technologien aufgewachsene Generation nicht mehr um sozialadäquates Verhalten in der Öffentlichkeit und es ist ihr egal, was die Überwacher von ihr halten. Vielleicht verändert sich die Einstellung zum sozialadäquaten Verhalten in der Öffentlichkeit.[1406]

Eine sich ausbreitende Gleichgültigkeit gegenüber Raumüberwachungsmassnahmen beraubte diese aber deren lenkender Funktion zu sozial-adäquatem Verhalten. Würde sich eine derartige Entwicklung auf breiter Linie durchsetzen, wäre ein weiterer Zweck der Raumüberwachung demnach nicht erreicht, im Gegenteil hätten sich in diesem Fall Verhaltensweisen verwirklicht, welche deren Kernzielen diametral gegenüberstünden. Die Anpassung könnte sich auf die Raumüberwachung folglich negativ auswirken, wodurch ein weiterer Rechtfertigungsgrund entfiele. Auch wenn Auflehnung die Reaktion auf Überwachungsmassnahmen ist, wird dadurch eher Abweichung erzeugt statt verhindert.

Gewöhnt sich die Gesellschaft an die Verhältnisse einer beginnenden Verüberwachlichung, könnte dies ab einem bestimmten Punkt gleichsam dazu führen, dass das Verständnis für gewisse „alte" Freiheitsrechte verloren ginge und dadurch bestimmte *Tugenden* verkümmerten, etwa politisches Engagement, Solidarität und Zivilcourage der Gleichgültigkeit weichen könnten.[1407] Auf der anderen Seite wäre es grundsätzlich auch plausibel, dass die Aufgabe der Privatsphäre ebendiese Tugenden aufblühen lassen würde.[1408] Mehr als spekulieren

---

1406 PETRI, G N. 50 nennt dies „entgrenztes Verhalten". Vgl. ZIMMER, S. 213 mit weiteren Hinweisen. M. E. weist auf die Plausibilität einer derartigen Entwicklung auch die Studie von SHORT/DITTON hin.

1407 Vgl. das Zitat von Jutta Limbach bei ALBRECHT P. A. 2003, S. 41 f.; SOLOVE 2008, S. 79; DERS. 2007, S. 765.

1408 Siehe SOLOVE 2008, S. 80 f. mit Beispielen. Anzumerken ist jedoch, dass die dort vorgestellten Gesellschaftsformen mit vernachlässigbarer Privatsphäre im Wesentlichen auf informeller Sozialkontrolle beruhen, also auf bodenständigen, persönlichen *sozialen* Strukturen. Mit der Kontrolle über (automatisierte) Raumüberwachungssysteme haben jene wenig

lässt sich momentan in dieser Frage wohl nicht. Erste Anzeichen für Umschwünge zeigen sich, wie dargestellt wurde, in Ländern mit fortgeschrittener technisierter Überwachung.

V. Bedingte Wirksamkeit rechtlicher Schranken

A. Was ist und was sein soll

JAKOBS stellt fest, das Feindstrafrecht habe in den Alltag Einzug gehalten. Er folgert daraus: Jeder, der nicht anerkenne, dass das Feindstrafrecht Wirklichkeit geworden sei, verhalte sich wirklichkeitsfremd.[1409] Indes muss jedoch der Soll-Zustand, oder das, was „nicht sein darf", im Diskurs über bekämpfungsstrafrechtliche Massnahmen keine untergeordnete Bedeutung haben. In seinem Konzept übersieht JAKOBS, darin gleicht das Konzept einmal mehr biokriminologischen Ansätzen, dass das Ordnungssystem Recht nicht in erster Linie die bestehende Wirklichkeit abbilden soll, sondern im Gegenteil durch Normen eine für die Gesellschaft bessere Wirklichkeit herzustellen versucht.[1410] Es muss aber zugestanden werden: Das traditionelle Strafrecht befindet sich im Wandel hin zu einem Bekämpfungsstrafrecht.[1411] JAKOBS ist insofern in funktionell-theoretischem Sinne zuzustimmen, dass die Gefahrenabwehr oder eben auch spezielle technisierte Massnahmen in der Regel auf tatsächliche Feinde zugeschnitten wären.[1412] Auf Bürger sollten extensive und exzessive Technologien der Gefahrenabwehr keine Anwendung finden.

Die Globalisierung bringt Herausforderungen für die Gefahrenabwehr und die Strafverfolgung mit sich. Es bestreitet niemand, dass die postmoderne und globalisierte Gesellschaft gewisse Gefahren in sich birgt. Häufige Mängel eines Anfangsverdachts (beispielweise durch eine Anzeige) bei Makrodelikten (insbesondere bei organisierter Kriminalität und Terrorismus) etwa führen zu einem

gemein, weshalb deren Lehren und Errungenschaften nicht (direkt) auf die hier besprochene Problematik übertragbar sind.

1409 JAKOBS 2006, S. 289 und insb. 294.

1410 LOADER/SPARKS, S. 131. Vgl. SENN, S. 10.

1411 KUNZ 2006, S. 72 und 73 f.; ZERBES, S. 323 f.

1412 Vgl. JAKOBS 2004a, S. 90.

gewissen Ermittlungsdefizit.[1413] Das Argument, die Kriminalitätsbekämpfungsbehörden gerieten ins „Hintertreffen“[1414], weshalb sie zum Einsatz sämtlicher oder immer neuer Überwachungstechnologien zu ermächtigen seien[1415], kann aber durchaus kritisiert werden: Neue technisierte und automatisierte Überwachungsmethoden holen nicht in erster Linie einen technischen Vorsprung Krimineller ein, sondern rüsten den Staat mit einem Mehr an zumeist proaktiven und heimlichen Instrumenten auf, die bei genauerer Betrachtung teilweise Paradigmenwechsel und rechtliche Inkompatibilitäten verursachen. Diese Aufrüstung kann durchaus legitim sein – sie ist aber offen zu legen.[1416] Es ist täuschend, von einem Erhalt des Überwachungsvermögens („maintain our capability“) zu sprechen, wenn es tatsächlich um einen Ausbau von Überwachungsmöglichkeiten geht.[1417] Fraglich ist indes zum einen, ob die vielfach als „neue“ Herausforderungen für die Gefahrenabwehr präsentierten Veränderungen der Postmoderne und Globalisierung tatsächlich so neu und die sich immer weiter entwickelnden Informations- und Kommunikationstechnologien tatsächlich so anders sind, dass sie nach einem Umdenken und neuen Methoden in der polizeilichen Gefahrenprävention und Strafverfolgung verlangen.[1418] Sollte dies der Fall sein, ist zum anderen äusserst fraglich, ob die heute häufig gewählten Methoden und Technologien des Bekämpfungsstrafrechts gute beziehungsweise hilfreiche Antworten auf diese neuen Herausforderungen geben.

Über den Einsatz auch sehr einschneidender Instrumente in Ausnahmefällen lässt sich sicherlich reden, zu bedenken ist aber, dass die vorgestellten Massnahmen in Bereichen der (professionellen) Schwerstkriminalität oder bezüglich Grossbedrohungen meist nur symbolisch praktizierbar sind.[1419] Nicht alles, was

---

1413 Vgl. etwa STEGMANN A., S. 127 f.; SÖLLNER, S. 22 f.; THIEL, S. 474. Siehe ausführlich zu diesen Herausforderungen: THIEL, S. 5-49; SIEBER, S. 4 ff.; SZUBA, S. 34 ff.

1414 So etwa HOFMANN, S. 121. Vgl. oben Erster Teil, Kapitel III.A.2.

1415 Kritisch gegenüber dieser Forderung: ALBRECHT F., N. 28.

1416 Gl. M. wie KUNZ 2000, S. 8. Vgl. auch HASSEMER 2006, S. 134.

1417 Gl. M. wie LSE Briefing, S. 6.

1418 Vgl. NOWAK, S. 11. Der Meinung, es herrsche ein neues Szenario, sind etwa: SAVONA/MIGNONE, S. 8 ff.; PAINTER, S. 69 ff.; CLARKE, S. 97 ff.; HOFMANN, S. 121. Skeptisch etwa: OBERHOLZER 2004, S. 54; LSE-Briefing, S. 6.

1419 Für die Schweiz gilt dies verstärkt. Wären die wirklich bedrohlichen Situationen oder Personen breiter gestreut, könnte die Automatisierung auch eine Chance sein, insofern sie nicht auf Kosten von Arbeitsplätzen verwirklicht und tatsächlich funktionieren würde (die frei gewordenen Polizeikräfte könnten stärker in den wirklich dringlichen Belangen eingesetzt werden).

technisch realisierbar ist, muss im Vorgehen gegen diese Gefahren wünschenswert oder zu rechtfertigen sein. In der „Normalkriminalität" auf alle Fälle sieht die Sache ohnehin anders aus: Herkömmliche Massnahmen, wie etwa erhöhte Polizeipräsenz, greifen in diesem Bereich in der Regel weniger in die Grundrechte ein, führen seltener zu einem Gefühl der ständigen Überwachung und sind insbesondere zumeist persönlicher.[1420]

B. Präventivwirkung des Nichtwissens

Die Polizeipatrouille kann den Raum nicht ständig und lückenlos kontrollieren, sondern stattdessen höchstens Stichprobenkontrollen in unregelmässigen zeitlichen Abständen und einer gewissen Häufigkeit einrichten. Das ist vor dem Hintergrund, dass Abschreckungswirkungen ohnehin stark begrenzt sind, gar nicht so verkehrt. Mit anderen Worten kann zum Beispiel eine gewisse Umständlichkeit der manuellen Überprüfung einer verdächtig agierenden Person durch eine Polizeipatrouille bereits eine faktische Schranke für ausufernde Identifizierungsbestrebungen sein.[1421] Das Gleiche gilt etwa für Papierakten im Verhältnis zu digitalisierten Akten.[1422] Die staatlichen Behörden werden zudem entlastet, wenn sie nicht Kenntnis von allen Sachverhalten erlangen, die verdächtig sein könnten, und nicht jedes Bagatelldelikt verfolgen müssen.[1423] Der Mut, in bestimmten Be-

---

1420 Vgl. HASSEMER 2000, S. 263; GRAS, S. 129; CUSSON, S. 77. Vgl. oben Vierter Teil, Kapitel IV.B. ZIMRING, S. 162 ist m. E. beizupflichten: „Police matter, and they matter a lot more than many experts thought as recently as 20 years ago." Siehe dazu DERS., S. 147, 158, 174 und 193 f. Für einige interessante Untersuchungsergebnisse, wie die Videoüberwachung die Polizeiarbeit behindern kann, siehe NORRIS/ARMSTRONG, S. 188 ff.; STAPEL, S. 53 f. mit weiteren Hinweisen. Siehe dazu auch YOUNG 1999, S. 192 f.

1421 Vgl. GRAS, S. 219; MARX 1984 („Technical impossibility and inefficiency have declined as the unplanned protectors of liberty."); oben Vierter Teil, Kapitel III.A. Siehe auch die dargestellten Meinungen von Polizeibeamten bei GATES, S. 82; Venice Commission 2007, S. 5 f. N. 17 und 21; BVerfGE 120, 378 (397 ff.). Ebenso hält eine geringe Kapazität der Speichermedien die Datenbankbetreiber zu Zurückhaltung beim Archivieren von wenig relevanten Informationen an. Je grösser die Speicherkapazitäten und je besser die Suchmechanismen von Datenbanksystemen werden, desto unbedachter können Informationen ohne Vorselektion, unbesehen und direkt auf Vorrat abgespeichert werden.

1422 CHESTERMAN, S. 226.

1423 FOUCAULT 1994b, S. 268 („Wenn alles gefährlich ist, dann haben wir immer etwas zu tun."). Ebenso POPITZ, S. 17 f. Vgl. auch SIMON D., S. 265; KUNZ 2002, S. 727.

reichen die „Präventivwirkung des Nichtwissens“[1424] spielen zu lassen, setzt Ressourcen für dringendere Angelegenheiten frei.

Das polizeiliche Opportunitätsprinzip verlor aber, im Gegensatz zum strafprozessualen, in Zeiten erhöhter Sicherheitsbedürfnisse der Gesellschaft an Bedeutung und wich der „Schutzpflicht aus grundrechtlicher Verpflichtung“.[1425] Mehr entdeckte Devianz zieht mehr Arbeit nach sich. Ist diese mit den verfügbaren Ressourcen nicht zur öffentlichen Zufriedenheit zu erledigen, blamiert der Misserfolg die staatlichen Behörden (zu Unrecht) und verunsichert die Bevölkerung zusätzlich (denn die Kriminalität scheint ja offensichtlich überhandzunehmen).[1426] Weiter bleibt die treibende Effizienzrationalität der Technologien ein Problem. Der Mensch wird in technisierte Rationalitäten hineingezwängt, kann aber nur schwer mithalten und setzt sich damit der Kritik aus, ineffizient zu arbeiten.[1427] Überwachungs- und Informationsverarbeitungstechnologien sind zudem bestenfalls Hilfsmittel, unerwünschtes Verhalten aufzudecken oder Gefahren zu erkennen, nicht sie unmittelbar zu bewältigen.[1428] Daher liegt es sicherlich auch nicht im Interesse der zuständigen Behörden, Bagatellen zu dramatisieren (beispielsweise mit der Bezeichnung des illegalen Herunterladens von Musik als „Piraterie“ oder die Bezeichnung derjeniger, die Musik illegal herunterladen als „Raubkopierer“). Sie auf breiter Ebene zu verfolgen und verhindern hiesse, dass die dafür aufgewendeten Ressourcen anderswo fehlten – hoffentlich nicht bei der

---

1424 Siehe POPITZ, insb. 14 ff. Dem Argument, „rechtsfreie Räume“ könnten wir uns bspw. im Internet (HENRICHS/WILHELM 2010b, S. 219) nicht leisten – wobei „rechtsfrei“ diese ja nicht sind, sondern vielmehr nicht abschliessend geregelt oder unüberwacht, siehe ROTERT, S. 438 und ausführlich zum virtuellen Raum: TESCHNER, S. 27 f., 41 f. und 46) –, liesse sich mit ZERBES, S. 376 entgegnen: „*Keine Freiheit ohne Risiko.*“ Gerade im Hinblick auf virtuelle Räume wandeln verstärkte, anlasslose Online-Überwachungstätigkeiten das Internet möglicherweise in einen Ort mit vermehrt verschlüsselten Inhalten um, in einen Ort, der nicht mehr als offene Austauschplattform dienen kann.

1425 Gemäss MOHLER 2012, S. 47 f., widerspräche ein polizeiliches Opportunitätsprinzip der heutigen Rechtslage. Siehe dazu auch HÄFELIN/MÜLLER/UHLMANN, S. 560 ff.; MÜLLER L. 2011, S. 191 ff.

1426 NOGALA 1998, S. 261, 311 und 316 ff.; HASSEMER 1995, S. 485 f. Ähnlich LSE Briefing, S. 38 f. Freilich ist es genau dieses Argument, das auch benutzt wird, um scheinbar effiziente Technologien zu rechtfertigen. Insofern mittels neuer Technologien diese zusätzliche Effizienz nicht auch bei der Erledigung von Fällen anstatt nur im Erkennen von Devianz geleistet werden kann, ergeben sich Teufelskreise.

1427 Vgl. oben Erster Teil, Kapitel III.F.-H.

1428 ZERBES, S. 322 f.

Bearbeitung wirklich wichtiger Fälle von Delinquenz.[1429] Zumindest ungefährliche Abweichler und Kleinstkriminelle sollten von den sich konform Verhaltenden nicht als Andersartige behandelt werden. Ihnen sollte, als Mitmenschen, auf faire Art und Weise begegnet werden. Überreaktionen sind nicht angebracht.[1430] Hingegen können technisierte Massnahmen dort erfolgversprechend als Hilfsmittel eingesetzt werden, wo es darum geht, Hot-Spots konsequent aufzulösen oder einzelne Verdächtige gezielt zu überwachen.[1431] Gewisse Formen der vorgestellten technisierten Mittel können sinnvoll eingesetzt werden, wenn sie wohlüberlegt, gezielt und anforderungsgerecht umgesetzt werden. Sie erleichtern dann die alltägliche Polizeiarbeit und helfen, in unspektakulärer Weise, Beeinträchtigungen zu verhindern oder Ermittlungen erfolgreich abzuschliessen. Sie können in diesen Fällen kleine, aber durchaus wichtige, Elemente einer Gesamtstrategie sein.

Nicht jede Verfehlung muss aber gleich mit jedem erdenklichen (technisierten) Mittel niedergerungen oder gar präventiv unterbunden werden. Wie dargestellt wurde, führen indes postmoderne Kriminalitätsbekämpfungsstrategien zu einem verstärkten Aktionismus in hinsichtlich des verursachten Schadens überwiegend unerheblichen Bereichen.[1432] Die grossen Gefahren liegen nicht in geringfügiger „Kriminalität" oder in Abweichungen von der gesellschaftlichen Norm. Im Einsatz gegen Bagatellen oder unerwünschte Verhaltensweisen gehen die neuen, automatisierten Methoden selbst dann zu weit, wenn sie nur leicht in Grundrechte eingreifen sollten – ausser freilich, der gesellschaftliche Konsens ist, dass die vorgestellten Kriminalitätsbekämpfungstechnologien ihren Zweck auf reine So-

---

1429 Vgl. RÜTHER, S. 104; MARX 2007 (Fallacy 37). Siehe auch den Bericht Bundesrat i. S. Savary, S. 10 ff.

1430 Gl. A. wie OBERHOLZER 2003, S. 332 f. Vgl. auch LÜDERSSEN, S. 205 („philanthropisches Strafrecht"); KUNZ 2010a, S. 133 ff; HASSEMER 2006, S. 131 f.; RZEPKA, S. 134 ff. Gerade bei Jugendlichen ist sicherlich viel Nachsicht angezeigt. So können Jugenddelikte im Gegenteil teilweise Ausdruck von grundsätzlich positiven Wesenszügen, wie Kreativität etc., sein. Dazu sehr erhellend die Studie von QUENSEL. Der Begriff des Feindes hat in diesem Zusammenhang eben nichts zu suchen, vgl. NEUMANN, S. 305.

1431 Vgl. dazu ZIMRING, S. 117 f., 125, 129 ff., 146 f., 150 und 192 f.

1432 Diese Delikte können, wenn sie sehr häufig begangen werden, *in ihrer Gesamtheit* einen gewissen wirtschaftlichen Schaden verursachen. Zumindest die Tathandlungen der Einzelnen besitzen indes zumeist nur einen sehr geringen Unrechtsgehalt.

zialkontrolle ausrichten sollen. Dazu scheinen sie sich zu eignen, dazu scheint ihr gegenwärtiger Einsatz zu neigen.[1433]

Die Behauptung der Wirksamkeit der besprochenen Massnahmen auf die schwerwiegenden Bereiche der Kriminalität (Terrorismus, Sexual- und Gewaltstraftaten etc.) wird bei genauerer Betrachtung in der Regel als falsch erkannt. Die wirklich gefährliche Person handelt entweder unvorhersehbar, weil beispielsweise impulsiv, oder sie versteht ihr Handwerk.[1434] Bei Letzterem wirken die meisten der postmodernen Methoden und Massnahmen nicht. Sie sind auf eine breite Masse *potenzieller* Risikopersonen, auf Merkmalsträger zugeschnitten und beruhen auf Prozessen des risikogeleiteten Generalverdachts, die in dieser Hinsicht nicht sonderlich schwer zu durchschauen sind. Insoweit beeindrucken diese Methoden vor allem die Konformen und erwischen einige an sich gar nicht so Gefährliche (BUERMEYER: „virtuelle Eierdiebe") und wenige akut Gefährliche, die sich Ausweichtaktiken nicht leisten können oder welche die Fähigkeit, bedacht oder mit Sachverstand zu handeln beziehungsweise vorausschauende Schutzvorkehrungen zu treffen, nicht haben.[1435]

1433 Mit der polizeilichen Durchsetzung von gemeinschaftlichen „Wert- und Moralvorstellungen" (VOLKMANN, S. 217) nähert sich die Polizeiaufgabe wieder der von vor 400 Jahren, siehe ZERBES, S. 250. Siehe dazu auch SINGELNSTEIN/STOLLE 2012, S. 52; TROTHA, S. 230 f.; WEBSTER, S. 13; GRAS, S. 202 ff. Siehe auch HESSDÖRFER/BACHMANN zur „Anti-social behaviour order (ASBO)" in Grossbritannien.

1434 Gl. A. wie BARTSCH, S. 46, welche die Verhinderung von terroristischen Anschlägen bzw. anderen Grossbedrohungen durch Videoüberwachung daher für zweifelhaft hält. Dasselbe gilt für die Verdachtsrregister (siehe oben Erster Teil, Kapitel IV.A.) und allgemeiner für Methoden der Risikologik (HARCOURT, S. 228 f.). Zugang zu mehr Ressourcen (Geld, Macht, Informationen etc.) erweitert die Möglichkeiten des Makrokriminellen (Bsp.: „white collar crime") diesen Überwachungs-/Kontrollstrategien zu entgehen oder sie zu missbrauchen stark, siehe MARX 2003, S. 385. Für einige erhellende Beispiele dafür, wer aufgrund von Videoüberwachungsmassnahmen in der Praxis tatsächlich gefasst wird, siehe SHORT/DITTON, S. 123 ff.

1435 Gl. A. wie APONTE, S. 302 f.; SIMON, S. 272 f.; BUERMEYER, S. 165 f.; HASSEMER 1995, S. 486; POPITZ, S. 20. Vgl. SINGELNSTEIN/STOLLE 2007, S. 115 f.; ZERBES, S. 330. Siehe die Selbstreflexionen von Bagatellstraftätern in SHORT/DITTON, S. 135 ff.: Die meisten passen sich den neuen Verhältnissen rasch an (sie warten z. B. ab, bis die Kamera in eine andere Richtung schaut bzw. kalkulieren sogar die Abfolge der Kamerarotation oder verlagern ihre Delikte in unüberwachte Areale bzw. bewegen sich vorsichtiger im überwachten Raum).

Eine „vernünftige Zweck-Mittel-Relation“[1436] ist als Voraussetzung, die Verhältnismässigkeit einer Massnahme zu bejahen, demnach sicherlich hoch zu gewichten. Erschwert wird dieser Anspruch aber dadurch, dass sich weniger einschneidende Massnahmen heute vor allem auch auf der *Ebene ihrer Effizienz* mit stark einschneidenden Massnahmen messen müssen.[1437] Regelmässige Kontrollen und eine fortwährende Evaluation der Wirksamkeit und der (Neben-)Effekte der konkret angewendeten Instrumente versprechen hierin eine gewisse Abhilfe. Untersuchungen zu den konkret gebräuchlichen Systemen, Techniken und Methoden können als Grundlage für die Prüfung der Verhältnismässigkeit dienen und zu einem sorgfältigen sowie durchdachten Umgang mit jenen beitragen, indem zum Beispiel nicht zweckgemäss wirkende Systeme wieder abgebaut werden.[1438] Ohnehin ist der Einsatz von einschneidenden, technischen Kriminalitätsbekämpfungsmethoden, beruhend auf einem nebulösen Wissensstand über die Wirksamkeit, wie er die postmodernen Technologien regelmässig begleitet, problematisch.[1439] Die Beurteilung der Geeignetheit dieser postmodernen Methoden der Verbrechensbekämpfung könnte sodann theoretisch, insofern ihr ein gewisses Gewicht beigemessen wird[1440], als Begründung zur Begrenzung ihres Einsatzes

---

1436 D. h.: „Eine Massnahme ist unverhältnismässig, wenn das Ziel mit einem weniger schweren Grundrechtseingriff erreicht werden kann.“ (siehe BGE 133 I 77 E. 4.1 S. 81 und 132 I 49 E. 7.2 S. 62 mit Hinweisen). Einschränkend aber gilt, dass bei hohen Kosten einer Massnahme mit leichtem Eingriff auf eine Massnahme mit höherem Eingriff, aber geringeren Kosten ausgewichen werden kann. Siehe dazu FLÜCKIGER/AUER, S. 938; BIER/SPIECKER GEN. DÖHMANN, S. 616; MÜLLER L. 2011, S. 234 jeweils mit weiteren Hinweisen. Vgl. RUDIN/STÄMPFLI, S. 147 f. und ferner BOERS, S. 14.

1437 Vgl. bspw. BGE 128 II 259 E. 3.6 S. 276. Diese Gegenüberstellung kann unfair sein und zu problematischen Resultaten führen.

1438 Gl. M. wie BARTSCH, S. 234; FLÜCKIGER/AUER, S. 937 f.; RUDIN/STÄMPFLI, S. 147; HASSEMER 2000, S. 254 und 260 f.; BÜLLESFELD 2007, S. 74; MÜLLER L. 2011, S. 363; PETRI, G N. 64; INTRONA/NISSENBAUM, S. 22, 35 und 38; ALBRECHT F., N. 29; BARTMANN, S. 279; Bericht HRW, S. 20; ähnlich BOERS, S. 14; HASSEMER 1995, S. 487. Siehe als Beispiel die Evaluation der Videoüberwachung am Luzerner Bahnhofplatz (ZEHNDER M.). Sicherlich sinnvoll scheint diesbzgl. die Regelung des Kantons Bern zur Videoüberwachung: Die Gemeinden sind dazu verpflichtet, alle fünf Jahre eine Wirksamkeitsüberprüfung durchzuführen und einen entsprechenden, zu publizierenden Bericht zu verfassen, siehe STEGMANN M., S. 78 f. Auch befristete Pilotprojekte können eine gute Herangehensweise sein, wobei darauf zu achten ist, dass die Ergebnisse nicht durch zweckfremd kalkulierende Erwägungen beeinflusst werden.

1439 Das gilt besonders, wenn, wie bei der Videoüberwachung, bereits eine grosse Anzahl Studien durchgeführt wurden.

1440 Vgl. indes unten Vierter Teil, Kapitel V.D.

herangezogen werden. Es ist allerdings nicht leicht, den objektiven oder subjektiven Nutzen dieser Technologien zu messen. Den postmodernen Kriminalitätsbekämpfungstechnologien können meist keine deutlichen Wirkungen nachgewiesen werden. Ausserdem sind die einzelnen Effekte schwerlich den verschiedenen Massnahmen zuzuordnen, weil diese üblicherweise parallel mit anderen Massnahmen und innerhalb eines Gesamtkonzepts angewendet werden.[1441] Einer überprüfbaren Evaluation noch weniger zugänglich sind verdeckt durchgeführte Massnahmen oder Methoden, die auf heimlich gewonnenen Informationen beruhen (Sondierung virtueller Räume, Führen nicht-öffentlicher Register etc.).[1442] Oft können auf die Fragen, *ob* und *wie* diese Methoden *was* beeinflussen, lediglich Vermutungen geäussert werden.[1443] Erkenntnisse aus Pilotprojekten oder Evaluationen können zudem, infolge der rasanten technischen Entwicklung, bereits nach kürzerer Zeit überholt sein. Sie sind ferner teuer durchzuführen und wohl deshalb nicht immer sehr populär.[1444] Abgesehen davon sind Ergebnisse aus Evaluationen und Pilotprojekten leicht zu instrumentalisieren, indem sie etwa für eine bestimmte Politik günstig interpretiert und dadurch zur fingierten Rechtfertigung für die entgrenzte Anwendung postmoderner Kriminalitätsbekämpfungstechnologien herhalten müssen.[1445]

Die Option, Massnahmen alternativlos und ohne Vergleich zu anderen Vorgehensweisen fallen zu lassen, ist zu bedenken. Wenn die Massnahme nichts oder wenig taugt, aber finanzielle Mittel verschlingt, dann ist ihr Einsatz einzustellen. Auch interessiert nicht die *theoretische* Machbarkeit. Hat eine Behörde beispielsweise nicht die finanziellen Mittel, ausreichend viele und genügend ausgebildete Personen für die Bedienung der Überwachungssysteme abzustellen, nützen Bekräftigungen der theoretischen Möglichkeiten eines Systems bei Idealbedingungen nichts. Da auch in der Kostenfrage keine eindeutigen Ergebnisse vorliegen (die postmodernen Massnahmen kosten nicht so wenig, wie deren Befürworter es gerne hätten[1446]), sollte im Zweifelsfalle den weniger problemati-

---

1441 VOLKMANN, S. 219; FLÜCKIGER/AUER, S. 937, die aber m. E. zu Recht festhalten, auch die Alternativen der Videoüberwachung seien relativ abstrakt und deren Effekte teilweise schwer zu beurteilen. Vgl. dazu REUBAND 2007, S. 82 und die Übersicht von MCDOUGALL/PERRY/FARRINGTON.

1442 Gl. M. wie NOWAK, S. 12.

1443 Vgl. BARTSCH, S. 190 ff.

1444 Vgl. NOGALA 1998, S. 157 und 165.

1445 SINGELNSTEIN/STOLLE 2012, S. 156 f.; KAMMERER 2008, S. 347.

1446 Siehe oben Erster Teil, Kapitel III.F.

schen Methoden der Vorzug gegeben werden. Die postmodernen, technisierten Methoden über Wirksamkeitsvermutungen oder aufgrund von legendären Einzelerfolgen zu rechtfertigen, ist sehr problematisch.[1447] Anderer Ansicht ist beispielweise der ehemalige Landespolizeipräsident Erwin Hetger, der meint, niemand könne abschätzen, inwieweit der „erzeugte Fahndungsdruck" von Rasterfahndungen weitere Terroranschläge verhindert, Terroristen von ihrem Vorhaben abgebracht oder in ihrem Aktionsradius einschränkt habe. Folglich könne der präventive Effekt dieser Fahndungsmethode nicht hoch genug eingeschätzt werden[1448] – was für eine behagliche Apologie. Dem lässt sich aber mit GARY T. MARX ebenso lapidar entgegnen: „Just because something negative *could* happen, does not mean that it *must* happen."[1449] Was dazu führte, dass etwas, was passieren hätte können, nicht passiert ist, muss nach der hier vertretenen Ansicht genau abschätzbar sein, damit es als rechtfertigende Grundlage für eingriffsintensive Methoden hinhalten kann.

Vielfach versuchen Befürworter die besprochenen Technologien auch damit zu rechtfertigen, dass bereits die *eine* dadurch verhinderte Straftat, das eine gerettete Menschenleben alle Aufwände und Kollateralschäden ausgleiche. Dieser Verweis auf den dramatischen Einzelfall ist dienlich. Er verschiebt die Diskussion auf eine emotionale Ebene, auf welcher nicht mehr primär rationale Argumente zählen, sondern auf welcher die Bevölkerung leicht auf proaktive und politisierte Konzepte anspricht.[1450] So kommt es etwa, dass Strategien der Terrorismusbe-

---

1447 Vgl. NOGALA 1998, S. 157. Auch stellen sich gross propagierte Erfolgsmeldungen im Nachhinein zuweilen als übertrieben heraus, siehe den Artikel „Anschlagspläne, die keine waren" in Süddeutsche.de vom 15. Juli 2013.

1448 Zitiert in KUBE, S. 63. Ähnlich optimistisch eingestellt gegenüber der Wirkungsmacht der Rasterfahndung sind MIDDEL, S. 171 ff. sowie ROGALL, S. 644 f. und gegenüber der Notwendigkeit („unabweisbares Bedürfnis") des Einsatzes von Govware HOFMANN, S. 125. M. E. zu Recht skeptisch zur Abschreckungswirkung der Rasterfahndung, PEHL, S. 256 und gegenüber dem Einsatz postmoderner „Technologien sozialer Kontrolle" gegen jegliches unerwünschte Verhalten und der Aussage, dass grosse Fische auch durch kleine Vergehen gefasst würden, KAMMERER 2008, S. 93 sowie sehr ähnlich BUERMEYER, S. 165.

1449 MARX 2003, S. 371. Auch diese Variation gilt: Nur weil etwas funktionieren könnte, muss es nicht funktionieren. Die von Hetger angeführte Rechtfertigung liefert keine solide Grundlage dafür, weitere Vorkehrungen für diese Methoden zu treffen.

1450 Nach LIENHARD/HÄSLER, S. 631, führen diese Tendenzen zu einer „legislatorischen Hektik des Bundes". Vgl. ALBRECHT P. A. 2003, S. 44; HASSEMER 2006, S. 135; ZURAWSKI in heise Online vom 29. Dezember 2007. Siehe zum Politisieren und Werben mit (abstrakten oder konkreten) Opferbeispielen und dem Koppeln der Abstimmung über Gesetzesvorlagen an mitleiderregende Fälle aus der Praxis: GARLAND, S. 55 ff.; KUNZ 2011, S. 362 ff.

kämpfung und der konsequent harsche Umgang mit Vandalen und Chaoten zu Vorschriften über ordnungsgemässes Spazieren („In diesem Park nicht herumlungern!"), Ahndungstatbeständen zum Abfallentsorgen auf der Strasse und Neigungen der Ausgrenzung und Vertreibung von Jugendlichen aus den „Arealen des Anstands" führen sowie die Ächtung von Sexualstraftätern zu einer allgemeinen Verteufelung von potenziellen Abweichlern und mutmasslichen Störern transformieren. Die eigentlich für schwerste Bedrohungen konzipierten Verfahren und Systeme des Bekämpfungsstrafrechts werden in dieser Weise auf andere Bereiche unerwünschten Verhaltens angepasst, auf welche sie tatsächlich (begrenzt) Einfluss nehmen können.[1451] Fehlschläge der postmodernen Kriminalitätsbekämpfungstechnologien werden mit einer Neuorientierung auf andere Ziele kaschiert; die an sich ungewollten Nebenwirkungen auf Bagatellstraftaten oder auf sich unkonform, aber nicht kriminell verhaltende Personen werden als seit jeher anvisierter Erfolg proklamiert. Die derart banalisierten Methoden entwinden sich zugleich des ausschliesslichen Einsatzes durch die Staatsmacht und fördern das Auslagern von Staatsaufgaben.[1452] Dieses Auslagern bedeutet einerseits Synergien zwischen Staat, Privatwirtschaft und Bürger zu suchen. Verschiedene Protagonisten der Kriminalitätsbekämpfung folgen parallel laufenden Zielen und nutzen deshalb verzahnte Interessen. Gegenseitige Zugeständnisse sind die logische Konsequenz.[1453] Dieses kooperative Element ermöglicht meist erst, postmoderne Technologien effizient zu nutzen.[1454] Auslagern heisst aber nicht nur

---

1451 Vgl. KUNZ 2000, S. 71; SÖLLNER, S. 123 und 125 f. BARTSCH, S. 210 f., hält diese Entwicklung für besonders problematisch im Lichte der Angemessenheit polizeilicher Videoüberwachung. FLÜCKIGER/AUER, S. 941, halten die Bekämpfung von „incivilités" für keine ausreichende Eingriffsrechtfertigung. Ebenso MÜLLER L. 2011, S. 360 f., der sich zudem m. E. zu Recht fragt, ob der Einsatz von Videoüberwachungstechnologien nicht grundsätzlich auf Verbrechen und Vergehen beschränkt werden sollte und durch sie lediglich ausnahmsweise auch massiv gehäuft vorkommende Übertretungen an neuralgischen Orten mittels Videoüberwachung eingedämmt werden sollten.

1452 Vgl. NOGALA 1998, S. 138. Ausführlicher zur Privatisierung und Kommodifizierung von Sicherheit, siehe SINGELNSTEIN/STOLLE 2012, S. 103 ff.

1453 Vgl. KREISSL/STEINERT, S. 962 ff.; NOGALA 1998, S. 267; KUNZ 2011, S. 352 f.; DERS. 2010b, S. 18 und 20 f. Bsp.: Provider, Internetfirmen wie Google etc. stehen von staatlicher Seite unter gewissem Druck, Daten herauszugeben. Dafür werden ihnen Ausrutscher verziehen, siehe BENDRATH 2009, S. 26. Vgl. bspw. die Überwachungsaffäre um PRISM und TEMPORA (vgl. oben Erster Teil, Kapitel II.B.2.).

1454 Siehe KAWASHIMA, S. 157 f.; SZUBA, S. 194 f.; VOLKMANN, S. 218; ENGLER, S. 167; KLEINER, S. 46 f. Nur einige wenige Bsp.: Hooliganregister beziehen Stadienbesitzer ein und bauen auf deren Meldungen gewaltbereiter Besucher von Sportveranstaltungen. Terrorlisten verlangen die Mitarbeit von Finanzinstituten. Govware wurde in der Schweiz und in

Partnerschaft zu bilden, sondern auch sich vor Konkurrenz wappnen zu müssen. Die mit der Kriminalitätsvorsorge betrauten Behörden stehen in einem „sicherheitspolitischen Wettbewerb".[1455] Was der Richter nicht bereit ist zu erbringen, wird mit einer Ermächtigungsnorm flugs an die Staatsanwaltschaft und Polizei delegiert. Was die staatliche Justiz nicht leisten will (oder kann), wird zur privaten Dienstleistung umfunktioniert oder über Eigenvorsorge und Selbstverantwortung abgedeckt.[1456] Vormals staatliche Kompetenzen und Kontrollmechanismen werden ausgelagert.[1457]

Die Probleme des Auslagerns zeigen sich beispielsweise, wenn Datensammlungen oder Videoüberwachungsaufnahmen Privater im Strafverfahren verwertet werden sollen.[1458] Aus der angesprochenen organisatorischen Kontrolle in Räumen, die grundsätzlich öffentlich zugänglich sind, aber in privatem Eigentum stehen, entsteht neben dem dargestellten Separationseffekt eine weitere schwer zu lösende Problematik mit zwei Ausdehnungen. Erstens kommt einigen der privaten Sanktionsmöglichkeiten, dadurch, dass sie folgenreich und relativ gravierend sein sowie auf ziemlich grosse Areale und Bereiche ausgedehnt werden können, quasi-strafrechtliche Natur zu. Es ist zwar grundsätzlich sehr wünschenswert, das staatliche Strafrecht als letztes Mittel zu brauchen und Lappalien informell zu lösen, jedoch nur dann, wenn auch die Konsequenzen und „Sanktionen" entsprechend belanglos sind. Sind sie es nicht, müssen das „Sanktionsverfahren" und die Sanktion selbst gewissen Ansprüchen genügen.[1459] Zweitens können die postmodernen technischen Instrumente im privaten Bereich wesentlich unbedarfter eingesetzt werden. Die Videoüberwachung im Kaufhaus ist

Deutschland in Zusammenarbeit mit einem spezialisierten privaten Unternehmen eingesetzt. Die Vorratsdatenspeicherung oder Antennensuchläufe funktionieren ohnehin nur mithilfe der entsprechenden Provider.

1455 ALBRECHT P. A. 2003, S. 148 f. Vgl. KUNZ 2002, S. 729.

1456 Vor allem die Raumüberwachungstechnologien und die öffentlichen Verdachtsregister ermutigen den Bürger dazu, selbst tätig zu werden. Sie binden ihn geradezu ein. Vgl. KRASMANN, S. 185. Aber auch etwa Hooligan-Register zählen auf Listungsanträge von Stadionbesitzern und Terrorlisten insbesondere auf die Mithilfe von Finanzinstituten, siehe bspw. BARTMANN, S. 107.

1457 Siehe etwa SCHMIDT-SEMISCH, S. 16. Zum Ganzen, siehe oben Dritter Teil, Kapitel IV.D.

1458 Siehe dazu bspw. HANSJAKOB 2010, N. 12 zu Art. 277 StPO mit weiteren Hinweisen; HÖHENER/VEST, S. 99; HÄRING, S. 230 ff.; GLESS 2011, N. 40 ff. zu Art. 141 StPO; MÜLLER L. 2011, S. 356 f.; HEIMGARTNER, S. 40; Urteil der Beschwerdekammer in Strafsachen (Bern) BK 11 9 vom 22. März 2011, E. 2.3.

1459 Beispiel: Ein Hausverbot bzw. Stadionverbot gewinnt deutlich an Intensität, wenn es für eine gesamte Einkaufsstrasse oder für alle Stadien einer Sportart gilt.

selbstverständlich. Ebenso vergrössern etwa freiwillig zur Verfügung gestellte Konsumenteninformationen private Datenbanken. Setzte hingegen der Staat selbst diese Methoden ein, unterliegen der Einsatz und die Verwendung der Ergebnisse strengeren polizei- oder strafprozessrechtlichen Vorschriften und Beschränkungen.[1460]

C. Arrangements

Postmoderne Kriminalitätsbekämpfungstechnologien werden häufig angepriesen, Grossbedrohungen zu verhindern und „Hintermänner und Drahtzieher" zu fassen.[1461] Die erläuterten postmodernen Technologien scheinen nun aber insbesondere bei denjenigen Gruppen zu funktionieren, für welche sie nicht gedacht sind, nämlich den geringfügig straffälligen Durchschnittsbürgern oder wenig bedrohlichen Abweichlern.[1462] Bei der eigentlichen Zielgruppe (Schwerstdelinquenten, organisierte Kriminalität, Terrorismus etc.) vermögen sie oftmals wenig überzeugende Erfolgsquoten vorzuweisen, die Gründe dafür wurden bereits erläutert. Für eine Anwendung auf die neu anvisierten Personengruppen sind das Bekämpfungsstrafrecht und seine Methoden aber denkbar unangemessen. Die antizipierende, prophylaktische Kriminalitätsbekämpfung mittels technisierter Methoden ist ein Instrument, das als schwerwiegende Ausnahme nur bei untragbarem Risiko oder übergrosser Anzahl von Delikten an Ballungspunkten zum Einsatz kommen kann.[1463] Im Einsatz als Mittel zur Sozialkontrolle oder Bagatelldeliktvorsorge schiesst es über das Ziel hinaus und vergibt damit auch die Chance, straffällige Bürger mit adäquaten Methoden wieder in die Konformität zu führen.

1460 Zur Videoüberwachung des öffentlichen Raums durch Private, siehe MÜLLER L. 2012a, der meint, es sei diesbzgl. zu prüfen, ob eine spezifische Regelung im DSG bzw. eine spezialgesetzliche Regelung zu schaffen sei (S. 75). Zu problematischen Datenverknüpfungen durch Private, siehe PROBST, S. 39 f. Zum „fishing for evidence" durch Private, siehe ZERBES, S. 318.

1461 ZERBES, S. 3 und 43. Ebenso SIMON D., S. 263.

1462 Vgl. APONTE, S. 303; ZERBES, S. 348 f. und 353. Nicht zuletzt führen Mankos des Einsatzes von postmodernen Kriminalitätsbekämpfungstechnologien in Verbindung mit hohen Sicherheitsbedürfnissen zum Arrangement, es sei unvermeidbar, zu akzeptieren, dass auch unbescholtene Bürger zuweilen von oberflächlicheren Scans mit erfasst oder, sofern sie sich irgendwie verdächtig verhalten haben oder verdächtige Eigenschaften besitzen, (zu Unrecht) Zielscheibe gründlicher Untersuchungen oder einschneidender Überwachungsmassnahmen werden.

1463 Vgl. etwa SPINNER, S. 271; BAUM, N. 40.

Der richtige Umgang mit „Abtrünnigen“ ist essentiell für das weitere Zusammenleben *mit* ihnen. Als eines der Hauptargumente gegen den überbordenden Einsatz von Kriminalitätsbekämpfungstechniken wird meist als Erstes das Risiko der „ungerechten“ Behandlung von verdächtigten Unschuldigen genannt. Auch ein anderer Aspekt soll aber nicht vergessen werden: Das despektierliche Verhalten gegenüber dem (schuldigen) Täter. Auch der Täter soll eine humane Behandlung erfahren dürfen.[1464] Dies ist nicht nur aus einer ethischen und menschenrechtlichen Position zu fordern, sondern auch aus einer praxisnahen. Einerseits soll die verachtende Behandlung nicht immer stärker ausgeweitet werden (vom aktuellen Täter über viele Zwischenschritte zum potenziell Auffälligen etc.). Nicht, dass es sich die Bürger im Ergebnis selbst aufbürden, jeden Einzelnen um sich herum und sich gegenseitig als Feinde zu behandeln (diese Tendenzen scheinen hingegen nicht nur in der Videoüberwachung bereits durch). Andererseits haben die Exklusionstendenzen, allen voran die öffentlichen Verdachtsregister, neben einer Demütigung ausserdem eine fortgesetzte, tiefgreifende entsozialisierende Wirkung. Die Gesellschaft gibt dem Fehlbaren, indem sie ihn und sich selbst ständig an seine Taten erinnert, keine Chance, sich zu rehabilitieren. Der Straffällige wird wie ein Aussätziger behandelt, was ihm die Rückkehr in die Gesellschaft praktisch verunmöglicht.[1465] Daraus entstehen einige der kaum lösbaren Probleme der Kriminalpolitik der Postmoderne. Wohin es führt, wenn grosse Teile der Bevölkerung mit falschen Massnahmen abgeurteilt werden, kann man anhand der Gefängnispolitik in den USA beobachten: Es entstehen zwei Klassen oder Schichten, die nicht mehr miteinander auskommen können.[1466] Die eine Klasse fristet ihr Dasein zusammengepfercht in Strafanstalten (Stichwort „prison binge“), die andere im selbstgebauten goldenen Käfig ihres Sicherheitswahns in sog. „gated communities“ (die Folgen daraus: Geisterstädte und „crime hotspots“ durch Verlagerung). Beide Klassen sind Opfer eines Systems des missglückten, genuin symbolischen „war on crime“.

Der Preis für unüberlegte Arrangements kann daher hoch ausfallen: Wendet man bekämpfungsstrafrechtliche Instrumente auf eine Person an, dann müsste diese, der inneren Logik des Feindstrafrechts folgend, zumindest ein *potenzieller* Feind

---

1464 Vgl. KUNZ 2011, S. 362 f.

1465 Und ihn überdies quasi zum Rückfall verleitet, was das Abstützen auf Rückfallquoten zur Legitimation einschneidender Massnahmen im Bekämpfungsstrafrecht zur sich nur rückwirkend erfüllenden Prophezeiung werden lässt. Vgl. HARCOURT , S. 161 und 192.

1466 Siehe zu diesen Folgen SIMON, S. 276 ff.; GARLAND, S. 361; KUNZ 2011, S. 372 f.; DERS. 2002, S. 740 ff.; YOUNG 1999, S. 190.

sein. Eine Person wie einen Feind zu behandeln, macht sie ungeachtet dessen de facto zu einem Feind. Die die Kriminalität bekämpfende Massnahme wird diesfalls durch eine spirfalförmige Post-hoc-Rechtfertigung „zulässig". Die Problematik besteht mithin darin, dass über die durch diese Scheinrechtfertigungen hochgeschaukelten Feindbilder Personengruppen ungewollt Risikokategorien zugeordnet werden können.[1467] Daraus ergeben sich unter anderem gravierende Zweifel an der demokratischen Legitimität der Kategorisierung des jeweiligen Personenstatus.[1468]

Es muss mithin überlegt werden, bis zu welchem Punkt Konstellationen geringfügiger Abweichungen geduldet werden sollen und ab wann das Interesse der Gemeinschaft überwiegt, eine Bagatellstraftat oder ein Antragsdelikt mittels technisierter Massnahmen zu verhindern oder zu verfolgen, und ob es überhaupt überwiegen kann.[1469] Die Methoden und Programme sowie die Wirkungen und Konsequenzen müssen für den Einzelnen und die Gesellschaft zumindest in den wesentlichen Zügen transparent sein. Diese kann nur in diesem Fall bewusst wählen (insofern sie die Wahl nicht dem Expertentum überlassen möchte), welche Vorgehensweisen mit ihren (aktuellen) Grundwerten vereinbar sind.[1470] In diesem Sinne sind Bestrebungen wie die Statuierung eines „Grundrechts auf Sicherheit" sicherlich abzulehnen. Dieses liesse mit seinem generellen Rechtfertigungsanspruch, welcher jedes Abwehrrecht des Einzelnen überwiegen soll, die dringend nötige Diskussion und besonnene Abwägung der verschiedenen Interessen im Einzelfall vergessen.[1471] Entscheide, gestützt auf einen globalen Verweis auf dieses Konstrukt, hingegen dürften unbedachter getroffen werden. Ab-

---

1467 Besonders problematisch ist dies hinschtlich jugendlicher Delinquenten, die ohnehin eine scheinbar beliebte Zielgruppe für die Überwachungsmassnahmen sind; gl. A. wie NORRIS/ARMSTRONG, S. 109 und 113 f. sowie ähnlich GOTTFREDSON/HIRSCHI, S. 270 f. Von diesem Fokus zeugen bspw. CHAU/XU, S. 489, die den gefährlichen Einfluss von Blogs mit zweifelhaftem Inhalt auf Jugendliche betonen. Gleichermassen problematisch ist es, wenn Anstrengungen der Kriminalitätsbekämpfung zu einem „war on poor" verkommt, siehe SINGELNSTEIN/STOLLE 2007, S. 111.

1468 Besteht beispielsweise eine Diskrepanz zwischen dem, was die Gesellschaft wirklich will und dem, was sie durch ihre verzerrte Wahrnehmung entscheidet, ist die Durchsetzung letzterer Entscheidung trotzdem legitim?

1469 Vgl. BESOZZI, S. 132; SIMON, S. 274; OBERHOLZER 2003, S. 332 f.; BÜLLESFELD 2002, S. 66 f.; RUDIN/STÄMPFLI, S. 149.

1470 Siehe KUNZ 2011, S. 376. Vgl. HEYMANN, S. 47. Personengruppen sollen zumindest nicht durch technische oder konzeptuelle Schwachstellen fälschlicherweise und von der Gesellschaft eigentlich ungewollt in die Kategorie „Gesellschaftsfeind" geraten.

1471 A. A. JAKOBS 2006, S. 297.

gesehen davon muss allgemeiner überdacht werden, ob das öffentliche Interesse „Sicherheit" in letzter Zeit nicht teilweise allzu unreflektiert herbeigezogen worden ist.[1472] Die Konsequenzen der Rechtfertigung von Gefahren abwehrenden Technologien mit einem Blanko-Scheck – vor allem derjenigen mit stark in die Zukunft gerichtetem Charakter – dürften sich für die Gesellschaft als äusserst schwer zu tragen herausstellen.[1473]

Diese Ausführungen sind nicht als Plädoyer gegen den Einsatz *jeglicher* Varianten der vorliegend besprochenen Überwachungs-, Informationsverarbeitungs- und Registrierungstechnologien zu verstehen. Sie können zum Teil hilfreich und entlastend verwendet werden. Technisierte Massnahmen können unter Umständen zweckmässig eingesetzt werden und teils möglicherweise geringere Eingriffe für Betroffene bedeuten als die Alternativen.[1474] Es geht mithin nicht darum, behördliche Spielräume möglichst zu minimieren, sondern darum, einen gewissen Rahmen vorzugeben und einzuhalten, neue Technologien vorausschauend zu regeln oder allenfalls frühzeitig auszuschliessen und abzuwägen, wohin die Technologien unter dem gesellschaftlichen Aspekt führen können und führen sollen. Es geht auch nicht darum, jede einzelne Ermittlungstaktik der Behörden im Detail offenzulegen, sondern ausreichend Transparenz herzustellen und angemessene Kontrollmöglichkeiten vorzusehen.[1475] Wenn über die Legitimation dieser Instrumente und Methoden gesprochen werden soll, dann nicht bezogen auf Ausnahmephänomene, sondern auf die Masse an Praxisfällen, bei denen sie tatsächlich zur Anwendung gelangen; nicht bezogen auf (genuin vage) nachrichtendienstliche Bedürfnisse, sondern auf Bedürfnisse der Strafverfolgung und der polizeilichen Kriminalprävention.[1476] „Phantomdebatten" zu führen, die vom eigentlichen Problem struktureller Veränderungen ablenken, darf nicht das Ziel

---

1472 Vgl. Vierter Teil, Kapitel IV.C.

1473 Dies gilt auch unabhängig davon, ob diese etwa unter dem Mantel staatlicher Fürsorge auftreten. Vgl. CAMPBELL, S. 82 f., der mit einem Bsp. verdeutlicht, dass auch Überwachung aus Fürsorgegründen zu stossenden Ergebnissen führen kann: Der Supreme Court hatte in einem Fall über die Rechtmässigkeit der ohne Wissen und Einwilligung von schwangeren Frauen zu ihrem und dem Kindeswohl von einer Krankenschwester an die Staatsanwaltschaft weitergereichten, auf Drogenkonsum getesteten Urinproben zu entscheiden.

1474 Vgl. etwa oben Zweiter Teil, Kapitel II.C.

1475 Alle diese Punkte kommen nicht nur den Betroffenen, sondern auch den einsetzenden Behörden zugute.

1476 Vgl. ZERBES, S. 311.

sein.[1477] Qualitativ gute, wirkungsvolle Instrumente zu optimieren, scheint erfolgversprechender und schonender als die Einsatzmöglichkeiten regelmässig mit neuen, ungetesteten Instrumenten zu erweitern.[1478]

D. Die normative Kraft des Verhältnismässigkeitsprinzips

Ein gewisser Spielraum ist in den gesetzlichen Grundlagen wohl einzuräumen, um künftige technologische Entwicklungen zu berücksichtigen und Normen nicht laufend anpassen zu müssen.[1479] Dieses Argument ist jedoch keine Entschuldigung dafür, etwa auf hinreichend bestimmte und klare gesetzliche Grundlagen zu verzichten.[1480] Beispielsweise liesse sich die Rasterfahndung, siehe Deutschland, auch in der Schweiz ohne Weiteres normieren. Sie *nicht* ausdrücklich zu regeln, sollte mit dem Bekenntnis einhergehen, sie nicht anzuwenden. Die Gesetzeslücke soll nicht im Gegenteil in dem Sinne ausgelegt werden, dass Rasterfahndungen (unter anderem Namen oder unter analoger Zuhilfenahme anderer Ermächtigungsnormen) eingesetzt werden dürfen, da sie ja schliesslich nicht verboten sind. Nicht „die Begrenzung staatlicher Ermittlungstätigkeit" bedarf „besonderer Legitimation", sondern „der staatliche Eingriff in Grundrechte".[1481]

Postmoderne Kriminalitätsbekämpfungstechnologien hebeln diesen Leitsatz aus. Die zunehmende Vereinnahmung der Kriminalitätskontrolle durch Bekämpfungsstrafrecht, proaktive Technologien und Strategien, lässt die Verhältnismässigkeit als Grundsatz und Schranke staatlicher Tätigkeit allmählich an Bedeutung verlieren. Die Ansicht von BIAGGINI überzeugt: Aufgrund der weit vorgelagerten Massnahmen der Gefahrenabwehr und -erkennung drohen „die bewährten Kriterien der Verhältnismässigkeitsprüfung" ihre „Massstabsfunktion einzubüssen" und das Verhältnismässigkeitsprinzip verliert „als wichtiges und bewährtes Mittel zur rechtsstaatlichen Begrenzung staatlichen Handelns an normativer Kraft und Wirksamkeit".[1482] Zum einen lässt also eine gewisse „Konturlosigkeit und

---

1477 Gl. M. wie QUEDNOW und SLABY, S. 386 bzgl. unwahrscheinlicher Verheissungen der Hirnforschung.

1478 Vgl. BARTMANN, S. 280.

1479 ISENRING/KESSLER, S. 34 f.

1480 Vgl. aber bspw. die gegenteiligen Ansichten aus der Praxis bei STÖCKLI, S. 17.

1481 PUSCHKE/SINGELNSTEIN, S. 119. Ebenso SZUBA, S. 293. Ähnlich ALBRECHT F., N. 28; ZERBES, S. 42.

1482 BIAGGINI, S. 262.

Beliebigkeit" des Verhältnismässigkeitsprinzips viel Ermessen zu.[1483] Zum anderen haben Strategien und Technologien der inneren Sicherheit in einem Klima der Unsicherheit eine grosse Überzeugungskraft, und angesichts furchteinflössend instrumentalisierbarer (potenzieller) Bedrohungen stellen die Prüfungsstufen des Verhältnismässigkeitsprinzips keine wirksamen Schranken dar.[1484] Speziell im Gefahren- oder Verdachtsvorfeld eingesetzte Massnahmen liegen ausserhalb des Horizonts des Verhältnismässigkeitsprinzips. Bei Grundrechtseingriffen im proaktiv geprägten Tätigkeitsfeld kann seine Funktion als begrenzendes Überprüfungsinstrument nur eingeschränkt beansprucht werden.[1485]

Ausfluss dieser Entwicklungen sind „Abwägungsautomatismen".[1486] Der Einsatz postmoderner Technologien wird bei den einzelnen Prüfpunkten des Verhältnismässigkeitsprinzips durchgewunken, sobald eine als genügend erachtete gesetzliche Grundlage – bereits dieser erste Prüfungspunkt wird in der Praxis teilweise nicht sehr ernst genommen[1487] – besteht.[1488] Das vorsorgliche Sammeln von möglichst vielen Informationen oder Daten erscheint vermeintlich selten nicht zumindest im abstrakten Sinn zur Abwehr einer Bedrohung durch eine (mutmasslich) gefährliche Person oder Personengruppe geeignet und erforderlich. Als Beurteilungsmassstab scheinen „vage Erfolgsprognosen" oder die „abstrakte Ge-

---

1483 SIMON D., S. 87 f. und 96.

1484 HASSEMER 2006, S. 138, 140 f. und 143; ZERBES, S. 296 f. Ähnlich auch KLESCZEWSKI, S. 756; TESCHNER, S. 49, 114 f. und 130; RUDIN, S. 283: „Offensichtlich drohen bei bestimmten Themen – wie Terrorismus und Kinderpornografie – die rechtsstaatlichen Sicherungen zu versagen."

1485 BIAGGINI, S. 262 ff.; MÜLLER L. 2011, S. 208; THIEL, S. 478. Vgl. HASSEMER 2006, S. 140; STEGMANN A., S. 230.

1486 Siehe CALLIESS. Ebenso SIMON D., S. 92. Vgl. auch NOGALA 1998, S. 140 und 176 ff.

1487 STEGMANN A., S. 231. Immerhin jedoch lässt das Bundesgericht allzu unbestimmte Normierungen nicht gelten (vgl. etwa BGE 136 I 87). Das Bundesgericht und der EGMR beispielsweise können sicherlich wertvolle Akzente setzen. Diesem Anspruch werden sie teilweise gerecht, ihr Einfluss ist aber beschränkt. Solange die Angstkultur nicht überwunden wird, wird die öffentliche (Un-)Sicherheitsmentalität hinsichtlich der Kriminalität weiterhin Grundlage bilden für einen relativ extensiven Einsatz hoheitlicher Gegenmassnahmen.

1488 Vgl. RUDIN/STÄMPFLI, S. 146 f. Bsp. öffentliches Interesse: Das Bundesgericht erachtet in BGE 120 Ia 147 E. 2.d S. 151 die „Verhinderung zukünftiger und Aufklärung geschehener Straftaten" immer als im öffentlichen Interesse liegend. Eine ähnliche Meinung vertritt der EGMR in seinem Entscheid Peck gg. Vereinigtes Königreich vom 28. Januar 2003, Nr. 44647/98, § 79.

eignetheit“ von Massnahmen oftmals zu genügen.[1489] Die Zumutbarkeit schliesslich beruht auf einer Interessenabwägung und diese auf der gesellschaftlich-politischen Räson.[1490] Die Interessenabwägung ist nur so viel wert, wie es der Grad an gesellschaftlicher Bedeutung vorgibt, welche dem zu schützenden Grundrecht im Augenblick und im Verhältnis zu anderen Werten (wie der Sicherheit) zukommt. In einer Zeit, in der Freiheiten von der Gesellschaft nicht besonders hoch auf der Werteskala eingestuft werden, bringen jene auch im Abwägungsmechanismus der Verhältnismässigkeit nur wenig Gewicht ein. Die Verhältnismässigkeitsprüfung kann somit nicht als unabhängiges, absolutes Beschränkungsinstitut postmoderner Kriminalitätsbekämpfungstechnologien verwendet werden (insbesondere nicht bei präventiven Methoden), sondern hängt stark von der jeweiligen (politischen) Stimmung in der Gesellschaft ab.[1491] Solange das öffentliche Interesse an universeller und vollkommener Gefahrenabwehr sehr hoch eingestuft wird, vermögen weniger wertgeschätzte Aspekte von Grundrechten diesem Interesse wenig entgegenzusetzen. Die Grundrechte werden durch die das Bekämpfungsstrafrecht begünstigende gesellschaftliche Mentalität im Verhältnis zur Sicherheit nicht genügend hoch bewertet, als dass sie einen wirksamen Schutz vor einer Eskalation bekämpfungsstrafrechtlicher Tendenzen gewährleisten könnten.[1492]

Das Verhältnismässigkeitsprinzip ist mithin kein Garant (mehr) für den unproblematischen Einsatz der besprochenen Massnahmen und Techniken. Der Grundsatz der Verhältnismässigkeit setzt insofern lediglich eine „weiche Grenze“.[1493] Zweck-Mittel-Relationen mögen in diesem Fall ein gewisses Verständnis vermitteln. Die Beurteilung der postmodernen Methoden auf dieser Ebene spielt ihnen indes in die Hände. Effizienz und Rationalisierung sind *ihre* Sprachen.[1494] Sie

---

1489 Siehe dazu kritisch BARTMANN, S. 279 f. mit Hinweis auf den Entschluss des Europäischen Parlaments zur Evaluierung der EU-Sanktionen (2009/C 925 E/49).

1490 Vgl. BIAGGINI, S. 262; MÜLLER L. 2011, S. 234; NOGALA 1998, S. 139; SIMON D., S. 87 f. und 92 ff. mit weiteren Hinweisen.

1491 ALBRECHT P. A. 2003, S. 84 f. Vgl. COUDERT, S. 380; HASSEMER 2000, S. 250 und 257; HÖHENER/VEST, S. 104 f.; SIMON D., S. 96; VETTERLI, S. 458 ff.; ZERBES, S. 296 f.; zum wandelbaren Charakter des öffentlichen Interesses LIENHARD/HÄSLER, S. 130 mit weiteren Hinweisen.

1492 NEUMANN, S. 307 f.; BVerfGE 115, 320 (363 ff.).

1493 ZERBES, S. 296. Ebenso SIMON D., S. 93.

1494 Vgl. NOGALA 1989, S. 46 f.; DERS. 1998, S. 130; HASSEMER 2006, S. 142; SINGELNSTEIN/STOLLE 2012, S. 157; VOLKMANN, S. 217. Insofern kann mit entsprechender Rhetorik deren

sind zudem unter anderem charakterisiert durch an sich leichte Eingriffe mit grosser Streubreite, durch die Behauptung, nur heimlich angewendet könnten sie wirksam sein, und durch Akzeptanz in der Bevölkerung. Letztere verdanken sie wohl in erster Linie dem Versprechen, die Massnahmen fokussierten lediglich Risikogruppen.[1495] Verschiedene Ideen, diesen Rationalitäten postmoderner Technologien entgegenzuwirken, stehen im Raum[1496], Erlösung bringen sie wohl nicht.[1497] Die höchsten Gerichte scheinen sich der dargestellten Probleme gewahr zu werden und versuchen teilweise gegenzusteuern[1498], ob sie die Problematik auf längere Sicht lösen können, ist offen.[1499]

Der Einsatz postmoderner Technologien steht zwar einer Schranken-Trias gegenüber: der technischen Machbarkeit, dem menschlichen Leistungsvermögen und der rechtlichen Zulässigkeit.[1500] Diese Hürden sind aber, wie bereits mehrfach dargestellt, nicht unumgänglich und verursachen mitunter weitere Probleme. Wichtig scheint jedenfalls, die Einsätze jeweils im Voraus auf ihre Zulässig-

„natürliche Wachstumsgrenze" durch beschränkte Behördenbudgets (NOGALA/SACK, S. 157) kaschiert werden, indem deren durchschlagende Effizienz inszeniert wird.

1495 Vgl. dazu HEYMANN, S. 93: „It has been tolerable to Americans only because it is implicitly and seemingly reliably limited to discrete groups to which most do not belong."

1496 Siehe etwa ALBRECHT P. A. 2010, S. 14; CALLIESS; SIMON D., S. 94 f.; SINGELNSTEIN/STOLLE 2012, S. 159 ff.; VOLKMANN, S. 219 ff.; ZERBES, S. 347 ff.

1497 Siehe dazu ausführlich SINGELNSTEIN/STOLLE 2012, S. 153 ff.; ZERBES, S. 324 ff. und 347 ff. Die Institution des Rechtsschutzbeauftragten in Österreich, siehe dazu ZERBES, S. 158 ff., 335, 354 f. und 367 f., ist sicherlich interessant, aber letztlich auch nicht ohne Schwachstellen, siehe ZERBES, S. 158 ff. Insbesondere bleibt auch das Problem der Verhältnismässigkeit als für proaktive Tätigkeiten relativ ungeeignete Schranke bestehen. Insofern ist zu bezweifeln, dass dieses ein ausreichendes Instrument darstellt, durchzusetzen, was ZERBES, S. 42 fordert: „Der Schutz von individuellen Freiheitsrechten soll auch dann noch gewährleistet sein, wenn möglichst gründliche und automatisiert ablaufende Ausforschungstechniken von der politischen Mehrheit gewollt und technisch möglich sind." Die heutigen rechtlichen Schranken in der Schweiz scheinen funktionierenden, erfolgversprechenden Technologien, die faktisch dem Volkswillen entsprechen oder mit diesem zumindest vereinbar sind, wenig entgegensetzen zu können.

1498 Siehe z. B. BGE 136 I 87 (PolG ZH); Entscheid des EGMR S. und Marper gg. Vereinigtes Königreich vom 4. Dezember 2008, Nr. 30562/04 und 30566/04; BVerfGE 125, 260 (Vorratsdatenspeicherung); 120, 274 (Online-Durchsuchungen); 115, 320 (Rasterfahndung II).

1499 Vgl. ALBRECHT P. A. 2010, S. 12; SINGELNSTEIN/STOLLE 2012, S. 162. Sie scheinen teils den Eindruck zu erwecken, den neueren Technologien „verständnis-" und „sprachlos" gegenüberzustehen, so VOLKMANN, S. 222 zur jüngeren Rechtsprechung des BVerfG. LOADER/SPARKS, S. 93 erachten diese Reaktion als typisch für den kriminologischen Liberalismus.

1500 Vgl. auch POPITZ, S. 8 ff.

keit zu prüfen und zu planen. Die dargestellten technischen Schwierigkeiten sind frühzeitig zu bedenken und zu berücksichtigen.[1501] Hypothesen und praktische Wirklichkeit sind zweierlei. Stehen mögliche Störungsquellen beispielsweise dem rechtlich zulässigen Einsatz von Govware entgegen oder verhindern technische Schwierigkeiten, dass Erfolge sehr wahrscheinlich zu erwarten sind, ist vom Einsatz abzusehen. Spätestens die Genehmigungsbehörde sollte ihn diesfalls ablehnen. Auch sind rechtliche Schranken zu beachten, *bevor* irgendwelche Schritte eingeleitet werden. Die (richterliche) Kontrolle im Nachhinein ist wichtig, kommt aber oft zu spät.

Demgegenüber ist die Hemmschwelle (gesetzlicher) Ausweitung tief.[1502] Manchmal werden postmoderne Technologien ohne ausdrückliche Ermächtigungsgrundlage solange eingesetzt, bis deren Einsatz bekannt und eine Regelung gefordert wird. Dann werden die Technologien im Schnellverfahren retrospektiv legalisiert. Als Argumente für die Implementierung werden die (jahrelang) „übliche Praxis" (freilich ohne ausdrückliche Ermächtigungsgrundlage) und die prekäre Situation bei Wegfall der praktizierten und zu regelnden Überwachungstechnologie oder Einsatzvariante angeführt.[1503] Diese Vorgehensweise ist nach der hier vertretenen Ansicht sehr problematisch; nicht, weil Ermächtigungsgrundlagen etwa für Antennensuchläufe nicht zweckmässig wären, sondern weil dieses Rechtfertigungsmuster Legislativverfahren in missbräuchlicher Weise verkürzt. Faktische Schranken, Technologien im *bestehenden* rechtlich zulässigen Rahmen einzusetzen, dürfen nicht überwunden werden, indem das qualitative Niveau des rechtlichen Rahmens unüberlegt zugunsten dieser Technologien gesenkt wird. Gesetzliche Grundlagen für neue Technologien zu schaffen, darf keine „Alibiübung" sein. Es sollen diejenigen Technologien reglementiert werden, derer die staatlichen Behörden konkret bedürfen (nicht im Sinne eines abstrakten „Mehr Information ist immer besser!"[1504]), die von der Gesellschaft akzeptiert sind und verfassungsrechtlichen Prinzipien nicht widersprechen. Hingegen soll nicht generell für jede neue Technologie standardmässig eine Ermächtigungsgrundlage eingefügt werden. Daraus abgeleitet stellt sich die Frage, wie der rechtliche Rahmen den einzelnen Technologien, Strategien und Methoden

---

1501 Vgl. HANSEN/PFITZMANN; PFITZMANN/KÖPSELL 2009b, S. 154.

1502 SINGELNSTEIN/STOLLE 2012, S. 54; FISAHN, S. 35 f. Siehe oben Zweiter Teil, Kapitel I.

1503 So geschehen bei Antennensuchläufen und de lege ferenda der Govware. Siehe auch SINGELNSTEIN/STOLLE 2012, S. 156. Siehe oben Erster Teil, Kapitel I.G.4 und II.D.2.

1504 Siehe zu dieser Tendenz etwa die kritische Äusserungen eines Polizeibeamten bei ERICSON/HAGGERTY, S. 243.

Schranken vorgeben kann. Bisher deckten jene zuweilen, quasi auf Vorrat, regelmässig mehr Funktionen ab, als rechtlich zulässig war.[1505]

VI. Aufheizende Symbolik

Das dem Bekämpfungsstrafrecht zugrundeliegende Konzept sieht keinen wirksamen Eingriffsschutz vor. Die „Unperson" im Speziellen ist eingeschlossen in einer Sphäre der „fast völligen Rechtslosigkeit".[1506] Tendenzen in die Richtung spezieller Interventionen bei Normbrechern, welche die Gesellschaft als „aussergewöhnlich bedrohlich" empfindet, werden im steigenden Funktionsverlust der Verhältnismässigkeitsprüfung deutlich ersichtlich. Mit dem symbolischen Bekämpfungsstrafrecht wird das Verhältnismässigkeitsprinzip ausgespielt. Das Resultat der praktischen Anwendung des präventiv-proaktiven Konzepts der Gefahrenabwehr ist unter anderem ein symbolisches „Gegnerstrafrecht", ein Bekämpfungsstrafrecht, welches sich nicht zwischen Feind und Bürger als Adressat entscheiden kann und welches die eigentliche Problematik nicht zu lösen vermag, ja verfehlt[1507]: Symbolisches Bekämpfungsstrafrecht und desto mehr dessen Technologien des Risikomanagements zielen nicht primär auf eine wirksame Verbrechensverhütung ab. Sie dienen in erster Linie dazu, die Bevölkerung oder bestimmte Interessengruppen zu beruhigen, damit mittelbar Normgeltung zu erhalten und das Handeln des Justizsystems beziehungsweise der Politik gegenüber der Gesellschaft zu rechtfertigen.[1508] Das symbolische Bekämpfungsstrafrecht kümmert sich somit unermüdlich um das eigene Ansehen und rechtfertigt sich tautologisch durch eigens geschaffene Konstrukte, indem es der Öffentlichkeit Bedrohungslagen vorführt und auf die entstehende Verunsicherung mit symbolischen Gesten antwortet.

1505 Vgl. oben Zweiter Teil, Kapitel I.D. Aus welchem Grund aber sollte eine von staatlichen Behörden benutzte Technologie etwas können, das sie ohnehin nicht darf?

1506 NEUMANN, S. 311.

1507 NEUMANN, S. 306 f.; APONTE, S. 302 f. Vgl. KUNZ 2011, S. 356 f. JAKOBS 2004a, S. 88 bezeichnet die Strafe im Feindstrafrecht selbst als „Mittel symbolischer Interaktion". Allgemein zur Symbolik des Strafrechts, siehe KUNZ 2010c; DERS. 2010b, S. 16 f.

1508 Vgl. ROSE, S. 87; STAPEL, S. 54; VOLKMANN, S. 219; HASSEMER 1995, S. 486. Auch im Sinne der Normbestätigung bzw. positiven Generalprävention, siehe SINGELNSTEIN/STOLLE 2007, S. 106. Wobei es nicht die hier vertretene Ansicht ist, dass die dargestellten Kriminalitätsbekämpfungstechniken immer rein symbolisch eingesetzt würden, vgl. GATES, S. 71.

Eine Patentlösung gegen die entgrenzte Anwendung postmoderner Kriminalitätsbekämpfungstechnologien, die sich aus der aufgeheizten postmodernen Kriminalpolitik ergibt, ist nicht ersichtlich. Indes können mögliche Reaktionsmuster diskutiert werden[1509]:

Die Kommunikation der Kriminalpolitik mit der Bevölkerung sollte die gesellschaftlichen Bedenken hinsichtlich ihrer Bedrohung durch Kriminalität beschwichtigen, nicht die Gemüter noch mehr erhitzen.[1510] Das Bekämpfungsstrafrecht führt zu Unmut und Enttäuschung in der Bevölkerung, indem es einerseits die Rechte aller beschneidet und es andererseits verfehlt, wirklich gefährliche Personen lückenlos zu erfassen und unter Kontrolle zu halten.[1511] Dasselbe gilt für die darauf beruhenden postmodernen Raumüberwachungs-, Massendatenverarbeitungs- und Registrierungstechnologien: Faktisch versagen diese häufig vor den Augen der Bevölkerung. Ihr Versagen wird aber nicht *ihnen* zugeschrieben. Sie werden deshalb von der Öffentlichkeit, bezüglich ihrer Möglichkeiten und Risiken, verzerrt wahrgenommen.[1512] Die Realität holt die Symbolik für die Öffentlichkeit sichtbar ein, was aber die Verfechter dieser Methoden nur dazu veranlasst, deren Mythos zu festigen. Effizienz ist zwar ein bedeutsamer Leitgedanke der postmodernen Strategien und Technologien, jedoch in einem symbolischen Sinn. In Verständnis des Bekämpfungsstrafrechts ist nicht das, *was* unternommen wird, von Interesse, sondern, *dass* etwas unternommen wird, das auf die Bedürfnisse, die Nachfrage der Öffentlichkeit sichtbar antwortet. Demgemäss braucht es mehr Technologie, potentere Technologie und früher ansetzende Technologie, um der scheinbar (ihrer überlegenen Technik, ihrer unmenschlichen Grausamkeit etc. wegen) bevorteilten „Kriminalität" beizukommen und um im Falle des (zuweilen unabdingbaren) Scheiterns darauf verweisen zu können, alles nur Mögliche getan oder alternativ zu wenig technische Mittel zur Verfü-

---

1509 LOADER/SPARKS, S. 2, 9 und 83 umschreiben die spannungsgeladene Kriminalpoltik mit Hitze-Methaphern („heating up", „raised political temperature", „hot climate") und nennen kriminologische Strategien, die darauf beschwichtigend antworten, „cooling devices".

1510 KUNZ 2011, S. 329 f.

1511 Diesbzgl. Marcel Alexander Niggli treffend im Interview im Artikel „Kampfzone Strafrecht" in der NZZ am Sonntag vom 7. Dezember 2008: „[…] weil das Strafrecht, wie es heute konzipiert ist, nichts anderes kann, als sie zu enttäuschen." Sehr ähnlich KUNZ 2011, S. 360; HASSEMER 1995, S. 485 f. Vgl. auch TROTHA, S. 230.

1512 KAMMERER 2008, S. 82. Vgl. MONAHAN/FISHER, S. 374.

gung gehabt zu haben.[1513] Die festgefahrene Verunsicherung in der Bevölkerung erstaunt daher nicht, sie wird unter anderem durch die dargestellten Rechtfertigungsmuster und die Interessen der Protagonisten der Kriminalitätsbekämpfung perpetuiert.[1514]

Abnutzungserscheinungen der Inszenierung postmoderner Technologien abzuwarten, könnte eine erste Taktik der kriminologischen Reaktion sein. Die Technologien sind teils noch jung, der Umgang mit ihnen wird erst allmählich alltäglich. BOERS konnte bei seiner Untersuchung der Kriminalitätsfurcht „Anpassungs- und Relativierungsprozesse", eine „mentale Eigendynamik" und „selbstregulative Prozesse" in der Bevölkerung feststellen.[1515] Vielleicht liegt hierin eine Erkenntnis, die allgemein auf den Trend der postmodernen Kriminalitätsbekämpfungstechnologien übertragen werden kann. Die Anpassung an die strukturellen Neuerungen der Postmoderne braucht ihre Zeit. Die Generationen, welche in diese Epoche der schnellen Information und Kommunikation und des Hinaustragens des Privaten in die Öffentlichkeit hineingeboren wurden oder noch werden, verunsichert das postmoderne Umfeld möglicherweise nicht mehr so sehr. Wagnisse könnten wieder bewusst eingegangen werden und die Ideologie der umfassenden Sicherheit, und damit entgrenzte postmoderne Kriminalitätsbekämpfungsinstrumente, an Bedeutung verlieren. Gesellschaftliche Vorstellungen kommen und gehen. Indes ist SINGELNSTEIN/STOLLE zuzustimmen, dass die postmodernen Kriminalitätsbekämpfungstechnologien bereits stark verwurzelt sind und ein allfälliger Transformationsprozess auf vielen Ebenen ablaufen müsste.[1516]

Eine aktivere Taktik könnte vielleicht Wandlungsprozesse einleiten und selbstregulierende Dynamiken unterstützen. Sowohl technische, rechtliche und kriminologische Bedenken bezüglich postmoderner Technologien zu äussern, als auch

---

1513 KREISSL/STEINERT, S. 969: Treten Katastrophen ein, „lässt sich immer argumentieren, man habe rechtzeitig darauf hingewiesen und entsprechende Massnahmen ergriffen." Vgl. auch HASSEMER 1995, S. 483.

1514 Vgl. oben Dritter Teil, Kapitel IV.D. Siehe dazu auch SIMONS Besprechung des Buchs von LOADER/SPARKS in seinem Blog vom 15. August 2010.

1515 BOERS, S. 13 f. Siehe auch NOGALA 1998, S. 322. Faszinieren diese Technologien nur solange, wie sie neu sind? Jedenfalls scheint sich in der Öffentlichkeit auch Widerstand gegen die herrschende Sicherheitslogik zu formieren, siehe dazu etwa SINGELNSTEIN/STOLLE 2012, S. 168 und TROTHA, S. 232 oder auch die Beiträge im Sammelband der LEIPZIGER KAMERA. Vgl. auch NOGALA 1998, S. 297. Siehe auch oben Vierter Teil, Kapitel IV.D.

1516 SINGELNSTEIN/STOLLE 2007, S. 116.

sie zu evaluieren und die Öffentlichkeit über sie und andere postmoderne Paradigmen aufzuklären, mag weiterhelfen. Die Form, *wie* kommuniziert wird, ist entscheidend. Ansätze der „Crime Science" führen die Kriminalpolitik vielleicht in andere unbefriedigende Richtungen[1517], und (über)dramatisierte Warnungen vor den Gefahren postmoderner Technologien tragen vielmehr zu einem Furchtklima bei. Die Unsicherheitsgefühle mit der Furcht vor dem Totalüberwachungsstaat, vor der totalen Kontrolle oder zumindest der Furcht vor dem Verlust zentraler Freiheiten zu bekämpfen, also eine Art „war on fear" zu lancieren, trifft weder den Kern der Problematik postmoderner Paradigmen und Entgrenzungsneigungen noch kühlt es die aufgeheizte Stimmung ab. Dieses Vorgehen kann sich vielmehr als kontraproduktiv herausstellen, da es den „Alarmismus" in der Gesellschaft genauso fördert wie die reissende Strömung, die es verlangsamen soll.[1518] Analog fehlleitend wirkt oftmals die Medienberichterstattung. Die Medien können zwar unter Umständen eine öffentliche Diskussion über (Überwachungs-)Skandale entfachen und damit staatlichem oder privatem Handeln (vorübergehend) Schranken setzen.[1519] Die grossen Überwachungseklats sollen durchaus aufgedeckt werden und an die Öffentlichkeit gelangen. Die daraus entstehenden, wenig nüchtern geführten Diskussionen lenken aber vom eigentlichen Problem ab, den schleichend eingeführten, kleinen Veränderungen des Bekämpfungsstrafrechts.[1520] Diese sind im Vergleich zu grossen Skandalen keine Sensation. Die kleinen Veränderungen bleiben meist unbeachtet, bis sie in ihrer Kombination zum Debakel gediehen sind und dem Enthüllungsjournalismus ein Spektakel versprechen. Zudem macht der Vergleich des Kleinen mit dem Grossen das Kleine für die Öffentlichkeit erträglich. Solange sie dem Grossen entgeht, kümmert sie sich, erleichtert, diesem entgangen zu sein, nicht um die vielen kleinen Probleme. Besonders beim Thema Kriminalität dürfte diese Feststellung zutreffen, unter anderem, da sie seit der Postmoderne selbst als Skandal gilt. Kleine Ungerechtigkeiten in der Kriminalitätsbekämpfung kümmern nicht, solange nur der totale Überwachungsstaat verhindert werden kann. Diesen haben wir aber wohl ohnehin nicht zu fürchten. Beunruhigen sollte stattdessen bei-

---

1517 Zur Kritik an den Ansätzen der „Crime Science", siehe etwa LOADER/SPARKS, S. 106 ff.; KUNZ 2008.

1518 SLABY, S. 385 ff. Vgl. auch HASSEMER 2000, S. 262; ULLRICH/LÊ, S.124 ff.

1519 Vgl. etwa CHESTERMAN, S. 135; NOGALA 1989, S. 71. Die „anfängliche Empörung" schlägt aber zuweilen rasch in „weitgehendes Desinteresse" um, siehe BELSER, S. 11 N. 20. Ebenso KREIS.

1520 Siehe etwa SINGELNSTEIN/STOLLE 2012, S. 162 f. Vgl. auch TESCHNER, S. 121 f.

spielsweise die zunehmende gesellschaftliche Abschottung von Delinquenten. In Anlehnung an BAUDRILLARD ist daher zu bedenken: Nicht die Kriminalität ist der Skandal, sondern deren instrumentalisierter Abgrenzungseffekt, der Nachweis der Konformität durch die Präsenz von Delinquenz, die Manifestation von Unsicherheit durch das Versprechen von Sicherheit.[1521]

Eine kommunikativere Kriminologie, die entdramatisiert, aufklärt und postmoderne Überwachungspraktiken, Sicherheitsrationalitäten und Menschenbilder des Risikos als Inszenierungen entlarvt[1522], kann möglicherweise zu einer besseren Kriminalpolitik beitragen[1523] und muss insbesondere nicht bedeuten, Partnerschaften mit den Protagonisten der herrschenden Sicherheitslogik einzugehen[1524], welche die Debatte bestimmen. Die Auswirkungen der postmodernen Kriminalitätsbekämpfungstechnologien der Öffentlichkeit offenzulegen, alternative Perspektiven und Strategien gegenüberzustellen und zu diskutieren, ohne dabei selbst Furcht zu verursachen, könnte somit eine dritte Taktik sein.[1525] Sich dem kriminalpolitischen Diskurs zu entziehen, Technologien und Strategien der postmodernen Kriminalitätsbekämpfung unkommentiert stehen zu lassen, befördert deren unkritischen Einsatz wohl nur.[1526] Eine aufklärende Kommunikation könnte hingegen Klischeevorstellungen über die Kriminalität und die dementsprechenden misstrauischen und hochgeschaukelten, gesellschaftlichen Sentiments zerstreuen. Es stellt sich aber die Frage, über welche Kanäle eine derartige Kommunikation erfolgen kann: Expertenmeinung, die notwendigerweise zumeist keine einfachen, unrelativierten Lösungen bieten, scheinen wenig beliebt. Medien sind auf Inhalte ausgelegt, von denen hohe Einschaltqouten zu erwarten bzw. die (konsumentengerecht?) sehr verkürzt darstellbar sind. Die Politik schei-

---

1521 BAUDRILLARD, S. 29 und 35. Vgl. auch KREIS, S. 56.

1522 SINGELNSTEIN/STOLLE 2012, S. 146 und 165 ff.

1523 LOADER/SPARKS, S. 121 f. („*contribute to a better politics"*) und 125 ff. Ebenso KUNZ 2011, S. 375 f.; HASSEMER 1995, S. 487. Auch wenn die derart aufklärende Kriminologie mitunter diffamiert wird, bspw. als „Täterschutz" (siehe dazu SINGELNSTEIN/STOLLE 2012, S. 164 f.; TESCHNER, S. 133; KUNZ 2002, S. 734), scheint die Ansicht von ALBRECHT P. A. 2010, S. 11 und 17, dass gegen die heutigen Sicherheitslogiken „kein Aufklärungskraut gewachsen" sei, zu pessimistisch. Vgl. auch HAYES 2009, S. 80; HASSEMER 2006, S. 140; DERS. 1995, S. 483.

1524 Wie etwa CLARKE, S. 102 f. vorschlägt.

1525 SINGELNSTEIN/STOLLE 2012, S. 162 f. und 172; LOADER/SPARKS, S. 127; FOUCAULT 1994a, S. 245 f.; HASSEMER 1995, S. 487; ROTHE, S. 70 und 74 (mit Verweis auf Foucaults „Etho-Poetik").

1526 Vgl. KUNZ 2000, S. 118 f. und 168. Siehe aber etwa SINN, S. 107 mit weiteren Hinweisen.

nen diejenigen Standpunkte und Vorschläge zu dominieren, welche kurzfristig am meisten Wählerstimmen versprechen.

Möglicherweise verbergen sich hinter oberflächlichen, punitiven Einstellungen der Gesellschaft zur Kriminalität hintergründige, reflektiertere Ansichten und die Verfälschung ist lediglich auf die Mühlen des „governing through crime" von Wirtschaft, Medien und Politik zurückzuführen.[1527] Indes ist auch in dieser Hinsicht mit GARLAND übereinstimmend anzuerkennen, dass eine nachhaltige Änderung der Einstellung der Gesellschaft gegenüber der Kriminalität, abweichendem Verhalten und Auffälligen die gesellschaftlichen Dynamiken in allen Aspekten betreffen müsste.[1528] Die gesellschaftliche Einstellung zur Kriminalität kann sich mithin kaum isoliert transformieren, sondern hängt vom Kontext mit anderen Wahrnehmungsprozessen und tatsächlichen Gegebenheiten der kulturellen, wirtschaftlichen, politischen und technischen Situation ab, in welche sie eingebettet ist.

[1527] KUNZ 2011, S. 376. Ähnlich SINGELNSTEIN/STOLLE 2012, S. 165.
[1528] GARLAND, S. 268 f.; ebenso KUNZ 2006, S. 72.

SCHLUSSWORT

Die postmoderne Gesellschaft scheint Kriminalität durch ein Kaleidoskop zu betrachten: Hyperreal verzerrt. Sie äussert Sicherheitsbedürfnisse, welchen der Staat zu entsprechen versucht, welche er aber nicht erfüllen kann. Postmoderne Kriminalitätsbekämpfungsstrategien offerieren Konzepte, Kriminalität zu managen. Deren Konzepte bieten indes kaum Lösungen.[1529] Vielmehr werden durch diese Konzepte Probleme aus den einen Bereichen in andere Bereiche umgelagert, indem durch sie Kriminalität reguliert wird. Beispielsweise wird durch sie soziale Sicherheit abgebaut und dafür technische Sicherheit beworben[1530], oder durch sie werden Logiken in staatliche Behörden eingeführt, durch welche die behördliche Tätigkeit effizienter gestaltet werden soll. Tatsächlich aber wird durch diese Logiken die behördliche Arbeit unter anderem erschwert, etwa durch zeitraubende und Ressourcen beanspruchende Bedürfnisse, immer mehr Informationen zusammenzutragen oder jegliche Devianz zu erkennen und zu bearbeiten.[1531] Die dargestellten Konzepte sind wenig fassbar und umgehen zuweilen bestehende rechtliche Schranken.

Die auf diesen Konzepten beruhenden postmodernen Kriminalitätsbekämpfungstechnologien sind verführerisch sowohl für die einsetzenden Behörden als auch für die Öffentlichkeit, da sie unter anderem zum einen effizientere Abläufe, Zugriff auf vormals schwerer zugängliche Plattformen sowie ein Einschreiten zu früheren Zeitpunkten und zum anderen objektiv-authentische Erzeugnisse versprechen. Ihre Wirkungspotenziale, Erfolge und Errungenschaften sind aber oftmals lediglich inszeniert. Auch arbeiten postmoderne Konzepte regelmässig mit reiner Symbolik, und es betätigen sich verschiedene Protagonisten mit unterschiedlichen Interessen auf dem Gebiet innerer Sicherheit. Dessen sollten sich alle Beteiligten, auch die Öffentlichkeit, bewusst sein.[1532]

In der vorliegenden Arbeit wird keineswegs die Meinung vertreten, staatliche Behörden seien völlig zu enttechnisieren oder dergleichen.[1533] Kritisiert wurden

---

1529 Siehe etwa ALBRECHT P. A. 2010, S. 12 ff.
1530 KREISSL/STEINERT, S. 969.
1531 Siehe etwa ERICSON/HAGGERTY; oben Vierter Teil, Kapitel V.B.
1532 Vgl. BIDLO, S. 41; NOGALA 1998, S. 267 f.
1533 Ohnehin sollen vorliegend keine Handlungsempfehlungen vorgeschlagen werden.

in erster Linie die ausgewählten, spezielleren postmodernen Kriminalitätsbekämpfungstechnologien, nicht der Einsatz von Technik im Allgemeinen. Aus dem heutigen Alltag der staatlichen Behörden ist ein Instrumentarium an computergestützter Datenverarbeitung kaum mehr wegzudenken.[1534] Ein Grossteil der verwendeten Technik mag Chancen eröffnen, hilfreich und legitim sein. Auch einige der vorliegend besprochenen spezielleren postmodernen Kriminalitätsbekämpfungstechnologien mögen unter Umständen, innerhalb bestimmter Grenzen oder in Ausnahmefällen gerechtfertigterweise und durchaus zweckmässig zum Einsatz kommen.

Viele dieser spezielleren Methoden sind aber noch technisch unausgereift und/oder zeigen höchstens vage oder ambivalente Wirkungen. In dieser Hinsicht werden sie, das ist eine der Haupterkenntnisse, oft falsch eingeschätzt.[1535] Es scheint daher wichtig, über die Prozesse und Funktionsweisen der Technologien informiert zu sein, damit diese allenfalls unter sehr kontrollierten Bedingungen eingesetzt werden können. Der Gesellschaft stellt sich diesbezüglich die Frage, ob und wie allenfalls einzelne Technologien nutzbringend angewendet werden können und sollen: Bringen sie im Vorgehen gegen Kriminalität den staatlichen Behörden einen tatsächlichen, mehr als symbolischen Mehrwert? Welche Folgen hat die Verwendung der damit gesammelten oder analysierten Daten auf den Delinquenten, auf bestimmte Personengruppen, auf Bürger, auf unsere Lebensweise und auf unsere Gesellschaft?[1536]

Keine Überwachung oder keine Kontrolle steht wohl ohnehin nicht zur Debatte. GARLAND stellt fest: „Surveillance and control, for better or for worse, occur as part of the normal process of social interaction.“[1537] Gesellschaft beziehungsweise Gemeinschaft bedeutet (gegenseitige) Überwachung und Kontrolle. Sie lassen sich nicht trennen. Es sollte aber weder im Rausch von Sicherheitsfantasien noch von Überwachungsstaatsängsten eingeschätzt werden, welche der Technologien gesellschaftlich tragbar und wünschenswert sind. Die Kriminalpolitik unterliegt vielen Dynamiken, und viele verschiedene Interessengruppen möchten ihre Ansprüche, nicht immer auf redliche Art und Weise, durchsetzen. Die Mitwirkung

---

1534 Vgl. NOGALA 1998, S. 60.

1535 Z. B. werden sie überschätzt bzgl. ihrer Wirkungen auf Kriminalitätsraten sowie Grossbedrohungen oder unterschätzt bzgl. ihrer Nebenfolgen auf die Gesellschaft. Vgl. etwa ALBRECHT H. J. ET AL., S. 218; HOFFMANN/MUSOLFF, S. 272 f.; STAPEL, S. 54.

1536 Vgl. HEYMANN, S. 157; GARLAND 1995, S. 132.

1537 GARLAND 1995, S. 131.

dieser Protagonisten trägt oft zu ausufernden Überwachungtätigkeiten bei. Kompromisse zu schliessen scheint daher nicht immer möglich und vor allem nicht immer ratsam zu sein.[1538]

Postmoderne Kriminalitätsbekämpfungstechnologien bergen ein beträchtliches Entgrenzungspotenzial in sich. Vor allem automatisierte Varianten sollen Bedrohungen und unerwünschtes Verhalten immer früher und auf breiterer Ebene bekämpfbar machen. Überschiessende Funktionalitäten, hohe Streubreiten oder auch Fehlerquellen führen zusätzlich zu ungewollt entgrenzenden Tendenzen. In der vorliegenden Arbeit kamen verschiedene beschränkende Ansätze rechtlicher, technischer und organisatorischer Art, zur Sprache. Diese mögen Einzelfallprobleme eingesetzter Technologien vermindern, stellen aber nicht immer ausreichende Barrieren dar.[1539]

Die Rechtslage der postmodernen Kriminalitätsbekämpfungstechnologien in der Schweiz ist manchmal schwer zu überschauen, manchmal unvollständig: Der föderale Staatsaufbau im Polizeirecht führt zu vielen, regional teilweise sehr unterschiedlichen Regelungen. Zudem werden insbesondere Ermächtigungsnormen zu Datenverarbeitungstätigkeiten oft recht vage formuliert. Auch bestehen für viele Varianten und Vorgehensweisen noch keine (ausdrücklichen) Ermächtigungsnormen, was Behörden nicht immer davon abhielt, sie trotzdem einzusetzen. Mittels Gesetzesrevisionen und neu geschaffener Gesetze, die teils zu Recht nicht unumstritten sind, wird versucht, dieser unsicheren Rechtslage entgegenzuwirken. Fraglich ist, ob und in welcher Weise sich die Gesellschaft mit dem Einsatz dieser Technologien zur Bekämpfung der Kriminalität arrangieren will und kann. Es gilt jedenfalls, sich mit ihnen, wie auch mit dem „Sicherheitsparadigma" unserer Zeit, und deren Folgen eingehend zu befassen.[1540]

1538 Vgl. den Kommentar von SIMON in seinem Blog vom 15. August 2010 zu LOADER/SPARKS: „Throughout the book the authors speak of «governing crime» as if there remained a real consensus that, at the end of the day, that is what both government and academic criminology care about. But as the title of this blog and my book suggest, both citizens and politicians in the US at least, have become invested in governing through crime. Given that investment, clearing the ground and removing rubbish is both a much more difficult and much more dangerous task than Loader and Sparks seem to imagine." Siehe auch VOLKMANN, S. 222.

1539 Siehe etwa VOLKMANN, S. 221; SIMON D., S. 129.

1540 Vgl. HASSEMER 2006, S. 140; DERS. 1995, S. 489; VOLKMANN, S. 222; YOUNG 1999, S. 199.

Viele der dargestellten Problembereiche lassen etwas rat- und orientierungslos zurück. Die eine, einfache Lösung konnte vorliegend nicht gefunden werden.[1541] Allenfalls konnten Ansatzpunkte aufgezeigt werden: Tiefgreifende Lösungen müssten wohl unmittelbar bei den postmodernen Kriminalitätsbekämpfungsstrategien und -rationalitäten ansetzen, die die heutigen Sicherheits- und Präventionsparadigmen verstärken, welche wiederum die untersuchten Kriminalitätsbekämpfungstechnologien antreiben und entgrenzen lassen.[1542] Lösungsansätze, diese Paradigmen zu entkräften, wären vielleicht in Gesprächen einer rationalen, beruhigenden, jedoch nicht verharmlosenden[1543] Kriminologie mit der Öffentlichkeit zu suchen.

1541 Vgl. HASSEMER 2006, S. 139. Vielleicht kann der Weg, mit einem tradionellen Verständnis, mit traditionellen Werten etc. an die „neuen Paradigmen" heranzugehen, das Ziel aber auch nur verfehlen.

1542 NOGALA 1998, S. 170 und 287 macht darin einen Wandel zu einem „Polizeitypus der Postmoderne" aus. Ähnlich VOLKMANN, S. 222; SIEBER, S. 37. Vgl. NOGALA/SACK, S. 136 f.; COHEN, S. 129 bzgl. der Mythologie des „crime-control talk": „We must look at the tellers – their distinctive structural position, vested interests, preferred language – and not the tales."

1543 Siehe HASSEMER 1995, S. 487.

QUELLENVERZEICHNIS

Die aufgeführten Autorinnen und Autoren werden, wenn bei den einzelnen Werken nicht anders angegeben, mit ihrem Nachnamen und der betreffenden Seitenzahl und/oder Randnote zitiert. Sämtliche Internetquellen wurden zuletzt besucht am 30. November 2013.

Literatur

AL-FAROUQ ABO YOUSSEF, OMAR, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 2012, S. 92–110.

ALBERTINI, GIANFRANCO, Einführung, in: Albertini, Gianfranco (Hrsg.), Polizeiliche Ermittlung, Zürich 2008, S. 10-16.

ALBRECHT, FLORIAN, Rechtswidrige Online-Durchsuchung durch das Bayerische Landeskriminalamt. Anmerkung zu LG Landshut, Beschl. v. 20. 01. 2011 – 4 Qs 346/10, JurPC Web-Dok. 59/2011, N. 1-30, zitiert als: ALBRECHT F.

ALBRECHT, HANS-JÖRG, Kriminalitätsumfang, Opferrisiken und Kriminalitätsfurcht in der Schweiz, in: Kunz, Karl-Ludwig / Moser, Rupert (Hrsg.), Innere Sicherheit und Lebensängste, Bern/Stuttgart/Wien 1997, S. 37-84, zitiert als: ALBRECHT H. J.

ALBRECHT, HANS-JÖRG / BRUNST, PHILLIP / BUSSER, ELS DE / GRUNDIES, VOLKER / KILCHLING, MICHAEL / RINCEANU, JOHANNA / KENZEL, BRIGITTE / NIKOLOVA, NINA / ROTINO, SOPHIE / TAUSCHWITZ, MORITZ, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht, 2. erweiterte Fassung, Freiburg i. Br. 2011, zitiert als: ALBRECHT H. J. ET AL.

ALBRECHT, PETER-ALEXIS, Die vergessene Freiheit, Strafrechtsprinzipien in der europäischen Sicherheitsdebatte, Berlin 2003, zitiert als: ALBRECHT P. A. 2003.

ALBRECHT, PETER-ALEXIS, Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: Herzog, Felix / Neumann, Ul-

frid (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg 2010, S. 3-18, zitiert als: ALBRECHT P. A. 2010.

ANDREJEVIC, MARK, iSpy, Surveillance and power in the interactive era, Lawrence 2007.

ANDRES, HERBERT, Internet-Überwachung in der Praxis, in: Cassani, Ursula / Dittmann, Volker / Maag, Renie / Steiner, Silvia (Hrsg.), Mehr Sicherheit – weniger Freiheit?, Chur 2003, S. 239-253.

APONTE, ALEJANDRO, Krieg und Politik – Das politische Feindstrafrecht im Alltag, HRRS 2006, S. 297-303.

ARNOLD, JÖRG, Entwicklungslinien des Feindstrafrechts in 5 Thesen, HRRS 2006, S. 303-315, zitiert als: ARNOLD 2006a.

ARNOLD, JÖRG, Zum Geleit: Ende der Gespensterjagd und Beginn der wissenschaftlichen Debatte, in: Uwer, Thomas (Hrsg.), „Bitte bewahren Sie Ruhe", Berlin 2006, S. 13-25, zitiert als: ARNOLD 2006b.

Artikel „Anschlagspläne, die keine waren", Süddeutsche.de vom 15. Juli 2013, <http://www.sueddeutsche.de/politik/geheimdiensterkenntnisse-durch-prism-anschlagsplaene-die-keine-waren-1.1721889>.

Artikel „Auch Facebook weiss, wo du bist", Tages-Anzeiger Online vom 24. August 2010, <http://www.tagesanzeiger.ch/digital/internet/Auch-Facebook-weiss-wo-Du-bist/story/17988221>.

Artikel „Big Brother kennt 23 Millionen Bürger", Spiegel 46/1986 vom 10. November 1986, <http://www.spiegel.de/spiegel/print/d-13520567.html>.

Artikel „Chaos Computer Club analysiert aktuelle Version des Staatstrojaners" des CCC vom 26. Oktober 2011, <http://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner>.

Artikel „Das Ende des Vergessens", NZZ am Sonntag vom 10. Oktober 2010, S. 79 f.

Artikel „Effizienz contra Datenschutz", NZZ Online vom 20. Juni 2006, <http://www.nzz.ch/2006/06/20/il/articlee7f3e_1.40836.html>.

Artikel „Gestatten: Terroristin, sechs Jahre alt", 20 Minuten Online vom 29. Juni 2010, <http://www.20min.ch/news/kreuz_und_quer/story/Gestatten--Terroristin--sechs-Jahre-alt-24611542>.

Artikel „Hooligan-Konkordat im Gegenwind“, NZZ Online vom 16. Februar 2013, <http://www.nzz.ch/aktuell/zuerich/uebersicht/hooligan-konkordat-im-gegenwind-1.18005018>.

Artikel „Hooligans am Internet-Pranger: Der erste hat sich gemeldet“, Tages-Anzeiger Online vom 13. August 2010, <http://www.tagesanzeiger.ch/panorama/vermischtes/Hooligans-am-InternetPranger-Der-erste-hat-sich-gemeldet/story/16097907>.

Artikel „Kampfzone Strafrecht“, NZZ am Sonntag vom 7. Dezember 2008, S. 25.

Artikel „Kein Ende in Sicht“, NZZ am Sonntag vom 5. Mai 2012.

Artikel „Lauschangriff von Google“, NZZ am Sonntag vom 23. Mai 2010, S. 54 f.

Artikel „MEPs want EU sex offender list“, BBC vom 22. August 2007, <http://news.bbc.co.uk/2/hi/uk_news/6958807.stm>.

Artikel „Nach «Prism» jetzt «Tempora»“, NZZ Online vom 23. Juni 2013, <http://www.nzz.ch/aktuell/international/uebersicht/nach-prism-jetzt-tempora-1.18103887>.

Artikel „Polizei soll auf Passfotos zugreifen können“, Tages-Anzeiger Online vom 14. März 2013, <http://www.tagesanzeiger.ch/schweiz/standard/Polizei-soll-auf-Passfotos-zugreifen-koennen/story/28881028>.

Artikel „Register der Schuldigen“, Die Zeit 13/2002 vom 21. März 2002, <http://www.zeit.de/2002/13/Register_der_Schuldigen>.

Artikel „Snowden enthüllt britische Spionage“, NZZ Online vom 22. Juni 2013, <http://www.nzz.ch/aktuell/international/uebersicht/snowden-enthuellt-britische-spionage-1.18103838>.

Artikel „Staatstrojaner: Behörden spähten 100mal Computer aus“, Spiegel Online vom 15. Oktober 2011, <http://www.spiegel.de/netzwelt/netzpolitik/staatstrojaner-behoerden-spaehten-100-mal-computer-aus-a-791941.html>.

Artikel „Trojaner passen nicht zu einem Rechtsstaat“, Tages-Anzeiger Online vom 14. Oktober 2011, <http://www.tagesanzeiger.ch/schweiz/standard/Trojaner-passen-nicht-zu-einem-Rechtsstaat/story/12528641>.

Artikel „Vorratsdatenspeicherung unverzichtbar – oft einziger Ermittlungsansatz“, Polizeispiegel vom 3. März 2012, S. 10, <http://www.dpolg.de/upload/pdfpolsp/PS03-2012.pdf>.

AUF DER MAUER, ROLF / STEINER, THOMAS, Technologiegerechte Haftungsstandards für Online-Dienstanbieter. Selbstregulierung als Benchmarks, in: Heinemann, Andreas / Hilty, Reto M. / Nobel, Peter / Sethe, Rolf / Zäch, Roger (Hrsg.), Kommunikation, Festschrift für Rolf H. Weber zum 60. Geburtstag, Bern 2011, S. 413-426.

BAKER, TOM / SIMON, JONATHAN, Embracing Risk, in: Baker, Tom / Simon, Jonathan (Hrsg.), Embracing risk, Chicago 2002, S. 1-25.

BARR, JEREMIAH R. / BOWYER, KEVIN W. / FLYNN, PATRICK J. / BISWAS, SOMA, Face recognition from video: A review, International Journal of Pattern Recognition and Artificial Intelligence 2012 16/5, S. 1-55, <http://www3.nd.edu/~kwb/BarrEtAlIJPRAI_2012.pdf>, zitiert als: BARR ET AL.

BARTMANN, JULIA, Terrorlisten, Ebenenübergreifende Sanktionsregime zur Bekämpfung der Terrorismusfinanzierung, Diss., Stuttgart 2011.

BARTSCH, VERENA, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA, Diss., Berlin 2004.

BARZ, HEINER, Religion ohne Institution?, Eine Bilanz der sozialwissenschaftlichen Jugendforschung, Opladen 1992.

BATESON, MELISSA / NETTLE, DANIEL / ROBERTS, GILBERT, Cues of being watched enhance cooperation in a real-world setting, Biology Letters 2006 2/3, S. 412-414.

BAUDRILLARD, JEAN, Simulacres et simulation, Paris 1981.

BAUM, OLIVIER, Rechtliche Fragestellung im Zusammenhang mit dem kriminalpräventiven Einsatz von Videoüberwachungsanlagen im öffentlichen Raum, Jusletter vom 8. Oktober 2007.

BAUMAN, ZYGMUNT, Ansichten der Postmoderne, Hamburg 1995.

BECKER, KIM-BJÖRN, Internetzensur in China, Aufbau und Grenzen des chinesischen Kontrollsystems, Wiesbaden 2011.

BEDNER, MARK, Rechtmässigkeit der „Deep Packet Inspection“, Universität Kassel, 2009, <http://d-nb.info/99889267X/34>.

BENDRATH, RALF, Global technology trends and national regulation: Explaining variation in the governance of Deep Packet Inspection, Paper prepared for the

International Studies Annual Convention, New York City, 15-18 Februar 2009, Version vom 3. März 2009, <http://userpage.fu-berlin.de/bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf>.

BELSER, EVA MARIA, 1. Kapitel: Einführung und 3. Kapitel: Verfassungsrechtlicher Rahmen, in: Belser, Eva Maria / Epiney, Astrid / Waldmann, Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, S. 1-51 und 297-410.

BELSER, EVA MARIA / EPINEY, ASTRID / WALDMANN, BERNHARD, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011.

BESOZZI, CLAUDIO, Rückfall nach Strafvollzug: eine empirische Untersuchung, in: Kunz, Karl-Ludwig (Hrsg.), Die Zukunft der Freiheitsstrafe, Bern 1989, S. 115-140.

BIAGGINI, GIOVANNI, Verfassungsrechtliche Abklärungen betreffend die Teilrevision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Vorlage „BWIS"), Gutachten vom Juni 2009, VPB. 2009.14, S. 238-330, <http://www.bk.admin.ch/dokumentation/02574/04607/>.

BIANCHI, ANDREA, Assessing the effectiveness of the UN Security Council's anti-terrorism measures: The quest for legitimacy and cohesion, European Journal of International Law 2006 17/5, S. 881-919.

BIDLO, OLIVER, 1414 – Ins elektronische Panoptikum der sozialen Kontrolle oder: Das Bild hat immer recht, in: Zurawski, Nils (Hrsg.), Überwachungspraxen – Praktiken der Überwachung, Opladen 2011, S. 35-46.

BIEDERMANN, ALEX / JOËLLE, VUILLE, Bewertung von DNA-Untersuchungsergebnissen aus der Sicht von Gerichten und Sachverständigen: Wie viel von unserer Wahrnehmung können wir „für wahr nehmen"?, ZStrR 2011, S. 278-295.

BIENDL, MICHAEL, Die Vorratsdatenspeicherung in Europa, Deutschland und Bayern, Eine vergleichende Betrachtung und Bewertung aus Sicht der IT-Sicherheit, 2011, <http://epub.uni-regensburg.de/24116/>.

BIER, CHRISTOPH / SPIECKER GEN. DÖHMANN, INDRA, Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?, CR 9/2012, S. 610-618.

BIERMANN KAI, Überwachungstrojaner kommt aus Bayern, Zeit Online vom 10. Oktober 2011, <http://www.zeit.de/digital/datenschutz/2011-10/ccc-staatstrojaner-bayern>.

BIGNAMI, FRANCESCA, Towards a right to privacy in transitional intelligence networks, Michigan Journal of International Law 28/2007, S. 663-686.

BISCHOF, SEVERIN / SCHWEIZER, RAINER J., Der Begriff der Personendaten, digma 4/2011, S. 152-159.

BLAUERT, ANDREAS / WIEBEL, EVA, Gauner- und Diebslisten. Registrieren, Identifizieren und Fahnden im 18. Jahrhundert, Frankfurt am Main 2001.

BOERS, KLAUS, Kriminalprävention und Kriminalpolitik mit der Kriminalitätsfurcht?, Neue Kriminalpolitik 2/2001, S. 10-15.

BOGARD, WILLIAM, Welcome to the society of control: The simulation of surveillance revisited, in: Haggerty, Kevin D. / Ericson, Richard V. (Hrsg.), The new politics of surveillance and visibility, Toronto/Buffalo 2006, S. 55-78.

BOMMER, FELIX, Hirnforschung und Schuldstrafrecht, in: Stichweh, Rudolf / Bommer, Felix (Hrsg.), Die zwei Kulturen?, Luzern 2007, S. 23-32.

BORNEWASSER, MANFRED, Was weiss man über die Wirksamkeit der Videoüberwachung im öffentlichen Raum? – Ergebnisse der kriminologischen Evaluationsforschung, in: Schwarzenegger, Christian / Nägeli, Rolf (Hrsg.), 3. Zürcher Präventionsforum – Videoüberwachung als Prävention?, Zürich/ Basel/Genf 2010, S. 133-157.

BORNEWASSER, MANFRED / SCHULZ, FRANZISKA, Systematische Videoüberwachung am Beispiel einer Massnahme in Brandenburg, in: Bücking, Hans-Jörg (Hrsg.), Polizeiliche Videoüberwachung öffentlicher Räume, Berlin 2007, S. 75-94.

BOWYER, KEVIN W., Face recognition technology: Security versus privacy, IEEE Technology and Society Magazine 2004, S. 9-20, <http://www3.nd.edu/~kwb/face_recognition.htm>.

BRADSHER, KEITH, China enacting a high-tech plan to track people, The New York Times Online vom 12. August 2007, <http://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?pagewanted=print>.

BRAUN, FRANK, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, Kommunikation & Recht 2011, S. 681-686.

BREDEKAMP, HORST / WERNER, GABRIELE, Interview: Bildunterschätzung – Bildüberschätzung. Ein Gespräch der „Bildwelten des Wissens“ mit Michael Hagner, in: Bilder in Prozessen, Bildwelten des Wissens, Kunsthistorisches Jahrbuch für Bildkritik, Band 1/1, Berlin 2003, S. 103-111.

BREITENMOSER, STEPHAN, Kommentar zu Art. 13 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

BRODEUR, JEAN-PAUL / LEMAN-LANGLOIS, STÉPHANE, Surveillance fiction or higher Policing, in: Haggerty, Kevin D. / Ericson, Richard V. (Hrsg.), The new politics of surveillance and visibility, Toronto/Buffalo 2006, S. 171-198.

BUBLITZ, HANNELORE, Foucaults Archäologie des kulturellen Unbewussten. Zum Wissensarchiv und Wissensbegehren moderner Gesellschaften, Frankfurt/New York 1999.

BUCHER, LAURA / HÄGGI, RETO, Täterfahndung im Internet, AJP 2009, S. 1088-1094.

BUCKLER, KEVIN / SALINAS, PATTI ROSS, Mass media in crime and justice, in: Miller, J. Mitchell (Hrsg.), 21st century criminology, Thousand Oaks 2009, S. 711-719.

BUERMEYER, ULF, Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154-166.

BUERMEYER, ULF / BÄCKER, MATTHIAS, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, HRRS 2009, S. 433-441.

BÜLLESFELD, DIRK, Polizeiliche Videoüberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge, Diss., Stuttgart 2002, zitiert als: BÜLLESFELD 2002.

BÜLLESFELD, DIRK, Verfassungs- und polizeirechtliche Aspekte polizeilicher Videoüberwachung öffentlicher Räume in Deutschland, in: Bücking Hans-Jörg (Hrsg.), Polizeiliche Videoüberwachung öffentlicher Räume, Berlin 2007, S. 63-74, zitiert als: BÜLLESFELD 2007.

BUNDESKRIMINALAMT, Gesichtserkennung als Fahndungshilfsmittel, Foto-Fahndung, Abschlussbericht, 2007, <http://www.bka.de/DE/ThemenABisZ/Forschung/FotoFahndung/fotoFahndung__node.html?__nnn=true>, zitiert als: Bericht BKA Fotofahndung.

BYGRAVE, LEE A., Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, 17/2011, S. 17-24.

CALLIESS, CHRISTIAN, Sicherheit im freiheitlichen Rechtsstaat, Eine verfassungsrechtliche Gratwanderung mit staatstheoretischem Kompass, ZRP 2002, S. 1-7.

CAMPBELL, NANCY D., Technologies of suspicion: Coercion and Compassion in Post-disciplinary surveillance regimes, Surveillance & Society 2004 2/1, S. 78-92.

CAVELTI, ULRICH, Kommentar zu Art. 24 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

CHAOS COMPUTER CLUB, Analyse einer Regierungs-Malware, 8. Oktober 2011, <http://www.ccc.de/de/updates/2011/staatstrojaner>, zitiert als: CCC Analyse.

CHAOS COMPUTER CLUB, Ozapftis – Teil 2. Analyse einer Regierungs-Malware, 26. Oktober 2011, <http://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner>, zitiert als: CCC Analyse Teil 2.

CHAU, MICHAEL / XU, JENNIFER, Using web mining and social network analysis to study the emergence of cyber communities in blogs, in: Chen, Hsinchun / Reid, Edna / Sinai, Joshua / Silke, Andrew / Ganor, Boaz (Hrsg.), Knowledge management and data mining for homeland security, New York 2008, S. 473-494.

CHESTERMAN, SIMON, One nation under surveillance, A new social contract to defend freedom without sacrificing liberty, Oxford/New York 2011.

CHOTHIA, TOM / COVA, MARCO / NOVAKOVIC, CHRIS / TORO, CAMILO GONZÁLEZ, The unbearable lightness of monitoring: Direct monitoring in BitTorrent, <http://www.cs.bham.ac.uk/~tpc/Papers/P2PSecComm2012.pdf>, zitiert als: CHOTHIA ET AL.

CLARKE, RONALD V., New challenges for research: Technology, criminology and crime science, in: Savona, Ernesto Ugo (Hrsg.), Crime and Technology, Dordrecht 2004, S. 97-104.

COBLER, SEBASTIAN, Herold gegen Alle, Gespräche mit dem Präsidenten des Bundeskriminalamtes, TransAtlantik 11/1980, S. 29-40, <http://blog.stummkonzert.de/wp-content/uploads/2012/08/1980-11-00-Transatlantik-Herold-gegen-Alle.pdf>.

COHEN, STANLEY, Social-Control talk: Correctional change, in: Garland, David / Young, Peter (Hrsg.), The power to punish. Contemporary penality and social analysis, London/New Jersey 1983, S. 101-129.

COMPUTERGRUPPE H48, Schritte zu einem sicher(er)en Computersystem, in: Leipziger Kamera (Hrsg.), Kontrollverluste, Münster 2009, S. 200-206.

COOPER, ALISSA, Doing the DPI dance. Assessing the privacy impact of Deep Packet Inspection, in: Aspray, William / Doty, Philip (Hrsg.), Privacy in America, Lanham 2011, S. 139-165.

COUDERT, FANNY, When video cameras watch and screen: Privacy implications of pattern recognition technologies, Computer Law & Security Review 4/2010, S. 377-384.

CROSSMAN, GARETH, Nothing to hide, nothing to fear?, International Review of Law, Computers & Technology 2008 22/1-2, S. 115-118.

CUSSON, MAURICE, Les nouvelles technologies font-elles baisser la criminalité?, in: Cimichella, Sandro / Kuhn, André / Niggli, Marcel Alexander (Hrsg.), Neue Technologien und Kriminalität: Neue Kriminologie?, Zürich 2006, S. 65-84.

DAENIKEN, URS VON, Sicherheit bei Sportveranstaltungen. Die neuen gesetzlichen Bestimmungen betreffend die Bekämpfung von Gewaltdelikten bei Sportveranstaltungen, digma 2006, S. 54-58.

D'ANGELO, DAVID / GRENZ, CARSTEN / KUNTZSCH, COLIN / BOGEN, MANFRED, CamInSens – An intelligent in-situ security system for public spaces, International Conference on Security and Management (SAM) 2012, <http://publica.fraunhofer.de/documents/N-209075.html>, zitiert als: D'ANGELO ET AL.

DELEUZE, GILLES, Kontrolle und Werden [1990], in: Deleuze, Gilles, Unterhandlungen, Frankfurt am Main 1993, S. 243-253, zitiert als: DELEUZE 1993a.

DELEUZE, GILLES, Postskriptum über die Kontrollgesellschaften [1990], in: Deleuze, Gilles, Unterhandlungen, Frankfurt am Main 1993, S. 252-262, zitiert als: DELEUZE 1993b.

DEPARIS, JEAN-PIERRE / DAVID, YVES, Project TR1016 CROMATICA, Final Report, <http://dilnxsrv.king.ac.uk/cromatica/FinalReport.pdf>.

DIGGELMANN, OLIVER, Targeted sanctions und Menschenrechte. Reflexionen zu einem ungeklärten Verhältnis, SZIER 2009, S. 301-335.

DITTMANN, VOLKER, Beurteilung und Behandlung sogenannter gemeingefährlicher Straftäter aus forensisch-psychiatrischer Sicht, in: Kunz, Karl-Ludwig / Moser, Rupert (Hrsg.), Innere Sicherheit und Lebensängste, Bern/Stuttgart/ Wien 1997, S. 123-140, zitiert als: DITTMANN 1997.

DITTMANN, VOLKER, Täterprofile und operative Fallanalysen – Mythen und Fakten, in: Cassani, Ursula / Dittmann, Volker / Maag, Renie / Steiner, Silvia (Hrsg.), Mehr Sicherheit – weniger Freiheit?, Chur 2003, S. 71-89, zitiert als: DITTMANN 2003.

DITTON, JASON / SHORT, EMMA, Yes, it works, no, it doesn't: Comparing the effects of open-Street CCTV in two adjacent scottish town centres, in: Norris, Clive / Wilson, Dean (Hrsg.), Surveillance, crime, and social control, Hampshire/Burlington 2006, S. 151-153.

DUDOUET, VÉRONIQUE, Anti-terrorism legislation: Impediments to conflict transformation, Berghof Policy Brief 02, November 2011, <http://www.berghof-conflictresearch.org/documents/publications/PolicyBrief02.pdf>, S. 1-16.

DUNSTONE, TED / YAGER, NEIL, Biometric system and data analysis: design, evaluation and data mining, Eveleigh 2009.

DÜRRENMATT, FRIEDRICH, Der Hund. Der Tunnel. Die Panne. Erzählungen, Zürich 1998.

DYER, CLARE, „There is no war on terror", The Guardian vom 24. Januar 2007, <http://www.theguardian.com/politics/2007/jan/24/uk.terrorism>.

EBNER, GERHARD / DITTMANN, VOLKER / STEINER-KÖNIG, URSULA / KURT, HANS, Verwahrung gefährlicher Straftäter: Kluft zwischen politischen Forderungen und medizinisch-wissenschaftlicher Machbarkeit, SZK 2/2005, S. 71-72, zitiert als: EBNER ET AL.

ELGER, CHRISTIAN E. / FRIEDERICI, ANGELA D. / KOCH, CHRISTOF / LUHMANN, HEIKO / MALSBURG, CHRISTOPH VON DER / MENZEL, RANDOLF / MONYER, HANNAH / RÖSLER, FRANK / ROTH, GERHARD / SCHEICH, HENNING / SINGER, WOLF, Das Manifest – Gegenwart und Zukunft der Hirnforschung, in: Könneker, Carsten (Hrsg.), Wer erklärt den Menschen?, Frankfurt am Main 2007, S. 77-84, zitiert als: Elger et al.

EMMERSON, BEN, Promotion and protection of human rights and fundamental freedoms while countering terrorism, Report to the United Nations General Assembly, Dokument A/67/396 vom 26. September 2012, <http://www.un.org/en/ga/third/67/documentslist.shtml>.

ENGLER, MARC, Sicherheit an Sportveranstaltungen unter strafrechtlichen Gesichtspunkten, Sicherheit & Recht 3/2008, S. 162-178.

ERICSON, RICHARD V. / HAGGERTY, KEVIN D., The policing of risk, in: Baker, Tom / Simon, Jonathan (Hrsg.), Embracing risk, Chicago 2002, S. 238-272.

ERNEST-JONES, MAX / NETTLE, DANIEL / BATESON, MELISSA, Effects of eye images on everyday cooperative behaviour: a field experiment, Evolution and Human Behavior 2011 32/3, S. 172-178.

EUGSTER, TIMM, Auch Basel fichierte ohne Schranken, Basler Zeitung vom 19. September 2009, <http://www.referendum-bwis.ch/BaZ_19092009.pdf>.

FARRINGTON, DAVID P. / GILL, MARTIN / WAPLES, SAM J. / ARGOMANIZ, JAVIER, The effects of closed-circuit television on crime: meta-analysis of an English national quasi-experimental multi-site evaluation, Journal of Experimental Criminology 2007 3/1, S. 21-38, zitiert als: FARRINGTON ET AL.

FARRINGTON, DAVID P. / WELSH, BRANDON C., Effects of improved street lightning on crime: a systematic review, Home Office Research Study 251, August 2002, <http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs2/hors251.pdf>.

FEELEY, MALCOLM / SIMON, JONATHAN, Actuarial justice: the emerging new criminal law, in: Nelken, David (Hrsg.), The futures of criminology, London/Thousand Oaks/New Delhi 1994, S. 173-201.

FERRAJOLI, LUIGI, L'illusione della sicurezza 2008, <www.festivaldeldiritto.it/2008/pdf/interventi/ferrajoli.pdf>.

FIENBERG, STEPHEN E., Homeland Insecurity, in: Chen, Hsinchun (Hrsg.), Terrorism informatics, New York 2008, S. 197-218.

FISAHN, ANDREAS, Überwachung und Repression. Logiken der Herrschaftssicherung, in: Leipziger Kamera (Hrsg.), Kontrollverluste, Münster 2009, S. 34-48.

FLÜCKIGER, ALEXANDRE, Droits fondamentaux et vidéosurveillance par les particuliers et les autorités des espaces ouverts au public, in: Schwarzenegger,

Christian / Nägeli, Rolf (Hrsg.), 3. Zürcher Präventionsforum – Videoüberwachung als Prävention?, Zürich/Basel/Genf 2010, S. 195-226.

FLÜCKIGER, ALEXANDRE / AUER ,ANDREAS, La vidéosurveillance dans l'oeil de la Constitution, AJP 2006, S. 924-942.

FOUCAULT, MICHEL, Das Subjekt und die Macht, Nachwort von Michel Foucault, in: Dreyfus, Hubert L. / Rabinow, Paul (Hrsg.), Michel Foucault, Weinheim 1994, S. 243-261, zitiert als: FOUCAULT 1994a.

FOUCAULT, MICHEL, Zur Genealogie der Ethik. Ein Überblick über laufende Arbeiten, in: Dreyfus, Hubert L. / Rabinow, Paul (Hrsg.), Michel Foucault, Weinheim 1994, S. 265-292, zitiert als: FOUCAULT 1994b.

FOUCAULT, MICHEL, Überwachen und Strafen, 1. Aufl., Frankfurt am Main 1994, zitiert als: FOUCAULT 1994c.

FOUCAULT, MICHEL, Die Gouvernementalität [1977-1978], in: Bröckling, Ulrich / Krasmann, Susanne / Lemke, Thomas (Hrsg.), Gouvernementalität der Gegenwart, Frankfurt am Main 2000, S. 41-67, zitiert als: FOUCAULT 2000.

FOUCAULT, MICHEL, Analytik der Macht, Frankfurt am Main 2005, zitiert als: FOUCAULT 2005.

FRATTINI, FRANCO, New challenges, new opportunities, Vortrag vom 26. März 2007 an der Security Research Conference in Berlin, <http://europa.eu/rapid/press-release_SPEECH-07-188_en.htm?locale=en>.

FREILING, FELIX C. / HEINSON, DENNIS, Probleme des Verkehrsdatenbegriffs im Rahmen der Vorratsdatenspeicherung, DuD 2009, S. 547-552.

FRICKER, CHRISTOPH / MAEDER, STEFAN, Kommentar Vor Art. 255 und zu Art. 255 StPO, in: Niggli, Marcel Alexander / Heer, Marianne / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011.

FUCHS, CHRISTIAN / BOERSMA, KEES / ALBRECHTSLUND, ANDERS / SANDOVAL, MARISOL, Introduction: Internet and surveillance, in: Fuchs, Christian / Boersma, Kees / Albrechtslund, Anders / Sandoval, Marisol (Hrsg.), Internet and surveillance, New York 2012, S. 1-30, zitiert als: FUCHS ET AL.

FÜRNKÄS, JOSEF, Automation und die Metamorphosen des Zuschauers, in: Pfeiffer, K. Ludwig / Schnell, Ralf (Hrsg.), Schwellen der Medialisierung, Bielefeld 2008, S. 181-221.

GANDY, O. H., The surveillance society. Information technology and bureaucratic social control, in: Goold, Benjamin J. (Hrsg.), Surveillance, Band I, New York 2009, S. 67-83.

GARLAND, DAVID, Kultur der Kontrolle, Verbrechensbekämpfung und soziale Ordnung in der Gegenwart, Frankfurt am Main 2008.

GARLAND, DAVID, Panopticon Days: Surveillance and society, Criminal Justice Matters 1995 20/1, S. 3-4, zitiert als: GARLAND 1995.

GATES, KELLY, The Tampa „Smart CCTV" experiment, Culture Unbound 2/2010, S. 67-89.

GAUTIER, DINU / BUSCH, HEINER, Internet-Überwachung à la suisse, CILIP 1/2011, S. 49-56.

GEHRING, PETRA, Ein Organ wie jedes andere?, Zur Rechtspolitik der Hirnbildverwendung und der Hirnmanipulation, in: Sokol, Bettina (Hrsg.), Die Gedanken sind frei … – Hirnforschung und Persönlichkeitsrechte, Düsseldorf 2007, S. 56-75.

GERCKE, MARCO / BRUNST, PHILLIP W., Praxishandbuch Internetstrafrecht, Stuttgart 2009.

GILL, MARTIN / SPRIGGS, ANGELA, Assessing the impact of CCTV, Home Office Research Study 292, Februar 2005, <http://www.popcenter.org/responses/video_surveillance/pdfs/gill&spriggs_2005.pdf>.

GILLIOM, JOHN, Overseers of the poor. Surveillance, resistance, and the limits of privacy, Chicago 2001.

GLESS, SABINE, Beweisverbote und Fernwirkung, ZStrR 2010, S. 146-159, zitiert als: GLESS 2010.

GLESS, SABINE, Kommentar zu Art. 139 und 141 StPO, in: Niggli, Marcel Alexander / Heer, Marianne / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011, zitiert als: GLESS 2011.

GLESS, SABINE, Strafverfolgung im Internet, ZStrR 2012, S. 3-22, zitiert als: GLESS 2012.

GMÜR, MARIO, Die Gefährlichkeitsprognose, AJP 2004, S. 1307-1318.

GODERBAUER, RAINER, Behandlungsnotwendigkeiten und Behandlungsvoraussetzungen bei Sexualstraftätern, in: Rehn, Gerhard / Wischka, Bernd / Lösel,

Friedrich / Walter, Michael (Hrsg.), Behandlung „gefährlicher Straftäter", Herbolzheim 2001, S. 111-121.

GOLDSCHMID, PETER, Der Einsatz technischer Überwachungsgeräte im Strafprozess. Unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern, Diss., Bern 2001.

GOOLD, BENJAMIN J., Public area surveillance and police work: the impact of CCTV on police behaviour and autonomy, Surveillance & Society 2003 1/2, S. 191-203.

GOTTFREDSON, MICHAEL R. / HIRSCHI, TRAVIS, A general theory of crime, Stanford 1990.

GRAHAM, STEPHEN / WOOD, DAVID, Digitizing surveillance: categorization, space, inequality, in: Norris, Clive / Wilson, Dean (Hrsg.), Surveillance, crime, and social control, Hampshire/Burlington 2006, S. 537-558.

GRAS, MARIANNE, Kriminalprävention durch Videoüberwachung, Gegenwart in Grossbritannien – Zukunft in Deutschland?, Diss., Baden-Baden 2003.

GRAU, ALEXANDER, Momentaufnahmen eines Geistes?, in: Könneker, Carsten (Hrsg.), Wer erklärt den Menschen?, Frankfurt am Main 2007, S. 167-175.

GREENWALD, GLENN, XKeyscore: NSA tool collects „nearly everything a user does on the internet", The Guardian vom 31. Juli 2013, <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.

GROEBNER, VALENTIN, Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, München 2004.

GRUBER, PATRIK, Kommentar zur Art. 365, Art. 369 und 371 StGB, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111-392 StGB, 3. Aufl., Basel 2013.

HÄFELIN, ULRICH / HALLER, WALTER / KELLER, HELEN, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich/Basel/Genf 2012.

HÄFELIN, ULRICH / MÜLLER, GEORG / UHLMANN, FELIX, Allgemeines Verwaltungsrecht, 6. Aufl., Zürich/St. Gallen 2010.

HÄNER, ISABELLE, Die Mindestgarantien für Strafverfahren und ihre Bedeutung für verwaltungsrechtliche Sanktionen, in: Häner, Isabelle / Waldmann, Bern-

hard (Hrsg.), Verwaltungsstrafrecht und sanktionierendes Verwaltungsrecht, Zürich/Basel/Genf 2010, S. 19-40.

HANSEN, MARKUS / PFITZMANN, ANDREAS, Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, Deutsche Richterzeitung August 2007, S. 225-228.

HANSJAKOB, THOMAS, BÜPF/VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2006, zitiert als: HANSJAKOB 2006.

HANSJAKOB, THOMAS, Kommentar zu Art. 277 und Art. 280 StPO, in: Donatsch, Andreas / Hansjakob, Thomas / Lieber, Viktor (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, Zürich/Basel/Genf 2010, zitiert als: HANSJAKOB 2010.

HANSJAKOB, THOMAS, Einsatz von Govware – zulässig oder nicht?, Zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie, Jusletter vom 5. Dezember 2011, S. 1-6, zitiert als: HANSJAKOB 2011.

HANSJAKOB, THOMAS, Zur Zulässigkeit von Antennensuchläufen, Jusletter vom 5. März 2012, zitiert als: HANSJAKOB 2012.

HARCOURT, BERNARD E., Against prediction. Profiling, policing, and punishing in an actuarial age, Chicago 2007.

HÄRING, DANIEL, Verwertbarkeit rechtswidrig erlangter Beweise gemäss Schweizerischer Strafprozessordnung – alte Zöpfe oder substanzielle Neuerungen?, ZStrR 2009, S. 225-257.

HASLER, FELIX, Neuromythologie, Eine Streitschrift gegen die Deutungsmacht der Hirnforschung, Bielefeld 2011.

HASSEMER, WINFRIED, Perspektiven einer neuen Kriminalpolitik, StV 9/1995, S. 483-490, zitiert als: HASSEMER 1995.

HASSEMER, WINFRIED, Strafen im Rechtsstaat, Baden-Baden 2000, zitiert als: HASSEMER 2000.

HASSEMER, WINFRIED, Sicherheit durch Strafrecht, HRRS 2006, S. 130-143, zitiert als: HASSEMER 2006.

HASSEMER, WINFRIED, Verantwortlichkeit im Strafrecht, in: Roth, Gerhard / Hubig, Stefanie / Bamberger, Heinz Georg (Hrsg.), Schuld und Strafe, München 2012, S. 7-17, zitiert als: HASSEMER 2012.

HAYES, BEN, There is no „balance“ between security and civil liberties – just less of each, ECLN Essays Nr. 12 2005, <http://www.statewatch.org/news/2005/oct/ecln/essay-12.pdf>, zitiert als: HAYES 2005.

HAYES, BEN, NeoConOpticon. The EU security-industrial complex, Bericht des Transnational Institute und der Statewatch, 2009, <http://www.statewatch.org/analyses/neoconopticon-report.pdf>, zitiert als: HAYES 2009.

HEIMGARTNER, STEFAN, Strafprozessuale Beschlagnahme. Wesen, Arten und Wirkungen: unter Berücksichtigung der Beweismittel-, Einziehungs-, Rückgabe- und Ersatzforderungsbeschlagnahme, Zürich/Basel/Genf 2011.

HEINE, GÜNTER, Organisierte Kriminalität und Kriminelle Organisationen, Landesbericht Schweiz 2007, <http://www.krim.unibe.ch/unibe/rechtswissenschaft/isk/content/e2464/e2479/files2480/OrganisierteKriminalittFertig_ger.pdf>.

HEINIGER, ANDREAS, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, Jusletter vom 17. September 2012.

HEINRICH, BERND, Die Grenzen des Strafrechts bei der Gefahrprävention. Brauchen oder haben wir ein „Feindstrafrecht“?, ZStW 2009, S. 94-130.

HEMPEL, LEON, Zur Evaluation von Videoüberwachung, in: Zurawski Nils (Hrsg.), Surveillance Studies, Opladen 2007, S. 117-148.

HEMPEL, LEON / TÖPFER, ERIC, CCTV in Europe, Final Report, August 2004, <http://www.urbaneye.net/results/ue_wp15.pdf>.

HENRICHS, AXEL / WILHELM, JÖRG, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 1/2010, S. 30-37, zitiert als: HENRICHS/WILLHELM 2010a.

HENRICHS, AXEL / WILHELM, JÖRG, Virtuelles Betretungsrecht, Ermittlungen in WKW, StudiVZ und Facebook, Kriminalistik 4/2010, S. 218-224, zitiert als: HENRICHS/WILHELM 2010b.

HENSEL, DIRK, Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht. Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung, DuD 2009, S. 527-530.

HENSLER, BEAT, Strafe ohne Strafrecht – Die poenale Wirkung von verwaltungsrechtlichen Massnahmen, insbesondere am Beispiel der Präventivmassnahmen des Hooligangesetzes (BWIS) bzw. Hooligankonkordats, Sicherheit & Recht 1/2011, S. 37-44.

HESSDÖRFER, FLORIAN / BACHMANN, JAN, ASBO. Die Gesellschaft existiert, in: Leipziger Kamera (Hrsg.), Kontrollverluste, Münster 2009, S. 168-173.

HEYMANN, PHILIP B., Terrorism, freedom, and security: Winning without war, Cambridge 2003.

HILGENDORF, ERIC, Die strafrechtliche Regulierung des Internet als Aufgabe eines modernen Technikrechts, JZ 17/2012, S. 825-832.

HITZLER, ROLAND, Riskante Reaktionen. Formen der Bewältigung von auf Kriminalitätsfurcht fokussierter alltäglicher Verunsicherung, in: Kunz, Karl-Ludwig / Moser, Rupert (Hrsg.), Innere Sicherheit und Lebensängste, Bern/ Stuttgart/Wien 1997, S. 183-207.

HOFFMANN, JENS / MUSOLFF, CORNELIA, Fallanalyse und Täterprofil, Wiesbaden 2000, <http://forensiseuropa.files.wordpress.com/2011/11/2000_taterprofilundfallanalyse.pdf>.

HOFINGER, VERONIKA, Der Rückfalltäter von Lombrosos „geborenem Verbrecher“ bis zu Moffits „Life-Course-Persister“, Kriminologisches Journal 1/2013, S. 8-24.

HOFMANN, MANFRED, Die Online-Durchsuchung – staatliches „Hacken“ oder zulässige Ermittlungsmassnahme?, NStZ 2005, S. 121-125.

HÖHENER, ANDREA / VEST, HANS, Beweisverwertungsverbote – quo vadis Bundesgericht?, ZStrR 2009, S. 95-108.

HOPPMANN, GERHARD, Die Entwicklung der Rasterfahndung und DNA-Reihenuntersuchung, Kriminalistik 3/2013, S. 147-155.

HORNUNG, GERRIT / DESOI, MONIKA, „Smart Cameras“ und automatische Verhaltensanalyse. Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung, Kommunikation & Recht 2011, S. 153-158.

HOWELLS, KIM, Could 7/7 have been prevented?, Review of the Intelligence on the London terrorist attacks on 7 July 2005, Surrey 2009.

HUMAN RIGHTS WATCH, No easy Answers. Sex Offender Laws in the US, September 2007, <http://www.hrw.org/reports/2007/09/11/no-easy-answers>, zitiert als: Bericht HRW.

INS, PETER VON /WYDER PETER-RENÉ, Kommentar zu Art. 179 StGB, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111-392 StGB, 3. Aufl., Basel 2013.

INTRONA, LUCAS D., Disclosive ethics and information technology: Disclosing facial recognition systems, Ethics Information Technology 2005 7/2, S. 75-86.

INTRONA, LUCAS D. / NISSENBAUM, HELEN, Facial recognition technology: A survey of policy and implementation issues, <http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf>.

INTRONA, LUCAS D. / WOOD, DAVID, Picturing algorithmic surveillance: The politics of facial recognition systems, Surveillance & Society 2004 2/2-3.

ISENRING, BERNHARD / KESSLER, MARTIN A., Die geplante Total-Revision des BÜPF im Überblick, Sicherheit & Recht 1/2011, S. 24-35.

JAAG, TOBIAS, Verwaltungsrechtliche Sanktionen: Einführung, in: Häner, Isabelle / Waldmann, Bernhard (Hrsg.) Verwaltungsstrafrecht und sanktionierendes Verwaltungsrecht, Zürich/Basel/Genf 2010, S. 1-18.

JAGGI, EMANUEL, Geheime Überwachungsmassnahmen, ZBJV 147/2011, S. 1-38.

JAKOBS, GÜNTHER, Das Selbstverständnis der Strafrechtswissenschaft vor Herausforderungen der Gegenwart (Kommentar), in: Eser, Albin / Hassemer, Winfried / Burkhardt, Björn (Hrsg.), Die Deutsche Strafrechtswissenschaft vor der Jahrtausendwende, München 2000, S. 47-56, zitiert als: JAKOBS 2000.

JAKOBS, GÜNTHER, Bürgerstrafrecht und Feindstrafrecht, HRRS 2004, S. 88-95, zitiert als: JAKOBS 2004a.

JAKOBS, GÜNTHER, Staatliche Strafe. Bedeutung und Zweck, Paderborn 2004, zitiert als: JAKOBS 2004b.

JAKOBS, GÜNTHER, Individuum und Person, ZStW 2005, S. 247-266, zitiert als: JAKOBS 2005.

JAKOBS, GÜNTHER, Feindstrafrecht? Eine Untersuchung zu den Bedingungen von Rechtlichkeit, HRRS 2006, S. 289-297, zitiert als: JAKOBS 2006.

JEAN-RICHARD-DIT-BRESSEL, MARC, Kommentar zu Art. 269, Art. 277, Art. 278 und Art. 280 StPO, in: Niggli, Marcel Alexander / Heer, Marianne /

Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011.

JOTTERAND, OLIVIER / MÜLLER, JEREMIE / TRECCANI, JEAN, L'utilisation du cheval de Troie comme mesure de surveillance secrète, Jusletter vom 21. Mai 2012.

KAESER, EDUARD, Der Mensch als durchsichtiges Gewohnheitstier, NZZ Online vom 8. August 2013, <http://www.nzz.ch/aktuell/feuilleton/uebersicht/der-mensch-als-durchsichtiges-gewohnheitstier-1.18129131>.

KAMMERER, DIETMAR, Bilder der Überwachung, Frankfurt am Main 2008, zitiert als: KAMMERER 2008.

KAMMERER, DIETMAR, Das Werden der „Kontrolle": Herkunft und Umfang eines Deleuze'schen Begriffs, in: Zurawski, Nils (Hrsg.), Überwachungspraxen – Praktiken der Überwachung, Opladen 2011, S. 19-34, zitiert als: KAMMERER 2011.

KANT, MARTINA / BUSCH, HEINER, Ermittlungen von Polizei und Geheimdiensten im Internet, CILIP 1/2011, S. 40-48.

KATZENSTEIN, ANNEGRET, Kommentar zu Art. 280 StPO, in: Niggli, Marcel Alexander / Heer, Marianne / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011.

KAWASHIMA, KENTARO, Digitale Videokameras als neue Strategie der Überwachung. Drei Szenen aus Japan, in: Pfeiffer, K. Ludwig / Schnell, Ralf (Hrsg.), Schwellen der Medialisierung, Bielefeld 2008, S. 153-170.

KILLIAS, MARTIN / HASS, HENRIETTE / TARONI, FRANCO / MARGOT, PIERRE, Welche Verurteilten müssen in einer DNA-Profil-Datenbank erfasst werden?, in: Cassani, Ursula / Dittmann, Volker / Maag, Renie / Steiner, Silvia (Hrsg.), Mehr Sicherheit – weniger Freiheit?, Chur 2003, S. 311-326, zitiert als: KILLIAS ET AL. 2003.

KILLIAS, MARTIN / KUHN, ANDRÉ / AEBI, MARCELO F., Grundriss der Kriminologie. Eine europäische Perspektive, 2. Aufl., Bern 2011, zitiert als: KILLIAS ET AL. 2011a.

KILLIAS, MARTIN / NIGGLI, MARCEL ALEXANDER, Die Kriminalität ist seit 70 Jahren stabil, Streitgespräch, in: plädoyer 1/2005, S. 8-10.

KILLIAS, MARTIN / STAUBLI, SILVIA / BIBERSTEIN, LORENZ / BÄNZIGER, MATTHIAS / IADANZA, SANDRO, Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Opferbefragung 2011, 31. August 2011, Zürich, <http://www.rwi.uzh.ch/lehreforschung/alphabetisch/killias/publikationen/ICVS_2011_StGallen.pdf>, zitiert als: KILLIAS ET AL. 2011b.

KLEIN, INGA, Überwachte Sicherheit oder sichere Überwachung? Kulturelle Deutungsmuster im Diskurs um den biometrischen Reisepass, in: Zurawski, Nils (Hrsg.), Überwachungspraxen – Praktiken der Überwachung, Opladen 2011, S. 87-101.

KLEINER, JAN, Rechtsfragen rund um Stadionverbote, in: Arter, Oliver / Baddeley, Margareta (Hrsg.), Sport und Recht, Bern 2008, S. 19-72.

KLENGER, FABIENNE, Nationalrat will DNA-Tests für „bestimmte Asylbewerber", Tages-Anzeiger Online vom 17. April 2013, <http://www.tagesanzeiger.ch/schweiz/standard/Nationalrat-will-DNATests-fuer-bestimmte-Asylbewerber/story/21039574>.

KLESCZEWSKI, DIETHELM, Straftatenaufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, ZStW 2011, S. 737-766.

KLEY, ANDREAS / ESTHER, TOPHINKE, Kommentar zu Art. 16 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

KOCHER, VICTOR, Terrorlisten. Die schwarzen Löcher des Völkerrechts, Wien 2011.

KRABBENBORG, WILLEM, Voraussetzungen und Auswirkungen der Videoüberwachung in Europa und in den Niederlanden, in: Bücking, Hans-Jörg (Hrsg.), Polizeiliche Videoüberwachung öffentlicher Räume, Berlin 2007, S. 53-62.

KRASMANN, SUSANNE, Die Kriminalität der Gesellschaft. Zur Gouvernementalität der Gegenwart, Habil., Konstanz 2003.

KREIS, GEORG, Staatsschutz im Laufe der Zeit. Von der Skandalisierung zur Gleichgültigkeit – ein Blick zurück auf die Fichenaffäre vor zwanzig Jahren, digma 2009, S. 54-59.

KREISSL, REINHARD / STEINERT, HEINZ, Politik mit der Angst: Warum es kaum Widerstand dagegen gibt und was wir alltäglich aus ihr lernen. Überwa-

chungswünsche und Kritik der Überwachung, in: Herzog, Felix / Neumann, Ulfrid (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg 2010, S. 961-969.

KREMPL, STEFAN, „Bundestrojaner" heisst jetzt angeblich „Remote Forensic Software", heise Online vom 3. August 2007, <http://www.heise.de/newsticker/meldung/Bundestrojaner-heisst-jetzt-angeblich-Remote-Forensic-Software-159078.html>.

KRÖBER, HANS-LUDWIG, Die Wiederbelebung des „geborenen Vebrechers" – Hirndeuter, Biologismus und die Freiheit des Rechtsbrechers, in: Hillenkamp, Thomas (Hrsg.), Neue Hirnforschung – Neues Strafrecht?, Baden-Baden 2006, S. 63-83.

KUBE, EDWIN, Rasterfahndung – Kriminologische und rechtliche Aspekte, in: Cassani, Ursula / Dittmann, Volker / Maag, Renie / Steiner, Silvia (Hrsg.), Mehr Sicherheit – weniger Freiheit?, Chur 2003, S. 49-69.

KUBERA, THOMAS, Evaluation der Videoüberwachung in Bielefeld, in: Bücking, Hans-Jörg (Hrsg.), Polizeiliche Videoüberwachung öffentlicher Räume, Berlin 2007, S. 119-146.

KUNZ, KARL-LUDWIG, Vorbeugen statt verfolgen. Polizeiliche Prävention von Kriminalität: Ein Konzept mit Zukunft?, Bern 1987, zitiert als: KUNZ 1987.

KUNZ, KARL-LUDWIG, Bürgerfreiheit und Sicherheit. Perspektiven von Strafrechtstheorie und Kriminalpolitik, Bern 2000, zitiert als: KUNZ 2000.

KUNZ, KARL-LUDWIG, Kriminalwissenschaften und gesellschaftliche Sicherheit, in: Duttge, Gunnar / Geilen, Gerd / Meyer-Gossner, Lutz / Warda, Günter (Hrsg.), Gedächtnisschrift für Ellen Schlüchter, Köln/Berlin/Bonn/ München 2002, S. 727-742, zitiert als: KUNZ 2002.

KUNZ, KARL-LUDWIG, Die Sicherung als gefährlich eingestufter Rechtsbrecher: Von der Strategie der Inklusion zur strafrechtlichen Exklusion, in: Barton, Stephan (Hrsg.), „… weil er für die Allgemeinheit gefährlich ist!", Baden-Baden 2006, S. 71-86, zitiert als: Kunz 2006.

KUNZ, KARL-LUDWIG, Die wissenschaftliche Zugänglichkeit von Kriminalität. Ein Beitrag zur Erkenntnistheorie der Sozialwissenschaften, Wiesbaden 2008, zitiert als: KUNZ 2008.

KUNZ, KARL-LUDWIG, Lebenswissenschaften und Biorenaissance in der Kriminologie, in: Böllinger, Lorenz / Jasch, Michael / Krasmann, Susanne / Pilgram, Arno / Prittwitz, Cornelius / Reinke, Herbert / Rzepka, Dorothea

(Hrsg.), Gefährliche Menschenbilder, Baden-Baden 2010, S. 124-135, zitiert als: Kunz 2010a.

KUNZ, KARL-LUDWIG, Strafrechtsmodelle und Gesellschaftsstruktur, Kriminologisches Journal 1/2010, S. 9-23, zitiert als: KUNZ 2010b.

KUNZ, KARL-LUDWIG, Zur Symbolik des Strafrechts, in: Dölling, Dieter / Schöch, Heinz (Hrsg.), Verbrechen, Strafe, Resozialisierung, Berlin 2010, S. 353-367, zitiert als: KUNZ 2010c.

KUNZ, KARL-LUDWIG, Kriminologie, 6. Aufl., Bern 2011, zitiert als: KUNZ 2011.

KURZ, CONSTANZE / RIEGER, FRANK, Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, 9. Juni 2009, <http://www.ccc.de/updates/2009/vds-gutachten>.

KUTSCHA, MARTIN, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042-1044.

LAKOTTA, BEATE, Neuronen sind nicht böse, Der Spiegel 31/2007 vom 30. Juli 2007, S. 117-123, <http://www.spiegel.de/spiegel/print/d-52417857.html>.

LATZER, MICHAEL / JUST, NATASCHA / METREVELI, SULKHAN / SAURWEIN, FLORIAN, Internetverbreitung und digitale Bruchlinien in der Schweiz, Themenbericht aus dem World Internet Projekt – Switzerland 2011, Zürich März 2012, <http://www.mediachange.ch/media/pdf/publications/Verbreitung_und_Bruchlinien.pdf>, zitiert als: LATZER ET AL.

LEE, TERENCE, internet control and auto-regulation in Singapore, Surveillance & Society 2005 3/1, S. 74-95.

LEGNARO, ALDO, Prekarität, Strafe und die Ökonomie der Freiheit, Kriminologisches Journal 1/2010, S. 59-67, zitiert als: LEGNARO 2010.

LEGNARO, ALDO, Subjektivität im Zeitalter ihrer simulativen Reproduzierbarkeit: Das Beispiel des Disney-Kontinents, in: Bröckling, Ulrich / Krasmann, Susanne / Lemke, Thomas (Hrsg.), Gouvernementalität der Gegenwart, Frankfurt am Main 2000, S. 286-314, zitiert als: LEGNARO 2000.

LEIPZIGER KAMERA (Hrsg.), Kontrollverluste, Münster 2009.

LEMKE, THOMAS, Die Polizei der Gene. Formen und Felder genetischer Diskriminierung, Frankfurt 2006.

LEWONTIN, RICHARD C., Sex, lies, and social science, The New York Review of Books 1995 42/7, 20. April 1995, S. 24-29, zitiert als: LEWONTIN 1995a.

LEWONTIN, RICHARD C., Reply to: „Sex, lies, and social science“: An exchange, The New York Review of Books 1995 42/9, 25. Mai 1995, S. 43-44, zitiert als: LEWONTIN 1995b.

LIENHARD, ANDREAS / HÄSLER, PHILIPP, Verfassungsrechtliche Grundlagen des Sicherheitsrechts, in: Schweizer, Rainer J. (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Schweizerisches Bundesverwaltungsrecht Band III/1, Basel 2008, S. 95-154.

LINGG, CARMEN, Videoüberwachung im öffentlichen Raum – eine Analyse kriminologischer Aspekte mit Blick auf die Videoüberwachung auf dem Bahnhofplatz in der Stadt Luzern, in: Schwarzenegger, Christian / Nägeli, Rolf (Hrsg.), 3. Zürcher Präventionsforum – Videoüberwachung als Prävention?, Zürich/Basel/Genf 2010, S. 11-107.

LISCHKA, KONRAD / REISSMANN, OLE, Die volle Kontrolle, Spiegel Online vom 13. November 2012, <http://www.spiegel.de/netzwelt/netzpolitik/eu-ueberwachungsprojekt-indect-die-volle-kontrolle-a-866785.html>.

LISZT, FRANZ VON, Der Zweckgedanke im Strafrecht, Berlin 1883.

LIVIO, SUSAN K., Report finds Megan's Law fails to reduce sex crimes, deter repeat offenders in N. J., nj.com vom 7. Februar 2009, <http://www.nj.com/news/index.ssf/2009/02/study_finds_megans_law_fails_t_1.html>.

LOADER, IAN / SPARKS, RICHARD, Public criminology?, New York 2011.

LOBSIGER, ADRIAN, Internet Monitoring, in: Keller, Roberto / Bernasconi, Giorgio A. / Guidicelli, Luca (Hrsg.), Internet e diritto, Lugano/Basel 2004, S. 65-69.

LOBSIGER, ADRIAN, Grundaufgaben des modernen Rechtsstaates, Teil I: Grundaufgaben der Verwaltung, Polizei und Justiz sowie des Zivilen Staatsschutzes, in: Schweizer, Rainer J. (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Schweizerisches Bundesverwaltungsrecht Band III/1, Basel 2008, S. 155-210, zitiert als: LOBSIGER 2008.

LOGAN, WAYNE A., A study in „Actuarial Justice“: Sex offender classification practice and procedure, Buffalo Criminal Law Review 2000 3/2, S. 593-637.

LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE, Briefing on the Interception Modernisation Programme, Policy engagement Network (PEN)

Paper 5, <http://www.lse.ac.uk/management/documents/IMP-briefing.pdf>, zitiert als: LSE Briefing.

LÜDERSSEN, KLAUS, Das Subjekt zwischen Metaphysik und Empirie. Einfluss der modernen Hirnforschung auf das Strafrecht?, in: Duncker, Hans-Rainer (Hrsg.), Beiträge zu einer aktuellen Anthropologie, Stuttgart 2006, S. 189-205.

MACASKILL, EWEN / BORGER, JULIAN / HOPKINS, NICK / BALL, JAMES, GCHQ taps fibre-optic cables for secret acces to world's communications, The Guardian vom 21. Juni 2013, <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

MACKINNON, REBECCA, China's Censorship 2.0: How companies censor bloggers, First Monday 2009 14/2, <http://firstmonday.org/article/view/2378/2089>.

MAEDER, STEFAN / NIGGLI, MARCEL ALEXANDER, Was schützt eigentlich Strafrecht (und schützt es überhaupt etwas)?, AJP 2011, S. 443-455.

MALEK, KLAUS, Abschied von der Wahrheitssuche, StV 9/2011, S. 559-567.

MARKOWITSCH, HANS J. / SIEFER, WERNER, Tatort Gehirn, Auf der Suche nach dem Ursprung des Verbrechens, Frankfurt/Main 2007.

MARX, GARY T., The iron fist and the velvet glove: Totalitarian potentials within democratic structures, 1984-1986, <http://web.mit.edu/gtmarx/www/iron.html#Top>, zitiert als: MARX 1984.

MARX, GARY T., A tack in the shoe: Neutralizing and resisting the new surveillance, Journal of Social Issues 2003 59/2, S. 369-390, zitiert als: MARX 2003.

MARX, GARY T., Rocky Bottoms and some information age techno-fallacies, 2007, <http://web.mit.edu/gtmarx/www/rockybottoms.html>, zitiert als: MARX 2007.

MARX, GARY T., Surveillance and Society. Encyclopedia of Social Theory, 2005, <http://web.mit.edu/gtmarx/www/surandsoc.html>, zitiert als: MARX 2005.

MARX, GARY T., The surveillance society. The threat of 1984-style techniques, in: Goold, Benjamin J. (Hrsg.), Surveillance, Band I, New York 2009, S. 59-66, zitiert als: MARX 1985.

MASTRONARDI, PHILIPPE, Kommentar zu Art. 7 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

MATHIESEN, THOMAS, The future of control systems – the case of Norway, International Journal of the Sociology of Law 8/1980, S. 149-164, zitiert als: MATHIESEN 1980.

MATHIESEN, THOMAS, Preface, in: Fuchs, Christian / Boersma, Kees / Albrechtslund, Anders / Sandoval, Marisol (Hrsg.), Internet and surveillance, New York 2012, S. xv-xxi, zitiert als: MATHIESEN 2012.

MAZZUCCHELLI, GORAN, Öffentliches Strafbedürfnis, Kriminalität und die Funktion der strafrechtlichen Sanktion aus kriminologischer Sicht, AJP 2000, S. 1337-1344.

MCCABE, DAVID P. / CASTEL, ALAN D., Seeing is believing: The effect of brain images on judgments of scientific reasoning, Cognition 2008, S. 343-352.

MCDOUGALL, CYNTHIA / PERRY, AMANDA E. / FARRINGTON, DAVID P., Overview of effectiveness of criminal justice interventions in the UK, in: Perry, Amanda E. / McDougall, Cynthia / Farrington, David P., Reducing crime. The effectiveness of criminal justice interventions, S. 163-226.

MCGOUGH, STEVE, We need a National Terrorist Offender Registry, Radioviceonline vom 13. Januar 2009, <http://radioviceonline.com/we-need-a-national-terrorist-offender-registry/>.

MEIER, PHILIPPE, Protection des données. Fondements, principes généraux et droit privé, Bern 2011.

MEIRITZ, ANNETT, Pläne für öffentliches Triebtäter-Register empören Datenschützer, Spiegel Online vom 7. März 2007, <http://www.spiegel.de/politik/deutschland/0,1518,470415,00.html>.

MELIA, CANCIO, Feind„strafrecht"?, ZStW 2005, S. 267-289.

MERKEL, GRISCHA / ROTH, GERHARD, Bestrafung oder Therapie? Möglichkeiten und Grenzen staatlicher Sanktion unter Berücksichtigung der Hirnforschung, in: Rechtswissenschaftliche Fakultät Universität Zürich (Hrsg.), Hirnforschung – Chancen und Risiken für das Recht, Zürich/Basel/Genf 2008, S. 21-49.

METILLE, SYLVAIN, Les mesures de surveillance prévues par le CPP. Quelles places pour le cheval de Troie, l'IMSI-Catcher ou les puces RFID?, Jusletter vom 19. Dezember 2011.

MEYER, FRANK, Rechtsstaat und Terrorlisten – Kaltstellung ohne Rechtsschutz?, HRRS 2010, S. 74-85.

MEYER, FRANK / MACKE, JULIA, Rechtliche Auswirkungen der Terroristenlisten im deutschen Recht, HRRS 2007, S. 445-465.

MIDDEL, STEFAN, Innere Sicherheit und präventive Terrorismusbekämpfung, Diss., Baden-Baden 2007.

MINOW, NEWTON N. / ABRAMS, FLOYD / BAIRD, ZOË / BELL, GRIFFIN / CASPER, GERHARD / COLEMAN, WILLIAM T. / CUTLER, LLOYD N. / MARSH, JOHN O. / DAVIS, LISA A. / CATE, FRED H., Safeguarding Privacy in the Fight Against Terrorism. Report of the Technology and Privacy Advisory Committee, März 2004, <http://epic.org/privacy/profiling/tia/tapac_report.pdf>.

MOECKLI, DANIEL, Drohnen: Militärischer Nutzen und politische Debatten, Center for Security Studies (CSS) Analysen zur Sicherheitspolitik vom Juli 2010, <http://www.css.ethz.ch/publications/pdfs/CSS-Analysen-78.pdf>.

MOECKLI, DANIEL / KELLER, RAPHAEL, Wegweisung und Rayonverbote – ein Überblick, Sicherheit & Recht 3/2012, S. 231-245.

MOECKLI, DANIEL / THURMAN, JAMES, Survey of Counter-Terrorism Data Mining and Related Programs, DETECTER D08.1, <http://www.detecter.bham.ac.uk/documents.html>.

MOECHEL, ERICH, Indect: Werkzeuge für den Präventivstaat, futurezone vom 16. November 2009, <http://www.fuzo-archiv.at/artikel/1631510v2>.

MOHLER, MARKUS H. F., Die polizeiliche Generalklausel – vom EGMR anerkannt und deren Anwendbarkeit begrenzt, Jusletter vom 11. Januar 2010, zitiert als: MOHLER 2010.

MOHLER, MARKUS H. F., Ethik in der Polizei, in: Fehérváry, János / Stangl, Wolfgang (Hrsg.), Menschenrecht und Staatsgewalt, Wien 2000, S. 199-214, zitiert als: MOHLER 2000.

MOHLER, MARKUS H. F., Sicherheitsrecht und Rechtssicherheit bei Sportveranstaltungen (staatliche Sicherheitsmassnahmen, Umfang und Grenzen), in: Arter, Oliver / Baddeley, Margareta (Hrsg.), Sport und Recht, Bern 2008, S. 73-98, zitiert als: MOHLER 2008.

MOHLER, MARKUS H. F., Staatsschutz braucht klare Regelungen. Schwierigkeiten im Staatsschutz an der Schnittstelle zwischen Bund und Kantonen, digma 2009, S. 60-63, zitiert als: MOHLER 2009.

MOHLER, MARKUS H. F, Grundzüge des Polizeirechts in der Schweiz, Basel 2012, zitiert als: MOHLER 2012.

MOHLER, MARKUS H. F. / SCHWEIZER, RAINER J., Sicherheitspolitik und Sicherheitsrecht – sicherheitsrechtliche Problemstellungen im Zusammenhang mit dem sicherheitspolitischen Bericht, Jusletter vom 7. Dezember 2009.

MONAHAN, TORIN / FISHER, JILL A., Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices, International Journal of Technology Assessment in Health Care 2010 26/4, S. 370–376.

MONROY, MATTHIAS / BUSCH, HEINER, Digitaler Untergrund: Kriminalisten und Kriminalisierte wetteifern im Web 2.0, CILIP 1/2011, S. 3-11.

MORSE, STEPHEN, Brain overclaim syndrome and criminal responsability: A diagnostic note, Ohio State Journal of Law 3/2006, S. 397-412, <http://lsr.nellco.org/upenn_wps/123>.

MÖSTL, MARKUS, Vorratsdatenspeicherung – wie geht es weiter?, Ein Zwischenbericht zum Stand der Dinge, ZRP 2011, S. 225-229.

MÜLLER, GÜNTER, Weiss Google mehr als jeder Geheimdienst?, in: Kirchschläger, Peter G. / Thomas, Kirchschläger (Hrsg.), Menschenrechte und Digitalisierung des Alltags, Bern 2010, S. 173-181, zitiert als: MÜLLER G.

MÜLLER, JOËL O., Das revidierte Konkordat über Massnahmen zur Bekämpfung der Gewalt an Sportveranstaltungen vom 2. Februar 2012 („Hooligan-Konkordat"), recht 2013, S. 109-121, zitiert als: MÜLLER J. O.

MÜLLER, LUCIEN, Private Videoüberwachung in öffentlich zugänglichen Räumen – Datenschutzrechtliche Aspekte, Sicherheit & Recht 2/2012, S. 63-75, zitiert als: MÜLLER L. 2012a.

MÜLLER, LUCIEN, Videoüberwachung in öffentlich zugänglichen Räumen. Insbesondere zur Verhütung und Ahndung von Straftaten, Zürich 2011, zitiert als: MÜLLER L. 2011.

MÜLLER, LUCIEN, Videoüberwachung des öffentlichen Raums, Workshopbericht, Sicherheit & Recht 3/2012, S. 248, zitiert als: MÜLLER L. 2012b.

MURDOCH, STEVEN J. / ANDERSON, ROSS, Tools and technology of internet filtering, in: Deibert, Ronald / Palfrey, John / Rohozinski, Rafal / Zittrain, Jonathan (Hrsg.), Access denied: the practice and policy of global Internet filtering, Cambridge 2008, S. 57-72.

NEDOPIL, NORBERT / DITTMANN, VOLKER, Forensische Psychiatrie, Klinik, Begutachtung und Behandlung zwischen Psychiatrie und Recht, 3. Aufl., Stuttgart 2007.

NEUHAUS, RALF, Fehlerquellen bei DNA-Analysen. Nur unbedeutende Sternschnuppen aus dem Firmament des lediglich theoretischen Zweifels?, in: Duttge, Gunnar / Geilen, Gerd / Meyer-Gossner, Lutz / Warda, Günter (Hrsg.), Gedächtnisschrift für Ellen Schlüchter, Köln/Berlin/Bonn/München 2002, S. 353-561.

NEUMANN, ULFRIED, Feindstrafrecht, in: Uwer, Thomas (Hrsg.), „Bitte bewahren Sie Ruhe", Berlin 2006, S. 299-314.

NIGGLI, MARCEL ALEXANDER, Mehr innere Sicherheit durch Strafjustiz und Strafvollzug?, in: Bauhofer, Stefan / Bolle, Pierre-Henri (Hrsg.), Innere Sicherheit – innere Unsicherheit?, Chur/Zürich 1995, S. 89-129, zitiert als: NIGGLI 1995.

NIGGLI, MARCEL ALEXANDER, Strenge Strafen als Beruhigungsmittel, plädoyer 5/2004, S. 32-41, zitiert als: NIGGLI 2004.

NIGGLI, MARCEL ALEXANDER / PFISTER, FRITZ, Verlorenes Paradies?, Über Romantik, Kriminalitätsentwicklung in der Schweiz und die Kunst, Geschichten zu erzählen, AJP 1997, S. 519-536.

NISCO, ATTILIO, Sicherheit und Strafrecht in der jüngsten italienischen Gesetzgebung, Monatsschrift für Kriminologie und Strafrecht 2/2011, S. 73-82.

NOCUN, KATHARINA MARIA, Andauernder Streit um die Vorratsdatenspeicherung, CILIP 1/2011, S. 22-31.

NOGALA, DETLEF, Polizei, avancierte Technik und soziale Kontrolle. Funktion und Ideologie technikbesetzter Kontrollstrategien im Prozess der Rationalisierung von Herrschaft, Pfaffenweiler 1989, zitiert als: NOGALA 1989.

NOGALA, DETLEF, Social control technologies. Verwendungsgrammatiken, Systematisierung und Problemfelder technisierter sozialer Kontrollarrangements, Diss., Berlin 1998, zitiert als: NOGALA 1998.

NOGALA, DETLEF / SACK, FRITZ, Folgerungen für die polizeiliche Arbeit aus der Technikausstattung, in: Bundeskriminalamt (Hrsg.), Aktuelle Methoden der Kriminaltechnik und Kriminalistik, Wiesbaden 1995, S. 115-167.

NORRIS, CLIVE, The intensification and bifurcation of surveillance in British criminal justice policy, European Journal of Criminal Policy and Research, 2007 13/1-2, S. 139-158.

NORRIS, CLIVE / ARMSTRONG, GARY, The maximum surveillance society. The rise of CCTV, Oxford/New York 1999.

NORRIS, CLIVE / MORAN, JADE / ARMSTRONG, GARY, Algorithmic surveillance: the future of automated visual surveillance, in: Norris, Clive / Wilson, Dean (Hrsg.), Surveillance, crime, and social control, Hampshire/Burlington 2006, S. 497-517.

NOWAK, KAROL, Efficient and human rights-compatible search criteria for monitoring Internet Communications, DETECTER Work Package 07, <http://www.detecter.bham.ac.uk/documents.html>.

NOWARA, SABINE, Die Beurteilung der Gefährlichkeit von Straftätern, in: Rehn, Gerhard / Wischka, Bernd / Lösel, Friedrich / Walter, Michael (Hrsg.), Behandlung „gefährlicher Straftäter", Herbolzheim 2001, S. 104-110.

NUSSBAUMER, DANIEL, Massnahmen gegen nicht fassbare Gewalt, Diss., Zürich 2008.

OBERHOLZER, NIKLAUS, DNA-Datenbanken Pro und Kontra – ein öffentlicher Disput, in: Cassani, Ursula / Dittmann, Volker / Maag, Renie / Steiner, Silvia (Hrsg.), Mehr Sicherheit – weniger Freiheit?, Chur 2003, S. 325-334, zitiert als: OBERHOLZER 2003.

OBERHOLZER, NIKLAUS, Internet – Neue Herausforderungen in Strafrecht und Strafprozessrecht?, in: Keller, Roberto / Bernasconi, Giorgio A. / Guidicelli, Luca (Hrsg.), Internet e diritto, Lugano/Basel 2004, S. 45-63, zitiert als: OBERHOLZER 2004.

OEHMICHEN, ANNA, Entwicklungen strafprozessualer Massnahmen in Europa im Rahmen der Terrorfurcht, ZIS 11/2011, S. 931-939.

OLTRAMARI, ALESSANDRO / LEBIERE, CHRISTIAN, Using ontologies in a cognitive-grounded system: Automatic action recognition in video surveillance, Proceedings of the Seventh International Conference on Semantic Technolo-

gy for Intelligence, Defense, and Security, Fairfax 2012, <http://stids.c4i.gmu.edu/papers/STIDSPapers/STIDS2012_T02_OltramariLebiere_CognitiveGroundedSystem.pdf>.

OFFICE OF PROGRAM POLICY ANALYSIS & GOVERNMENT ACCOUNTABILITY (OPPAGA), Sex offender registration and public notification improved. Some aspects of the process could be streamlined, Bericht Nr. 08-60, Oktober 2008, <http://www.oppaga.state.fl.us/Summary.aspx?reportNum=08-60>, zitiert als: OPPAGA 2008.

OFFICE OF PROGRAM POLICY ANALYSIS & GOVERNMENT ACCOUNTABILITY (OPPAGA), Registered sex offenders in Florida communities increased to over 23'000. Transient offender present challenges, Bericht Nr. 12-12, Dezember 2012, <http://www.oppaga.state.fl.us/Summary.aspx?reportNum=12-12>, zitiert als: OPPAGA 2012.

ORWELL, GEORGE, Nineteen eighty-four, London 2008 [1949].

OTT, BERNHARD / KOLLBRUNNER, TIMO, Verdächtige am Internetpranger, Der Bund Online vom 12. Juni 2013, <http://www.derbund.ch/bern/nachrichten/Verdaechtige-am-Internetpranger/story/31791484>.

PAINTER, CHRISTOPHER, Threats to the net: Trends and law enforcement responses, in: Savona, Ernesto Ugo (Hrsg.), Crime and technology, Dordrecht 2004, S. 69-77.

PATON WALSH, NICK, Smart cameras will spot the guilty before they commit a crime, The Observer vom 22. Juli 2001, <http://www.guardian.co.uk/uk/2001/jul/22/socialsciences.research>.

PEHL, DIRK, Die Implementation der Rasterfahndung. Eine empirische Untersuchung zur Anwendung, Umsetzung und Wirkung der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung, Diss., Berlin 2008.

PERREY, ELKE, Gefahrenabwehr und Internet. Befugnisse der Polizei im Lichte eines Rechts auf informationelle Selbstbestimmung, Diss., Berlin 2003.

PETRI, THOMAS, Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Kapitel G, in: Bergemann, Nils / Denninger, Erhard / Lisken, Hans (Hrsg.), Handbuch des Polizeirechts, 5. Aufl., München 2012, S. 710-913.

PFITZMANN, ANDREAS / KÖPSELL, STEFAN, Risiken der Vorratsdatenspeicherung. Grenzen der Nutzungsüberwachung, DuD 2009, S. 542-546, zitiert als: PFITZMANN/KÖPSELL 2009a.

PFITZMANN, ANDREAS / KÖPSELL, STEFAN, Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in der freiheitlichen demokratischen Gesellschaft an den Beispielen Vorratsdatenspeicherung und Online-Durchsuchung, in: Alcatel-Lucent Stiftung (Hrsg.), Mensch, Technik, Kommunikation, Stuttgart 2009, S. 142-159, zitiert als: PFITZMANN/KÖPSELL 2009b.

PIATEK, MICHAEL / KOHNO, TADAYOSHI / KRISHNAMURTHY, ARVIND, Challenges and directions for monitoring P2P file sharing networks -or- why my printer received a DMCA takedown notice, zitiert als: PIATEK ET AL.

PIETH, MARK, Schweizerisches Strafprozessrecht, Grundriss für Studium und Praxis, Basel 2009.

PLATZ, ERNST, Rechtliche Zulässigkeit von „Remote Forensic Software" in der Schweiz. Inwieweit existiert in der Schweiz eine rechtliche Grundlage für den Einsatz von „Remote Forensic Software" durch Ermittlungsbehörden?, Sic! 2008, S. 838-844.

POINDEXTER, JOHN, Overview of the Information Awareness Office, Rede an der DARPATech 2002 Conference, Anaheim, 2. August 2002, <http://www.fas.org/irp/agency/dod/poindexter.html>.

POPITZ, HEINRICH, Über die Präventivwirkung des Nichtwissens (1968), Berlin 2003.

POPP, ROBERT / POINDEXTER, JOHN, Countering terrorism through information and privacy protection technologies, IEEE Security & Privacy November/ Dezember 2006, S. 24-33.

POSNER, RICHARD A., Our Domestic Intelligence Crisis, The Washington Post vom 21. Dezember 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>.

PRATT, TRAVIS C. / CULLEN, FRANCIS T. / BLEVINS, KRISTIE R. / DAIGLE, LEAH E. / MADENSEN, TAMARA D., The empirical status of deterrence theory: A meta-analysis, in: Cullen, Francis T. / Wright, John Paul / Blevins, Kristie R. (Hrsg.), Taking stock, New Brunswick 2006, S. 367-395, zitiert als: PRATT ET AL.

PRITTWITZ, CORNELIUS, Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft, Frankfurt am Main 1993.

PROBST, THOMAS, Die Verknüpfung von Personendaten und deren rechtliche Tragweite, in: Epiney, Astrid / Probst, Thomas / Gammenthaler, Nina (Hrsg.), Datenverknüpfung, Problematik und rechtlicher Rahmen, Zürich/ Basel/Genf 2011, S. 1-40.

PUSCHKE, JENS / SINGELNSTEIN, TOBIAS, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmassnahmen der StPO nach der Neuregelung zum 1. 1. 2008, NJW 2008, S. 113-119.

QUEDNOW, BORIS B., Ethics of neuroenhancement: a phantom debate, BioSocieties 2010 5/1, S. 153-156, <http://www.zora.uzh.ch/39871/4/Quednow_Review_BioSocieties_09064_1209_revised_BQ_AM_V.pdf>.

QUENSEL, STEPHAN, Wer raucht, der stiehlt. Zur Interpretation quantitativer Daten in der Jugendsoziologie. Eine jugendkriminologische Studie, Wiesbaden 2009.

RANCIÈRE, JACQUES, Das Unvernehmen: Politik und Philosophie, Frankfurt am Main 2002.

RENZ, FABIAN, Der Nachrichtendienst arbeitet an einer neuen Datenbank, Tages-Anzeiger Online vom 3. Mai. 2011, <http://www.tagesanzeiger.ch/schweiz/standard/Der-Nachrichtendienst-arbeitet-an-einer-neuen-Datenbank-/story/29176592>.

REUBAND, KARL-HEINZ, Videoüberwachung: Was die Bürger von der Überwachung halten, Neue Kriminalpolitik 2/2001, S. 5-9, zitiert als: REUBAND 2001.

REUBAND, KARL-HEINZ, Steigende Kriminalitätsbedrohung, Medienberichterstattung und Kriminalitätsfurcht der Bürger, Kriminologisches Journal 9. Beiheft 2007, S. 71-86, zitiert als: REUBAND 2007.

RHYNER, BEAT / STÜSSI, DIETER, Überwachung mit technischen Überwachungsgeräten (Art. 280-281), in: Albertini, Gianfranco (Hrsg.), Polizeiliche Ermittlung, Zürich 2008, S. 462-470.

RICKLI, NATALIE, Für eine Verschärfung des Strafrechts, Der Zürcher Bote vom 8. Mai 2009, <http://www.svp-zuerich.ch/svpzh-dl/zb/bote090508.pdf>.

RISS, CIRIL / BERANEK ZANON, NICOLE, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, Jusletter vom 9. Juli 2012.

ROGALL, KLAUS, Rasterfahndung in Zeiten des Terrorismus, in: Duttge Gunnar/Geilen Gerd/Meyer-Gossner Lutz/Warda Günter (Hrsg.), Gedächtnisschrift für Ellen Schlüchter, Köln/Berlin/Bonn/München 2002, S. 611-645.

ROGGAN, FREDRIK, Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, NJW 2009, S. 257-262, zitiert als: ROGGAN 2009.

ROGGAN, FREDRIK, Die Videoüberwachung von öffentlichen Plätzen. Oder: Immer mehr gefährliche Orte für Freiheitsrechte, NVwZ 2001, S. 134-141, zitiert als: ROGGAN 2001.

ROHNER, CHRISTOPH, Kommentar zu Art. 22 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

ROOS EVELINE / JEKER KONRAD, Antennensuchlauf im Rahmen einer Rasterfahndung, forumpoenale 3/2012, S. 175-180.

ROSE, NIKOLAS, „Screen and intervene": governing risky brains, History of the Human Sciences 2010 23/1, S. 79-105.

RÖSLER, FRANK, Grenzen der Erkenntnis, Individualität und Plastizität des menschlichen Gehirns machen eine genaue Vorhersage des Verhaltens einer einzelnen Person prinzipiell unmöglich, in: Könneker, Carsten (Hrsg.), Wer erklärt den Menschen?, Frankfurt am Main 2007, S. 85-86.

ROSSNAGEL, ALEXANDER, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, S. 1238-1242.

ROSSNAGEL, ALEXANDER / BEDNER, MARK / KNOPP, MICHAEL, Rechtliche Anforderungen an die Aufbewahrung von Vorratsdaten, DuD 2009, S. 536-541.

ROSSNAGEL, ALEXANDER / DESOI, MONIKA / HORNUNG, GERRIT, Gestufte Kontrolle bei Videoüberwachungsanlagen. Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung, DuD 2011, S. 694-701, zitiert als: ROSSNAGEL/DESOI/HORNUNG 2011.

ROSSNAGEL, ALEXANDER / DESOI, MONIKA / HORNUNG, GERRIT, Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik. Am Beispiel der smarten Videoüberwachung, ZD 2012, S. 459-461, zitiert als: ROSSNAGEL/DESOI/HORNUNG 2012.

ROTERT, MICHAEL, Internetüberwachung zwischen Anspruch und Wirklichkeit, Kriminalistik 7/2004, S. 435-440.

ROTH, GERHARD, Aus Sicht des Gehirns, Frankfurt am Main 2003, zitiert als: ROTH 2003a.

ROTH, GERHARD, Fühlen, Denken, Handeln. Wie das Gehirn unser Verhalten steuert, Neue vollständig überarbeitete Aufl., Frankfurt am Main 2003, zitiert als: ROTH 2003b.

ROTH, GERHARD, Gewaltstraftäter – böse oder psychisch kranke Menschen?, in: Roth Gerhard/Hubig Stefanie/Bamberger Heinz Georg (Hrsg.), Schuld und Strafe, München 2012, S. 89-107, zitiert als: ROTH 2012.

ROTH, GERHARD / LÜCK, MONIKA / STRÜBER, DANIEL, „Freier Wille" und Schuld von Gewaltstraftätern aus Sicht der Hirnforschung und Neuropsychologie, Neue Kriminalpolitik 2/2006, S. 55-59, zitiert als: ROTH ET AL. 2006.

ROTHE, MATTHIAS, Um die Überwachung geht es nicht, in: Leipziger Kamera (Hrsg.), Kontrollverluste, Münster 2009, S. 68-75.

RUDIN, BEAT, Auf der Suche nach dem „Bodensatz" – Datenschutzrechtliche Aspekte der präventiven Rasterfahndung, AwR 2007, S. 276-283.

RUDIN, BEAT / STÄMPFLI, SANDRA, Wunderheilmittel Videoüberwachung?, digma 2009, S. 144-151.

RÜESCH, ANDREAS, Grossflächige Überwachung des Internets, NZZ Online vom 7. Juni 2013, <http://www.nzz.ch/aktuell/international/uebersicht/geheimdienst-zapft-laut-zeitung-server-von-internet-firmen-an-1.18094805>.

RÜTHER, WERNER, Phänomene der Internetdelinquenz – Ansätze, Probleme und Erkenntnisse zu ihrer gesellschaftlichen Definition und zu ihrer quantitativen Erfassung, in: Cimichella, Sandro / Kuhn, André / Niggli, Marcel Alexander (Hrsg.), Neue Technologien und Kriminalität: Neue Kriminologie?, Zürich 2006, S. 85-120.

RUX, JOHANNES, Die Festplatte als Wohnung?, JZ 17/2007, S. 828-833.

RZEPKA, DOROTHEA, Wider einfache Lösungen: „Kriminalität" aus kriminologisch-sozialwissenschaftlicher Perspektive, in: Barton, Stephan (Hrsg.), „… weil er für die Allgemeinheit gefährlich ist!", Baden-Baden 2006, S. 119-142.

SARAT, AUSTIN, „… the law is all over": Power, resistance and the legal consciousness of the welfare poor, Yale Journal of Law & the Humanities 1990 2/2, S. 343-379.

SAUNDERS, DEBRA J., Norway's strange definition of insanity, SFGate vom 1. Dezember 2011, <http://www.sfgate.com/opinion/saunders/article/Norway-s-strange-definition-of-insanity-2339878.php>.

SAVONA, ERNESTO UGO / MIGNONE, MARA, The fox and the hunters: How IC technologies change the crime race, in: Savona, Ernesto Ugo (Hrsg.), Crime and technology, Dordrecht 2004, S. 7-28.

SCHEFER, MARKUS, BWIS I: Kompetenzen und Grundrechte, digma 2006, S. 60-65.

SCHEININ, MARTIN, Förderung und Schutz aller Menschenrechte, der bürgerlichen, politischen, wirtschaftlichen, sozialen und kulturellen Rechte, einschliesslich des Rechts auf Entwicklung, Bericht an die Generalversammlung der Vereinten Nationen, Dokument A/HRC/10/3 vom 4. Februar 2009, <http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx>.

SCHLEIM, STEPHAN, Die Neurogesellschaft. Wie die Hirnforschung Recht und Moral herausfordert, Hannover 2010.

SCHLEPPER, CHRISTINA / PETER, SASCHA / LÜDEMANN, CHRISTIAN, Self-Policing als Substitut formeller sozialer Kontrolle?, Kriminologisches Journal 2/2011, S. 82-98.

SCHMID, ANDREAS / BAUMGARTNER, FABIAN, „Staatstrojaner" im Fall Stauffacher eingesetzt, NZZ Online vom 15. Oktober 2011, <http://www.nzz.ch/aktuell/schweiz/trojaner-im-fall-stauffacher-eingesetzt-1.12994241>.

SCHMID, NIKLAUS, Handbuch des schweizerischen Strafprozessrechts, Zürich/St. Gallen 2009, zitiert als: SCHMID 2009a.

SCHMID, NIKLAUS, Schweizerische Strafprozessordnung, Praxiskommentar, Zürich/St. Gallen 2009, zitiert als: SCHMID 2009b.

SCHMIDT, JÜRGEN, Bundestrojaner: Geht was – was geht?, heise Online vom 11. März 2007, <http://www.heise.de/security/artikel/Bundestrojaner-Geht-was-was-geht-270880.html>.

SCHMIDT-SEMISCH, HENNING, Kriminalität als Risiko, Schadenmanagement zwischen Strafrecht und Versicherung, München 2002.

SCHNEIDER, HANS JULIUS, Reden über Inneres, Ein Blick mit Ludwig Wittgenstein auf Gerhard Roth, in: Krüger Hans-Peter (Hrsg.), Hirn als Subjekt?, Berlin 2007, S. 223-239.

SCHNEIER, BRUCE, The future of privacy, vom 6. März 2006, <http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html>.

SCHNEIER, BRUCE, Data maning for terrorists, Blog vom 9. März 2006, <http://www.schneier.com/blog/archives/2006/03/data_mining_for.html>.

SCHRÖDER, DETLEF, Videoüberwachung in Grossbritannien und den USA, in: Bücking, Hans-Jörg (Hrsg.), Polizeiliche Videoüberwachung öffentlicher Räume, Berlin 2007, S. 41-52.

SCHULTE, DOMINIK, Der Schutz individueller Rechte gegen Terrorlisten. Internationale, europäische und nationale Menschenrechtsstandards im Spannungsverhältnis zwischen effektiver Terrorismusbekämpfung und notwendigem Individualrechtsschutz, Diss., Baden-Baden 2010.

SCHULZKI-HADDOUTI, CHRISTIANE, Gläserne Soziale Netzwerke, CILIP 1/2011, S. 32-39.

SCHWARZENEGGER, CHRISTIAN, „L'uomo delinquente" aus aktueller kriminologischer Sicht, in: Brägger, Benjamin Frederick / Albrecht, Peter (Hrsg.), Kriminologie – Wissenschaftliche und praktische Entwicklungen, Chur/Zürich 2004, S. 113-134.

SCHWEITZER, N. J. / SAKS, MICHAEL J., Neuroimage evidence and the insanity defense, Behavioral Sciences and the Law 2011, S. 592-607.

SCHWEIZER, RAINER J., Vorbemerkungen zur Sicherheitsverfassung sowie Kommentar zu Art. 10 und 13 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008, zitiert als: SCHWEIZER 2008.

SCHWEIZER, RAINER J., Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz, DuD 2009, S. 462-468, zitiert als: SCHWEIZER 2009.

SCHWEIZER, RAINER J., Unnötige und fragwürdige Datenbearbeitungen auf NZZ Online vom 22. Juli 2010, <http://www.nzz.ch/aktuell/startseite/unnoetige-und-fragwuerdige-datenbearbeitungen-1.6783097>.

SCHWEIZER, RAINER J. / BISCHOF, SEVERIN, Switzerland: Brain Research and the Law, in: Spranger, Tade Matthias (Hrsg.), International neurolaw, Berlin 2012, S. 269-287.

SCHWEIZER, RAINER J. / MÜLLER, LUCIEN, Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, LeGes 3/2008, S. 379-399.

SCHWEIZER, RAINER J. / SUTTER, PATRICK / WIDMER, NINA, Grundbegriffe, in: Schweizer Rainer J. (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Schweizerisches Bundesverwaltungsrecht Band III/1, Basel 2008, S. 53-94.

SCOTT, CHARLES L. / GERBASI, JOAN B., Sex offender registration and community notification challenges: The Supreme Court continues its trend, The Journal of the American Academy of Psychiatry and the Law 2003, S. 494-501.

SENN, MARCEL, Grenzen und Risiken der Hirnforschung – Folgerungen für die Rechtsordnung, in: Rechtswissenschaftliche Fakultät Universität Zürich (Hrsg.), Hirnforschung – Chancen und Risiken für das Recht, Zürich/Basel/Genf 2008, S. 1-12.

SESSAR, KLAUS, Die Angst vor dem Draussen. Über gemischte Gefühle angesichts einer unwirtlichen Welt, in: Sessar, Klaus / Stangl, Wolfgang / Swaaningen, René (Hrsg.), Grossstadtängste. Untersuchungen zu Unsicherheitsgefühlen und Sicherheitspolitiken in europäischen Kommunen, Wien 2007, S. 128-154.

SHEARING, CLIFFORD D. / STENNING, PHILIP C., From the panopticon to Disney world. The development of discipline, in: Goold, Benjamin J. (Hrsg.), Surveillance, Band I, New York 2009, S. 45-58.

SHORT, EMMA / DITTON, JASON, Seen and now heard: Talking to the targets of open street CCTV, in: Norris, Clive / Wilson, Dean (Hrsg.), Surveillance, crime, and social control, Hampshire/Burlington 2006, S. 121-145.

SIEBER, ULRICH, Grenzen des Strafrechts, ZStW 2007, S. 1-68.

SIMON, DIRK, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Diss., Frankfurt am Main 2009.

SIMON, JONATHAN, Governing through crime. How the war on crime transformed American democracy and created a culture of fear, Oxford 2007.

SINGELNSTEIN, TOBIAS / STOLLE, PEER, Soziale Kontrolle in High Control Societies, Kriminologisches Journal 9/2007, S. 105-118, zitiert als: SINGELNSTEIN/STOLLE 2007.

SINGELNSTEIN, TOBIAS / STOLLE, PEER, Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., Wiesbaden 2012, zitiert als: SINGELNSTEIN/STOLLE 2012.

SINN, ARNDT, Moderne Verbrechensverfolgung – auf dem Weg zu einem Feindstrafrecht?, ZIS 2006, S. 107-117.

SIMON, JONATHAN, Public criminology? A cool read on a hot topic, Blog vom 15. August 2010, <http://governingthroughcrime.blogspot.ch/2010/08/public-criminology-cool-read-on-hot.html>.

SIMON, JONATHAN, Whose public safety? Trayvon Martin and neighborhood watch, Blog vom 24. März 2012, <http://governingthroughcrime.blogspot.ch/2012/03/trayvon-martins-death-sheds-light-on.html>.

SKILLICORN, DAVID B., Individual and collective analysis of anomalies in message traffic, in: Chen Hsinchun (Hrsg.), Terrorism informatics, New York 2008, S. 425-449, zitiert als: SKILLICORN 2008a.

SKILLICORN, DAVID B., Knowledge discovery for counterterrorism and law enforcement, Boca Raton 2008, zitiert als: SKILLICORN 2008b.

SLABY, JAN, Perspektiven einer kritischen Philosophie der Neurowissenschaften, Deutsche Zeitschrift für Philosophie 2011, S. 375-390.

SÖLLNER, SEBASTIAN, Die Verpolizeilichung. Grenzen, Chancen und Risiken einer neuen Sicherheitsarchitektur, Diss., Köln 2011.

SOLOVE, DANIEL J., „I've got nothing to hide" and other misunderstandings of privacy, San Diego Law Review 2007, S. 745-772, zitiert als: SOLOVE 2007.

SOLOVE, DANIEL J., Understanding privacy, Cambridge 2008, zitiert als: SOLOVE 2008.

SOÒS, ROBERTO / VÖGELI, CHRISTOPH, BWIS-Massnahmen gegen Gewalt an Sportveranstaltungen: Top oder Flop? – Das Rayonverbot und die Meldeauflage in der Praxis, Sicherheit & Recht 3/2008, S. 156-161.

SORELL, TOM, Moral Risks of Preventive Policing in Counter-Terrorism, DETECTER Deliverable 25, <http://www.detecter.bham.ac.uk/documents.html>.

SPINNER, HELMUT, Wo liegen die Grenzen von Kriminaltechnik und Kriminalistik – Statement Helmut Spinner, in: Bundeskriminalamt (Hrsg.), Aktuelle Methoden der Kriminaltechnik und Kriminalistik, Wiesbaden 1995, S. 260-273.

SPRANGER, TADE MATTHIAS (Hrsg.), International neurolaw, Berlin 2012, S. 269-287.

STALDER, FELIX, Opinion. Privacy is not the antidote to surveillance, Surveillance & Society 2002 1/1, S. 120-124.

STALLMACH, LENA, Normal oder gestört – wo verläuft die Grenze?, NZZ Online vom 16. April 2013, <http://www.nzz.ch/wissen/wissenschaft/normal-oder-gestoert--wo-verlaeuft-die-grenze-1.18065478>.

STAPEL, HENNING, Das Auge der Macht? Videoüberwachungskameras im öffentlichen Raum, Kriminologisches Journal 1/2009, S. 46-57.

STEGMANN, ANDREA, Organisierte Kriminalität. Feindstrafrechtliche Tendenzen in der Rechtsetzung zur Bekämpfung organisierter Kriminalität, Diss., Bern 2004, zitiert als: STEGMANN A.

STEGMANN, MARIO, Videoüberwachung des öffentlichen Raumes in bernischen Gemeinden – Ein Fallbeispiel, Sicherheit & Recht 2/2012, S. 76-86, zitiert als: STEGMANN M.

STEIER, HENNING, Rucksack oder Bombe?, NZZ Online vom 29. Oktober 2012, <http://www.nzz.ch/aktuell/digital/maschinen-ueberwachen-menschen-1.17731842>.

STEIER, HENNING, „Vorder- oder Hintertür?“, NZZ Online vom 7. Juni 2013, <http://www.nzz.ch/aktuell/digital/prism-1.18094882>.

STEIER, HENNING, Wie Microsoft der NSA geholfen haben soll, NZZ Online vom 12. Juli 2013, <http://www.nzz.ch/aktuell/digital/wie-microsoft-der-nsa-geholfen-haben-soll-1.18115433>.

STEIER, HENNING, Freunde von Freunden im Visier, NZZ Online vom 18. Juli 2013, <http://www.nzz.ch/aktuell/digital/nsa-freunde-von-freunden-im-visier-1.18118739>.

STEINBOCK, DANIEL J., Data Matching, Data Mining, and Due Process, Georgia Law Review 2005 40/1, S. 1-84.

STEWART, MITCHELL, Anger over mass web surveillance plans, PCPro vom 20. Februar 2012, <http://www.pcpro.co.uk/news/security/372985/anger-over-mass-web-surveillance-plans>.

STÖCKLI, CORINNE, „Einfach nur dreist", plädoyer 6/2011, S. 15-17.

STRASSER, PETER, Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen, 2. Aufl., Frankfurt/Main 2005.

STREBEL, DOMINIQUE, Prepaid-Handys: Registrierung nutzlos, NZZ am Sonntag vom 10. Oktober 2004, <http://www.augenauf.ch/bs/archiv/prepay/20041010.pdf>.

STRÖM, PÄR, Die Überwachungsmafia. Das gute Geschäft mit unseren Daten, München 2005.

STUDER, MARCEL, Mit Datenbanken gegen Hooliganismus, digma 2006, S. 66-69.

STUTZER, ALOIS / ZEHNDER, MICHAEL, Herausforderungen bei der Evaluation von Kameraüberwachung als Präventionsinstrument – eine ökonomische Perspektive, in: Schwarzenegger, Christian / Nägeli, Rolf (Hrsg.), 3. Zürcher Präventionsforum – Videoüberwachung als Prävention?, Zürich/Basel/Genf 2010, S. 109-132.

SULLIVAN, GAVIN / HAYES, BEN, Blacklisted. Targeted sanctions, preemptive security and fundamental rights, European Center for Constitutional and Human Rights, Dezember 2010, <http://www.ecchr.de/index.php/ecchr-publications/articles/blacklisted-targeted-sanctions-preemptive-security-and-fundamental-rights.html>.

SZVIRCSEV TRESCH, TIBOR/WENGER, ANDREAS, Sicherheit 2012, Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend, Center for Security Studies ETH Zürich, Zürich 2012, <http://www.css.ethz.ch/publications/Sicherheit>.

SZVIRCSEV TRESCH, TIBOR/WENGER, ANDREAS, Sicherheit 2013, Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend, Center

for Security Studies ETH Zürich, Zürich 2013, <http://www.css.ethz.ch/publications/Sicherheit>.

SZUBA, DOROTHEE, Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Diss., Baden-Baden 2011.

TANENBAUM, ANDREW S. / WETHERALL, DAVID J., Computernetzwerke, 5. Aufl., München 2012.

TATTERSALL, IAN, Evolution, genes, and behaviour, Zygon 2001 36/4, S. 657-666, <http://www.hss.caltech.edu/~steve/files/tattersall.pdf>.

TEMME, GABY, Die Polizeiliche Kriminalstatistik als Instrument der Inszenierung und disziplinierenden Überwachung, in: Zurawski, Nils (Hrsg.), Überwachungspraxen – Praktiken der Überwachung, Opladen 2011, S. 159-172.

TESCHNER, DENNIS, Die soziale Kontrolle im virtuellen Raum, Diss., Frankfurt am Main 2009.

THIEL, MARKUS, Die „Entgrenzung" der Gefahrenabwehr. Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, Habil., Tübingen 2011.

THIRIET, MAURICE, Gesperrt für jedes Amt, Spiel und Integrationsprogramm, Basler Zeitung Online vom 17. Juli 2010, <http://bazonline.ch/schweiz/standard/Gesperrt-fuer-jedes-Amt-Spiel-und-Integrationsprogramm-/story/15314937>.

THORMANN, OLIVIER / BRECHBÜHL, BEAT, Art. 246 StPO, in: Niggli, Marcel Alexander / Heer, Marianne / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Basel 2011.

THORNE, KRISTINA, „Terrorist" lists – A brief overview of lists and their sanctions in the US, UN, and Europe, Juni 2006, <http://www.hdcentre.org/fileadmin/user_upload/Resources/Publications/pdf/140%E2%80%9CTerroristlists%E2%80%93AbriefoverviewoflistsandtheirsanctionsintheUSUNandEurope.pdf>.

THÜR, HANSPETER, Die Privatsphäre im Zeitalter der digitalen Revolution, in: Kirchschläger Peter G./Thomas Kirchschläger (Hrsg.), Menschenrechte und Digitalisierung des Alltags, Bern 2010, S. 101-113.

TINNEFELD, MARIE-THERES / BUCHNER, BENEDIKT / PETRI, THOMAS, Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Aufl., München 2012.

TOLMEIN, OLIVER, Wissen ohne Macht, Gen-ethischer Informationsdienst 143 2000/2001, <http://www.menschenundrechte.de/cms2/documents-upload/pdf/1153160486.pdf>.

TONDORF, GÜNTER, Neue kriminaltechnische Entwicklungen – eine Herausforderung für den Strafverteidiger, StV 1/1993, S. 39-47.

TÖPFER, ERIC, Videoüberwachung als Kriminalprävention? Plädoyer für einen Blickwechsel, Kriminologisches Journal 4/2009, S. 272-282.

TROCHSLER-HUGENTOBLER, CARMEN / LOBSIGER, ADRIAN, Polizeiliche Befugnisse und Handlungsformen, in: Schweizer, Rainer J. (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Schweizerisches Bundesverwaltungsrecht Band III/1, Basel 2008, S. 279-336.

TROSCIANKO, TOM / HOLMES, ALISON / STILLMAN, JENNIFER / MIRMEHDI, MAJID / WRIGHT, DANIEL / WILSON, ANNA, What happens next? The predictability of natural behaviour viewed through CCTV cameras, Perception 2004 33/1, S. 87-101, zitiert als: TROSCIANKO ET AL.

TROTHA, TRUTZ VON, Vom Wandel des Gewaltmonopols oder der Aufstieg der präventiven Sicherheitsordnung, Kriminologisches Journal 3/2010, S. 218-234.

TRUNZ, MIRJAM / WOHLERS, WOLFGANG, Hooliganismus-Bekämpfung: Kann die Schweiz von England lernen?, CaS 2011, S. 176-202.

TSCHENTSCHER, AXEL, Das Grundrecht auf Computerschutz, AJP 2008, S. 383-393.

UECKER, PHILIP, Host-Provider, Content-Provider, Acces-Provider oder was? Zur rechtlichen Abgrenzung dieser Provider-Typen, DFN-Infobrief Recht Juni 2009, S. 5-6.

ULLRICH, PETER / LÊ, ANJA, Bilder der Überwachungskritik, Kriminologisches Journal 2/2011, S. 112-130.

UWER, THOMAS (Hrsg.), „Bitte bewahren Sie Ruhe“, Leben im Feindrechtsstaat, Berlin 2006.

VALERIUS, BRIAN, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, Hoheitliche Recherchen in einem grenzüberschreitenden Medium, Diss., Berlin 2004.

VAN DER HILST ROZEMARIJN, Human Right Risks of Selected Detection Technologies, Sample Uses by Governments of Selected Detection Technologies, DETECTER D17.1, <http://www.detecter.bham.ac.uk/documents.html>.

VERKAIK, ROBERT, Big Brother Database threatens to „break the back of freedom", The Independent Online vom 21. Oktober 2008 auf, <http://corruptus judicialsystem.org/bigbrotherthreat2-breakthebackoffreedom.pdf>.

VETTERLI, LUZIA, Kehrtwende in der bundesgerichtlichen Praxis zu den Verwertungsverboten, ZStrR 2012, S. 447-470.

VEST, HANS, Kommentar zu Art. 32 BV, in: Ehrenzeller, Bernhard / Mastronardi, Philippe / Schweizer, Rainer J. / Vallender, Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 1-93 BV, 2. Aufl., Zürich/St. Gallen 2008.

VOLKMANN, UWE, Polizeirecht als Sozialtechnologie, NVwZ 2009, S. 216-222.

VOREGGER, MICHAEL, Überwachung auf dem Vormarsch, Spiegel Online vom 23. September 2009, <http://www.spiegel.de/netzwelt/tech/0,1518,376153, 00.html>.

WAGNER, BEN, Deep Packet Inspection and Internet Censorship: International Convergence on an „Integrated Technology of Control", Juni 2009, <http:// advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/>.

WALDER, HANS / HANSJAKOB, THOMAS, Kriminalistisches Denken, 9. Aufl., Heidelberg 2012.

WEBER, ROLF H. / WOLF, CHRISTOPH A. / HEINRICH, ULRIKE I., Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung. Vorratsdatenspeicherung – Staatstrojaner – Geolokalisierungsdaten, Jusletter vom 12. März 2012.

WEBER-HASSEMER, KRISTIANE, Der „gläserne Mensch" in den Zeiten genetischer Forschung. Was bleibt noch übrig von Selbstbestimmung und Datenschutz?, in: Herzog, Felix / Neumann, Ulfrid (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg 2010, S. 1249-1261.

WEBSTER, WILLIAM, CCTV policy in the UK: reconsidering the evidence base, Surveillance & Society 2009 6/1, S. 10-22.

WEICHERT, THILO, Wie viel Sicherheit verträgt der Sport?, digma 2006, S. 70-75.

WEIGERT, MARTIN, Facebook Places: Das Wichtigste zu Facebooks Location-Dienst (startet heute in den USA), netzwertig.com vom 19. August 2010, <http://netzwertig.com/2010/08/19/facebook-places-facebooks-location-dienst-startet-heute-in-den-usa/>.

WEISSENBERGER, PHILIPPE, Kommentar zu Art. 143bis StGB, in: Niggli, Marcel Alexander / Wiprächtiger, Hans (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111-392 StGB, 3. Aufl., Basel 2013.

WELSH, BRANDON C. / FARRINGTON, DAVID P., Crime prevention effects of closed circuit television: a systematic review, Home Office Research Study 252, August 2002, <http://www.popcenter.org/Responses/video_surveillance/PDFs/Welsh&Farrington_2002.pdf>.

WEMANS, GUIDO, Prof. Dr. Christian Schwarzenegger: Ermittler tappen bei „Cybercrimes" oft im Dunkeln, asut-bulletin 2/2007, S. 28-33.

WERDER, GREGORI, Rechtsnatur und Charakter der Massnahmen des Hooligan-Konkordats, Sicherheit & Recht. 3/2012 3/2012, S. 249–252.

WESTIN, ALAN F., Social and Political Dimensions of Privacy, Journal of Social Issues 2003 59/2, S. 431-453.

WOHLERS, WOLFGANG, Kommentar zu Art. 139 und Art. 141 StPO, in: Donatsch, Andreas / Hansjakob, Thomas / Lieber, Viktor (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, Zürich/Basel/Genf 2010.

WOOD, DAVID MURAKAMI, A new „baroque arsenal"? Surveillance in a global recession, Surveillance & Society 2009 6/1, S. 1-2.

WOOD, DAVID MURAKAMI, Chicago: the future of US CCTV, Blog vom 21. Februar 2009, <http://ubisurv.wordpress.com/2009/02/21/chicago-the-future-of-us-cctv/>.

YOUNG, JOCK, Voodoo Criminology and the Numbers Game, 2004, <http://blogs.kent.ac.uk/culturalcriminology/files/2011/03/chap1-jock-young.pdf>, zitiert als: YOUNG 2004.

YOUNG, JOCK, The exclusive society. Social exclusion, crime and difference in late modernity, London 1999, zitiert als: YOUNG 1999.

ZEHNDER, CARL AUGUST, Informationssysteme und Datenbanken, 8. Aufl., Zürich 2005.

ZEHNDER, MICHAEL, Kameraüberwachung als Präventionsinstrument im öffentlichen urbanen Raum, Evaluation für den Bahnhofplatz der Stadt Luzern, Bericht zuhanden der Direktion Umwelt, Verkehr und Sicherheit der Stadt Luzern, Januar 2011, <http://www.luzernerzeitung.ch/storage/med/redaktion/226715_Videoueberwachung_Studie_171012.pdf>.

ZERBES, INGEBORG, Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation, Habil., Wien 2010.

ZGOBA, KRISTEN / WITT, PHILIP / DALLESSANDRO, MELISSA / VEYSEY, BONITA, Studie der Research & Evaluation Unit des Office of Policy and Planning des New Jersey Departement of Correction, Megan's Law: Assessing the Practical and Monetary Efficacy, Dezember 2008, <http://www.ncjrs.gov/pdffiles1/nij/grants/225370.pdf>.

ZIMMER, HEIKO, Zugriff auf Internetzugangsdaten. Unter besonderer Berücksichtigung der Verhältnismässigkeit einer verdachtsunabhängigen Vorratsdatenspeicherung, Diss., Frankfurt am Main 2012.

ZIMRING, FRANKLIN E., The city that became safe, New York's lessons for urban crime and its control, New York 2012.

ZITTRAIN, JONATHAN / EDELMAN, Benjamin, Empirical Analysis of internet filtering in China, 2003, <http://cyber.law.harvard.edu/filtering/china/>.

ZSCHOCH, DIANA, Die präventiv-polizeiliche Rasterfahndung. Im Spannungsverhältnis zwischen der Staatsaufgabe Sicherheit und dem informationellen Selbstbestimmungsrecht der betroffenen Nichtverantwortlichen, Diss., Frankfurt am Main 2007.

ZURAWSKI, NILS, Täter gefasst – Videoüberwachung als Erfolgsmodell?, heise Online vom 29. Dezember 2007, <http://www.heise.de/tp/artikel/26/26954/1.html>.

ZURAWSKI, NILS, Die praktischen Dimensionen von Überwachung, Kontrolle und Überprüfung, in: Zurawski, Nils (Hrsg.), Überwachungspraxen – Praktiken der Überwachung, Opladen 2011, S. 7-18.

Materialien

Abstimmungszeitung der Stadt Zürich vom 27. September 2009, <http://www.stadt-zuerich.ch/portal/de/index/politik_u_recht/abstimmungen_u_wahlen/vergangene_termine/090927/abstimmungszeitung_090927.html>.

Änderungen BWIS 2006: Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) (Gewaltpropaganda/Gewalt bei Sportveranstaltungen) Änderung vom 24. März 2006, AS 2006 3703 ff.

Bearbeitungsreglement HOOGAN des Bundesamts für Polizei fedpol vom Dezember 2009, <http://www.ejpd.admin.ch/content/dam/data/sicherheit/hooliganismus/bearbeitungsreglement-d.pdf>.

Begleitbericht EJPD 2001: Begleitbericht zum Vorentwurf für eine Schweizerische Strafprozessordnung, EJPD, Bern Juni 2001, <http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/strafprozess/vn-ber-1-d.pdf>.

Bericht BJ inter net: Neues Medium – neue Fragen ans Recht, Bericht einer interdepartementalen Arbeitsgruppe zu strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet, Bundesamt für Justiz, Bern 1996.

Bericht BKA Mindestspeicherfristen: Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu „Mindestspeicherfristen", Abschlussbericht, <http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html>.

Bericht Bundesrat i. S. Savary: Bericht des Bundesrates zur unerlaubten Werknutzung über das Internet in Erfüllung des Postulates 10.3263 Savary, EJPD, Bern 2011, <http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2011/2011-11-30/ber-br-d.pdf>.

Bericht der Arbeitsgruppe Genesis: Modell für eine effiziente Strafverfolgung bei kantonsübergreifenden und/oder internationalen Fällen von Netzwerkkriminalität, Vorschläge der von Bund und Kantonen eingesetzten Arbeitsgruppe zur Analyse der Operation „Genesis", fedpol, 12. November 2003, <http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2004/2004-12-10.html>.

Bericht EJPD 2003: Netzwerk-Kriminalität, Bericht der Expertenkommission „Netzwerkkriminalität“, EJPD, Bern Juni 2003, <http://www.ejpd.admin.ch/content/dam/data/kriminalitaet/gesetzgebung/netzwerkkriminalitaet/ber-netzwerkkrim-d.pdf>.

Bericht EJPD 2007: Bericht des EJPD vom September 2007, Videoüberwachung zu Sicherheitszwecken in Bahnhöfen, Flughäfen und an anderen öffentlichen Orten, <http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2007/pm_2007-09-28__bericht/070926_bericht_videoueberwachungpubld.pdf>.

Bericht GPDel: Datenbearbeitung im Staatsschutzinformationssystem ISIS, Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 21. Juni 2010, <http://www.admin.ch/opc/de/federal-gazette/2010/7665.pdf>.

Bericht INDECT D9.4, **Bericht INDECT D1.1** und **Bericht INDECT D0.5**: Berichte des Projekts „Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment“ (INDECT): Bericht Evaluation of Components, Deliverable 9.4 Work-Package 9 vom 31. Dezember 2009; Bericht D1.1 Report on the collection and analysis of user requirements vom 29. Oktober 2009; Bericht D0.5 INDECT – Ethical Issues – 2009 vom 17. August 2010; <http://www.indect-project.eu/files/deliverables/public>.

Bericht KKJPD: Änderungen des Konkordats vom 15. November 2007 über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen, Bericht der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren vom 2. Februar 2012, <http://www.kkjpd.ch/frameset.asp?sprache=d>.

Bericht Maher Arar: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the events relating to Maher Arar, Factual Background, Volume I, Ottawa 2006, <http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf>.

Bericht PolAG: Vorentwurf zum Bundesgesetz über die polizeilichen Aufgaben des Bundes: Bericht über das Ergebnis des Vernehmlassungsverfahrens, Bundesamt für Polizei, Oktober 2010, <http://www.admin.ch/ch/d/gg/pc/documents/1787/Vernehmlassungsbericht_PolAG_de.pdf>.

Bericht RK-NR vom 29. April 2010: Bericht der Kommission für Rechtsfragen Nationalrat vom 29. April 2010, <http://www.parlament.ch/afs/data/D/bericht/2009/d_bericht_n_k12_0_20090423_0_20100429.htm>.

Bericht S/2008/324: Report of the Analytical Support and Sanctions Monitoring Team pursuant to resolution 1735 (2006) concerning Al-Qaida and the Taliban and associated individuals and entities, Dokument S/2008/324 vom 14. Mai 2008, <http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terrorism%20S%202008%20324.pdf>.

Bericht S/2012/305: Report of the Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Quaida and associated individuals and entities, Dokument S/2012/305 vom 8. Mai 2012, <http://www.un.org/sc/committees/1267/annualreports.shtml>.

Bericht S/2012/968: Thirteenth report of the Analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to resolution 1989 (2011) concerning Al-Quaida and associated individuals and entities, Dokument S/2012/968 vom 31. Dezember 2012, <https://www.un.org/sc/committees/1267/monitoringteam.shtml>.

Bericht SIPOL: Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz vom 23. Juni 2010 (Sicherheitspolitischer Bericht), <http://www.sipol09.ethz.ch/>.

Bericht Vorentwurf NDG: Bericht vom 8. März 2013 zum Vorentwurf des Nachrichtendienstgesetzes (NDG), <http://www.news.admin.ch/NSBSubscriber/message/attachments/29932.pdf>.

Bericht WSIPP Nr. 05-12-1202, **Bericht WSIPP 05-12-1203** und **Bericht WSIPP 06-01-1204**: Berichte Nr. 05-12- 1202, Nr. 05-12-1203 und Nr. 01-01-1204 des Washington State Institute for Public Policy (WSIPP) zur Bestrafung von Sexualstraftätern im Bundesstaat Washington, <http://www.wsipp.wa.gov/series.asp?seriesid=1>.

Botschaft BÜPF 2013: Botschaft vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), BBl 2013 2683 ff.

Botschaft BWIS 1994: Botschaft vom 7. März 1994 zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative „S. O. S. Schweiz ohne Schnüffelpolizei“, BBl 1994 II 1127 ff.

Botschaft BWIS 2005: Botschaft vom 17. August 2005 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Massnahmen gegen Gewaltpropaganda und gegen Gewalt anlässlich von Sportveranstaltungen), BBl 2005 5613 ff.

Botschaft BWIS II 2007a: Botschaft vom 15. Juni 2007 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) (Besondere Mittel der Informationsbeschaffung), BBl 2007 5037.

Botschaft BWIS II 2007b: Botschaft vom 29. August 2007 zu einer Verfassungsbestimmung über die Bekämpfung von Gewalttätigkeiten anlässlich von Sportveranstaltungen (Hooliganismus) sowie zu einer Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), BBl 2007 6465.

Botschaft StPO: Botschaft vom 21. Dezember 2005 zur Vereinheitlichung des Strafprozessrechts, BBl 2006 1085.

Committee Guidelines: Security Council Committee pursuant to Resolutions 1267 (1999) and 1989 (2011) concerning Al-Quida and associated individuals and entities, Guidelines of the Committee for the Conduct of its Work vom 15. April 2013, <http://www.un.org/sc/committees/1267/pdf/1267_guidelines.pdf>.

Drucksache 17/9003 vom 16. März 2012: Deutscher Bundestag, 17. Wahlperiode, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Katrin Kunert, Agnes Alpers, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 17/9003 vom 16. März 2012, <http://dipbt.bundestag.de/dip21/btd/17/090/1709003.pdf>.

Entschluss des Europäischen Parlaments zur Evaluierung der EU-Sanktionen (2009/C 925 E/49): Evaluierung der EU-Sanktionen als Teil der Aktionen und Massnahmen der EU im Bereich der Menschenrechte, Amtsblatt der Europäischen Union 2009/C 295 E/49 vom 4. Dezember 2009.

Entwurf BWIS 2007: Entwurf vom 15. Juni 2007 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Besondere Mittel der Informationsbeschaffung), BBl 2007 5139 ff.

Entwurf der Änderungen der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs, <http://www.ejpd.admin.ch/content/dam/data/sicherheit/uepf/vorentw-gebv-uepf-d.pdf>.

Erläuternder Bericht BÜPF: Erläuternder Bericht zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), <http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-d.pdf>.

Erläuternder Bericht zum Vorentwurf BWIS II: Erläuternder Bericht vom 31. Januar 2006 zum Vorentwurf des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), fedpol, <http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/innere_sicherheit/entwuerfe__erlaeuterungen.html>.

Erläuterungen EJPD vom 8. Juni 2011: Erläuterungen zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11) sowie Änderung der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1), <http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2011/2011-06-08/110608_ber-de.pdf>.

Evaluationsbericht der Europäischen Kommission: Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brüssel, Dokument COM (2011) 225 final vom 18. April 2011, <http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf>.

Kommissionsbericht Aussenpolitische Kommission des Nationalrates vom 1. März 2010, 09.3719, <http://parlament.ch/d/suche/seiten/resultate.aspx?afspath=bericht&collection=CV&from=76&gvk_urh_key=KOM_4_&mask=sucuria-vista&query=&sort=GN&titel=&way=asc>.

Korruptionsregister-Gesetz: Gesetzesentwurf zur Einrichtung eines Registers über unzuverlässige Unternehmen (Korruptionsregister-Gesetz) vom 25. Juni 2008 (Drucksache 16/9780), <http://dipbt.bundestag.de/dip21/btd/16/097/1609780.pdf>.

Länderbericht KKJPD: Länderbericht vom 19. August 2009, Arbeitsreise der KKJPD vom 6. bis 8. August 2009 nach England, Holland, Belgien und Deutschland, <http://www.kkjpd.ch/images/upload/190818%20Reisebericht%20d.pdf>.

Medienmitteilung EJPD vom 30. März 2011: „Bundesgesetz über die polizeilichen Aufgaben des Bundes“: Weiteres Vorgehen, Medienmitteilung EJPD vom 30. März 2011, <http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-03-30.html>.

Medienmitteilung fedpol vom 25. Juli 2003: Ein Jahr nach der Operation Genesis. Bedingte Gefängnisstrafen und Bussen, Medienmitteilung fedpol vom

25. Juli 2003, <http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2003/ref_2003-07-25.html>.

Medienmitteilung fedpol vom 31. Januar 2013: Aktuelle Zahlen aus dem Informationssystem HOOGAN, Medienmitteilung fedpol vom 31. Januar 2013, <http://www.fedpol.admin.ch/content/fedpol/de/home/dokumentation/medieninformationen/2013/2013-01-31.html>.

Motion Andrea Martina Geissbühler vom 2. Dezember 2010: Motion „Zugriff seitens der Polizei auf die ISA-Datenbank" (10.3917) vom 2. Dezember 2010 eingereicht von Nationalrätin Andrea Martina Geissbühler, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20103917>.

Motion Dick Marty vom 12. Juni 2009: Motion „Die Uno untergräbt das Fundament unserer Rechtsordnung" (09.3719) vom 12. Juni 2009 eingereicht von Ständerat Dick Marty, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20093719>.

Motion Natalie Simone Rickli vom 5. März 2008: Motion „Schaffung eines nationalen Registers für vorbestrafte Pädophile" (08.3033) vom 5. März 2008, eingereicht von Nationalrätin Natalie Simone Rickli, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20083033>.

Motion Natalie Simone Rickli vom 20. März 2013: Motion „Einführung eines Registers für Sexual- und Gewaltstraftäter" (13.3127) vom 20. März 2013, eingereicht von Nationalrätin Natalie Simone Rickli, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133127>.

Motion Rolf Schweiger vom 24. März 2006: Motion „Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf den elektronischen Netzwerken" (06.3170) vom 24. März 2006, eingereicht von Nationalrat Rolf Schweiger, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20063170>.

Parlamentarische Initiative Natalie Simone Rickli vom 20. März 2009: Parlamentarische Initiative „Register für Pädophile, Sexual- und schwere Gewaltstraftäter" (09.423) vom 20. März 2009 eingereicht von Nationalrätin Natalie Simone Rickli, <http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20090423>.

Plenarprotokoll des Deutschen Bundestags 16/212 vom 20. März 2009, <http://dip21.bundestag.de/dip21/btp/16/16212.pdf>.

Plenarprotokoll 17/132 des Deutschen Bundestags vom 19. Oktober 2011, <http://dip21.bundestag.de/dip21/btp/17/17132.pdf>.

Postulat der Sicherheitspolitischen Kommission des Ständerats vom 21. Februar 2005: Postulat „Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen" (05.3006) vom 21. Februar 2005 eingereicht von der Sicherheitspolitischen Kommission des Ständerats, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20053006>.

Postulat Peter Malama vom 3. März 2010: Postulat „Innere Sicherheit. Klärung der Kompetenzen" vom 3. März 2010 (10.3045) eingereicht von Nationalrat Peter Malama, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20103045>.

Stellungnahme des Bundesrats i. S. Bericht GPDel: Datenbearbeitung im Staatsschutzinformationssystem ISIS, Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 21. Juni 2010, Stellungnahme des Bundesrates vom 20. Oktober 2010, <http://www.admin.ch/opc/de/federal-gazette/2010/7739.pdf>.

Stellungnahme des Bundesrats vom 7. Dezember 2001 i. S. Theophil Pfister: Stellungnahme des Bundesrats vom 7. Dezember 2001 zur einfachen Anfrage „Terroranschläge. Rasterfahndung" (01.1114) vom 5. Oktober 2001 eingereicht von Nationalrat Theophil Pfister, <http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20011114>.

Stellungnahme des Bundesrats vom 13. Februar 2008 i. S. Daniel Vischer: Antwort des Bundesrats vom 13. Februar 2008 zur Motion „Boykott der Uno-Terrorliste" (07.3872) vom 21. Dezember 2007 eingereicht von Nationalrat Daniel Vischer, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20073872>.

Stellungnahme des Bundesrats vom 7. Mai 2008 i. S. Natalie Simone Rickli: Stellungnahme des Bundesrats vom 7. Mai 2008 zur Motion „Schaffung eines nationalen Registers für vorbestrafte Pädophile" (08.3033) vom 5. März 2008 eingereicht von Nationalrätin Natalie Simone Rickli, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20083033>.

Stellungnahme des Bundesrats vom 25. Februar 2009 i. S. Margret Kiener Nellen: Stellungnahme des Bundesrats vom 25. Februar 2009 zur Interpellation „Umsetzung der Empfehlungen aus dem Bericht über Videoüberwachung" vom 19. Dezember 2008 eingereicht von Nationalrätin Margret Kie-

ner Nellen, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20083940>.

Stellungnahme des Bundesrats vom 23. Februar 2011 i. S. Andrea Martina Geissbühler: Stellungnahme des Bundesrats vom 23. Februar 2011 zur Motion „Zugriff seitens der Polizei auf die ISA-Datenbank" (10.3917) vom 2. Dezember 2010 eingereicht von Nationalrätin Andrea Martina Geissbühler, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20103917>.

Stellungnahme des Bundesrats vom 15. Mai 2013 i. S. Natalie Simone Ricklli: Stellungnahme des Bundesrats vom 15. Mai 2013 zur Motion „Einführung eines Registers für Sexual- und Gewaltstraftäter" (13.3127) vom 20. März 2013 eingereicht von Nationalrätin Natalie Simone Rickli, <http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133127>.

Venice Commission 2007: European Commission for Democracy through Law (Venice Commission), Opinion on video surveillance in public places by public authorities and the protection of human rights, Dokument CDL-AD(2007)041 vom 23. März 2007, <http://www.statewatch.org/news/2007/aug/venice-commission-video-surveillance.pdf>.

Versionsvergleich Hooligan-Konkordat KKJPD: Versionsvergleich Hooligankonkordat KKJPD, <http://www.kkjpd.ch/frameset.asp?sprache=d>.

Vorentwurf des Polizeiaufgabengesetzes: Vorentwurf vom November 2009 des Bundesgesetzes über die polizeilichen Aufgaben des Bundes (Polizeiaufgabengesetz, PolAG), <http://www.admin.ch/ch/d/gg/pc/documents/1787/Vorlage_k.pdf>.

Vorentwurf NDG: Vorentwurf Nachrichtendienstgesetz (NDG) vom 8. März 2013, <http://www.news.admin.ch/NSBSubscriber/message/attachments/29931.pdf>.

Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens BÜPF: Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), Bern Mai 2011, <http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ve-ber-d.pdf>.

Zusatzbotschaft BWIS II 2010: Zusatzbotschaft vom 27. Oktober 2010 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit («BWIS II reduziert»), BBl 2010 7841 ff.

Veio Zanolini

Wiedergutmachung durch Mediation

Eine Untersuchung über praktische Erfahrungen in Strafsachen

Schweizerische kriminologische Untersuchungen. Band 17
2014. 533 Seiten, 92 Abbildungen, 69 Tabellen, kartoniert
ISBN 978-3-258-07833-5

Die aussergerichtliche Konfliktbeilegung stellt einen Bestandteil der Schweizer Tradition dar. Im Strafrecht sorgte das Thema der Mediation allerdings für starke Polarisierung und die Einführung einer gesetzlichen Grundlage gelang nur im Jugendstrafrecht. Soll die Mediation der Ergänzung der strafrechtlichen Reaktion dienen, so wäre das Mediationsverfahren gemäss den Erkenntnissen der vorliegenden Studie möglichst nach den Verfahrensprinzipien der Restorative Justice zu gestalten. Die Orientierung an dieser Gerechtigkeitstheorie würde die Mediation von «neuen» Wegen integrierenden Sanktionierens und rein verfahrensökonomischen Überlegungen abgrenzen, zugleich wichtige (prozessuale) Grundwerte ins Zentrum stellen. Als integrativer Prozess könnte die Mediation unter Umständen den Bedürfnissen von Täter, Opfer und Gesellschaft gerecht werden und gleichzeitig einen sinnvollen Beitrag im Rahmen des strafrechtlichen Wiedergutmachungsgedankens leisten.

Haupt **Haupt Verlag**
verlag@haupt.ch · www.haupt.ch