Datenschutz in Spezialgrundrechten

Lothar Gamper

Universität Innsbruck
Institut für Europarecht und Völkerrecht
Innrain 52, 6020 Innsbruck
csab2457@uibk.ac.at

Schlagworte: Datenschutz, EMRK, Privatsphäre, Grundrechte
Abstract: Sowohl Geheimdienste als auch Strafverfolgungsbehörden verfügen heute über neue Befugnisse und Möglichkeiten, die ihnen erst durch moderne Technik oder legislativ auf Grund des Anti-Terror-Kampfes seit 2001 zugänglich wurden. Sofern es sich dabei um Eingriffe in die Privatsphäre handelt, bietet sich häufig nicht nur eine ausschließliche Bewertung anhand von Datenschutzprinzipien an. Es können auch andere Grundrechte berührt sein, die im Einzelfall als „*lex specialis*" im Verhältnis zum Recht auf Privatsphäre dem Betroffenen weitergehende Rechte einräumen, auf die er sich berufen kann. Einige gelten im Strafrecht absolut und stellen daher unüberwindliche Hürden für Ermittler auf.

1. These

Schwere Eingriffe in die Privatsphäre berühren nicht nur den Datenschutz im engeren Sinn, sondern auch andere Grundrechte und geraten vor allem im strafrechtlichen Bereich aus meiner Sicht mittlerweile häufig an Grenzen, die nicht überschritten werden dürften.[1] Da es sich teilweise um völlig neue Möglichkeiten für Sicherheitsbehörden handelt, die es in dieser Form aus technischen Gründen bisher nicht gab oder die gesetzlich erstmals seit dem Zweiten Weltkrieg wieder eingeräumt wurden, fehlen (noch) höchstrichterliche Urteile. Eine Grenzziehung wird aber gerade bei den absoluten Grundrechten in den nächsten Jahren wohl unumgänglich sein und ist m. E. auch höchst wünschenswert.

1 Siehe zum Thema auch *Gamper, Lothar*, EMRK und Datenschutz am Beispiel der Übermittlung von Passagierdaten im Flugverkehr an Zollbehörden unter Berücksichtigung europarechtlicher Aspekte, Innsbruck 2007, unveröff. Diplomarbeit, S. 69 f.

2. Die Europäische Menschenrechtskonvention als europäischer Mindeststandard

Die Garantie und Reichweite dieser Grundrechte in den Verfassungen bzw. in der Rechtsprechung der europäischen Staaten deckt sich nicht völlig, weshalb sich eine Betrachtung der Europäischen Konvention für Menschenrechte (EMRK) anbietet, die für alle Mitgliedsstaaten des Europarates einen Mindeststandard setzt und auch vom Europäischen Gerichtshof bereits seit 1974 mit dem *Nold*-Urteil bzw. seit 1975 mit dem Urteil *Rutili* beachtet wird.[2]

Bei den im Folgenden genannten Konventionsbestimmungen ergeben sich Überschneidungen mit dem Recht auf Achtung der Privatsphäre aus Art. 8 EMRK, zu dem der Europäische Gerichtshof für Menschenrechte (EGMR) – insbesondere seit dem Jahr 2000 mit den Urteilen *Amann*[3] und *Rotaru*[4] – eine umfangreiche Rechtsprechung zum Datenschutz entwickelt hat. Nicht vergessen werden darf dabei, dass dort, wo der Schutzbereich dieser Grundrechte endet, der stärker beschränkte Art. 8 EMRK seine Wirksamkeit entfaltet.

2.1 Art. 9, 10, 11 EMRK

Datenverarbeitung durch Sicherheitsbehörden oder die Überwachung öffentlicher Räume kann, im Einzelfall selbst durch die reine Erfassung ohne darauf folgende Aufzeichnung von Daten oder Bildmaterial, die in den Art. 9, 10 und 11 EMRK geschützte Gedanken-, Gewissens- und Religionsfreiheit, das Recht auf freie Meinungsäußerung und die Versammlungs- und Vereinigungsfreiheit berühren. Ein Eingriff liegt dann vor, wenn die (auch nur befürchtete) Beobachtung und eventuell daran anschließende Datensammlung und -verwertung das Verhalten der Grundrechtsträger in der Ausübung ihrer Rechte beeinflussen oder sie zu einem Verzicht bewegen kann.[5]

---

2 *Alber, Siegbert / Widmaier, Ulrich*, Die EU-Charta der Grundrechte und ihre Auswirkungen auf die Rechtsprechung: zu den Beziehungen zwischen EuGH und EGMR, in: EuGRZ 2000, S. 503, und *Zuleeg, Manfred*, Das Verhältnis nationaler und europäischer Grundrechte: Funktionen einer EU-Charta der Grundrechte, in: EuGRZ, 2000, S. 514.

3 *Amann gg. die Schweiz*, Rs. Nr. 27798/95, Urteil der Großen Kammer vom 16. 2. 2000.

4 *Rotaru gg. Rumänien*, Rs. Nr. 28341/95, Urteil der Großen Kammer vom 4. 5. 2000.

5 *Pohl, Joachim*, Videoüberwachung im öffentlichen Raum, KJ 2003, S. 317 ff.

Vorstellbar sind eine ganze Reihe von Situationen. Polizeikräfte und Sicherheitsbehörden dürfen etwa nicht uneingeschränkt Demonstrationen oder öffentliche Versammlungen mit Kameras überwachen oder gar Daten aufnehmen. Sobald das Gebaren der Sicherheitskräfte eine Intensität erreicht, die Menschen von der Teilnahme an einer Demonstration abhält oder bei erlaubten Handlungen beeinträchtigt, werden Grundrechte meist unzulässig eingeschränkt. Dasselbe gilt aber auch für die Beobachtung eines Parteigebäudes, einer Kirche, Synagoge oder einer Moschee. Im Zusammenhang mit Art. 10 EMRK sind auch die Pressefreiheit und der Informantenschutz als Voraussetzungen für unabhängige und kritische Berichterstattung zu nennen, die jedoch vor allem durch verfahrensrechtliche Sicherungen garantiert werden müssen.[6]

Was die Rechtsprechung des EGMR angeht, so war dieser bisher – allerdings nur mit Blick auf Art. 8 EMRK – bei der Bewertung der Videoüberwachung im öffentlichen Raum eher zurückhaltend und setzte diese mit der Beobachtung durch eine zufällig anwesende Person gleich.[7] Ob diese Spruchpraxis auch in Zukunft noch haltbar ist, kann angesichts der Ausmaße, die die Videoüberwachung heute in Großbritannien und zunehmend auch in anderen europäischen Ländern erreicht, angezweifelt werden. Durch die Verbindung von Video- mit Audiodaten werden die Eingriffsmöglichkeiten noch einmal erweitert. Die englische Stadt Middlesbrough verband die Kameras in einem Pilotversuch 2006 sogar mit Lautsprechern, durch die Jugendliche beispielsweise ermahnt werden, Straßen nicht zu verschmutzen. Mit derlei Maßnahmen vollzieht sich aus meiner Sicht ein schleichender Übergang vom demokratischen Staat zum Polizeistaat. Der Wunsch nach Unterdrückung unerwünschten sozialen Verhaltens mag aus Sicht mancher Bürger gerechtfertigt sein, geht in pluralistischen Demokratien aber zu weit.[8]

---

6 *Gola, Peter / Klug, Christoph / Reif, Yvette*, Datenschutz und presserechtliche Bewertung der „Vorratsdatenspeicherung", NJW 36/2007, S. 2.600.

7 *Herbecq und Anderer gg. Belgien*, Rs. Nr. 32200/96 und 32001/96, Entscheidung der Europäischen Kommission für Menschenrechte (EKMR) vom 14. 1. 1998; *Perry gg. Großbritannien*, Rs. Nr. 63737/00, Urteil vom 17. 7. 2003. Die Veröffentlichung solcher Aufzeichnungen wird jedoch strenger bewertet und kann eine Verletzung des Art. 8 EMRK darstellen: *Peck gg. Großbritannien*, Rs. Nr. 44647/98, Urteil vom 28. 1. 2003.

8 Richtungweisend ist hier das Urteil des Bundesverfassungsgerichts vom 11. März 2008 (BVerfG, 1 BvR 2074/05), das Gesetze der deutschen Bundesländer Hessen und Schleswig-Holstein zur automatisierten Erfassung von KFZ-Kennzeichen für nichtig erklärt und die Zulassung von derlei Überwachungsmaßnahmen selbst zwecks Abgleichung der Kennzeichen mit Fahndungslisten unter strenge Auflagen stellt.

Bahnbrechend war der EGMR mit der Feststellung einer Verletzung der Artikel 10 und 11 EMRK durch „bloße" Datenspeicherung im Urteil *Segerstedt-Wiberg u. a. gg. Schweden*, Rs. Nr. 62332/00, vom 6. 6. 2006. Im Urteil wurde die Sammlung von Daten allein aus Gründen politischer Betätigung der Betroffenen als Verstoß gegen die Freiheit der Meinungsäußerung und die Versammlungsfreiheit gewertet, auch wenn die Erkenntnisse vom erhebenden Geheimdienst nicht für weitere Vorgänge benutzt worden waren und die Beschwerdeführer keine tatsächliche Behinderung der Ausübung ihrer Rechte beklagten. In § 107 des Urteils stellte der Gerichtshof darüber hinaus fest, dass eine Speicherung von Daten zu politischen Überzeugungen, Tätigkeiten und Parteizugehörigkeit, die nicht nach Art. 8 Abs. 2 EMRK gerechtfertigt werden kann, ipso facto auch eine Verletzung der politischen Rechte aus Art. 10 und 11 der Konvention bedeutet.

2.2 Artikel 5, 6 EMRK

Art. 5 (Recht auf Freiheit und Sicherheit) und Art. 6 (Recht auf ein faires Verfahren) der EMRK gewährleisten eine Reihe von Verfahrensgarantien sowohl im Zivil- als auch im Strafrecht. Diese wurden, soweit nicht explizit im Text der Konvention verankert, in erheblichem Ausmaß vom EGMR durch seine Rechtsprechung und Interpretation dieser beiden Konventionsbestimmungen entwickelt.

2.2.1 Akteneinsicht

Lange bevor der EGMR Akteneinsicht zum Schutz der Privatsphäre aus Art. 8 EMRK gewährte, galt dies beschränkt auf Gerichtsverfahren bereits auf Grund der Art. 5 Abs. 4 sowie Art. 6 Abs. 1 EMRK und führte etwa zum Strafrechtsänderungsgesetz von 1971 in Österreich.[9] Auch heute noch ist die leicht unterschiedliche Schutzrichtung dieser Konventionsbestimmungen und des Art. 8 EMRK im Einzelfall nicht völlig bedeutungslos,[10] tritt aber immer weiter in den Hintergrund.

---

9 *Rech, Elisabeth*, Auswirkungen von EGMR-Urteilen zu Art. 6 EMRK auf das österreichische Strafprozessrecht, in DACH Europäische Anwaltsvereinigung, Das faire Verfahren nach Art. 6 EMRK, 28. Tagung der Dach in Bregenz 2003 (2005), S. 83 ff.

10 *Gamper, L.* (FN 1), S. 42, sowie exemplarisch das Urteil der Großen Kammer des EGMR vom 19. 10. 2005 in der Rs. Nr. 32555/96, *Roche gg. Großbritannien.*

2.2.2 Schutz vor Selbstbelastung und Unschuldsvermutung

Der ebenso aus Art. 6 Abs. 1 abgeleitete Schutz vor Selbstbelastung umfasst das Schweigerecht und das Verbot des Zwanges zur Selbstbezichtigung, das wegen des Grundsatzes „nemo tenetur se ipsum accusare" verkürzt auch als „nemo-tenetur-Prinzip" bezeichnet wird und letztlich die Informationsgewinnung betrifft. Im Verwaltungsverfahren ist dieses Grundrecht zwar nicht unverletzlich, doch im Strafrecht gilt es absolut und darf auch nicht zur Aufklärung schwerster Straftaten eingeschränkt werden. Diese rigide Bestimmung gilt vor dem Hintergrund, dass damit vor allem das Folterverbot abgesichert werden soll.[11] Die Absolutheit des Prinzips verlangt aber auch eine genaue Definition und Eingrenzung seiner Reichweite. Während ein Verdächtiger nicht zur Aussage oder zur Herausgabe von Beweisen oder ganz allgemein zu aktivem Verhalten gezwungen werden darf, muss er erdulden, dass zufällig noch vorhandene Spuren eines Verbrechens ausgewertet werden oder ein Abgleich von Blut- und DNA-Proben mit freiwillig am Tatort hinterlassenen Spuren erfolgt.

Was den Datenschutz betrifft, bedeutet dies, dass niemand zur Herausgabe von Unterlagen gezwungen werden darf, etwa durch die Verhängung einer Verwaltungsstrafe, während ein Verdächtiger eine Hausdurchsuchung zulassen muss, die innerhalb des von Art. 8 Abs. 2 EMRK erlaubten Rahmens erfolgt (Urteil *Funke gg. Frankreich*, Rs. Nr. 10828/84, vom 25. 2. 1993).

Das nemo-tenetur-Prinzip verlangt meines Erachtens aber auch, Daten, deren Herausgabe nicht zu Strafverfolgungszwecken von öffentlichen Behörden erzwungen wird, mit einem strafrechtlichen Verwertungsverbot zu belegen. Das diesbezügliche Leiturteil des EGMR ist *Saunders gg. Großbritannien*, Rs. Nr. 19187/91, vom 17. 12. 1996. Ein typisches Beispiel der Zwangserhebung ist die Datenbank EURODAC mit Fingerabdrücken von Asylwerbern zur Verhinderung von Mehrfachansuchen in verschiedenen EU-Ländern, bei der der Zugriff zur Strafverfolgung aus den erwähnten Überlegungen bisher ausgeschlossen ist, manche Politiker jedoch schon Begehrlichkeiten angemeldet haben. Doch auch die Daten in Reisepässen und Personalausweisen, die der Identifikation ihres Trägers und der legalen Aus- und Einreise dienen, müssten konsequenterweise von einer strafrechtlichen Nutzung ausgeschlossen sein, was auch für die enthaltenen biome-

11 *Müller, Rudolf*, Neue Ermittlungsmethoden und das Verbot des Zwanges zur Selbstbelastung, EuGRZ 2002, S. 553 f. Besonders deutlich wird diese Funktion im EGMR-Urteil der Großen Kammer *Jalloh gg. Deutschland*, Rs. Nr. 54810/00, vom 11. 7. 2006.

trischen Merkmale gelten muss. Dazu liegt bisher nur relativ lange zurückliegende Rechtsprechung des EGMR vor, die keinen Verstoß gegen Art. 8 EMRK sah – mit der Frage einer möglichen Verletzung des nemo-tenetur-Prinzips war der Gerichtshof meines Wissens noch nicht befasst, und auch die sehr zurückhaltende Rechtsprechung im Fall *Lupker u. a. gg. die Niederlande*[12] würde heute wohl revidiert.

Bedeutsam ist das nemo-tenetur-Prinzip aus meiner Sicht weiters bei der Vorratsdatenspeicherung. Zweifellos ist die gesetzlich erzwungene Aufbewahrung von Verbindungsdaten bei privatrechtlichen Telekommunikationsunternehmen der öffentlichen Gewalt zuzurechnen[13] – ob diese Daten daher von Strafverfolgungsbehörden überhaupt verwendet werden dürften und nicht eine Einschränkung auf die bei den Telekommunikationsdienstleistern noch zu Abrechnungszwecken vorhandenen Daten vorzunehmen wäre, müsste gerichtlich dringend überprüft werden. Es wäre bei den zunehmenden Mengen an digital übertragenen Daten sonst allzu verführerisch, die Speicherung jeglichen Alltagsvorgangs bei Dritten gesetzlich anzuordnen und das Verbot des Zwanges zur Selbstbelastung auf diese Weise sehr einfach zu umgehen. Es stehen, beispielsweise mit dem „Quick Freeze"-Verfahren, das die vorläufige Speicherung nach einem Anfangsverdacht bis zu einer richterlichen Entscheidung über die Datenfreigabe vorsieht, auch fast gleichwertige und wesentlich gelindere Mittel zur Verfügung.[14]

Nicht in unmittelbarem Zusammenhang mit dem nemo-tenetur-Prinzip stehend, aber eng damit verwandt ist die Unschuldsvermutung. Auch diese erlangt in den aufgezählten Fällen Bedeutung, denn in den demokratisch-rechtsstaatlichen Grundordnungen moderner Prägung, die sich bewusst vom Polizeistaat abheben wollen, erfüllt das Strafrecht primär eine *reaktive* und keine *präventive* Funktion. Nach dem Zweiten Weltkrieg sollten die autoritären Strukturen der Vergangenheit ganz bewusst überwunden und Systeme mit einem grundsätzlichen Vertrauen in die Loyalität und Gesetzestreue der Bürger geschaffen werden, die im Kontrast zu den vorherigen staatlichen Bespitzelungs- und Überwachungsstrukturen stehen sollten. Unter diesem Aspekt stellt also nicht nur jegliche Sammlung von Daten auf Vorrat ohne jeglichen Anfangsverdacht einer Straftat durch Sicherheitskräfte einen möglichen Verstoß gegen die Unschuldsvermutung dar. Auch

12 Rs. Nr. 18395/91, Entscheidung der Europäischen Kommission für Menschenrechte (EKMR) vom 7. 12. 1992.

13 Siehe FN 6, S. 2599.

14 Siehe FN 6.

bei zunächst erlaubter Datenerhebung kann die daran anschließende Datenverwertung und Aufbewahrung unzulässig sein. Beispielsweise dürften DNA-Profile Unschuldiger in der Regel nicht zur präventiven Verbrechensbekämpfung dauerhaft gespeichert werden, nur in engen Grenzen könnten derartige Vorgänge im Einzelfall gerechtfertigt sein[15].

Die Frage, ob die verdachtsunabhängige, massenhafte und unbegrenzte Informationsgewinnung von verschiedensten Daten durch Nachrichtendienste einer Verletzung des nemo-tenetur-Prinzips gleichzusetzen ist, muss verneint werden, wenn kein Zwang vorliegt. Europäische Höchstgerichte übersehen nicht die Schwierigkeiten, vor die Sicherheitsorgane bei zu restriktivem Einsatz von modernen Technologien bei der Kriminalitätsbekämpfung gestellt wären. Zu bewerten ist bei derlei Maßnahmen allerdings die Verhältnismäßigkeit nach strengen Kriterien.[16] In diesem Zusammenhang muss außerdem bemängelt werden, dass seit Jahren eine Vermischung der Aufgaben von Nachrichtendiensten – zu denen die Abwehr von Bedrohungen für die demokratische Ordnung und staatliche Organe zählt – und von Strafverfolgungsbehörden zu beobachten ist. Da Erstere aus gutem Grund stärker in Grundrechte eingreifen dürfen als Letztere, müssten auch die Erkenntnisse von Geheimdiensten im Regelfall (mit der Ausnahme einiger weniger streng definierter Straftaten) mit einem strafrechtlichen Verwertungsverbot belegt werden.

2.3 Artikel 13 EMRK

Das Recht auf eine wirksame Beschwerde gegen Konventionsverstöße vor staatlichen Behörden und Gerichten verlangt, dass dem Bürger Möglichkeiten geboten werden, seine Konventionsrechte zu verteidigen. So stellte die EKMR in der Entscheidung *Friedl gg. Österreich* in der Rs. Nr. 15225/89 vom 19. 5. 1994 etwa fest, dass der Verfassungsgerichtshof Art. 13 EMRK damit verletzt hatte, dass er in der Datenerhebung der Polizei bei Teilnehmern einer Demonstration keinen Eingriff in das Recht auf Achtung der Privatsphäre aus Art. 8 EMRK gesehen und diesen Fall daher gar nicht zur Entscheidung zugelassen hatte.

15 *Müller, R.* (FN 11), S. 558, allerdings mit Bezug auf Datenschutzprinzipien und Art. 8 EMRK.
16 *Gamper, L.* (FN 1), S. 72, mit Nachweisen.

2.4 Art. 8 EMRK in Verbindung mit Art. 14 EMRK

Das Diskriminierungsverbot in Art. 14 EMRK gilt nur in Verbindung mit einem anderen Konventionsrecht[17]; in unserem Fall ist hier in erster Linie Art. 8 EMRK von Interesse. Während Art. 14 i. V. m. Art. 8 EMRK bei Datenschutz m.W. nur ganz selten angerufen wurde und der EGMR in den Fällen *Odièvre* und *Z. c. Finnland* für die behaupteten Ungleichbehandlungen keine Anhaltspunkte fand, sind derartige Situationen immerhin sehr leicht vorstellbar. Eine häufig beklagte Diskriminierung ist die Benachteiligung bestimmter Gruppen in der Privatwirtschaft durch Bewertung der Kreditwürdigkeit oder der Kaufkraft auf Grund allgemeiner Faktoren wie Alter oder Wohnviertel. Unzulässige Eingriffe erfordern m. E. mittelbaren Schutz durch den Gesetzgeber, der in europäischen Staaten teilweise bereits gewährt wird.[18]

Doch auch Verletzungen der Unschuldsvermutung aus Art. 6 i. V. m. Art. 14 EMRK fallen darunter. Strafrechtlichem Generalverdacht ausgesetzte religiöse und ethnische Minderheiten oder auch nur ärmere Bevölkerungsschichten könnten in Ermittlungen in ihrem Recht auf Nicht-Diskriminierung verletzt werden. So hat *Michael R. Curry* aufgezeigt, dass das im internationalen Flugverkehr zum Aufspüren von Kriminellen oder Terroristen verwendete „Profiling" im Grunde auf eher simplen, geodemografischen und potenziell diskriminierenden Annahmen basiert, deren Erfolge zudem im heutigen Massenverkehr fragwürdig sind.[19] Dasselbe kann je nach den benutzten Filtern für die Rasterfahndung gelten. Ebenso legt beispielsweise der Aufbau von großen DNA-Datenbanken, in denen bestimmte Bevölkerungsgruppen überproportional vertreten sind, in manchen Ländern den Verdacht auf gezielte oder faktische Diskriminierung bestimmter Bevölkerungsgruppen durch das Justizsystem nahe. Weitere Beispiele ließen sich auch für andere Grundrechte in Bezug auf Datenschutz und Diskriminierung anführen.

---

17 Mit dem 12. Zusatzprotokoll zur EMRK geht ein Staat zusätzlich die Verpflichtung ein, jegliche gesetzliche Diskriminierung aus irgendwelchen Gründen wie Rasse, Geschlecht, Status usw. zu unterlassen.

18 *Gamper, L.* (FN 1), S. 78.

19 *Curry, Michael R.*, The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation, Surveillance & Society 1 (4) 2004, S. 475 ff.

3. Schlussbetrachtungen

Der hier zur Verfügung stehende Raum reicht nicht aus, auch nur ansatzweise alle Aspekte, die bei den behandelten Grundrechten im Einzelfall zu berücksichtigen sind, aufzuzeigen, doch zumindest das Grundkonzept sollte deutlich geworden sein. Das ist auch ganz im Sinne des Grundthemas der IRIS 2008: „Reduktion der Komplexität". Wenn wir uns heute in m. E. gesamtgesellschaftlich notwendigen, aber noch zu wenig geführten Diskursen darüber einigen möchten, welche Werkzeuge wir Strafverfolgungsbehörden zur Verfügung stellen möchten und welche nicht, dann sollten wir uns nicht nur an den vergleichsweise komplexen Datenschutzprinzipien orientieren, die im Einzelfall unzureichend sein können, sondern auch andere Grundrechte nicht aus den Augen verlieren und uns dabei immer wieder daran erinnern, was mit deren Einführung bezweckt wurde – etwa die Absicherung des Folterverbots und der Aufbau eines positiven Vertrauensverhältnisses der Bürger zu ihrem Staat und seinen Sicherheitsbehörden. Dies könnte dazu beitragen, die Diskussion zu vereinfachen und gleichzeitig zu verbreitern.