

Orientierung

Dominika Blonski

Datenverknüpfungen – Problematik und rechtlicher Rahmen

Dritter Schweizerischer Datenschutzrechtstag, 22. Januar 2010, Universität Fribourg

Das Institut für Europarecht der Universität Fribourg organisiert zusammen mit dem eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten regelmässig zweisprachige Schweizerische Datenschutzrechtstage. Ziel dieser Tagungen ist die Einblickvermittlung in nationale und europarechtliche Normen sowie die Analyse von Problemen, welche sich bei der Anwendung dieser Regelungen ergeben.

Der dritte Datenschutzrechtstag wandte sich dem Thema der Datenverknüpfungen zu. Die Referierenden untersuchten das zwischen Datenverknüpfungen und Datenschutzrecht entstehende Spannungsverhältnis und präsentierten aus unterschiedlichen Blickwinkeln Lösungsansätze. Auffällig war, dass die Vortragenden mit unterschiedlichen Definitionen des Begriffs Datenverknüpfung arbeiteten. Aus den verschiedenen Umschreibungen ergab sich als Charakteristikum von Datenverknüpfungen die Verbindung von mehreren Einzeldaten.

Inhalt:

- I. Die Sicherheit biometrischer Daten
- II. Die rechtliche Problematik von Datenverknüpfungen
- III. Datenverknüpfungen in der Praxis, ein Problem- auftritt unter besonderer Berücksichtigung der Statistik
- IV. Datenverknüpfung in ausgewählten Bereichen: Gesundheitswesen
- V. Die Profilbildung

I. Die Sicherheit biometrischer Daten

Der öffentliche Vortrag am Vorabend eröffnete den dritten Schweizerischen Datenschutzrechtstag. *Christophe Champod*¹ referierte über die Sicherheit von biometrischen Daten. Zunächst präsentierte *Champod* allgemeine Informationen zu Definition und Prozessen der Biometrie. Biometrische Daten sind Verhaltenseigenschaften (zum Beispiel die Stimme oder die Gangart) oder physiologische Merkmale (beispielsweise der Fingerabdruck, das Gesichtsbild oder das Irisbild). Aufgrund der Einzigartigkeit und der Messbarkeit der Kennzeichen, eignen sich diese als Identifikationsmerkmale. Biometrische Verfahren wer-

den in zwei Phasen aufgeteilt. In der ersten Phase werden die Daten erstmals verarbeitet und gespeichert (Enrollment). Die so erfassten Daten ermöglichen in der zweiten Phase die Verifikation (Vergleich 1:1) oder Identifikation (Vergleich 1:n) eines Individuums.

Danach ging der Vortragende auf Besonderheiten des biometrischen Passes ein und kam zum Schluss, dass aus seiner Sicht die Sicherheit der im biometrischen Pass gespeicherten Daten grundsätzlich gegeben sei. Jedoch sei die Supervision der Systeme wichtig, da diese nicht fehlerfrei alleine arbeiteten. Der rechtliche Rahmen sei zu allgemein gehalten, daher benötige es mehr spezifische Regeln.

II. Die rechtliche Problematik von Datenverknüpfungen

Nach einigen einleitenden Worten von *Hanspeter Thür*² und *Johannes Frölicher*³, welche beide auf die Brisanz des Themas aufmerksam machten und diese mit der technischen Entwicklung erklärten, führte *Thomas Probst*⁴ mit seiner Darstellung der rechtlichen Problematik von Datenverknüpfungen in die Thematik ein.

Zunächst erläuterte *Probst* eine ganze Reihe von Abgrenzungen. Es ist zu unterscheiden zwischen der Verknüpfung von Sach- mit Sachdaten, von Sach- mit Personendaten und von Personen- mit Personendaten. Weiter besteht eine unterschiedliche Schutzwürdigkeit von Personendaten, wobei die Abstufung von einfachen über qualifizierte bis besonders schützenswerte Personendaten reicht. Die Differenzierung von öffentlichen und privaten Quellen von Personendaten zeigt drei Verknüpfungskontellationen auf: die Verknüpfung von Daten aus einer öffentlichen Quelle mit solchen aus einer weiteren öffentlichen Quelle, die Verknüpfung von Daten aus einer öffentlichen Quelle mit solchen aus einer privaten Quelle und schliesslich die Verknüpfung von Daten aus zwei privaten Quellen. Eine weitere Abgrenzung ergibt sich bezüglich der freiwilligen im Gegensatz zur obligatorischen Kundgabe von Personendaten. Für die Offenbarung gewisser Personendaten besteht eine gesetzliche Auskunftspflicht (zum Beispiel bei der Steuererklärung). Andere Personendaten werden freiwillig, beispielsweise bei Umfragen und dergleichen, abgegeben. Hier muss eine Einwilligung sowohl für die Erhebung als auch für die Verknüpfung vorliegen. Es gibt drei Formen der Entpersonalisierung von Personendaten. Bei der Anonymisierung werden die Identifikationsmerkmale in einem definitiven Schritt gelöscht beziehungsweise vernichtet. Die Identifikationsmerkmale werden im Gegensatz dazu bei der Pseudonymisierung

² *Hanspeter Thür*, lic. iur., Rechtsanwalt, eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Bern.

³ *Johannes Frölicher*, lic. iur., Rechtsanwalt, Präsident der Kommission der kantonalen Aufsichtsbehörde für Datenschutz des Kantons Fribourg und Bundesverwaltungsrichter, Bern.

⁴ *Thomas Probst*, Dr. iur., LL.M., lic. oec. HSG, Professor am Lehrstuhl für Obligationenrecht, Europäisches Privatrecht und Rechtsvergleichung an der Universität Fribourg i.Ue.

MLaw, Assistentin am Institut für öffentliches Recht der Universität Bern

¹ *Christophe Champod*, Dr. der forensischen Wissenschaften, Professor an der Fakultät für Rechts- und Kriminalwissenschaften der Universität Lausanne.

durch ein Pseudonym (beispielsweise durch eine nicht sprechende Nummern- oder Buchstabenfolge) ersetzt. Dabei bleibt die Zuordnung mit einem Schlüssel immer noch möglich. Die dritte Depersonalisierungsform ist die Verschlüsselung, wobei eine «Geheimsprache» oder ein enkryptischer Algorithmus verwendet wird. Die Verknüpfung anonymer Einzeldaten aus verschiedenen Datenquellen schafft die Gefahr der Reidentifikation der betroffenen Person. Je umfangreicher die Menge, desto höher die Wahrscheinlichkeit der Reidentifikation. Auch die örtliche Lokalisierung (Geokodierung) erhöht die Wahrscheinlichkeit der Deanonymisierung.

Im zweiten Teil seines Vortrages ging der Referent auf die Datenverknüpfung ein. Da es keine gesetzliche Definition gibt, machte *Probst* einen Definitionsvorschlag: Datenverknüpfungen sind das Zusammenführen von Einzeldaten aus einer oder mehreren Datenquellen. Gegenstand sind nur Einzeldaten, keine aggregierten Daten. Es können Personen- oder Sachdaten sein, und es kann bloss ein einzelnes Merkmal oder der ganze Inhalt verwendet werden.

Es gibt drei Arten von Datenverknüpfungen. Bei der Abgleichung von Daten – als erste Art – wird die formelle oder inhaltliche Qualität von Daten anhand einer Kontrolldatenmenge überprüft. Ziel ist die formelle Berichtigung oder die materielle Ergänzung. Die zweite Art ist die Longitudinalverknüpfung, das heisst eine Zeitreihenbildung. Dabei werden datenschutzrechtlich problematische Längsprofile über die Zeit erstellt, welche Verhaltensmuster darstellen. Als dritte Art gibt es die Querschnittsverknüpfung, welche eine zeitliche Momentaufnahme aufzeigt.

Für Datenverknüpfungen gibt es verschiedene Rechtsgrundlagen. Als Erste ist das Datenschutzgesetz⁵ zu erwähnen. Art. 3 lit. e DSGVO enthält eine Legaldefinition von Datenbearbeitung. Die Datenverknüpfung fällt als Bearbeitungsform unter diesen Begriff. Bei der Datenverknüpfung können – falls es sich um Daten von natürlichen Personen handelt – Persönlichkeitsprofile entstehen, welche in Art. 3 lit. d DSGVO speziell definiert werden und für welche besondere Regeln gelten. Weitere Rechtsquellen finden sich in Art. 14a des Bundesstatistikgesetzes⁶, Art. 16 Abs. 4 des Registerharmonisierungsgesetzes⁷ sowie Art. 26 Abs. 2 und 3 der Volkszählungsverordnung⁸.

Abschliessend fasste der Vortragende die wichtigsten Rechtsprobleme bei Datenverknüpfungen zusammen. Bedeutsamstes Problem ist die Entstehung von Persönlichkeitsprofilen, welche durch Verknüpfung von Personendaten erstellt werden können. Ein weiteres Problem ist die Reidentifikation und Deanonymisierung von Nichtpersonendaten. Bezüglich der Bekanntgabe von Daten muss bei der Offenbarungspflicht eine gesetzliche Grundlage und bei der freiwilligen Offenbarung eine gültige Einwilligung vorliegen. Zum Schluss äusserte *Probst* den Verdacht, dass im öffentlichen Recht die heute bestehende Datenschutzgesetzgebung nicht genüge, um die Datenverknüpfung zu regeln. Danach wäre die aktuelle Regelung nicht ausreichend. Bezüglich des Privatrechts wies der Referent auf

eine Lücke in der Gesetzgebung hin: Die Regelungen betreffend Persönlichkeitsprofil schützen nur natürliche Personen. Die Rechtslage bezüglich juristischer Personen ist nicht geklärt.

III. Datenverknüpfungen in der Praxis, ein Problemaufriss unter besonderer Berücksichtigung der Statistik

*Rolf Ritschard*⁹ widmete sich in seinem Vortrag der Datenverknüpfung in der Praxis. Er präsentierte einen Problemaufriss unter besonderer Berücksichtigung der Statistik.

Der Referent umschrieb eine Datenverknüpfung als Vorgang, in dem Merkmale einer (natürlichen oder juristischen) Person, einer Personengruppe oder von Sachobjekten verbunden werden. Die Merkmale einer natürlichen Person lassen sich in drei Datenschutzzustufen einteilen. Ein Beispiel für einfache Merkmale ist die Körpergrösse. Der Beruf gehört zu den qualifizierten Merkmalen. Besonders schützenswerte Merkmale sind beispielsweise Krankheiten. *Ritschard* wies darauf hin, dass es in der Statistik bis heute keine Persönlichkeitsprofile gibt.

Wichtigste Datenquellen in der Statistik sind Umfragen bei der Bevölkerung oder bei Unternehmen sowie Registererhebungen. Umfragen finden mündlich, schriftlich oder via Internet statt. Register, welche als Grundlage von statistischen Erhebungen dienen, sind einerseits statistische Register (zum Beispiel das Stichprobenregister: Name, Adresse, Telefonnummer) und andererseits administrative Register (zum Beispiel kantonale oder kommunale Einwohnerregister). Es gibt auch Mischformen von administrativen und statistischen Registern (zum Beispiel das Gebäude- und Wohnungsregister oder das Betriebs- und Unternehmensregister).

Statistische Verknüpfungen entstehen, wenn Daten aus mehreren Datenquellen oder aus einer Datenquelle, aber in verschiedenen Zeitpunkten gesammelt werden. Werden Daten aus nur einer Datenquelle erhoben, handelt es sich nicht um eine statistische Verknüpfung. Es gibt drei Kategorien von Verknüpfungen: technische Verknüpfungen, Verknüpfungen mit Schlüsselmerkmalen und thematisch relevante Verknüpfungen. Technische Verknüpfungen sind beispielsweise Verknüpfungen von Personenbezeichnungen mit Hilfsmerkmalen (Namen, Adressen, Telefonnummern) oder Datenabgleiche (Validierung von Daten). Bei Verknüpfungen mit Schlüsselmerkmalen werden zum Beispiel folgende Merkmale verwendet: Merkmale des Stichprobenregisters, des Einwohnerregisters, des Betriebs- und Unternehmensregisters oder Merkmale, welche mit Umfragen erfasst wurden. Beispiele der thematisch relevanten Verknüpfungen sind Datenquellen für die Analyse zur Rückfälligkeit von verurteilten Personen oder Datenquellen der Volkszählung 2010.

Zum Schluss stellte *Ritschard* das Projekt SESAM¹⁰ vor. Dieses Projekt hat zum Ziel, die Beschäftigung und die Sozialversicherungen in einen Zusammenhang zu bringen

⁵ Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG), SR 235.1.

⁶ Bundesstatistikgesetz vom 9. Oktober 1992 (BStatG), SR 431.01.

⁷ Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister vom 23. Juni 2006 (Registerharmonisierungsgesetz, RHG), SR 431.02.

⁸ Verordnung über die eidgenössische Volkszählung vom 19. Dezember 2008 (Volkszählungsverordnung), SR 431.112.1.

⁹ *Rolf Ritschard*, lic. phil. I, Soziologe, ehemaliger Direktionsadjunkt des Bundesamtes für Statistik, Walkringen.

¹⁰ Synthesestatistik soziale Sicherheit und Arbeitsmarkt. Weitere Informationen sind unter http://www.bfs.admin.ch/bfs/portal/de/index/infoteh/erhebungen_quellen/blank/blank/sesam/01.html zu finden. Die Statistik ist trotz Namensgleichheit vom gescheiterten Projekt über die psychische Gesundheit in der Familie zu unterscheiden.

und diesen zu analysieren. Es werden Informationen aus folgenden Datenquellen verknüpft: Schweizerische Arbeitskräfteerhebung (SAKE) und verschiedene Register der Sozialversicherungen (AHV, IV, EL, ALV). Die Daten werden über mehrere Schritte miteinander verknüpft. Bei der Bearbeitung der auf diese Weise pseudonymisierten Daten werden die Datenschutzvorschriften eingehalten.

IV. Datenverknüpfung in ausgewählten Bereichen: Gesundheitswesen

Am Anfang seiner Präsentation umschrieb *Thomas Casanova*¹¹ den Begriff Verknüpfung. Demnach ist eine Verknüpfung die allgemeine Verbindung von zwei oder mehreren Dingen oder Daten. Im Vordergrund des Vortrages steht die Datenverknüpfung im Gesundheitswesen. Aus der Sicht des Patienten gibt es verschiedene Datenquellen: Behörden, Hausarzt, Spital/Heim, Versicherungen, Arbeitgeber, Familie usw. Aus der Sicht eines Spitals gibt es ebenso verschiedene Datenquellen, welche weitere Quellen enthalten: Behörden, Dritte, medizinische Aussenstellen, Patientenumfeld, Versicherungen usw.

Der Vortragende ging kurz auf die datenschutzrechtlichen Grundsätze ein. Die Grundsätze sind ausdrücklich im Datenschutzgesetz verankert. Das Prinzip der Gesetzmässigkeit¹² besagt, dass Daten nur bearbeitet werden dürfen, wenn dafür eine gesetzliche Grundlage vorliegt. Die Datenbearbeitung muss verhältnismässig¹³ sein. Die Daten dürfen nur zum angegebenen Zweck¹⁴ bearbeitet werden. Zur Gewährung der Datensicherheit¹⁵ müssen die Daten durch angemessene Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Der betroffenen Person steht das Recht auf Auskunft¹⁶ zu. Sie kann beim Datenbearbeiter Einsicht in sie betreffende Daten verlangen.

Anschliessend befasste sich der Referent mit den rechtlichen Rahmenbedingungen. Im Krankenversicherungsgesetz¹⁷ finden sich keine Regelungen, welche die Verknüpfung von Gesundheitsdaten, die im weitesten Sinne medizinische Informationen enthalten, zum Inhalt haben. Ebenso wenig enthält das Unfallversicherungsgesetz¹⁸ entsprechende Regelungen. Auch in kantonalen Gesetzen (zum Beispiel Gesundheitsgesetze, Patientenrechtsgesetze) und weiteren Spezialgesetzen (AHVG¹⁹, IVG²⁰, ATSG²¹, StGB²²) sind keine Regelungen ersichtlich. Als Zwischenfazit hielt der Referent fest, dass keine Grundlagen für die Berechtigung von Verknüpfungen von Daten

zwischen öffentlich-rechtlichen Spitälern und Dritten zu finden sind.

Soll die IT-Krankendatenbearbeitung durch Outsourcing ausgelagert werden, müssen insbesondere die Grundsätze in Art. 10a DSGVO eingehalten werden. Das heisst, dass die Daten nur so bearbeitet werden dürfen, wie der Auftraggeber selbst es tun dürfte, sowie dass nur eine Bearbeitung stattfinden darf, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Als weitere wichtige Rechtsgrundlage ist Art. 321 StGB zu erwähnen. Hier stellt sich insbesondere die Frage der Zurechnung von Handlungen von Hilfspersonen. Eine Hilfsperson ist eine Person, die bei der Berufstätigkeit des Geheimnisträgers in einer Weise mitwirkt, dass sie grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält. Nach der Meinung des Bundesamtes für Gesundheit ist ein Outsourcing möglich. Der eidgenössische Datenschutzbeauftragte ist gegenteiliger Auffassung. Da kein Hilfspersonenstatus gemäss Art. 321 StGB vorliege, sondern Hilfspersonen im Sinne von Art. 101 OR²³ beteiligt seien, ist Outsourcing seiner Ansicht nach nur bei Einwilligung zulässig. Casanova vertritt den Standpunkt, dass Outsourcing zulässig sei, weil es sich um Hilfspersonen im Sinne von Art. 321 StGB handle. Dies sei eine Organisationsfrage. Das entscheidende Kriterium sei die Mitwirkung bei der Tätigkeit des Geheimnisträgers, hier des Arztes.

Beim Fallmanagement zeigt sich ein anderes Bild. Es handelt sich nicht um Hilfspersonen, sondern um eine eigenständige Tätigkeit. Die Basis sind Vereinbarungen zwischen den Krankenkassen und den Spitälern. Es liegt keine gesetzliche Grundlage vor. Die Vereinbarungen ersetzen die fehlende gesetzliche Grundlage nicht. Dies ist im Ergebnis unstrittig.

Als Fazit hielt der Redner fest, dass Verknüpfungen eine gesetzliche Grundlage benötigen. Im privaten Bereich bedürfen Verknüpfungen eines Rechtfertigungsgrundes. Werden in öffentlich-rechtlichen Spitälern im spitalinternen Bereich Daten verknüpft, ist dies nur unter Berücksichtigung der geltenden Grundsätze des Datenschutzgesetzes möglich.

V. Die Profilbildung

Nach verschiedenen Ateliers, in welchen die Gelegenheit bestand, einzelne Themen zu vertiefen (Amtshilfe und Datenschutz, Aus der Praxis des EDÖB: Diskussion ausgewählter Fälle, unter besonderer Berücksichtigung der Kreditauskunftserteilung, Datenschutz und Öffentlichkeitsprinzip, Datenverknüpfung im Versicherungswesen), ging *Jean-Philippe Walter*²⁴ auf das Thema der Profilbildung ein. In der heutigen digitalisierten Zeit verliert das Individuum die Beherrschung über es betreffende Informationen. Die Internettechnologie ermöglicht die Entwicklung von Individualisierungsmechanismen, welche die Handlungen und damit verbundenen Entscheidungen von Einzelnen systematisch aufzeigen. Dies basiert auf der Akkumulierung von Daten, welche die Profilbildung über eine Einzelperson zu-

¹¹ *Thomas Casanova*, Lic. iur., Rechtsanwalt, Datenschutzbeauftragter der kantonalen Verwaltung des Kantons Graubünden, Chur.

¹² Art. 4 Abs. 1 DSGVO.

¹³ Art. 4 Abs. 2 DSGVO.

¹⁴ Art. 4 Abs. 3 DSGVO.

¹⁵ Art. 7 DSGVO.

¹⁶ Art. 8 DSGVO.

¹⁷ Bundesgesetz über die Krankenversicherung vom 18. März 1994 (KVG), SR 832.10.

¹⁸ Bundesgesetz über die Unfallversicherung vom 20. März 1981 (UVG), SR 832.20.

¹⁹ Bundesgesetz über die Alters- und Hinterlassenenversicherung vom 20. Dezember 1946 (AHVG), SR 831.10.

²⁰ Bundesgesetz über die Invalidenversicherung vom 19. Juni 1959 (IVG), SR 831.20.

²¹ Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000 (ATSG), SR 830.1.

²² Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

²³ Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (OR), SR 220.

²⁴ *Jean-Philippe Walter*, Dr. iur., Stellvertreter des eidgenössischen Datenschutzbeauftragten, Bern.

lässt. Diese Möglichkeiten sind sowohl für die Wirtschaft wie auch für die öffentliche Verwaltung von Interesse. Jedoch trägt die Herstellung von Profilen auch Risiken in sich. Aufgrund des entstandenen Profils kann das Auswahlverhalten einer Person beeinflusst werden.

Bei der Profilbildung als Datenbearbeitungsart entstehen datenschutzrechtliche Bedenken. Durch diese Art von Datensammlung werden Informationen aufgedeckt, welche für das Individuum, das Entscheidungen trifft oder ein bestimmtes Verhalten an den Tag legt, nicht ersichtlich sind. Auch fehlt die Transparenz, weil Daten im Unwissen des Internetbenutzers bearbeitet werden. Für die betroffene Person ist es schwierig, ihre Rechte geltend zu machen. Es besteht die Gefahr der ungerechtfertigten Zuweisung zu einer Profilgruppe.

In der Folge erläuterte der Referent einige Begriffe. Die Profilerstellung definiert sich als Technik der Überwachung und Auswertung von Daten, welche verschiedene Verhaltensweisen eines Individuums betreffen und dieses charakterisieren. Es handelt sich um eine computerisierte Informationsverarbeitungsmethode, welche sich mit Datensammelverfahren behilft und es erlaubt, die Daten mit einer gewissen Wahrscheinlichkeit zu klassieren. Mit einer gewissen Fehlerrate kann dann ein Individuum in eine besondere Kategorie eingeordnet werden. Es wird zwischen abstrakter und spezieller Profilbildung unterschieden. Die Profilbildung ist abstrakt, wenn sie auf Daten basiert, welche nicht jene von der betroffenen Person sind (Gruppenprofile). Spezifisch ist die Profilbildung, wenn sie auf dem Verbund von der betroffenen Person zugehörigen Daten beruht (Individualprofil). Es gibt verschiedene Arten von Profilen: vorhersagendes Profil (Personenbeobachtung über die Zeit, beispielsweise die Aufzeichnung von getätigten Klicks im Internet), eindeutiges Profil (basierend auf von der betroffenen Person selbst gelieferten Daten, zum Beispiel die Registrierung bei einem Onlinedienst oder die Veröffentlichung in einem sozialen Netzwerk), Gruppenprofil (Profilbildung aus einer Population und Gegenüberstellung einer bestimmten Person mit dem Ziel, ihr Charakteristiken zuzuschreiben), Individualprofil (Profilbildung aus Daten der betroffenen Person).

Walter benannte einige typische Ziele der Profilbildung. Der Zweck von Profilen ist die Kundenbeziehungsverwaltung (Kundenbindung, Lokalisation von potenziellen Kunden, Identifikation von Interessen empfänglicher Kunden für ein neues Produkt, privilegierte Angebote usw.), die Risikoverwaltung (differenzierte Versicherungsprämien, schlechte Zahler, Solvenz, Gesundheit, Risiko für krimi-

nelle Aktivität usw.) und die zukunftsorientierte Personenverwaltung (Kennzeichnung von Talenten, Markierung von Kompetenzen usw.).

Bezüglich der datenschutzrechtlichen Regelung hielt der Referierende fest, dass aktuell keine spezifischen Anordnungen vorliegen. Art. 3 lit. d DSGVO definiert das Persönlichkeitsprofil. Diese Regelung hat nur eine beschränkte Tragweite, weil nur auf Individualprofile abgezielt wird. Die Definition ist darüber hinaus generell gehalten und weist eine grosse Interpretationsspanne auf. Art. 15 der EG-Richtlinie 96/46²⁵ erwähnt die automatisierte Einzelentscheidung. Demnach ist einzelnen Personen grundsätzlich ein Recht einzuräumen, keiner Entscheidung unterworfen zu werden, die ausschliesslich aus einer automatisierten Datenverarbeitung hervorgeht (Abs. 1). Unter bestimmten Voraussetzungen kann ein Individuum dennoch einer solchen Entscheidung unterworfen werden (Abs. 2) – beispielsweise beim Abschluss oder bei der Erfüllung eines Vertrages.

De lege ferenda gibt es ein Projekt einer Empfehlung des Europarats, welche einen rechtlichen Rahmen definieren soll, der ein ausgewogenes Gleichgewicht zwischen dem Datenschutz von Einzelnen und den Interessen der mit Profilen Arbeitenden herstellt. In der Empfehlung werden die Bedingungen für das Sammeln und die Bearbeitung von personenbezogenen Daten für die Profilbildung, die Information und die Rechte der betroffenen Personen, die Datensicherheit und die Überwachung festgehalten. Walter formulierte einige Vorschläge für die Umsetzung des Datenschutzes im Rahmen einer zukünftigen Gesetzgebung. Es brauche eine weite Interpretation des Konzepts der persönlichen Daten. Die Profilerstellung aus Daten von Kindern sollte verboten werden. Das Zweckgebundenheitsprinzip müsse respektiert und die Transparenz sowie die Information durchgesetzt werden. Zur Verwirklichung der Rechte müsse für betroffene Einzelne die Möglichkeit bestehen, sich gegen Entscheidungen der automatisierten Profilbildung zu wehren. Ebenso müsse die Durchsetzung von Sanktionen sichergestellt werden.

Der Vortragende kam abschliessend zu folgender Konklusion: Angesichts der heute eingesetzten Profilbildungstechniken muss das Recht auf informationelle Selbstbestimmung eine neue Dimension annehmen. Die modernen Informationstechnologien und Kommunikationsformen sollten für den Menschen eine positive Dienstleistung darstellen und nicht umgekehrt: Das Individuum darf nicht deren Sklave sein!

²⁵ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, 31–50.