



Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht

Personendaten und anonymisierte Einzeldaten in der globalisierten Informationsgesellschaft – Quo vaditis?

THOMAS PROBST

Das schweizerische und europäische Datenschutzrecht basiert auf dem zentralen Begriff der Personendaten und deren zuverlässigen Abgrenzung von den Nicht-Personendaten. Dieses Konzept stammt aus einer Zeit, als das Internet noch nicht jedermann als weltumspannendes Kommunikationsmittel zur Verfügung stand, um die Identität einer von Daten betroffenen Person zu bestimmen. In der heutigen Informationsgesellschaft nehmen die Möglichkeiten der «Bestimmbarkeit» einer Person aufgrund des technologischen Fortschritts und der immer breiteren Anwendung von Datenverknüpfungen laufend zu. Es ist deshalb dringend nötig, dass Rechtswissenschaft und Praxis sich vertiefter mit dem datenschutzrechtlichen Kernbegriff der Personendaten auseinandersetzen, namentlich mit der zentralen Frage des relevanten Beurteilungshorizonts bei der Bestimmung der «Bestimmbarkeit» der Identität einer betroffenen Person. Der vorliegende Beitrag macht einen ersten Schritt in diese Richtung.

Le droit de la protection des données, tant au niveau européen que suisse, est basé sur la notion fondamentale des données personnelles et leur délimitation fiable des données non-personnelles. Ce concept date d'une période où Internet n'était pas encore accessible à tout le monde comme moyen de communication universel. Dans notre société moderne dite de l'information, le progrès technologique et le recours progressif à des appariement de données ne cessent de faciliter l'identification d'une personne concernée par des données. Aussi est-il urgent que la science et la pratique juridiques s'apprentent à examiner de plus près la notion centrale de données personnelles, tout particulièrement la question essentielle de savoir de quel point de vue il faut déterminer si une personne concernée est identifiable ou non. La présente contribution fait un premier pas dans ce sens.

Inhaltsübersicht

- I. Einleitung
- II. Ausgangsfrage: Welche Daten stellen datenschutzrechtlich geschützte «Personendaten» dar?
 1. Allgemeines
 2. Zwei Illustrationsbeispiele
 - a. Die Sozialversicherungsnummer
 - b. Die IP-Adresse von Netzwerk-Computern
 3. Zwischenergebnis
- III. Eine rechtsvergleichender Blick auf ausländische Rechtsordnungen
 1. Überblick
 - a. Europäische Union/Euoparat
 - b. Deutschland
 - c. Frankreich
 - d. Spanien
 - e. Portugal
 - f. Vereinigtes Königreich
 2. Fazit
- IV. Rechtsprechung in der Schweiz
 1. BGE 136 II 508
 2. BGE 138 II 346
- V. Kriterien zur Bestimmung der «Bestimmbarkeit» der von Daten betroffenen Person
 1. Allgemeines
 2. Welcher Beurteilungshorizont ist massgeblich?
 - a. Stand der Gesetzgebung
 - b. Stand der Rechtsprechung

- c. Stand der Lehre
- d. Fazit

- VI. Ansätze für eine Fallgruppenbildung zur Bestimmung der «Bestimmbarkeit» der betroffenen Person
 1. Erörterung von vier Sachverhaltsvarianten
 - a. Variante 1 (einseitiger Datenerwerb)
 - b. Variante 2 (bilaterale Datenweitergabe)
 - c. Variante 3 (multilaterale Datenweitergabe)
 - d. Variante 4 (Datenveröffentlichung)
 2. Grundsätze zur Bestimmung des Beurteilungshorizonts
- VII. Schlussfolgerung

I. Einleitung¹

Ein Kernbegriff des schweizerischen Datenschutzrechts ist jener der *Personendaten*. Gemäss Bundesverfassung

¹ Der vorliegende Aufsatz ist meinem Fakultätskollegen *Paul-Henri Steinauer* gewidmet und hätte ursprünglich in seiner *Festschrift* zum 65. Geburtstag erscheinen sollen, erwies sich aber als zu umfangreich, weshalb er in dieser Fachzeitschrift erscheint. Paul-Henri Steinauer ist ein Meister des ZGB. Ob Personenrecht, Familienrecht, Erbrecht oder Sachenrecht – überall ist er mit seinen überragenden Rechtskenntnissen zu Hause. Davon legen nicht zuletzt seine fundierten, präzise und verständlich geschriebenen Lehrbücher beredtes Zeugnis ab. Auf dem Gebiet des Personenrechts haben ihn u.a. auch Fragen des *Datenschutzes* beschäftigt (namentlich als ehemaliger Vizepräsident der Eidgenössischen Datenschutz- und Öffentlichkeitskommission sowie in seinen beiden Beiträgen «La jurisprudence de la Commission fédérale de la protection des données et de la transparence au sujet du traitement de données par des personnes privées», ZBl 2007,

ist jede (natürliche und juristische²) Person vor dem Missbrauch ihrer *persönlichen* Daten geschützt bzw. zu schützen³. Damit hat der Verfassungsgeber – und ihm notwendigerweise folgend auch der Gesetzgeber⁴ – den Begriff der Personendaten zum *Triangulationspunkt* des Datenschutzrechts gemacht⁵: Während *Personendaten* in den Schutzbereich der einschlägigen Datenschutzgesetzgebung fallen⁶, stehen *Nicht-Personendaten* ausserhalb deren Schutzes⁷. Dieses datenschutzrechtliche Konzept

basiert auf der grundlegenden *Hypothese*, dass die Kategorie der (geschützten) *Personendaten* sich zuverlässig von der Kategorie der (nicht geschützten) *Nicht-Personendaten* abgrenzen lässt, da der Datenschutz als Teilaspekt des Schutzes der Persönlichkeit verstanden wird⁸.

Der vorliegende Beitrag überprüft diese Hypothese und zeigt auf, dass der Begriff der Personendaten weit *weniger klar* ist, als man annehmen könnte, und dass die *Abgrenzung* von *Personendaten* und *Nicht-Personendaten* in einer globalisierten Informationsgesellschaft sich allmählich zu verflüchtigen droht. Dieser schleichende Prozess stellt die Funktionsfähigkeit des Begriffs der Personendaten als Kernbegriff des Datenschutzes in Frage und führt zu wachsender Rechtsunsicherheit.

In einem ersten Schritt soll die Problemlage anhand von *zwei Beispielen* konkretisiert und illustriert werden (Abschnitt II). Anschliessend wird ein *rechtsvergleichender* Blick auf entsprechende *ausländische Gesetzesbestimmungen* geworfen (Abschnitt III) und sodann die Auslegung der schweizerischen Gesetzesbestimmungen durch die *Rechtsprechung* betrachtet (Abschnitt IV). In einem nächsten Schritt wird untersucht, nach welchen *Kriterien* die Bestimmbarkeit der Identität einer von Daten betroffenen Person festgestellt werden kann bzw. soll (Abschnitt V), um auf dieser Grundlage dann kategorisierende *Differenzierungen* (Fallgruppen) vorzuschlagen (Abschnitt VI). Kurze *Schlussfolgerungen* schliessen den Beitrag ab (Abschnitt VII).

II. Ausgangsfrage: Welche Daten stellen datenschutzrechtlich geschützte «Personendaten» dar?

1. Allgemeines

Das schweizerische Datenschutzgesetz (DSG) versteht unter dem Begriff der «Personendaten» Angaben⁹ über eine Person, die entweder *bestimmt* oder zumindest *bestimmbar* ist («informations qui se rapportent à une personne *identifiée ou identifiable*»; «informazioni relative a

374 ff. und «Le droit d'action des associations visant à défendre la personnalité de leurs membres, en particulier en matière de protection des données», in: Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, Bern 1999, 495 ff.). Grund genug, um zu seinen Ehren einer Frage nachzugehen, die – trotz ihrer *theoretischen und praktischen Relevanz* und Evidenz – von der Wissenschaft bisher zu wenig thematisiert worden ist. – Als Ausnahmen seien erwähnt: SEVERIN BISCHOFF/RAINER J. SCHWEIZER, Der Begriff der Personendaten, *digma* 2011, 152 ff.; vgl. sodann auch ORSOLYA FERCSIK SCHNYDER/ROLF H. WEBER, «Was für 'ne Sorte von Geschöpf ist euer Krokodil» – Zur datenschutzrechtlichen Qualifikation von IP-Adressen, *sic!* 2009, 577 ff.

² Während in vielen ausländischen Rechtsordnungen nur *natürliche* Personen in den Geltungsbereich des Datenschutzes fallen – vgl. z.B. § 3 (1) des *deutschen* Bundesdatenschutzgesetzes; Art. 1 der *französischen* Loi n° 2004–801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (im Folgenden: «französisches Datenschutzgesetz») sowie Art. 1 der *spanischen* Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal –, sind nach schweizerischer Auffassung auch *juristische* Personen geschützt (vgl. statt vieler BGE 138 III 429; RAINER J. SCHWEIZER, in: Bernhard Ehrenzeller et al. [Hrsg.], Die schweizerische Bundesverfassung, Kommentar, 2. A., Zürich/St. Gallen 2008, Art. 13 N 40). – Auf Gesetzesebene vgl. namentlich Art. 3 lit. b des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG, SR 235.1), wonach «betroffene Personen»: natürliche oder juristische Personen, über die Daten bearbeitet werden», sind.

³ Vgl. Art. 13 Abs. 2 BV («Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten»). – Diese Formulierung ist zu eng ausgefallen, da es inhaltlich nicht bloss um den *Datenmissbrauch*, sondern viel grundlegender um das Grundrecht auf *informationelle Selbstbestimmung* geht (vgl. SCHWEIZER [FN 2], BV N 39).

⁴ Vgl. Art. 1, 2 und 3 lit. a DSG.

⁵ Vgl. auch BGE 136 II 508, 522. – Für die EU ist Art. 16 AEUV massgeblich, wonach jede Person das Recht «auf Schutz der sie betreffenden personenbezogenen Daten» hat.

⁶ Siehe namentlich das (schweizerische) DSG sowie die Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11).

⁷ Inwieweit *Nicht-Personendaten* ausserhalb des DSG durch *anderweitige* Rechtsnormen geschützt sind, ist im *Einzelfall* zu prüfen. Ein allgemeiner Verweis auf Art. 28 ZGB oder Art. 179^{novies} StGB – (so z.B. bei FERCSIK SCHNYDER/WEBER [FN 1], 578) – ist nicht zielführend, da auch diese Bestimmungen an die *Persönlichkeit* (Art. 28 ZGB) bzw. das unbefugte Beschaffen von *Personendaten* anknüpfen (Art. 179^{novies} StGB).

⁸ Vgl. dazu die allgemeine privatrechtliche Bestimmung in Art. 28 ZGB sowie BGE 138 III 346, 358; Art. 1, 15 DSG; DAVID ROSENTHAL, in: David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008, Art. 3 lit. a N 1.

⁹ Als «Angaben» sind alle (auch falsche) Informationen (Tatsachen, Werturteile oder Kombinationen davon) zu betrachten, unabhängig von *Form* (z.B. Zeichen, Wort, Bild, Ton) und *Datenträger* (z.B. Papier, Leinwand, elektronischer Träger). Vgl. auch ROSENTHAL (FN 8), Art. 3 lit. a N 8 ff.

una persona *identificata o identificabile*)¹⁰. Das Gesetz unterscheidet demnach zwei Konstellationen:

- Falls Angaben über eine Person direkt deren *Identität* offenbaren, liegen – im Sinne der *ersten* Konstellation – Informationen über eine *bestimmte* Person vor, welche als Personendaten unter dem Schutz des DSG stehen. Dies trifft etwa auf eine *Visitenkarte* (mit Angabe von Namen, Adresse und Telefonnummer), eine *Identitätskarte* oder einen *Pass* (mit Foto, Namen, Geburtsdatum, Geschlecht, Grösse und Heimatort) zu¹¹ und bietet in der Praxis kaum Schwierigkeiten, da das Vorliegen von Personendaten in solchen Fällen evident ist.
- Anders präsentiert sich die Lage bei der *zweiten* Konstellation, wo Angaben über eine Person vorliegen, aus denen sich zwar deren Identität *nicht* ergibt, aber durch den Einbezug weiterer Angaben, d.h. durch *Verknüpfung* mit *zusätzlichen Informationen*, die Identität der betroffenen Person immerhin *bestimmbar* wird¹². Wer z.B. die Telefonnummer, die Fahrzeug-Kennnummer oder das Geburtsdatum einer ihm nicht bekannten Person kennt, verfügt erst dann über (geschützte) Personendaten – im Sinne der *zweiten* Alternative nach DSG –, wenn weitere Informationen (z.B. Name, Wohnort oder Beruf) hinzukommen, welche die Identität der Person *bestimmbar* machen. Bei dieser Konstellation hängt also das Vorliegen von Personendaten davon ab, ob durch die *Verknüpfung* mit *weiteren Informationen*¹³ die Identität der betroffenen Person festgestellt werden kann oder nicht. Ob dies der Fall ist, wird weitgehend durch den *Umfang* und die *Qualität* der verfügbaren Zusatzinformationen bestimmt. Welche zusätzlichen Informationen verfügbar gemacht werden können, hängt wiederum vom *zeitlichen* und *finanziellen Aufwand* ab, den jemand zu betreiben bereit ist, um weitere Informationen über die betroffene Person zu beschaffen¹⁴. Im Rahmen ei-

ner *Kosten-Nutzen Abwägung* wird dieser Aufwand sowohl vom verfolgten (rechtsstaatlichen, wirtschaftlichen, ideellen oder anderweitigen) *Interesse*, das jemand an der Identifizierung einer gewissen Person hat, als auch von den *technischen* und *rechtlichen* Möglichkeiten der Informationsbeschaffung in einer globalisierten Informationsgesellschaft bestimmt, wo z.B. Google, Facebook und Twitter zu viel benutzten Informationskanälen geworden sind¹⁵. Die Bestimmbarkeit der Identität einer Person, über die gewisse Angaben vorliegen, hängt somit von einer *Vielzahl* von *Faktoren* ab, deren gegenseitiges Verhältnis und relative Bedeutung noch wenig geklärt sind. Oder um es – wie im Titel zu diesem Beitrag – etwas prägnanter auf den Punkt zu bringen: Der Begriff der *Bestimmbarkeit* der Identität einer Person als Kernbegriff des Datenschutzrechts ist weitgehend *unbestimmt*. Zwei Beispiele mögen dies konkretisieren und illustrieren.

2. Zwei Illustrationsbeispiele

a. Die Sozialversicherungsnummer

Jede in der Schweiz wohnhafte (natürliche) Person erhält von der Zentralen Ausgleichsstelle (ZAS) eine *Sozialversicherungsnummer* zugeordnet¹⁶, welche die eindeutige Identifizierung dieser Person ermöglicht¹⁷. Während früher die – im Volksmund meist als «AHV-Nummer» bezeichnete – elfstellige Zahlenfolge die Anfangsbuchstaben des Familiennamens, das Geburtsdatum sowie das Geschlecht und die Nationalität (Schweizerbürger oder Ausländer) in arithmetischer Form abbildete¹⁸, ist die – seit dem 1. Juli 2008 schrittweise eingeführte – dreizehnstellige neue Sozialversicherungsnummer¹⁹

¹⁰ Art. 3 lit. a DSG umschreibt den Begriff der *Personendaten* als «alle Angaben, die sich auf eine *bestimmte* oder *bestimmbare* Person beziehen.» (Hervorhebung ergänzt).

¹¹ Vgl. auch BGE 138 II 346, 353.

¹² Vgl. BGE 138 II 346, 353; BGE 136 II 508, 514.

¹³ Zur Grundproblematik der Verknüpfung von Daten: THOMAS PROBST, Die Verknüpfung von Personendaten und deren rechtliche Tragweite, in: Astrid Epiney/Thomas Probst/Nina Gammethaler (Hrsg.), Datenverknüpfung – Problematik und rechtlicher Rahmen, Zürich/Basel/Genf 2011, 1 ff. – Die Vornahme von Datenverknüpfungen im Bereich der Statistik hat der Gesetzgeber in Art. 14a des BStatG (Bundesstatistikgesetz vom 9. Oktober 1992) geregelt; SR 431.01. Die zugehörigen Verordnungsbestimmungen werden voraussichtlich Anfang 2014 in Kraft treten.

¹⁴ Vgl. auch BGE 138 II 346, 354; BGE 136 II 508, 514.

¹⁵ Vgl. auch BGE 138 II 346, 353 f.; BGE 136 II 508, 514.

¹⁶ Siehe Art. 133^{bis} AHVV (Verordnung über die Alters- und Hinterlassenenversicherung vom 31. Oktober 1947; SR 831.101).

¹⁷ Für weitere Einzelheiten siehe Art. 53c AHVG (Bundesgesetz über die Alters- und Hinterlassenenversicherung vom 20. Dezember 1946; SR 831.10).

¹⁸ Siehe der frühere Art. 133 aAHVV («Die Versichertennummer ist elfstellig und setzt sich zusammen aus: a. einer dreistelligen Zifferngruppe aufgrund des Namens; b. den letzten beiden Ziffern des Geburtsjahres; c. einer dreistelligen Zifferngruppe bestehend aus einer Ziffer für das Geburtsquartal und das Geschlecht und zwei Ziffern für den Tag der Geburt innerhalb des Quartals; d. einer zweistelligen, nach Schweizern und Ausländern differenzierten Ordnungsnummer und einer einstelligen Prüfziffer.»).

¹⁹ Die neue Sozialversicherungsnummer besteht aus dem dreistelligen *Ländercode* «756» für die Schweiz, einer *neunstelligen*, eindeutigen zufallsgenerierten Ziffer ohne Rückschlussmöglichkeit und einer *Kontrollziffer*. Vgl. Art. 133 AHVV.

eine sogenannte *nicht-sprechende* Nummer, die *keinerlei Rückschlüsse* auf die betroffene Person zulässt²⁰. Die Identität der betroffenen Person ist daher aus der neuen Sozialversicherungsnummer *per se* nicht ersichtlich, weshalb diese Nummer *kein* geschütztes Personendatum im Sinne der *ersten* Alternative von Art. 3 lit. a DSG («bestimmte» Person) darstellt. Ob im Sinne der *zweiten* Alternative von Art. 3 lit. a DSG («bestimmbare» Person) die Bestimmbarkeit der Identität der betroffenen Person gegeben ist, hängt davon ab, ob mit vernünftigen Aufwand die Verknüpfung mit zusätzlichen Informationen möglich ist, welche die Identität des Trägers der Sozialversicherungsnummer zu bestimmen erlauben.

Bei der (früheren) elfstelligen (sprechenden) AHV-Nummer war dies einfacher möglich, da mit den im Internet zugänglichen Informationen²¹ ohne viel Aufwand die ersten Buchstaben des *Familiennamens*, das *Geburtsdatum*, das *Geschlecht* und die *Nationalität* (Schweizer oder Ausländer) abgeleitet werden konnten. Durch diese, aus der AHV-Nummer ableitbaren Informationen wurde ein Rückschluss auf die Identität des Trägers der AHV-Nummer wesentlich erleichtert. Bei der neuen dreizehnstelligen (nichtsprechenden) Sozialversicherungsnummer sind entsprechende Ableitungen dagegen nicht mehr möglich, weshalb hier die Bestimmbarkeit der betroffenen Person erschwert ist. Damit ist allerdings die Frage, ob die neue Sozialversicherungsnummer datenschutzrechtlich als (geschütztes) *Personendatum* oder als (nicht geschütztes) *anonymes Einzeldatum* zu qualifizieren ist, nicht beantwortet, denn der Gesetzgeber hat interessanterweise die letztlich *entscheidende Frage offen gelassen*. Es ist dies die Frage, aus *wessen Sicht* die Bestimmbarkeit der Identität der betroffenen Person zu beurteilen ist. Mit anderen Worten, welches ist der massgebliche *Beurteilungshorizont*²²? Ist die Sicht des Datenbearbeiters, die Sicht des Datenherrn, die Sicht des Datenlieferanten, die Sicht des Datenempfängers, die Sicht eines durchschnittlich

interessierten Konkurrenten, die Sicht eines investigativen Journalisten oder schlicht die Sicht eines beliebigen Dritten massgeblich? Ohne einen konkretisierenden *Referenzmasstab* zur Bestimmung des Begriffs der «Bestimmbarkeit» der von Daten betroffenen Person stellt dieser Begriff faktisch eine *Leerformel* dar, die rechtsstaatlichen Massstäben (Bestimmtheitsgebot) nicht genügt und unerwünschte Rechtsunsicherheit verursacht²³.

b. Die IP-Adresse von Netzwerk-Computern

Ähnlich wie jeder Postempfänger eine postalische Zustelladresse besitzt, hat auch jeder ans Internet angeschlossene Rechner bzw. Computer – und damit indirekt dessen Benutzer – eine (statische oder dynamische)²⁴ IP-Adresse²⁵, die den Computer identifizierbar macht. Anhand dieser IP-Adresse können die im Internet versendeten Datenpakete dem richtigen Rechner bzw. Computer als Empfänger zugeordnet werden²⁶. Die traditionelle IP-Adresse (Version 4) besteht aus vier Zahlenblöcken, z.B. 118.27.33.147²⁷. Aus dieser Zahlenfolge lässt sich *per se* die Identität des *PC-Benutzers* nicht bestimmen, weshalb die IP-Adresse *kein* Personendatum gemäss der *ersten* Alternative von Art. 3 lit. a DSG darstellt²⁸. Es stellt sich aber die Frage, ob die Bestimmbarkeit des PC-Benutzers

²⁰ Art. 50c Abs. 3 AHVG («Die Zusammensetzung der Versichertennummer darf keine Rückschlüsse auf die Person zulassen, der die Nummer zugewiesen wird.») und Art. 133 AHVV.

²¹ Siehe z.B. die Angaben unter www.ahvnummer.ch.

²² Vgl. dazu hinten Abschnitt V/2, S. 1431 – Der EuGH hat in seinem Urteil vom 8. November 2007 in Sachen *The Bavarian Lager Co. Ltd & Europäischer Datenschutzbeauftragter gegen Kommission*, Rs. T-194/04, Slg. 2007, II-4523, N 104 – ganz beiläufig und ohne Begründung – die Sozialversicherungsnummer als Personendatum bezeichnet. Daraus lässt sich für die schweizerische Sozialversicherungsnummer *nichts* ableiten, da keinerlei Angaben vorliegen, welche Art von Sozialversicherungsnummer der EuGH damit meinte und er zudem diesbezüglich nichts zu entscheiden hatte, weshalb ein blosses *obiter dictum* vorliegt.

²³ Vgl. hingegen Art. 2 des *französischen* Datenschutzgesetzes, welches sich (redlich, aber ohne durchschlagenden Erfolg) um eine Präzisierung des Begriffs der Bestimmbarkeit bemüht. Ebenso Art. 2 lit. a *Verordnung (EG) Nr. 45/2001* des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (im Folgenden: *Verordnung [EG] Nr. 45/2001*) und Art. 2 lit. a der *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. November 1995, 31 ff.).

²⁴ Während die statische IP-Adresse einem bestimmten Rechner bzw. Computer auf Dauer zugeordnet ist, wechselt die dynamische IP-Adresse bei jeder Verbindung, die der Computer mit dem Internet herstellt, da sie *ad hoc* zugeteilt wird. Vgl. BGE 136 II 508, 514 f. – Für weitere Einzelheiten, siehe z.B. FERCSIK SCHNYDER/WEBER (FN 1), 579 f.

²⁵ Der Anhang zur Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV) vom 6. Oktober 1997 (SR 784.104) gibt folgende Definition: «Internet- oder IP-Adresse (Internetworking Protocol Addresses): Numerischer Kommunikationsparameter, der die Identifikation einer insbesondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglicht.»

²⁶ Siehe auch FERCSIK SCHNYDER/WEBER (FN 1), 578 f.

²⁷ Angaben zur IP-Adresse des eigenen Computers können im Netzwerkcenter mit wenigen Mausklicks gefunden werden.

²⁸ So auch ROSENTHAL (FN 8), Art. 3 lit. a N 27.

mittels der *Verknüpfung* mit weiteren Informationen gemäss der *zweiten* Alternative von Art. 3 lit. a DSGVO gegeben ist. Wie bereits im Fall der Sozialversicherungsnummer hängt die Antwort auf diese Frage weitgehend davon ab, aus *wessen Sicht* die Bestimmbarkeit beurteilt wird. Geht es um die Sicht des Datenbearbeiters, die Sicht des Internetdienst-Anbieters, die Sicht des PC-Benutzers oder die Sicht eines beliebigen Dritten?

3. Zwischenergebnis

Die bisherigen Ausführungen zeigen, dass in der überwiegenden Mehrzahl der praktischen Fälle die *Bestimmbarkeit* des unbestimmten Kriteriums der «Bestimmbarkeit» (der von Daten betroffenen Person) darüber entscheidet, ob die Bearbeitung gewisser Daten in den Geltungsbereich der datenschutzrechtlichen Bestimmungen (namentlich des DSGVO) fällt oder nicht²⁹.

Aus rechtsstaatlicher Sicht ist zu verlangen, dass sich die Umschreibung des *Geltungsbereichs* des Datenschutzes auf semantisch möglichst *klare* und *griffige Kriterien* stützt. Der unbestimmte Begriff der «Bestimmbarkeit» der von Daten betroffenen Person erfüllt diese Anforderung nicht und schafft unerwünschte Rechtsunsicherheit. Es stellt sich daher die Frage, inwieweit die *Rechtsvergleichung* und die *Rechtsprechung* zur Verbesserung der unbefriedigenden Gesetzeslage beitragen können.

III. Eine rechtsvergleichender Blick auf ausländische Rechtsordnungen

1. Überblick

Vor dem Hintergrund von Art. 3 lit. a DSGVO, wonach als *Personendaten* alle Angaben gelten, «die sich auf eine bestimmte oder bestimmbare Person beziehen», ist von Interesse, wie die *Europäische Union* und der *Europarat* sowie der Gesetzgeber in einigen *ausländischen Rechtsordnungen* (namentlich Deutschland, Frankreich, Spa-

nien, Portugal und Grossbritannien) diesen Begriff umschreiben. Dabei wird – angesichts des knappen Raumes, welcher dem vorliegenden Beitrag zur Verfügung steht – naheliegenderweise keine Vollständigkeit angestrebt, sondern beabsichtigt ist nur eine beispielhafte Illustration.

a. Europäische Union/Europarat

aa. Unionsrecht

Im *Unionsrecht* wird der Begriff der «personenbezogenen Daten» in Art. 2 lit. a der *Richtlinie 95/46/EG*³⁰ wie folgt umschrieben:

*«alle Informationen über eine bestimmte oder bestimmbare natürliche Person (betroffene Person); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind»*³¹.

Diese Definition stellt für die «Bestimmbarkeit» der von Daten betroffenen Person auf das Kriterium der *direkten* oder *indirekten Identifizierung* ab. In *Erwägung 26* führt die Richtlinie zur Frage der Bestimmbarkeit der betroffenen Person präzisierend aus, dass *«alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.»* Mit andern Worten: Für die hier interessierende Kernfrage, nach wessen *Beurteilungshorizont* sich die Bestimmbarkeit der Identität der betroffenen Person richtet, nennt die Richtlinie den *Verantwortlichen* der Datenbearbeitung und alternativ jeden *Dritten*.

In der *Verordnung (EG) Nr. 45/2001*³² findet sich unter den Begriffsbestimmungen in Art. 2 lit. a die *wortgleiche Definition* des Begriffs der «personenbezogene Daten».

²⁹ Vgl. auch die Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe vom 20. Juni 2007 zum Begriff der «personenbezogenen Daten», 14 («Allgemein ist eine natürliche Person als «bestimmte Person» anzusehen, wenn sie sich in einer Personengruppe von allen anderen Mitgliedern der Gruppe unterscheidet. Folglich ist die natürliche Person «bestimmbar», wenn grundsätzlich die Möglichkeit besteht, ihre Identität festzustellen [...], auch wenn dies noch nicht geschehen ist. Daher ist diese zweite Alternative in der Praxis die Grenzbedingung, die darüber entscheidet, ob die Information in den Anwendungsbereich des dritten Elements fällt.»).

³⁰ 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, unter den Begriffsbestimmungen, ABl. L 281 vom 23 November 1995, 31 ff.

³¹ Vgl. dazu folgende Entscheidungen des EuGH: Rs. C-342/12, Urteil vom 30. Mai 2013 in Sachen *Worden – Equipamentos para o Lar SA* gegen *Autoridade para as Condições de Trabalho*, N 18 ff.; Rs. T-194/04, Urteil vom 8. November 2007 in Sachen *The Bavarian Lager Co. Ltd & Europäischer Datenschutzbeauftragter gegen Kommission*, Slg. 2007, II-4523, N 104.

³² Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12. Januar 2001, 1 ff.

bb. Europarat-Übereinkommen

Das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, welches am 28. Januar 1981 in Strassburg abgeschlossen wurde und für die Schweiz am 1. Februar 1998 in Kraft getreten ist³³, enthält in Art. 2 lit. a folgende knappe Umschreibung des Begriffs der *personenbezogenen Daten*: «jede Information über eine bestimmte oder bestimmbar natürliche Person (*Betroffener*)». Weiterführende Präzisierungen, welche als Interpretationshilfe zur Konkretisierung des Begriffs der «Bestimmbarkeit» beigezogen werden könnten, enthält das Übereinkommen nicht.

b. Deutschland

§ 3(1) des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BDSG) definiert den Begriff der *personenbezogenen Daten* als «Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person (*Betroffener*)». Auch hier fehlt es an weiteren Präzisierungen, aber aus dem komplementären Begriff der *anonymisierten Daten* lassen sich weitere Anhaltspunkte gewinnen. So umschreibt § 3(6) BDSG den Vorgang des Anonymisierens als «...das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismässig grossen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.» Die Bestimmbarkeit der Identität der von Daten betroffenen Person hat sich also am Zusatzkriterium des *verhältnismässigen Aufwandes* an Zeit, Geld und Arbeitskraft zu orientieren. Auch hier bleibt aber die entscheidende Frage offen, für wen der Aufwand zur Identifizierung der betroffenen Person (un-)verhältnismässig sein muss.

c. Frankreich

In Frankreich findet sich in Art. 2 der *Loi n° 2004–801*³⁴ eine gesetzliche Definition des Begriffs der Personendaten. Danach gilt als

«donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres».

Auch das französische Recht stellt demnach auf die direkte oder indirekte Identifizierbarkeit der betroffenen Person ab. Diese Gesetzesbestimmung enthält zudem folgende Präzisierung:

«Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.»

Analog zum Unionsrecht wird für den *Beurteilungshorizont* der Bestimmbarkeit der Identität (der betroffenen Person) also auf die Perspektive des *Verantwortlichen* der Datenbearbeitung oder alternativ auf die Sicht eines beliebigen *Dritten* abgestellt.

d. Spanien

In Spanien versteht Art. 3 der *Ley orgánica 15/1999*³⁵ unter dem Begriff der Personendaten «cualquier información concerniente a personas físicas identificadas o identificables.» Das spanische Datenschutzrecht stellt damit auf die *Identifizierbarkeit* der von Daten betroffenen Person ab, ohne dieses Kriterium weiter zu präzisieren oder zu erläutern. Auch hier bleibt die Frage nach dem massgeblichen Beurteilungshorizont offen.

e. Portugal

In Portugal definiert die *Lei da protecção de dados pessoais* (Gesetz Nr. 67/98 vom 26 Oktober 1998) in Art. 3 lit. a den Begriff der Personendaten wie folgt:

«qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (*titular dos dados*); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;».

Das portugiesische Recht hält sich damit eng an die unionsrechtlichen Vorgaben und stellt für die Bestimmbarkeit auf die *direkte* oder *indirekte Identifizierung* der betroffenen Person ab, ohne irgendwelche weiteren Ausführungen zum massgeblichen Beurteilungshorizont zu machen.

³³ Zu den Revisionsbestrebungen des Übereinkommens, siehe CECILE DE TERWAGNE, La modernisation de la Convention 108 du Conseil de l'Europe, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, Zürich/Basel/Genf 2012, 23 ff.

³⁴ Loi n° 2004–801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004, 14063.

³⁵ Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

f. Vereinigtes Königreich

Im Vereinigten Königreich umschreibt der *Data Protection Act, No. 25/1988* in Art. 1(1) den Begriff der Personendaten als Daten

«relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller; and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.»³⁶.

Mit dieser Definition orientiert der britische Gesetzgeber die Bestimmbarkeit der Identität der von Daten betroffenen Person am Beurteilungshorizont des *Datenherrn*, indem er darauf abstellt, welche Informationen in dessen Besitz sind. Als *data controller* gilt grundsätzlich jene Person «*who, (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.*»³⁷.

2. Fazit

Aus dem kurzen rechtsvergleichenden Überblick ergibt sich, dass sich im *ausländischen* Recht einzelne Gesetzgeber zumindest bemüht haben, den Begriff der Bestimmbarkeit (der von Daten betroffenen Person) zu *konkretisieren*, um damit die *Rechtsunsicherheit*, welche mit der relativ offenen Gesetzesdefinition der Personendaten verbunden ist, in Grenzen zu halten.

IV. Rechtsprechung in der Schweiz

Vor diesem rechtsvergleichenden Hintergrund stellt sich aus schweizerischer Sicht die Frage, wie hiezulande die *Rechtsprechung* mit der offenen gesetzlichen Umschreibung der Personendaten in Art. 3 lit. a DSG umgegangen ist. Dabei stehen *zwei jüngere Bundesgerichtsentscheide* im Vordergrund³⁸, nämlich einerseits das Urteil in Sachen *Logistep AG*³⁹ und andererseits das Urteil in Sachen *Google Street View*⁴⁰.

1. BGE 136 II 508

Im Fall *Logistep AG* hatte das Bundesgericht zu entscheiden⁴¹, ob *IP-Adressen* als «Personendaten» gemäss Art. 3 lit. a DSG zu qualifizieren sind und damit in den Geltungsbereich des Datenschutzgesetzes fallen oder nicht. Der massgebliche Sachverhalt war folgender: Die Firma *Logistep AG* hatte eine spezielle Software entwickelt, mit der sie in Peer-to-Peer Netzwerken u.a. die IP-Adressen von Computern registrieren konnte, welche im Netzwerk urheberrechtlich geschützte Werke (illegal) anboten, um von Dritten heruntergeladen zu werden. Die registrierten Daten der Anbieter (insbesondere deren IP-Adressen) übergab die *Logistep AG* – im Rahmen eines entgeltlichen Auftragsverhältnisses – den jeweiligen Inhabern der Urheberrechte, welche mittels einer Strafanzeige gegen Unbekannt und der anschliessenden Einsichtnahme in die Verfahrensakten die Identität des Inhabers des betreffenden Internetanschlusses eruieren und Schadenersatzforderungen gegen die massgeblichen Urheberrechteverletzer erheben konnten.

Das Bundesgericht kam im konkreten Fall zum Schluss, dass sowohl *statische* als auch *dynamische* IP-Adressen als *Personendaten* zu qualifizieren seien, da die Identität des Inhabers des Internetanschlusses – ohne unverhältnismässigen Aufwand – im Sinne von Art. 3 lit. a DSG «bestimmbar» sei⁴². Bei der Beurteilung der «Bestimmbarkeit» sei auf die «Sicht des *jeweiligen Inhabers der Information*»⁴³ abzustellen, wobei es bei einer Weitergabe der Information ausreiche, «wenn der *Empfänger* die betroffene Person zu identifizieren»⁴⁴ vermöge. Die Bestimmbarkeit des Verletzers des Urheberrechts anhand der IP-Adresse brauche für die *Logistep AG* selber *nicht* gegeben zu sein, sondern es genüge, wenn das Erfordernis der Bestimmbarkeit für den *Urheberrechteinhaber* erfüllt sei. Treffe letzteres zu, so gelange das DSG auch auf die *Logistep AG* zur Anwendung – obwohl *notabene* aus ih-

³⁶ Vgl. in diesem Zusammenhang folgende Entscheidungen: Urteil des House of Lords vom 9. Juli 2008 in Sachen *Common Services Agency gegen Scottish Information Commissioner*, [2008] UK HL 47; Urteil des England and Wales Court of Appeal vom 8. Dezember 2003 in Sachen *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

³⁷ Art. 1 Data Protection Act.

³⁸ Auf eine vollständige Darstellung der Rechtsprechung muss aus Platzgründen verzichtet werden.

³⁹ BGE 136 II 508 ff.

⁴⁰ BGE 138 II 346 ff.

⁴¹ Vgl. BGE 136 II 508, 509 f., 524.

⁴² BGE 136 II 505, 513 ff., Erw. 3. – In seinem Urteil vom 24. November 2011, in Sachen *Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Rs. C-70/10 hat der EuGH – nebenbei und ohne Begründung – IP-Adressen als Personendaten bezeichnet (Nr. 51: «Zum einen steht nämlich fest, dass die Anordnung, das streitige Filtersystem einzurichten, eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen.»).

⁴³ BGE 136 II 505, 515, Erw. 3.4 [Hervorhebung ergänzt].

⁴⁴ *Ibidem* [Hervorhebung ergänzt].

rer Sicht das Kriterium der Bestimmbarkeit gerade *nicht* erfüllt war –, da sonst das DSG nur auf den jeweiligen Datenempfänger, nicht aber auf den Datenlieferanten anwendbar wäre, was dem Gesetzeszweck widerspreche⁴⁵. Auch wenn davon auszugehen sei, dass selbst der *Urheberrechteinhaber* in vielen Fällen den Urheberrechtsverletzer *nicht* ausfindig machen könne (z.B. weil mehrere Personen denselben Internetanschluss benutzen), sei dies nicht entscheidend, da es genüge, dass die Bestimmbarkeit der Identität der betroffenen Person bei einem *Teil* der von der Logistep AG gespeicherten – und an die Urheberrechteinhaber gelieferten – *Informationen* durch die Urheberrechteinhaber möglich sei⁴⁶.

Der bundesgerichtlichen Begründung dieser – deutlich ergebnisorientierten – Entscheidung liegt implizit folgendes Verständnis der «Bestimmbarkeit» der von Daten betroffenen Person gemäss Art. 3 lit. a DSG zugrunde: Wenn jemand – *in casu* die Logistep AG – Daten (*in casu* insbesondere dynamische IP-Adressen) erhebt, die sich auf Personen beziehen, deren Identität für den *Datenerheber nicht bestimmbar* ist, so dass sie aus seiner Sicht *anonyme* (dem DSG nicht unterstehende) *Einzeldaten* darstellen, und er anschliessend diese Daten im Rahmen von Auftragsverhältnissen an verschiedene *private Auftraggeber* – *in casu* die Urheberrechteinhaber – weitergibt, genügt es – im Extremfall –, dass ein *einzig* der *Datenempfänger* in einem *einzig* konkreten Fall ohne verhältnismässigen Aufwand durch Verknüpfung mit weiteren, von ihm beschaffbaren Informationen die *Identität* einer *einzig* von den Daten betroffenen Person bestimmen kann, damit *alle* vom *Datenerheber* beschafften Daten, obschon sie für ihn selber *anonyme Daten* darstellen, als *Personendaten* zu behandeln sind.

Diese Betrachtungsweise vermag nicht zu überzeugen, da sie in einer globalisierten Informationsgesellschaft im Ergebnis auf eine Beseitigung der gesetzlichen Unterscheidung zwischen *Personendaten* und *anonymen Einzeldaten* (als Nicht-Personendaten) hinausläuft, was z.B. für die *Forschung* und *Statistik* gravierende Konsequenzen hätte. So wäre für die *Forschung* und *Statistik* eine Weitergabe *anonymer Einzeldaten* nicht mehr möglich, wenn diese Daten – wegen der Bestimmbarkeit zumindest *einer* betroffenen Person aus der Sicht mindestens *eines* der Datenempfänger – letztlich doch als *nominative Einzeldaten* (Personendaten) behandelt werden müssten⁴⁷.

Der *pauschalen These*, dass anonyme Einzeldaten durch die blosser Weitergabe an einen Empfänger, der durch Verknüpfung mit weiteren Informationen bei einzelnen der erhaltenen Daten, die betroffene Person bestimmen kann, insgesamt und automatisch zu Personendaten werden, kann nicht gefolgt werden. Dies umso weniger, als dieselbe Argumentation dann auch gelten müsste, wenn der erste Datenempfänger seinerseits die Daten als Datenlieferant an einen oder mehrere *nachgelagerte* Datenempfänger liefern würde, und bei mindestens einem dieser Datenempfänger (zweiter Stufe) infolge der Verknüpfung mit weiteren von diesem beschafften Daten mindestens in *einem* konkreten Fall die Bestimmbarkeit der betroffenen Person zu bejahen wäre. Die Auffassung, wonach immer dann, wenn die Bestimmbarkeit der betroffenen Person aus der Sicht eines einzelnen *Datenempfängers* (erster, zweiter oder weiterer Stufe) zu bejahen ist, diese Qualifikation im Sinne eines *Rückschlusses* auch für den *Datenlieferanten* gelten müsse, weil anders zu entscheiden dem Zweck des Datenschutzgesetzes widerspreche⁴⁸, stellt für eine globalisierte Informationsgesellschaft *kein tragfähiges Konzept* dar und würde im Ergebnis alle jene Gesetzesbestimmungen unterlaufen, die zwar die Lieferung *anonymer Einzeldaten*, nicht aber die Lieferung von Personendaten zulassen. Das Urteil Logistep AG kann daher für die Bestimmung des Begriffs der Personendaten im Datenschutzrecht *nicht als richtungsweisendes Präjudiz* betrachtet werden.

2. BGE 138 II 346

Im Fall *Google Street View* hatte das Bundesgericht zu entscheiden, ob die von Google in vielen Städten und Dörfern der Schweiz mit mobilen 360°-Panorama Kameras gemachten und ins Internet gestellten Aufnahmen von Strassenzügen, Gebäuden, Verkehrsteilnehmern (Autos mit Kennzeichen, Personen mit teilweise erkennbaren Gesichtern etc.) als Personendaten im Sinne von Art. 3 lit. a DSD zu betrachten sind. Diese – kaum problematische Frage – hat das Bundesgericht richtigerweise bejaht⁴⁹.

⁴⁵ *Ibidem*.

⁴⁶ BGE 136 II 505, 516, Erw. 3.5 *in fine*.

⁴⁷ So könnten beispielsweise nach Art. 9 lit. a der Verordnung über die Durchführung von statistischen Erhebungen des Bundes (Sta-

tistikerhebungsverordnung) vom 30. Juni 1993 (SR 431.012.1) die Erhebungsorgane keine Einzeldaten mehr an private oder öffentliche Stellen oder an Statistikstellen internationaler Organisationen liefern, wenn aus der Sicht eines Datenempfängers die Bestimmbarkeit der betroffenen Person auf dem Wege allfälliger Verknüpfungen mit weiteren Informationen in einem Einzelfall zu bejahen wäre, da diese Bestimmung die Weitergabe von *Personendaten* nicht erlaubt.

⁴⁸ Vgl. BGE 136 II 508, 515.

⁴⁹ BGE 138 II 346, 355 f.

Zur Begründung wiederholte es die bereits im Urteil Logistep AG gemachten Ausführungen, wonach die Bestimmbarkeit der betroffenen Person sich «aus der Sicht des jeweiligen *Inhabers* der Information»⁵⁰ beurteile. Bei einer Weitergabe der Information reiche es aus wenn, «der *Empfänger* die betroffene Person zu identifizieren»⁵¹ vermöge. Zudem sei die Bestimmbarkeit gegeben, «wenn sie sich zumindest auf einen *Teil* der gespeicherten Informationen»⁵² beziehe.

Auf den fundamentalen *Sachverhaltsunterschied*, dass Google aus seiner eigenen Sicht als *Personendaten* zu betrachtende Daten (Bilder von Strassenzügen mit identifizierbaren Verkehrsteilnehmern) ins *Internet* stellte und damit *veröffentlichte*, während die Logistep AG aus ihrer eigenen Sicht als *anonyme Einzeldaten* zu betrachtende Daten (IP-Adressen) im Rahmen von Auftragsverhältnissen an ihre *private Auftraggeber* weitergegeben hatte, geht das Urteil überraschenderweise mit keinem Wort ein.

V. Kriterien zur Bestimmung der «Bestimmbarkeit» der von Daten betroffenen Person

1. Allgemeines

Die bisherigen Ausführungen belegen, dass die «Bestimmbarkeit» der betroffenen Person als datenschutzrechtlicher Kernbegriff mehr Mühe bereitet, als man auf den ersten Blick vermuten würde. In der Schweiz kann tendenziell als anerkannt gelten, dass die Bestimmbarkeit jeweils anhand der *konkreten Umstände des Einzelfalls* zu beurteilen ist⁵³ und dass eine rein *theoretische Möglichkeit*, die Identität der betroffenen Person zu bestimmen, nicht ausreicht, um die «Bestimmbarkeit» zu bejahen⁵⁴. Unklarheit und Rechtsunsicherheit herrscht dagegen insbesondere bei der Beantwortung der Frage, *für wen* die «Bestimmbarkeit» gegeben sein muss. Es ist dies die Frage nach dem massgeblichen *Beurteilungshorizont* zur Bestimmung des Begriffs der «Bestimmbarkeit» der betroffenen Person. Oder anders formuliert: Aus *wessen Sicht*

ist im konkreten Fall zu beurteilen, ob vernünftigerweise der erforderliche zeitliche und finanzielle Aufwand für die Beschaffung von weiteren Informationen zur Identifizierung der betroffenen Person betrieben werden wird?

2. Welcher Beurteilungshorizont ist massgeblich?

In Gesetzgebung, Rechtsprechung und Lehre werden – meist ohne nähere Begründung – unterschiedliche Beurteilungshorizonte befürwortet. Kurz zusammengefasst ergibt sich dazu folgendes heterogenes Bild:

a. Stand der Gesetzgebung

Während das *schweizerische Datenschutzgesetz* die Frage vollständig offen lässt⁵⁵, wird im *Unionsrecht* zwar nicht im Gesetzestext selber, aber immerhin in Erwägung 26 zur Richtlinie 95/46/EG⁵⁶ der *Verantwortliche* der Datenbearbeitung und alternativ jeder *Dritte* als Referenzperson genannt. Damit ist allerdings nicht allzu viel gewonnen, da der alternative Verweis auf beliebige Dritte faktisch keine substantielle Präzisierung darstellt. Gleiches gilt für das *französische* Datenschutzgesetz⁵⁷. Einen Schritt weiter geht dagegen der englische *Data Protection Act*, welcher den *data controller*, also den Datenherrn als Referenzperson betrachtet und darunter jene Person versteht, die über den Zweck und die Art und Weise der Datenbearbeitung entscheidet⁵⁸.

Nach dem aktuellen *Vorschlag* der EU-Kommission vom 25. Januar 2012 für eine *neue Datenschutzrichtlinie*⁵⁹ sollen gemäss Art. 3(1) künftig direkt im Gesetzestext der für die Datenverarbeitung *Verantwortliche* oder *jede andere Person* als massgebliche Referenzpersonen genannt werden. Dabei wird unter dem für die Datenbearbeitung Verantwortlichen die zuständige *Behörde* verstanden, welche über den Zweck, die Bedingungen und die Mittel der Bearbeitung der personenbezogenen Daten entschei-

⁵⁰ BGE 138 II 346, 354 [Hervorhebung ergänzt].

⁵¹ *Ibidem* [Hervorhebung ergänzt].

⁵² *Ibidem* [Hervorhebung ergänzt].

⁵³ Vgl. BGE 138 II 346, 353; BGE 136 II 508, 514; ROSENTHAL (FN 8), Art. 3 lit. a N 30.

⁵⁴ Vgl. BGE 138 II 346, 353; BGE 136 II 508, 514; Botschaft DSG, BBl 1988 II 444; PHILIPPE MEIER, *Protection des données, Fondements, principes généraux et droit privé*, Berne 2011, N 445; ROSENTHAL (FN 8), Art. 3 lit. a N 24.

⁵⁵ Auch in der Botschaft finden sich dazu keine weiterführenden Hinweise, da lediglich vom «Interessenten» gesprochen wird (BBl 1988 II 444 f.).

⁵⁶ Siehe dazu vorne, Abschnitt III/1/a/aa, S. 1427.

⁵⁷ Siehe dazu vorne, Abschnitt III/1/c, S. 1428.

⁵⁸ Siehe dazu vorne, Abschnitt III/1/f, S. 1429.

⁵⁹ Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig.

det⁶⁰, was paradoxerweise eine inhaltliche *Ausweitung* statt *Präzisierung* des Begriffs der Personendaten mit sich bringt. Dasselbe gilt gemäss Art. 4(1) des *Vorschlags* der EU-Kommission vom 25. Januar 2012 für eine *neue Datenschutz-Grundverordnung*⁶¹.

b. Stand der Rechtsprechung

Das *Bundesgericht* nennt in seinen Entscheidungen *Logistep AG* und *Google Street View*⁶² unterschiedliche Bezugspersonen, aus deren Sicht die Bestimmbarkeit der Identität der betroffenen Person zu beurteilen ist. So spricht es einerseits – in Anlehnung an die Botschaft zum *DSG*⁶³ – vom «Interessenten»⁶⁴, andererseits vom «Datenbearbeiter» oder von «Dritten»⁶⁵. Im Falle einer Weitergabe der Daten betrachtet es die Sicht des «Datenempfängers» als massgeblich⁶⁶. Das *Bundesverwaltungsgericht* spricht in seiner Rechtsprechung vom «Interessenten», vom «jeweiligen Inhaber der Information» und im Fall der Datenweitergabe vom Datenempfänger⁶⁷.

c. Stand der Lehre

Die schweizerische *Lehre* bezieht sich – meist ohne nähere Begründung – auf recht unterschiedliche Beurteilungshorizonte zur Bestimmung der «Bestimmbarkeit» der von Daten betroffenen Person. Die Rede ist etwa vom «Interessenten»⁶⁸ oder «Dateninteressenten»⁶⁹, vom «Betrachter»⁷⁰, vom «Datenempfänger»⁷¹, von «der Person, welche

die Angaben bearbeitet, beurteilt»⁷², vom «détenteur ou ...destinataire des informations»⁷³, vom «denkbaren Datennutzer»⁷⁴, vom «Dritten, der ein Interesse an diesen Angaben hat»⁷⁵ oder von der «Sicht derjenigen Person, der die Daten vorliegen»⁷⁶.

d. Fazit

Die beachtliche *Vielfalt* von *Beurteilungshorizonten*, die in Gesetzgebung, Rechtsprechung und Literatur – meist ohne Begründung oder nähere Erläuterungen – als massgeblich erachtet werden, um den Begriff der «Bestimmbarkeit» der von Daten «betroffenen Person» zu konkretisieren, einerseits, sowie die daraus sich ergebende Rechtsunsicherheit andererseits, führen zu einem doppelten Schluss:

1. Es ist *nicht möglich*, die «Bestimmbarkeit» der betroffenen Person nach einem *einzigem* Beurteilungshorizont (z.B. jenem des Datenbearbeiters) auszurichten, da die *Vielfalt* tatsächlicher Konstellationen gewisse *Differenzierungen* erforderlich macht.
2. Im Interesse der Rechtssicherheit und der Funktionsfähigkeit des datenschutzrechtlichen Kernbegriffs der «Personendaten» sollten Wissenschaft und Praxis ihre Bemühungen darauf konzentrieren, anhand von *Fallkategorien* zu spezifizieren suchen, in welcher Konstellation welcher Beurteilungshorizont massgeblich ist. Dies ist deshalb notwendig, weil ein pauschaler Hinweis auf die *Relativität* der Betrachtungsweise rechtsstaatlich nicht ausreicht. Abschliessend sollen daher in diesem Aufsatz Ansätze für eine Differenzierung von *Fallgruppen* skizziert werden.

⁶⁰ Als für die «Verarbeitung Verantwortlicher» gilt nach Art. 3 (6) des Richtlinien-Vorschlags «die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet...».

⁶¹ Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

⁶² Siehe vorne, Abschnitt IV, S. 1429 ff.

⁶³ Botschaft DSG, BBl 1988 II 445.

⁶⁴ BGE 136 II 508, 514, BGE 138 II 346, 353.

⁶⁵ BGE 136 II 508, 514, BGE 138 II 346, 354.

⁶⁶ BGE 136 II 508, 515, BGE 138 II 346, 354.

⁶⁷ Urteil vom 10. April 2012 (A-4467/2011) in Sachen *EDÖB gegen Axa Stiftung Berufliche Vorsorge Winterthur*, Erw. 5 (Erwägung in in BVGE 2012, 273 ff. nicht veröffentlicht). Vgl. auch Urteil vom 27. Mai 2009 (A-3144/2008) in Sachen *EDÖB gegen Logistep AG*, Erw. 2.2.1; Urteil vom 7. Mai 2009 (A-7183/2008) in Sachen *A. gegen EDA*, Erw. 5.2.2.

⁶⁸ BEAT RUDIN, *Datenschutz-Pendenzen bei OGD*, *digma* 2012, 65; ROSENTHAL (FN 8), Art. 3 lit. a N 24 f.

⁶⁹ BISCHOFF/SCHWEIZER (FN 1), 153.

⁷⁰ FERCSIK SCHNYDER/WEBER (FN 1), 583; ROSENTHAL (FN 8), Art. 3 lit. a N 20.

⁷¹ ERIC OLIVIER MEIER, *Due Diligence bei Unternehmensübernahmen*, Zürich 2010, Fn. 887 («Obwohl im Gesetz nicht explizit erwähnt, beurteilt sich die Bestimmbarkeit grundsätzlich aus subjektiver Sicht des Datenempfängers, nicht des -bekanntgebers oder eines Dritten»).

⁷² EVA MARIA BELSER/HUSSEIN NOUREDDINE, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, *Datenschutzrecht – Grundlagen und öffentliches Recht*, Bern 2011, § 7 N 40.

⁷³ MEIER (FN 54), N 445.

⁷⁴ BISCHOFF/SCHWEIZER (FN 1), 153.

⁷⁵ BSK DSG-BELSER (FN 72), Art. 3 N 6.

⁷⁶ ROSENTHAL (FN 8), Art. 3 lit. a N 25.

VI. Ansätze für eine Fallgruppenbildung zur Bestimmung der «Bestimmbarkeit» der betroffenen Person

1. Erörterung von vier Sachverhaltsvarianten

a. Variante 1 (einseitiger Datenerwerb)

X. hebt an einem Bancomaten den Betrag von 500 Franken von seinem Bankkonto ab und lässt den ausgedruckten *Transaktionsbeleg* versehentlich liegen. Der nachfolgende Bancomat-Benutzer Y. findet diesen Beleg, auf welchem u.a. die *IBAN*⁷⁷, der *bezogene Betrag* und das *Datum* stehen, und nimmt ihn mit. Ist er dadurch in den Besitz von Personendaten des X. gelangt?

Bei einem solchen *zufälligen* Erwerb von Daten liegt *keine Datenlieferung* vor, so dass als massgeblicher Beurteilungshorizont zur Beantwortung der Frage, ob der Kontoinhaber X. eine bestimmbare Person ist oder nicht, lediglich die *Sicht von Y.* als *Dateninhaber* in Betracht kommt. Aus seiner Sicht wird die IBAN des X. regelmässig *kein* Personendatum darstellen, da es Y. mit verhältnismässigem Aufwand normalerweise nicht möglich sein wird, X. zu identifizieren. Zwar wird Y. anhand der in der IBAN enthaltenen *Bank-Clearing Nummer* durch weitere Recherchen (z.B. im Internet⁷⁸) die *Bank B.* als kontoführende Bank von X. eruieren können, aber bei dieser Bank wird er wegen des Bankkundengeheimnisses durch entsprechende Anfrage die Identität des X. nicht ermitteln können. Der *Transaktionsbeleg* enthält somit aus seiner Sicht *keine Personendaten* des X. und das DSG ist nicht anwendbar.

b. Variante 2 (bilaterale Datenweitergabe)

Y. übergibt eine Kopie des *Transaktionsbelegs* seinem *Bekanntem Z.*, welcher (zufälligerweise) auf der kontoführenden *Bank B.* arbeitet. Ist Z. damit in den Besitz von Personendaten des X. gelangt? Falls ja, kommt der Beantwortung dieser Frage für die Beurteilung der Rechtslage von Y. als Datenlieferant Bedeutung zu?

Grundsätzlich kommen bei dieser Konstellation *zwei* Beurteilungshorizonte zur Bestimmung der Identität von X. in Betracht, nämlich jener des *Datenlieferanten Y.* und

jener des *Datenempfängers Z.* Wie soeben bei Variante 1 festgestellt, enthält der *Transaktionsbeleg* des Bancomaten aus der *Sicht von Y.* *keine Personendaten* des X.⁷⁹ Aus der Sicht des Datenempfängers Z. präsentiert sich die Lage dagegen anders. Aufgrund seiner Stellung als Mitarbeiter der Bank B. wird es für ihn ohne grossen Aufwand möglich sein, bankintern festzustellen, dass hinter der von Y. erhaltenen IBAN die Person X. als Kontoinhaber steht. Dessen Identität ist somit aufgrund der IBAN für Z. *bestimmbar*; weshalb für ihn der *Transaktionsbeleg Personendaten* des X. enthält. Welcher der beiden Beurteilungshorizonte ist nun massgeblich? Jener des Datenlieferanten Y. oder jener des Datenempfängers Z.?

Abzustellen ist auf die Sicht des *Datenempfängers Z.*, da es keinen relevanten Unterschied machen kann, ob er die IBAN von Y. *geliefert* erhält oder den *Transaktionsbeleg* – anstelle von Y. – selber am Bancomaten findet. Beide Konstellationen sind *gleich* zu behandeln, da Z. in *beiden Fällen* aufgrund seines (legalen) Zugangs zu Kontoangaben bei der Bank B. über zusätzliche Informationen verfügt, die es ihm ermöglichen, in Verbindung mit der auf dem *Transaktionsbeleg* abgedruckten IBAN die Identität von X. festzustellen.

Bedeutet dies, dass der *Transaktionsbeleg* im Sinne eines *Rückschlusses* nun auch für den Datenlieferanten Y. Personendaten des X. enthält, obschon aus der *eigenen Sicht* von Y. die Identifikation des X. nicht möglich ist⁸⁰? Diese Frage ist entsprechend dem Grundsatz der *Relativität der Beurteilungshorizonte*⁸¹ grundsätzlich zu *verneinen*. Es liegt in der Natur einer *subjektivierten* Beurteilung der Bestimmbarkeit der von Daten betroffenen Person, dass sich für verschiedene Bearbeiter *derselben Daten* – je nach *individuellem* Informationsstand bzw. *individuellen* Möglichkeiten der Informationsbeschaffung – die Identifizierbarkeit der betroffenen Person *unterschiedlich beurteilt*. Einem *Datenlieferanten* sind daher die weitergehenden Informationen bzw. Informationsmöglichkeiten des *Datenempfängers* grundsätzlich *nicht zuzurechnen*. Eine *Ausnahme* von dieser Regel rechtfertigt sich aber dann, wenn der Datenlieferant die zusätzlichen Informationen bzw. Informationsmöglichkeiten des Datenempfängers *kannte* oder *kennen musste* und es trotzdem *unterlassen* hat, rechtliche oder faktische Schutzmassnahmen

⁷⁷ IBAN steht für *International Banking Account Number* und stellt die standardisierte Bankkontonummer für einen effizienten Zahlungsverkehr in Europa dar.

⁷⁸ Siehe z.B. die Adresse <http://www.six-interbank-clearing.com/de/home/standardization/iban/inquiry-iban.html>.

⁷⁹ Vgl. die Ausführungen zu Variante 1, Abschnitt VI/1/a, S. 1433.

⁸⁰ Diese Auffassung vertritt das Bundesgericht im Urteil *Logistep AG*, wo es sinngemäss ausführt, es widerspreche dem Zweck des DSG, wenn zwar für den *Datenempfänger*, nicht aber für den *Datenlieferanten* Personendaten vorliegen würden. Vgl. BGE 136 II 508, 515.

⁸¹ Vgl. auch ROSENTHAL (FN 8), Art. 3 lit. a N 25.

(z.B. durch Abschluss eines Datenschutzvertrags oder durch Verschlüsselung der Daten) zu ergreifen, um sicherzustellen, dass der Datenempfänger seine zusätzlichen Informationen bzw. Informationsmöglichkeiten *nicht* zur Identifizierung der betroffenen Person *einsetzt*. In diesem Sonderfall rechtfertigt es sich, auf den fehlbaren *Datenlieferanten* die für *Personendaten* geltenden Datenschutzregeln des Datenempfängers anzuwenden. Dies wäre somit der Fall, wenn Y. wusste oder wissen musste, dass Z. bei der Bank B. arbeitet und Zugang zu Kontoinformationen des X. hat.

c. Variante 3 (multilaterale Datenweitergabe)

Y. übermittelt eine Kopie des Transaktionsbelegs des X. nicht nur dem Bankangestellten Z., sondern zwei *weiteren Personen F. und G.*, die unabhängig voneinander sind und je keine besonderen Informationen bzw. Informationsmöglichkeiten besitzen, um die Identität des Kontoinhabers X. aufgrund der von Y. erhaltenen IBAN zu bestimmen. Nach welchem Beurteilungshorizont bestimmt sich in diesem Fall die Identifizierbarkeit des X.?

Bei dieser Konstellation gelten grundsätzlich die für Variante 2 gemachten Ausführungen⁸², d.h. es ist für die Bestimmbarkeit der Identität des X. auf die *individuelle* Sicht des *jeweiligen Datenempfängers Z., F. oder G.* abzustellen. Dabei ist zu beachten, dass für jeden Datenempfänger die *individuellen* Informationen und Informationsmöglichkeiten massgeblich sind. Der Umstand, dass Z. Zugang zu zusätzlichen Bankinformationen hat, ist für F. und G. *nicht* relevant. Dementsprechend stellt die IBAN des X. für den Bankangestellten Z. ein *Personendatum* dar, während sie aus der Sicht von F. und G. als *Nicht-Personendatum* zu qualifizieren ist. Für den Datenlieferanten Y. bedeutet dies, dass er an F. und G. *Nicht-Personendaten* und an Z. – im Sinne der *Ausnahme* in Variante 2 – nur dann *Personendaten* liefert, wenn er um dessen zusätzliche Informationen bzw. Informationsmöglichkeiten *wusste* oder *wissen musste*, ohne die erforderlichen Sicherheitsmassnahmen zu ergreifen. Falls gegenüber Z. dieser Ausnahmefall vorliegt, hat dies *keine Auswirkungen* auf die Datenlieferung von Y. an die beiden *Datenempfänger F. und G.*, d.h. diesen gegenüber stellt die Weitergabe der IBAN des X. weiterhin ein *Nicht-Personendatum* dar. Es darf also nicht aus dem Umstand, dass Z. die Möglichkeit hat, anhand der IBAN (in Verbindung mit weiteren Informationen) die Identität des X. zu bestimmen, gefolgert

werden, die IBAN habe auch für die Weitergabe an F. und G. als Personendatum zu gelten⁸³.

d. Variante 4 (Datenveröffentlichung)

Y. *veröffentlicht* eine Kopie des Bancomatauszugs mit der IBAN des X. in einer *Zeitung* oder stellt eine Kopie des Auszugs ins *Internet*. Nach *wessen Beurteilungshorizont* bestimmt sich in diesem Fall die Identifizierbarkeit des X.?

Im Falle der Veröffentlichung einer IBAN kann *nicht* mehr von einer «*Datenlieferung*» im eigentlichen Sinn gesprochen werden⁸⁴, da die Übermittlung der Daten sich nicht an eine bestimmte oder bestimmbare Anzahl *spezifizierter Adressaten* richtet, sondern an jedermann, d.h. an *jeden beliebigen Dritten*. Daraus ist für die Frage der Bestimmbarkeit der Identität des X. zu folgern, dass der *Beurteilungshorizont jedes potentiell Interessierten* relevant ist. Im Ergebnis bedeutet dies faktisch, dass wohl stets irgendwo auf der Welt jemand zu finden ist (z.B. der Bankangestellte Z.), der mit vernünftigem Aufwand die Identität des X. aufgrund der IBAN auf dem Bancomatbeleg bestimmen kann. Bei einer Veröffentlichung von Daten rechtfertigt es sich deshalb von der (widerlegbaren) *Vermutung* auszugehen, dass die betroffene Person *identifizierbar* ist und somit *Personendaten* vorliegen. Dem für die Veröffentlichung der Daten Verantwortlichen muss jedoch die Möglichkeit eingeräumt werden, diese Vermutung zu *widerlegen*, indem er z.B. nachweist, dass es sich bei den veröffentlichten Daten um aggregierte oder anonymisierte Daten handelt, die *keiner identifizierbaren Einzelperson* mehr zugeordnet werden können.

2. Grundsätze zur Bestimmung des Beurteilungshorizonts

Was anhand der vier vorgenannten Varianten⁸⁵ für die *IBAN* diskutiert worden ist, gilt *mutatis mutandis* für an-

⁸² Siehe vorne Abschnitt VI/1/b, S. 1433.

⁸³ Genau dies tat aber das Bundesgericht im Fall *Logistep AG*, wo es sinngemäss argumentiert, dass, obwohl der Urheberrechtinhaber aufgrund der von Logistep AG gelieferten IP-Adressen in vielen Fällen den Urheberrechtsverletzer *nicht* identifizieren könne, *alle* von der Logistep gespeicherten IP-Adressen als Personendaten zu gelten hätten. Vgl. BGE 136 II 508, 516.

⁸⁴ Im Fall *Logistep AG* hat das Bundesgericht die *multilaterale Datenlieferung* an mehrere Urheberrechtinhaber (Variante 3) mit der *Datenveröffentlichung* (Variante 4) verwechselt und sich daher irrtümlicherweise massgeblich auf eine Literaturstelle gestützt (ROSENTHAL [FN 8], Art. 3 lit. a N 30), welche den Fall einer *Veröffentlichung* in der Zeitung betrifft. Vgl. BGE 136 II 508, 515.

⁸⁵ Es liessen sich noch weitere *Untervarianten* oder *Kombinationen* von Varianten bilden, aber im Rahmen dieses kurzen Beitrags ist es

dere Daten einer betroffenen Person – wie z.B. die Kreditkartennummer, die Sozialversicherungsnummer, die Telefonnummer oder andere Identifikatoren – wenn es um die Beantwortung der Frage geht, ob die Identität der betroffenen Person bestimmbar ist oder nicht, ob also Personendaten oder Nicht-Personendaten vorliegen. Aus den vorstehenden Erörterungen lassen sich folgende *Grundsätze* für den *relevanten Beurteilungshorizont* zur Bestimmung der Identifizierbarkeit einer von Daten betroffenen Person formulieren:

1. Bei einem *einseitigen Datenerwerb (Variante 1)*, wo einer Person – ohne willentliche Datenlieferung eines Datenlieferanten und ohne allgemeine Datenveröffentlichung – Daten mehr oder weniger zufällig zur Kenntnis gelangen, ist für die Bestimmung der «Bestimmbarkeit der betroffenen Person» auf den *Beurteilungshorizont* des *Dateninhabers* nach Inbesitznahme bzw. Kenntnisnahme der Daten abzustellen.
2. Bei einer *bilateralen Datenweitergabe* durch den Datenlieferanten an einen *einzelnen Datenempfänger (Variante 2)* ist zur Beurteilung der Identifizierbarkeit der «betroffenen Person» auf den Beurteilungshorizont des *Datenempfängers* abzustellen. Dem Datenlieferanten dürfen die besonderen Informationen und Informationsmöglichkeiten des Datenempfängers nur *ausnahmsweise* zugerechnet werden, nämlich dann, wenn er diese *kannte* oder *kennen musste* und es dennoch *unterlassen* hat, die erforderlichen *Massnahmen* zu ergreifen, um die Identifizierung der «betroffenen Person» durch den Datenempfänger zu unterbinden.
3. Bei einer *multilateralen Datenweitergabe* durch den Datenlieferanten an *mehrere* (voneinander unabhängige) *Datenempfänger (Variante 3)* ist für die Bestimmbarkeit der Identität der «betroffenen Person» auf den *individuellen* Beurteilungshorizont des *jeweiligen Datenempfängers* abzustellen. Dem *Datenlieferanten* können die individuellen Informationen und Informationsmöglichkeiten des einzelnen Datenempfängers nur zugerechnet werden, wenn er sie *kannte* oder *kennen musste* und es *unterliess*, die erforderlichen *Massnahmen* zu ergreifen, um die Identifizierung der «betroffenen Person» zu vermeiden.
4. Bei einer *Veröffentlichung* von Daten (*Variante 4*) ist zur Bestimmung der Identifizierbarkeit der «betroffenen Person» auf den jeweiligen *Beurteilungshorizont jedes potentiell Interessierten* abzustellen. Es gilt da-

her die *Vermutung*, dass die «betroffene Person» *identifizierbar* ist. Diese Vermutung kann von dem für die Veröffentlichung der Daten Verantwortlichen durch den Nachweis *widerlegt* werden, dass die fraglichen Daten *keiner identifizierbaren Person* zugeordnet werden können.

5. Bei der Beurteilung der *Informationsbeschaffungsmöglichkeiten* zur Identifizierung der «betroffenen Person» sind grundsätzlich nur *legale* Mittel der Informationsbeschaffung zu berücksichtigen. Falls jedoch hinreichende *Anhaltspunkte* dafür bestehen, dass ein Dateninhaber (Varianten 1 und 4) oder Datenempfänger (Variante 2 und 3) auch *illegale* Mittel einsetzen könnte, sind diese mit zu berücksichtigen.
6. Bei einer (im weitesten Sinne) *kommerziell* ausgerichteten Datenbearbeitung ist die Identifizierbarkeit der betroffenen Personen *eher zu bejahen* als bei einer Datenbearbeitung für Zwecke der *Forschung* und *Statistik*.
7. Bei der Datenbearbeitung *innerhalb* von (privaten oder öffentlichen) *Institutionen* und *Organisationen* ist zur Beurteilung der Identifizierbarkeit der betroffenen Person *nicht* auf die *rechtliche* Einheit, sondern auf die tatsächliche *organisatorische Struktur* und *Aufgliederung* abzustellen⁸⁶. Es kommt also nicht darauf an, ob eine öffentlich-rechtliche Körperschaft (wie der Bund oder die Kantone), eine spezialgesetzliche Körperschaft (wie die Swisscom⁸⁷ oder die Post⁸⁸) oder eine juristische Person des Privatrechts als Trägerin eines Unternehmens (z.B. Grossbank, Versicherung, Kreditkartenunternehmung) als *Ganzes* die Identität einer von Daten betroffenen Person bestimmen kann, sondern ob der *Datenbearbeiter* innerhalb seiner *organisatorischen Einheit* über die erforderlichen Informationen verfügt oder diese beschaffen kann, um die Identität der betroffenen Person zu bestimmen.

VII. Schlussfolgerung

Der Begriff der *Personendaten* stammt aus einer Zeit, als das Internet noch nicht jedermann als *weltumspannendes Kommunikationsmittel* zur Verfügung stand. Der zwi-

wünschenswert, sich auf wenige *Grundvarianten* zu beschränken, da es lediglich um eine grundsätzliche Strukturierung der Problematik geht.

⁸⁶ So auch ROSENTHAL (FN 8), Art. 3 lit. a N 28.

⁸⁷ Vgl. Art. 2 des Bundesgesetzes über die Organisation der Telekommunikationsunternehmung des Bundes (Telekommunikationsunternehmungsgesetz, TUG) vom 30. April 1997 (SR 784.11).

⁸⁸ Vgl. Postgesetz (PG) vom 17. Dezember 2010 (SR 783.0) und die Post CH AG als im Handelsregister eingetragene Aktiengesellschaft.

schenzeitlich eingetretene technologische Fortschritt ist nicht ohne Auswirkungen auf das *rechtliche Konzept* der Personendaten als Kernelement des Datenschutzrechts geblieben. Insbesondere die zunehmenden Möglichkeiten von *Datenverknüpfungen* haben zu einer *faktischen Ausweitung* der Bestimmbarkeit der von Daten betroffenen Person geführt und damit zu einer gleichzeitigen *Erweiterung* des Begriffs der *Personendaten*. Damit korreliert spiegelbildlich eine faktische *Reduktion* des Bereichs der *Nicht-Personendaten*, namentlich des Bereichs der *anonymen Einzeldaten*, welche etwa für die Arbeit auf dem Gebiet der *Forschung* und *Statistik* von grosser Bedeutung sind. Es wäre deshalb irrtümlich anzunehmen, die schleichende Ausweitung des Begriffs der Personendaten sei unproblematisch, da sie bloss zu einer breiteren Anwendung der Regeln über den Schutz von Personendaten führe. Vielmehr muss im Interesse des Forschungsstandortes Schweiz darauf geachtet werden, dass der laufende technische Fortschritt der Kommunikationstechnologie den Begriff der «Bestimmbarkeit» der von Daten betroffenen Person nicht zu einem *uferlosen Konzept* werden lässt. Dies kann dadurch verhindert werden, dass Wissenschaft und Praxis sich zur Frage der Identifizierbarkeit einer von Daten betroffenen Person, und ganz besonders zum relevanten *Beurteilungshorizont* vermehrt Gedanken machen. Der vorliegende Beitrag macht einen ersten Schritt in diese Richtung. Weitere werden folgen müssen.