Jahrbuch

nw neuer wissenschaftlicher Verlag
Recht

Datenschutzrecht

11

herausgegeben von

Dietmar Jahnel

Rainer KNYRIM / Renate RIEDL

Datenschutzrechtliche Fragen zur automatischen Suche nach kritischen Ereignissen in Videoarchiven

Inhaltsübersicht

I. Einleitung

Im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS wird das Thema „Sicherheit" – der Auf- und Ausbau von Exzellenz im Bereich Sicherheitsforschung – gefördert. In der Programmlinie 2 widmet sich das Projekt SECRET[1] (Search of Critical Events in Videoarchives) der Erforschung von Algo-

1 http://www.kiras.at/gefoerderte-projekte/programmlinie-2/secret/.

rithmen, Methoden und Prozessen, um die Aufgabe der Suche und Verfolgung von Ereignissen in Videoarchiven für das Sicherheitspersonal zu erleichtern und um einen Faktor 10 bis 100 zu beschleunigen. Sicherheitsbehörden sind mit der Aufgabe konfrontiert, bestimmte Ereignisse, Objekte, Personen oder Verhaltensmuster in Videoaufnahmen eines umfassenden Videoarchivs aufzufinden. Aufgrund der derzeit vorhandenen technischen Gegebenheiten ist die Suche nach einem bestimmten Objekt oder bestimmten Ereignis extrem zeitintensiv und die Aufgabe kaum noch bewältigbar.

A. Technische Aufgabenstellung

Kernpunkt der technischen Aufgabestellung im Projekt ist eine Ähnlichkeitssuche. Die Beschreibung einer gewünschten Person oder eines gewünschten Objekts wird durch eine Avatar-ähnliche Beschreibungssprache oder ein Bildbeispiel in eine mathematische Beschreibung der optischen Eigenschaften des gesuchten Objekts umgesetzt. Diese mathematische Beschreibung wird mit den vorhandenen Videobildern aus dem Archiv verglichen, wobei zuerst die Bilder aus den Videobildern des Archivs vereinzelt extrahiert werden. Jeder Vergleich zwischen der gesuchten Beschreibung und dem vereinzelten Videoarchivbild ergibt einen Wert, der angibt, mit welcher Wahrscheinlichkeit das gesuchte Objekt oder die gesuchte Person mit dem Ergebnis im Bild identisch ist. Als Ergebnis bekommt der Bearbeiter die Bilder mit der höchsten Trefferwahrscheinlichkeit angezeigt. Je höher die Prozentzahl im Ergebnis ist, umso ähnlicher ist das Ergebnis der gesuchten Anfrage. Durch diesen interaktiven Prozess kann das zu durchsuchende Material zeitlich und örtlich erheblich eingeschränkt werden.

B. Konkrete datenschutzrechtliche Fragestellung

Im Zuge dieses Projektes stellte sich auch die Frage nach verschiedenen juristischen/datenschutzrechtlichen Aspekten. Ziel der rechtlichen Untersuchung war die Erhebung und Analyse der juristischen/datenschutzrechtlichen Aspekte in Österreich zur gültigen österreichischen Rechtslage laut den folgenden technisch-wissenschaftlichen Zielen:

Automatische Suche in Videoarchiven mit verschiedenen graduierbaren Triggermöglichkeiten, wodurch es möglich sein müsste, nach Ablage oder Entfernung von Gegenständen (ohne Suche nach Gesichtern) sowie Bildänderungen in frei definierbaren Bereichen zu suchen und automatisch Standbilder speichern zu lassen.

Suche in Videoarchiven nach Personen mit oder aufgrund vorliegender Vergleichsbilder – ohne Suche nach Gesichtern – Verfolgung von Personen in größeren Videoanlagen (mehrere Videokameras wie zB Flughafen) oder aufgrund von Referenzdaten (markante Kleidung).

Aufgrund der besonderen Sensibilität und des Projektumfangs wurde eine rechtliche Untersuchung der Gesichtserkennung sowie der Kennzeichenerkennung nicht in das Projekt mit einbezogen. Außerdem wurden verschiedene andere Aspekte wie zB Rechtschutz oder Beweisverwertung ausgeklammert.[2]

2 Zum Rechtschutz siehe: *Vogl*, Der Rechtschutzbeauftragte in Österreich, NWV, 2004.

Im folgenden Artikel wird ein Teil des rechtlichen Gutachtens zusammenfassend anhand eines der Use-Cases dargestellt und einige der rechtlichen Probleme thematisiert. Zu trennen ist die Beurteilung in den Vorgang der Ermittlung der Daten (der Vorgang der Aufnahme des Bildmaterials) und die anschließende Auswertung der Bilddaten mit der geschilderten technischen Suchabfrage.

C. Die konkrete Situation der Sicherheitsbehörden bei der Überwachung eines Hauseinganges

Ein umfangreicher Teil der rechtlichen Untersuchung wurde anhand eines von den Sicherheitsbehörden geschilderten praktischen Szenarios durchgeführt.[3] Zur Verhinderung oder Aufklärung von Straftaten, insbesondere des organisierten Verbrechens, sind verdeckte Ermittlungen notwendig. Ziel der konkreten Maßnahme ist die Videoüberwachung des Hauseinganges eines Privathauses. Vom zu überwachenden Haus ist bekannt, dass sich verdächtige Personen darin aufhalten, oder das es von verdächtigen Personen betreten wird. Diese Personen sollen identifiziert werden bzw sollen Personen, die mit den verdächtigen Personen in Verbindung treten, identifiziert werden. Die Observation mit optisch-technischen Mitteln wird für einen Zeitraum von 24 Stunden am Tag mit Videokameras durchgeführt, und das für die Dauer von mehreren Tagen bis Wochen. Es erfolgt keine Echtzeitüberwachung, gespeichert werden ausschließlich Bilddaten, Tondaten werden nicht erhoben. Konkret verwendet werden Bandmaschinen, bei denen das Material erst digitalisiert werden muss, seltener bereits digitale Geräte. Dies geschieht aufgrund der besseren Durchsuchbarkeit des analogen Materials, bei digitalen Aufnahmen werden manchmal Bilder übersprungen bzw stellt die Industrie nicht extra Videoüberwachungsgeräte her, die auf die Bedürfnisse der Sicherheitsbehörden zugeschnitten sind. Die Aufnahmedauer eines Bandes beträgt in der Regel 24 bzw 48 Stunden. Im Anschluss an die Bildaufnahme findet eine forensische Auswertung des Bildmaterials durch die Behörden statt. Die Durchsuchung des Materials erfolgt anhand von Merkmalen, die von den Kriminalisten festzulegen sind und sich aus der bisherigen Ermittlungsarbeit ergeben. Momentan erfolgt diese Durchsuchung des Videomaterials noch händisch im optischen Schnelldurchlauf des Videobandes am Bildschirm, was einen enormen Zeitaufwand bedeutet.

Mit der im SECRET-Projekt entwickelten Software ist es nun möglich, eine gesuchte Person oder ein gesuchtes Objekt im Bild abzusondern und unter mehreren gleichartigen Personen oder Objekten herauszufiltern. Diese so vereinzelte Person oder das vereinzelte Objekt, welche(s) sich oft in Bewegung befindet, kann nun im Videomaterial verfolgt werden. Denkbar ist auch, sollte die Überwachung in einem größeren räumlichen Umfeld getätigt werden, die Person oder das Objekt über mehrere Kameraaufnahmen hinweg zu verfolgen. Wird eine größere Örtlichkeit von mehreren Kameras überwacht, ist es so möglich, die gesuchte Person oder das gesuchte Objekt nicht „aus dem Bild zu verlieren", und den Suchradius entsprechend zu erweitern.

3 Die Informationen zum vorliegenden Use-Case wurden uns von Mitarbeitern des niederösterreichischen Landeskriminalamtes zur Verfügung gestellt.

II. Rechtliche Aspekte bei der Ermittlung der Bilddaten

Bei der Überwachung eines Hauseinganges durch die Behörden sind mehrere verfassungsmäßig geschützte Rechte betroffen. Im besonderen Maße sind der Schutz des Hausrechts und der Wohnung, der Schutz des Familienlebens, sowie der Schutz personenbezogener Daten zu prüfen.

A. Verfassungsrechtliche Grundlagen

1. Schutz des Hausrechtes

Das Hausrecht wird gemäß § 1 Hausrechtsgesetz, das nach Art 9 Abs 2 StGG einen integralen Bestandteil des Staatsgrundgesetzes bildet, und gemäß Art 149 Abs 1 B-VG als Verfassungsgesetz angesehen.[4]

Schutzobjekte sind die Wohnung und die sonstigen zum Hauswesen gehörigen Räumlichkeiten. Die Rechtsprechung legt diese Begriffe weit aus. Nach der Rechtsprechung des VfGH dient das Grundrecht der Wahrung der Intimsphäre, es umfasst unter Berücksichtigung des Schutzzwecks der Norm jeden abgeschlossenen räumlichen Bereich, der dem-Einblick Außenstehender grundsätzlich entzogen ist.[5]

Grundrechtsträger ist nicht nur der Eigentümer, sondern jeder Inhaber einer geschützten Räumlichkeit. Das Hausrechtsgesetz schützt die jeweiligen Wohnungsinhaber, nicht hingegen Dritte wie zum Beispiel Besucher.[6]

Das Hausrecht soll vor Hausdurchsuchungen schützen, nicht aber unbedingt vor anderen Beeinträchtigungen der geschützten Häuslichkeit, wobei angesichts der technischen Möglichkeiten auf die Intensität des Eingriffs abzustellen ist.[7]

Fraglich ist nun, ob ein Hauseingang den Schutz des Hausrechts genießt. Der Hauseingang ist jener Teil des Hauses, in den man sich vom öffentlichen Raum in das Haus hinein begibt. Durch die Beobachtung dieses Wohnungsumfeldes (Verlassen und Wiederbetreten durch die Bewohner, die Besucherfrequenz, die Identität der Besucher und ähnliches) kann Rückschlüsse auf Sachverhalte in der Wohnung gezogen werden.[8] Trotz der Möglichkeit, Dritte vom Betreten des Hauses auszuschließen, liegt kein der Öffentlichkeit gegenüber abgeschlossener oder abschließbarer Raum vor, welcher der häuslichen Gemeinschaft oder sonstigen persönlichen oder wirtschaftlichen Zwecken gewidmet ist. Die Beobachtung und Überwachung des Wohnungsumfeldes ist daher nicht als Hausdurchsuchung im Sinne des § 1 Hausrechtsgesetzes anzusehen.

Auch der deutsche Bundesgerichtshof entschied im Jahr 1998, dass eine langfristige Videoüberwachung eines zum Haus führenden Gehwegs nur Verlassens- und Wiederkehrzeiten des Angeklagten und das Erkennen von Besuchern

4 *Wiederin*, Privatsphäre und Überwachungsstaat, Sicherheitspolizeiliche Datenermittlungen im Lichte des Art 8 EMRK und der Art 9-10a StGG, 41.
5 *Berka*, Die Grundrechte: Grundfreiheiten und Menschenrecht in Österreich, Rz 489.
6 *Wiederin*, aaO, 51.
7 *Wiederin*, aaO, 50 ff.
8 *König*, Videoüberwachung-Fakten, Rechtslage und Ethik, 88.

erfasste und darum nicht auf die Gewinnung von Erkenntnissen aus dem durch Art 13 Grundgesetz geschützten Bereich (Schutz der Wohnung) abzielte.[9]

2. Schutz des Familienlebens

Gemäß Art 8 Abs 1 EMRK hat jedermann Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

Eine eindeutige und abschließende Definition des Begriffs Privatleben ist weder in der Literatur noch in der Rechtsprechung zu finden. Garantiert werden soll durch Art 8 EMRK der Freiraum eines Einzelnen, der für die freie Entfaltung der Persönlichkeit unabdingbar ist.[10] Jedenfalls Teil des geschützten Privatlebens ist die Verfügung über den eigenen Körper, das Sexualverhalten und die körperlichen und geistigen Befindlichkeiten (zB sein Gesundheitszustand), aber auch das private Tun und Treiben, die Kontakte mit engen Bezugspersonen und die persönliche Identität.[11] Ähnlich große Schwierigkeiten wie die Definition bereitet die Abgrenzung des Privatlebens von der Öffentlichkeit. Auch das Verhalten einer Person außer Haus kann uU als privates Verhalten eingeschätzt werden.[12]

Ein Eingriff in das Privatleben eines Menschen liegt auch vor, wenn sich Außenstehende Informationen aus diesem Bereich verschaffen (sogenannte Informationseingriffe), damit sind auch die verschiedenen Formen der staatlichen Datensammlung umfasst. Hier kommt es unter anderem auf die Art der Informationen an, auf den Umfang der Datenerfassung und die weitere Verwendung der Daten bzw die Dauer der Aufbewahrung.[13]

Die im Jahr 1997 eingeführten besonderen Ermittlungsmaßnahmen (Lauschangriff, Rasterfahndung)[14] im Rahmen der Erweiterung der Befugnisse der Sicherheitspolizei stellen besonders intensive Grundrechtseingriffe dar, insbesondere, weil Menschen oft ohne ihr Wissen einer Überwachung ausgesetzt sind bzw zahlreiche unbeteiligte Personen miterfasst werden.[15]

Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Grundrechts ist gemäß Art 8 Abs 2 EMRK nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.[16] Ein Eingriff in das Grundrecht kann also nur bei Vorliegen von außergewöhnlichen Situationen und in engen Grenzen zulässig sein, und hat sowohl notwendig als auch verhältnismäßig zu sein.[17] Die Verhältnismäßigkeit des Eingriffs hängt von der

9 *König*, aaO, 89.
10 *Grabenwarter*, Europäische Menschenrechtskonvention³, § 22 Rz 1.
11 *Grabenwarter*, aaO, § 22 Rz 6ff.
12 Siehe *EGMR* 28.1.2006, Peck gegen UK, ÖJZ 2004/20 (MRK).
13 *Berka*, aaO, Rz 466.
14 BGBl I 105/1997.
15 *Miklau/Pilnacek*, Optische und akustische Überwachungsmaßnahmen zur Bekämpfung organisierter Kriminalität („Lauschangriff")-Paradigmenwechsel im Verfahrensrecht, JRP 1997, 286.
16 Ausführlich u.a. *Wiederin*, Art 8 EMRK Rz 22ff.
17 *Berka*, aaO, Rz 244.

Legitimität des Zwecks, der Eignung und der Erforderlichkeit ab. Insgesamt hat ein angemessenes Verhältnis zwischen dem eingesetzten Mittel und der damit verbundenen Grundrechtsbeeinträchtigung gewahrt zu bleiben.[18]

3. Datenschutz

Die Datenschutzrichtlinie[19] nimmt in den Erwägungsgründen 14 bis 16 auf Bild- und Tondaten explizit Bezug, allerdings wird die Anwendbarkeit ausgenommen, sofern es sich um Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder Tätigkeiten des Staates im Bereich des Strafrechtes oder anderer Tätigkeiten handelt, die nicht unter das Gemeinschaftsrecht fallen.

Das Grundrecht auf Datenschutz ist im Datenschutzgesetz 2000 verankert.[20] Gemäß § 4 Z 4 DSG 2000 sind personenbezogene Daten Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Nur indirekt personenbezogen sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug derart ist, das dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann. Für den Personenbezug von Personen in Videos im Sinne des Datenschutzgesetzes ist bereits die Möglichkeit der Identifizierung ausreichend, ob dies tatsächlich erfolgt, oder unter welchem Aufwand, ist nicht relevant.[21] Eine explizite Normierung der Videoüberwachung im DSG 2000 hat mit der Novelle 2010 stattgefunden.[22] Der Bereich der Videoüberwachung wird jetzt in einem eigens eingefügten Abschnitt 9a in den §§ 50a-50e DSG 2000 geregelt, wobei insbesondere die Videoüberwachung durch Private geregelt wird.[23]

Videoüberwachungen im Rahmen der Hoheitsverwaltung sind in den entsprechenden Materiengesetzen zu regeln. Entsprechende Überwachungen im öffentlichen Raum sind grundsätzlich den Sicherheitsbehörden vorbehalten.[24]

4. Weitere Regelungen

Im Zusammenhang mit der Überwachung mit optisch-technischen Mitteln können noch zahlreiche andere Gesetze beachtlich sein, wie die Europäische Charta der Grundrechte, § 16 ABGB, das Urheberrechtsgesetz, Persönlichkeitsrechte, etc. Auf diese wird hier nicht weiter eingegangen.

18 *Berka*, aaO, Rz 266ff.
19 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
20 *Jahnel*, Datenschutz, 2/3ff.
21 *König*, Videoüberwachung, in: Handbuch Datenschutzrecht, *Bauer/Reimer* (Hrsg), 318.
22 BGBl I 133/2009.
23 Siehe §§ 50a bis 50e DSG 2000.
24 Zum Spannungsfeld zwischen Datenschutz und Sicherheitspolizei: Roundtable Sicherheitspolizei und Datenschutz, jusIT 2008/18.

B. Einfachgesetzliche Grundlagen

1. Unterscheidung SPG und StPO

Für das Vorgehen der Behörden ist aufgrund der grundrechtlichen Relevanz eine gesetzliche Regelung zwingend notwendig.[25] Als einfachgesetzliche Grundlagen für die Vornahme einer Überwachung eines Hauseinganges durch die Sicherheitsbehörden sind insbesondere das Sicherheitspolizeigesetz (SPG) bzw die Strafprozessordnung (StPO) einschlägig.

Das SPG zielt auf die Abwehr von allgemeinen Gefahren ab, also solchen, die nicht unbedingt mit einer bestimmten Materie verbunden sind.[26] Die Strafprozessordnung hingegen beinhaltet das Tätigwerden der Strafjustiz und verfolgt die Aufklärung von gerichtlich strafbaren Handlungen.[27] Akte von Sicherheitsorganen, die aufgrund eines richterlichen Befehls tätig werden, werden der Gerichtsbarkeit zugerechnet. Liegt kein solcher Befehl vor, etwa wegen Gefahr in Verzug oder wenn die in Durchführung eines richterlichen Befehls handelnden Organe ihre Ermächtigung offenkundig überschreiten, liegt ein Akt unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt vor.[28]

Eine klare Trennung der Zuständigkeiten ist im konkreten Fall nicht immer möglich.[29] Erst bei Vorliegen eines Verdachtes gegen eine bestimmte Person endet die Nachforschungsbefugnis nach dem SPG, und es ist dann nach den strafprozessualen Regeln weiter vorzugehen. Die Kenntnis des Namens des Verdächtigen ist nicht nötig, eine Konkretisierung des Verdächtigen reicht aus.[30] Es ist allerdings möglich, nach Ende eines gefährlichen Angriffs die maßgebenden Umstände zu klären, soweit dies zur Vorbeugung weiterer gefährlicher Angriffe erforderlich ist.[31] Hier können Nachforschungen weiter auf das SPG gestützt werden.[32] Eine inhaltliche Überschneidung liegt vor, wenn einerseits ein noch nicht beendeter gefährlicher Angriff vorliegt, anderseits eine bereits verwirklichte Straftat gegeben ist. Hier kann ein Nebeneinander von SPG und StPO vorliegen. § 21 Abs 2 SPG bietet einen Ansatzpunkt zur Lösung. Demgemäß haben die Sicherheitsbehörden einem gefährlichen Angriff unverzüglich ein Ende zu setzen. Hierfür ist dann das SPG auch weiterhin maßgeblich, selbst wenn bereits ein bestimmter Mensch der strafbaren Handlung verdächtig ist. Die Gefahrenabwehr steht dabei im Vordergrund.

Bei Vorliegen eines zu beurteilenden Sachverhaltes ist es ratsam, sowohl die StPO als auch das SPG zu prüfen. Die jeweilige gesetzliche Grundlage ist dann Ansatz von allfälligen Beschwerden.[33]

25 *Pradler*, Datenmissbrauch in der öffentlichen Verwaltung, 44ff.
26 § 3 SPG.
27 *Reindl-Krauskopf*, WK-StPO § 134 Rz 76.
28 *Schmid*, Grundrechte im strafgerichtlichen Verfahren, RZ 2009, 155.
29 *Reindl-Krauskopf*, WK-StPO § 134 Rz 77.
30 *Reindl-Krauskopf*, WK-StPO § 134 Rz 77.
31 *Fichtinger*, Öffentliche Sicherheit 9-10/06, 146.
32 *Reindl-Krauskopf*, WK-StPO § 134 Rz 76.
33 *Ennöckl*, Der Rechtsschutz gegen sicherheitsbehördliche Maßnahmen nach Inkrafttreten des Strafprozessgesetzes, JBl 2008, 409ff; *Wessely*, Wege und Irrwege des datenschutzrechtlichen Rechtsschutzes im Sicherheits- und Militärbefugnisrecht, juridikum 2006, 51ff.

2. Rechtsgrundlage der Überwachung im SPG

Das SPG regelt im vierten Teil die Verwendung personenbezogener Daten im Rahmen der Sicherheitspolizei, wobei hinsichtlich der Terminologie an die Verwendung der Begriffe im DSG 2000 angeknüpft wird.[34] Subsidiär finden, sofern nicht ausdrücklich anderes angeordnet wird, auf das Verwenden personenbezogener Daten die Bestimmungen des DSG 2000 Anwendung.[35] Nach dem Grundsatz der Aufgabenbezogenheit dürfen die Sicherheitsbehörden personenbezogene Daten gemäß den §§ 53-63 SPG nur verwenden, soweit das zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist.

§ 53 Abs 1 SPG regelt die Zulässigkeit der Verarbeitung personenbezogener Daten im sicherheitspolizeilichen Ermittlungsdienst durch die taxative Aufzählung der Zwecke, für welche die Daten ermittelt und verarbeitet werden dürfen. Beachtlich ist der Ausschluss der Rasterfahndung im Dienste der Sicherheitspolizei in beträchtlichen Bereichen. Verboten ist demnach der automationsunterstützte (nicht auch der manuelle) Abgleich (Rasterung) mehrerer Datenbestände (mehrerer Dateien), nicht hingegen die automationsunterstützte Durchsuchung einer Datei nach abstrakten Kriterien (etwa nach allen Personen, auf die in Wien ein Kraftfahrzeug einer bestimmten Type zugelassen ist).[36] Der automationsunterstützte Datenabgleich im Sinne des § 149i StPO (siehe unten) nur zwischen sicherheitspolizeilichen Daten und Dateien, die die Sicherheitsbehörden aufgrund anderer Bundes- oder Landesgesetze angelegt haben, ist unzulässig. Die Rasterung verschiedener sicherheitspolizeilicher Dateien untereinander wird dadurch nicht untersagt.[37]

Neu eingeführt wurde im Jahr 2007 ein § 53a SPG, der die Datenanwendungen der Sicherheitsbehörden näher determiniert.[38] Die genaue Aufzählung der Datenarten, welche so im Gegensatz dazu bei den §§ 53 und 54 SPG nicht vorhanden ist, soll eine hinreichende Determinierung im Sinne des Datenschutzgesetzes schaffen. Ungeklärt ist, ob damit die §§ 53 und 54 SPG zu wenig determiniert sind, bzw wie das Verhältnis der Paragraphen zum neuen § 53a SPG ist.[39]

Eine Anfertigung von eigenem Datenmaterial auf Grundlage des SPG ist nur für sehr enge Zwecke, nämlich die Abwehr von gefährlichen Angriffen und kriminellen Verbindungen möglich und in verdeckter Form nur dann, wenn die Aufgabenerfüllung sonst gefährdet oder erheblich erschwert wäre.

Unabhängig davon besteht natürlich auch die Möglichkeit, dass relevantes Bildmaterial im Rahmen der Videoüberwachung durch Private festgehalten wurde. Bisher war es nur möglich im Anwendungsbereich der StPO durch Beschlagnahme Videomaterial Dritter herauszubekommen und in der Folge das Material auszuwerten.[40] Stellt sich im Rahmen der Ermittlung heraus, dass Videomaterial von Privaten, zB von Banken, öffentlichen Verkehrsbetrieben oder anderen, für

34 § 51 ff SPG.
35 § 51 Abs 2 SPG.
36 *Wiederin*, aaO, 86f, siehe FN 4.
37 Hauer/Keplinger SPG[3] A.6.
38 BGBl I 114/2007.
39 *Flendrovsky*, Datenverwendung und Datenschutz in der allgemeinen Sicherheitspolizei, in: *Bauer/Reimer* (Hrsg) Handbuch Datenschutzrecht, 360.
40 *Lepuschitz/Schindler*, SPG[5] (2008), 157.

die Erfüllung der Sicherheitspolizeilichen Aufgaben wertvoll wäre, besteht nunmehr eine Möglichkeit, diese Daten herauszubekommen.[41] Die parlamentarischen Materialien sprechen in diesem Zusammenhang von einer „freiwilligen" Herausgabe des Materials.[42] Eine Verwendung dieser Daten durch die Sicherheitsbehörden ist freilich nur in einem sehr eingeschränkten Fall möglich. Die Übermittlung und Weiterverwendung durch die Sicherheitsbehörden ist jeweils nur im Zusammenhang mit einem konkreten Anlassfall im Rahmen der ausdrücklich genannten sicherheitspolizeilichen Aufgabenstellung möglich. Es ist nur die Verwendung von Bilddaten möglich und nur für Fälle von Gefahrenabwehr, in denen schwere Gefahr für die öffentliche Sicherheit zu befürchten ist, das bedeutet, eine besonders gewichtige, aus der Durchschnittskriminalität deutlich herausragende Gefahr.[43] Im Ergebnis wird dadurch die Verwendung von Datenmaterial Dritter auf Fälle beschränkt, bei denen die Begehung von Verbrechen (§ 17 StGB) droht.[44]

Besonderes Augenmerk muss bei der rechtlichen Beurteilung auch darauf gelegt werden, ob das Ziel der Überwachung ein öffentlicher oder ein privater Ort ist. Je nachdem sind unterschiedliche Rechtsgrundlagen heranzuziehen. Das SPG definiert öffentliche Orte in § 27 Abs 2 SPG als solche, die von einem nicht von vornherein bestimmten Personenkreis betreten werden können. Die Eigentumsverhältnisse an der Örtlichkeit sind dabei nicht entscheidend. Es ist lediglich relevant, dass dies zu einem beurteilungsrelevanten Zeitpunkt der Fall ist.[45] In der Rechtsprechung finden sich für öffentliche Orte folgende Beispiele: Straßen mit öffentlichem Verkehr, das Stiegenhaus allgemein zugänglicher Gebäude, für jedermann zugängliche Gänge und Höfe eines Hauses, eine Geschäftspassage mit Fußgängerverkehr, oder der Platz vor einem Gasthof.[46]

Konkreter Gegenstand der Untersuchung ist ein privater Hauseingang, der von mehreren, meist unbekannten Personen betreten bzw verlassen wird. Ebenfalls zu sehen ist im jeweiligen Bildausschnitt, woher die Personen kommen bzw wohin sie sich bewegen, nachdem sie den Hauseingang verlassen haben. Von der Überwachung erfasst werden außerdem Personen, die den Hauseingang lediglich passieren. Erfasst werden somit zum Haus zugehörige Personen wie Bewohner, als auch Besucher, Lieferanten, der Postbeamte, oder andere Dritte, die aus welchen Gründen auch immer das Haus betreten oder verlassen. Ins Bild rücken auch solche Personen, die sich im öffentlichen Raum, etwa auf dem Gehsteig bzw im davor sichtbaren Teil der Straße bewegen. Diese sind nicht Gegenstand der Überwachung, werden aber trotzdem von der Kameraüberwachung erfasst.

Der Hauseingang selbst ist zwar nicht vom Hausrecht umfasst, gehört aber jedenfalls zum Wohnungsumfeld. Aufgrund der Personen, die den Hauseingang betreten bzw das Haus verlassen, lassen sich Rückschlüsse auf den Umgang der Bewohner des Hauses ziehen. Ebenso lässt sich durch eine zeitliche Einordnung, wann Personen das Haus verlassen oder betreten, zu welchen Tages-

41 § 115 StPO.
42 *Lepuschitz/Schindler*, aaO, 158.
43 1188 BlgNR 22. GP, RV 06/2.
44 *Lepuschitz/Schindler*, aaO, 15.
45 *Hauer/Keplinger*, SPG[3] A.6.
46 *Hauer/Keplinger*, SPG[3], A.7.

zeiten sie dies tun, oder die Regelmäßigkeit, mit der sie dies tun, Rückschlüsse auf die Lebensgewohnheiten der Personen treffen.

In die rechtliche Beurteilung mit einzubeziehen, und zwar besonders im Hinblick auf die Verhältnismäßigkeit des Eingriffs, ist das Haus bzw die Örtlichkeit selbst, dessen Hauseingang überwacht werden soll. Es ist eine große Bandbreite an Konstellationen, welche Art von Haus überwacht wird, denkbar. Es kann sich nicht nur um ein Privathaus rein zu Wohnzwecken handeln, sondern auch um ein Haus, in dem zB mehrere Arztpraxen beheimatet sind, eine Gesundheitsberatungsstelle, Einrichtungen von politischen Parteien oder der Gewerkschaft, soziale oder kulturelle Einrichtungen mit besonders hohem Ausländeranteil, bis hin zu religiösen Einrichtungen oder religiösen Häusern wie zB einer Moschee. In diesem Fall ist ein Bereich Gegenstand der Überwachung, in dem fast ausschließlich besonders schutzwürdige Daten erhoben werden.[47]

Der beschriebene Use-Case zeichnet sich nicht nur durch die Verwendung von Kameras, sondern auch durch die Vornahme als verdeckte Ermittlung aus. Die gesetzliche Grundlage für die Verwendung von Bild- und Tonaufzeichnungsgeräten ist in § 54 Abs 4 SPG zu finden. Demgemäß ist die Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten nur für die Abwehr gefährlicher Angriffe und krimineller Verbindungen zulässig; sie darf unter den Voraussetzungen des Abs 3 auch verdeckt erfolgen. Dabei ist das Einholen von Auskünften in Form einer verdeckten Ermittlung nur zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre. Verdecktes Ermitteln ist die Durchführung einer Überwachung, ohne dass auf das Vorliegen eines amtlichen Charakters hingewiesen wird.[48] Damit wird im Gegensatz zu einer offenen Überwachung der Vorgang der Videoüberwachung nicht extra gekennzeichnet. Die überwachten Personen, und solche, die ebenfalls mit in das Bild geraten, sind nicht in Kenntnis einer Überwachung und haben demgemäß auch keine Möglichkeit, den überwachten Bereich zu vermeiden bzw zu umgehen.

Das Gesetz selbst schränkt die Verwendung von Bildaufzeichnungsgeräten auf die Tatsache ein, dass sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre.

Gemäß § 54 Abs 4 letzter Satz Punkt 2 SPG ist die Ermittlung von personenbezogenen Daten jedoch unzulässig, wenn sie mit Bildaufzeichnungsgeräten durchgeführt werden, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgendes Verhalten aufzuzeichnen. Dem steht also nicht entgegen, dass es sich um öffentliches Verhalten handelt, welches mit Bildaufzeichnungsgeräten aufgezeichnet werden kann.[49] Ein Hauseingang kann als ein solcher öffentlicher Platz gesehen werden. Er ist von der Straße her von Dritten stets einsehbar.

Der Einsatz von Bildaufzeichnungsgeräten zur Abwehr einer kriminellen Verbindung ist nur zulässig, wenn die Begehung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17) zu erwarten ist.[50] Demnach handelt es sich um gerichtlich strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind. Weiters ist bei jeglichem Einsatz von Bildaufzeichnungsgeräten besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren. Damit wird nochmals besonders auf das Prinzip der Verhältnismäßigkeit hingewiesen. Das bedeutet, dass es jeweils auf die konkreten Umstände des Einzelfalles ankommt, ob die besonderen Voraussetzungen für eine verdeckte Ermittlung mit Bildaufzeichnungsgeräten gegeben sind. Der Schutz der Grundrechte ist sowohl vom Antragsteller, als auch insbesondere vom Richter, der die Überwachung genehmigt, zu prüfen.[51] Damit ist die Überwachung eines Hauseinganges mittels Videoüberwachung über einen längeren Zeitraum nur unter gewissen Umständen möglich und auf schwere Verbrechen beschränkt.

47 *König*, Videoüberwachung, in: Handbuch Datenschutzrecht, *Bauer/Reimer* (Hrsg), 328.
48 *Hauer/Keplinger*, SPG[3] A.3.
49 Hauer/Keplinger, SPG[3] A.12.
50 § 54 Abs 4a SPG.

3. Rechtsgrundlage für die Observation mit technischen Mitteln in der StPO

Die fragliche Rechtsgrundlage in der StPO bringt ähnlich hohe Hürden für die Zulässigkeit wie das SPG. Der sog „große Lauschangriff" gemäß § 136 Abs 1 Z 3 StPO kann nur vorgenommen werden, wenn bereits ein dringender Tatverdacht vorliegt. Es muss also eine entsprechend hohe Verdachtslage gegeben sein, und es muss mit großer Wahrscheinlichkeit vom Vorliegen einer kriminellen Organisation ausgegangen werden.[52] Diese Ausgangslage muss auch beim Verbrechen der terroristischen Vereinigung vorliegen. Ansatzpunkt der Überwachung ist die dringend tatverdächtige Person selbst, oder eine solche Person, von der anzunehmen ist, dass die dringend tatverdächtige Person mit ihr in Verbindungen treten wird.[53] Die Durchführung eines solchen Lauschangriffes ist möglich, wenn die Aufklärung oder Verhinderung weiterer Taten oder die Aufenthaltsermittlung ansonsten aussichtslos oder wesentlich erschwert wäre. Das bedeutet, dass die Durchführung dieser Maßnahme notwendig ist, oder andere Ermittlungsmaßnahmen zwar möglich sind, aber wesentlich weniger Erfolgsaussichten haben.[54] Zusätzlich stehen sie unter der Bedingung der Verhältnismäßigkeit.

In den Fällen der rein optischen Überwachung gemäß § 136 Abs 3 StPO wird die Überwachung innerhalb bzw außerhalb von Wohnungen geregelt. Eine Erläuterung der Überwachung innerhalb einer Wohnung kann aufgrund der zu behandelnden Fragestellung außer Acht gelassen werden. Als gesetzliche Grundlage für die Überwachung eines Hauseingangs im konkreten Fall ist daher § 136 Abs 3 Z 1 StPO zu prüfen. Demgemäß ist die optische Überwachung von Personen zur Aufklärung einer Straftat zulässig, wenn sie sich auf Vorgänge außerhalb einer Wohnung oder anderer durch das Hausrecht geschützter Räume beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt treten oder die Örtlichkeiten betreten.

51 *Schmid*, Grundrechte im strafgerichtlichen Verfahren, RZ 2009, 153.
52 *Reindl-Krauskopf*, WK-StPO § 136 Rz 16.
53 *Reindl-Krauskopf*, WK-StPO § 136 Rz 18.
54 *Reindl-Krauskopf*, WK-StPO § 136 Rz 21.

4. Problem einer fehlenden rechtlichen Grundlage für den konkreten Fall?

Damit stellt sich gerade die Frage, ob ein Hauseingang von dieser Bestimmung umfasst sein kann. Gemeint ist eine Objektüberwachung, bei der das Verhalten von Personen erfasst werden soll, die diese Örtlichkeiten betreten. Betrachtet man den Wortlaut der Bestimmung, so bezieht sich dieser „auf Vorgänge außerhalb einer Wohnung oder anderer durch das Hausrecht geschützte Räume". Wie bereits oben ausgeführt, ist ein Hauseingang gerade nicht vom Hausrecht geschützt. Ebenso befindet sich der Hauseingang klar außerhalb der Wohnung.

Demgegenüber steht außerdem die Legaldefinition des § 134 Z 4 StPO, in der die optische und akustische Überwachung von Personen als die Überwachung des Verhaltens von Personen unter „Durchbrechung der Privatsphäre" definiert wird.[55] Eine Überwachung des Hauseinganges wäre daher nur von der Bestimmung erfasst, wenn man ihn zur Privatsphäre zählen könnte. Dieser Sachverhalt wird nur dann vorliegen, wenn der Hauseingang so gelegen ist, dass er von Dritten nicht einsehbar ist.[56] Daraus folgt, dass für die Überwachung öffentlichen Verhaltens unter der Verwendung von Bildaufnahmegeräten eine gesetzliche Grundlage in der StPO fehlt. Diese ist aber aufgrund des Eingriffs in die Grundrechte notwendig.[57] Im Ergebnis ist die Überwachung eines Hauseinganges mittels optisch-technischen Mitteln auf der Rechtsgrundlage StPO nicht zulässig.

Gemäß einer Meinung ist eine Lösung in Form eines Größenschlusses zu § 136 Abs 3 Z 1 StPO denkbar: Wenn unter den dort genannten Voraussetzungen eine Überwachung nicht öffentlichen Verhaltens zulässig ist, dann muss unter denselben Voraussetzungen auch die weniger eingreifende Maßnahme, also die Überwachung des ohnehin öffentlich zur Schau getragenen Verhaltens, zulässig sein. Unter diesen Voraussetzungen wäre die Überwachung öffentlichen Verhaltens auch nach der StPO möglich. Diesbezüglich ist aber wieder auf die Abgrenzung von SPG und StPO Bedacht zu nehmen. Gemäß StPO ist an die Aufklärung von bereits begangenen Straftaten zu denken, während beim SPG die Abwehr von gefährlichen Angriffen im Vordergrund steht.[58] Eine eigene Definition für den Begriff der Öffentlichkeit fehlt in der StPO.

III. Rechtliche Aspekte bei der Auswertung der Bilddaten

A. Bisherige praktische Relevanz

Die tatsächliche Anwendung der Software des SECRET-Projektes findet bei der Analyse des Videomaterials statt. Entscheidend für die rechtliche Beurteilung ist nun, ob es sich bei der automatischen Durchsuchung um eine bloße Analyse des Materials handelt, oder ob die Kriterien eines automationsunterstützten Datenabgleichs erfüllt sind. Eine solche „Rasterfahndung" wäre nur unter bestimmten strengen Voraussetzungen zulässig. Im zuletzt veröffentlichten Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen im Jahr 2009 wurde die Durchführung eines automationsunterstützten Datenabgleichs nach den §§ 141 ff StPO in keinem Fall angeordnet.[59] Laut dem Sicherheitsbericht 2008, dem Bericht der Bundesregierung über die innere Sicherheit in Österreich, gab es lediglich im Jahr 2004 einen automationsunterstützten Datenabgleich („Rasterfahndung"). In den Jahren 2005 bis 2008 kam es zu keinem Fall.[60]

55 *Birklbauer/Hauer/Keplinger/Tischlinger*, Strafprozessordnung, Polizeiausgabe, prolibris 2011, 204.
56 *Reindl-Krauskopf*, WK-StPO § 136 Rz 28.
57 *Reindl-Krauskopf*, WK-StPO § 136 Rz 29.
58 *Reindl-Krauskopf*, WK-StPO § 136 Rz 29; *Birklbauer/Hauer/Keplinger/Tischlinger*, Strafprozessordnung, 208.

B. Abgrenzung zwischen Analyse und Datenabgleich

Gemäß Legaldefinition des § 141 Abs 1 StPO ist der Datenabgleich der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmal enthalten, sowie Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die aufgrund dieser Merkmale als verdächtig in Betracht kommen. Aufgrund der Grundrechtsrelevanz ist für den Eingriff eine gesetzliche Grundlage, die Notwendigkeit und die Verhältnismäßigkeit Voraussetzung für die Rechtmäßigkeit eines solchen Datenabgleichs.

Unter den Merkmalen, die für einen Datenabgleich herangezogen werden, gibt es einerseits die den mutmaßlichen Täter kennzeichnenden Merkmale, als auch solche, die ausschließende Merkmale enthalten.[61] Demgemäß spricht man von einer „positiven" oder einer „negativen" Rasterfahndung.[62] Kennzeichnend für einen automationsunterstützten Datenabgleich ist einerseits die Zuhilfenahme von elektronischen Mitteln und Suchkriterien, andererseits eine programmgesteuerte Überprüfung mehrerer verschiedener Datenbestände.[63] Bewegt sich der Auswertende innerhalb einer Datenanwendung, so entspricht dies lediglich einer Filterung bzw einer Analyse des vorhandenen Materials.[64] Zu einem Abgleich kommt es erst, wenn man einen Vergleich von Teilmengen an Daten vornimmt. Im Einzelnen gewinnt man aus den einzelnen Datenanwendungen Teilmengen, die man vorher nach gewissen Suchkriterien gefiltert hat. Aus den Teilmengen von verschiedenen Datenanwendungen wird eine Schnittmenge gebildet. Diese enthält sowohl die Suchkriterien der einen Datenanwendung, als auch die Suchkriterien der anderen Datenanwendung. Die Schnittmenge filtert nun jene Personen heraus, deren Merkmale sowohl in der einen Datenanwendung, als auch in der anderen Datenanwendung vorhanden sind. Damit verkleinert man den Kreis der Tatverdächtigen. Es ist keinesfalls sicher, dass ein Datenabgleich zu einem gewünschten Ergebnis führt. Unter Umständen führt ein Datenabgleich auch dazu, dass keine einzige Person den gesuchten Merkmalen entspricht.[65] Das Ergebnis eines automationsunterstützten Datenabgleichs bildet keinen Beweis für die Schuld- bzw die Täterschaft einer Person. Die ermittelten abgeglichenen

59 http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00206/fname_204174.pdf.
60 Sicherheitsbericht 2008 des Bundesministeriums für Inneres, III-99 der Beilagen XXIV.G.P.- Bericht-Hauptdokument (Teil I), 589.
61 *Birklbauer/Hauer/Keplinger/Tischlinger*, Strafprozessordnung, 214.
62 *Reindl-Krauskopf*, WK-StPO § 141 Rz 11.
63 *Reindl-Krauskopf*, WK-StPO § 141 Rz 9.
64 OLG Wien 3.3.2000, 21 Bs 21/00, JBl 2001, 257.
65 *Reindl-Krauskopf*, WK-StPO § 141 Rz 10.

Daten nach Durchführung des Datenabgleichs können lediglich als Ausgangspunkt und Ansatz für weitere Ermittlungen dienen.[66]

Die Merkmale, die man für eine Suche heranzieht, müssen bereits vorhanden sein, um überhaupt zu einem automationsunterstützten Datenabgleich zu kommen. Diese Merkmale gewinnt man aus der bisherigen erkennungsdienstlichen Arbeit. Ein automationsunterstützter Datenabgleich wird also erst dann Sinn machen, wenn man bereits eine gewisse Vorstellung vom Täter hat.[67]

Da ein automationsunterstützter Datenabgleich nur unter gewissen strengen Voraussetzungen durchgeführt werden kann, ist es notwendig, eine genaue Abgrenzung zu anderen Suchvorgängen innerhalb eines Datenmaterials zu finden.

Nach der Legaldefinition des § 4 Z 7 DSG 2000 ist eine Datenanwendung die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zwecks der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise und automationsunterstützt, also maschinell und programmgesteuert, erfolgen. (Automationsunterstützte Datenanwendung). Eine solche Datenanwendung ist nun die Basis für den Datenabgleich im Sinne des § 141 StPO. Gemäß dem Gesetzeswortlaut ist dabei nicht ausschlaggebend, ob es bei den Datenanwendungen einen oder mehrere Auftraggeber im Sinne des Datenschutzgesetzes gibt.[68]

Kein automationsunterstützter Datenabgleich liegt jedenfalls vor, solange der Auswertende sich innerhalb einer Datenanwendung bewegt. Er kann daher innerhalb einer Datenanwendung Daten suchen, sortieren, ordnen oder analysieren. Solange der Auswertende in ein und demselben Videomaterial bestimmte Trigger (= auslösende Merkmale) definiert und für eine Ähnlichkeitssuche heranzieht, bewegt er sich lediglich im Bereich der Analyse. Auch das Erstellen eines Bildausschnittes aus einem Datenmaterial als Basis für die weitere Suche ist nur eine Analyse bzw Ordnung des Materials.

Als Basis für eine Ähnlichkeitssuche kann auch ein bereits ermittelter Bildausschnitt herangezogen werden. In diesem Fall nimmt der Auswertende die Bildsequenz und verwendet diese als Ausgangspunkt für eine neue Suchabfrage. Der Bildausschnitt kann aus derselben Datenanwendung, also aus dem bereits vorhandenen Videomaterial stammen.

Es ist allerdings auch möglich, ein Bild aus anderem vorhandenen Videomaterial auszuschneiden und in die laufende Videosuche zur Vornahme einer Ähnlichkeitssuche zu übertragen. Die technische Formatierung der Videoaufnahmen – und somit die Vergleichbarkeit – stellt im Wesentlichen kein Problem dar. In diesem Fall wird eine Schnittmenge aus verschiedenen Datenanwendungen gebildet und der Auswertende führt somit einen automationsunterstützten Datenabgleich durch, der strengen rechtlichen Voraussetzungen unterliegt.

Festzuhalten ist, dass die Auswertung der Daten in Form eines automationsunterstützten Datenabgleichs im Sinne des § 141 StPO den Sicherheitsbehörden nach § 53 Abs 2 SPG ausdrücklich verboten ist.[69]

66 *Reindl-Krauskopf*, WK-StPO § 141 Rz 11.
67 Zur praktischen Durchführung: *Leitner*, Fahndung durch Sicherheitsbehörden und Sicherheitsorgane, 62.
68 *Reindl-Krauskopf*, WK-StPO § 141 Rz 12.
69 *Reindl-Krauskopf*, WK-StPO § 141 Rz 15.

Im Ergebnis zeigt sich, dass zwischen der (rechtlich zulässigen) Analyse des vorhandenen Videomaterials mit automatischer Suche und dem Abgleich des Videomaterials mit anderen Videodaten im Sinne der Durchführung einer Rasterfahndung nur ein schmaler Grat besteht.

IV. Resümee

Bereits bei der Herstellung von Videomaterial durch die Sicherheitsbehörden ist auf die Heranziehung der korrekten Rechtsgrundlage zu achten. Sowohl im SPG, als auch in der StPO bestehen strenge Voraussetzungen für die optische Überwachung eines Hauseinganges. Die Frage der Zulässigkeit der Bildaufnahmen ist eine wesentliche Voraussetzung für die rechtmäßige erfolgende Weiterverwendung des Bilddatenmaterials. Bei der automatischen Suche nach Ereignissen, Objekten und Personen im Videoarchiv ist streng zwischen der reinen Analyse des Videomaterials und der Durchführung eines automationsunterstützten Datenabgleichs zu unterscheiden. Die Durchführung eines Suchvorganges, unter Einbeziehung von Elementen bzw Suchausschnitten aus einer anderen Datenanwendung, der technisch gesehen keinen großen Aufwand macht, kann rechtlich gesehen eine völlig andere Bedeutung haben.

Das Bedürfnis die Sicherheit für die Menschen zu erhöhen ist ein Antriebsmotor für Forschung und Entwicklung. Allerdings zeigt sich, dass die Behörden bei den bestehenden gesetzlichen Regelungen mit Situationen konfrontiert sind und auch in Zukunft sein werden, die bei Erlassung der Vorschriften noch nicht im Bereich des Möglichen lagen. Die Anwendung der Technik ohne genaue rechtliche Prüfung kann vielmehr sogar einen Eingriff in die Grundrechte der Menschen darstellen, der so nicht gedacht war. Die Rechtsanwender sind hier aufgerufen, die entsprechenden rechtlichen Grundlagen für die Zulässigkeit der Anwendung genau zu beachten. Für den Gesetzgeber stellt sich die Aufgabe, die gesetzlichen Grundlagen, sofern sie fehlen, zu schaffen und dabei das Gebot der Verhältnismäßigkeit und Notwendigkeit stets im Auge zu behalten.