Anmerkungen zur Systemrelativität des Personenbezuges im Datenschutzrecht

JULIAN HÖLZEL

Auch mehr als 40 Jahre nach dem Aufkommen des sog. Personenbezugs als zentraler Kategorie des zunächst bundesdeutschen, inzwischen europäischen Datenschutzrechts sind die Fundamente dieses Begriffes kaum geklärt. Die Diskussion orientiert sich in guter Tradition an über die Dekaden aufgeschichteter Kasuistik, ohne dass bislang eine überzeugende theoretische Beschreibung dieses Rechtsbegriffes angefertigt werden konnte. Nach der hier vertretenen Auffassung liegt die Ursache dafür in dem Versuch einer objektivistischen Fassung des Begriffes, der ohne Reflexion auf den jeweiligen Interpretationshorizont der Rechtsanwenderinnen auskommen soll. Dies soll Anlass sein, einen konsequent anwendungsrelativen Begriff zu skizzieren.

DER KONTEXT DER UNTERSCHEIDUNG

Die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten taucht aus Rechtsanwendungsperspektive in zwei unterschiedlichen Kontexten auf: zum einen als Kriterium der Verarbeiterin, die EDV-Prozesse auf deren datenschutzrechtliche Relevanz hin beobachtet, sowie als Kriterium der Datenschutz-Aufsichtsbehörden, deren Aufgabe es ist, die verarbeitenden Organisationen daraufhin zu beobachten, ob diese sich entsprechend den ihnen durch das Datenschutzrecht auferlegten Pflichten verhalten[1], um schließlich bei einer etwaigen Differenz zwischen den rechtlichen Anforderungen und tatsächlichem Verhalten durch geeignete Maßnahmen[2] auf eine Differenzverringerung hinzuarbeiten.

Im Hinblick auf unser Thema bedeutet das insbesondere, dass die Aufsichtsbehörden die Verarbeiterinnen bei der Anwendung der Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten auf ihre eigenen Verarbeitungsprozesse hin beobachten. Diese Feststellung ist trivial, aber von großer Tragweite, denn sie bedingt, dass die Interpretation der Merkmale des Tatbestandes der personenbezogenen Daten immer vor dem Hintergrund einer Verarbeiterin erfolgt:

[1] Eine entsprechende Beobachterinnen-Position nehmen die Mitbewerberinnen der Verarbeiterin und entsprechende Verbände ein, insoweit diese aktivlegitimiert nach den lauterkeitsrechtlichen Vorschriften sind. Im Detail ist noch Vieles umstritten, siehe z.B. Ohly, GRUR 2019, S. 686ff. Für unsere weiteren Betrachtung ist diese Frage ohne Belang und wird daher im Folgenden ausgeklammert.

[2] Dabei hat sich das Datenschutzrecht längst von einem klassischen Sanktionen- hin zu einem Aufsichtsrecht entwickelt, das eine Vielzahl von unterschiedlichen Maßnahmeformen kennt, siehe nur Artikel 57, 58 der DS-GVO.

Personenbezogene Daten sind nur personenbezogene Daten relativ zu einer Verarbeiterin[3]. Die Personenbezogenheit von Daten ist nicht – wie es der Sprachgebrauch in Form des „Personenbezuges" nahelegen mag – eine diesen intrinsische Eigenschaft, sondern sie bezeichnet eine bestimmte Beziehung, die eine Verarbeiterin aufgrund ihrer Interpretation des Datums zwischen diesem und einer Person herstellt[4]. Es handelt sich daher vielmehr um eine Eigenschaft, die die Beziehung zwischen Verarbeiterin und Datum kennzeichnet. Damit rückt bei der Beurteilung, ob eine Verarbeiterin personenbezogene Daten verarbeitet, die Frage nach den Kriterien in den Mittelpunkt, nach welchen eine solche Relation zwischen dieser und einem Datum gerechtfertigter Weise angenommen werden kann. Ausgeschlossen ist damit auch, diese Annahme für bestimmte Darstellungsformate von Daten pauschal ohne Rücksicht auf die Verarbeiterin zu treffen. Eine IP-Adresse ist nicht schlechterdings personenbezogen, genausowenig wie für sog. „synthetische Daten" oder „aggregierte Daten" ein Personenbezug ohne Weiteres abzulehnen ist.

Die kanonische Analyse der Artikel-29-Gruppe[5], die vielfach zur Auslegung herangezogen wird, zerlegt den Begriff in vier Elemente, mit denen sich der Interpretationsvorschlag an dem Wortlaut der inzwischen außer Kraft getretenen Datenschutz-Richtlinie orientiert. Gleichwohl weist die Gruppe darauf hin, dass sich die „Begriffsbausteine" wechselseitig beeinflussten, die Trennung daher im Wesentlichen ihrem analytischen Ansatz geschuldet sei. Ohne dies methodisch zu reflektieren oder auch nur explizit zu machen, geht diese Analyse von einer Art objektivistischem Beurteilungshorizont aus, bei der der Verwendungskontext fast vollständig[6] außer Betracht bleibt. In Anlehnung an die Trennung dieser vier Elemente[7] wollen wir vor dem Hintergrund unseres vorangestellten Interpretationshorizontes der Verarbeitungsrelativität des Personenbezugs begriffliche Umdispositionen vor-

[3] Damit ist zugleich angezeigt, dass wir die seit gut 40 Jahren in der datenschutzrechtlichen Diskussion verankerte Unterscheidung zwischen dem sog. „relativen" und „absoluten" Personenbezug nicht mitvollziehen. Denn selbst der Begriff des sog. „absoluten Personenbezugs" imaginiert auch nur Mittel und Fähigkeiten irgendeiner Akteurin, um von dort aus den Personenbezug zu bestimmen, aber eben doch auch nur relativ zu eben diesem. Der Unterschied besteht lediglich in dem, was einer konkreten Verarbeiterin, deren Eigenschaft als Verantwortliche in Rede steht, als Mittel und Fähigkeiten noch eben zugerechnet wird.

[4] Oder, unterstellt bestimmt Fähigkeiten und Mittel, durch die Verarbeiterin herstellbar, im überkommenen Datenschutzrechtsdiskurs „Personenbeziehbarkeit" genannt. Dies ist aber nicht viel mehr als eine Modalisierung der Personenbezogenheit.

[5] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (im Folgenden WP136).

[6] Diese Perspektive scheint nur sehr kurz bei Ausdefinition des dritten Elementes „über" auf, wenn dieses trotz Fehlens eines (objektivistischen) Inhaltselementes mit Rücksicht auf den Verarbeitungszweck oder gar nur aufgrund der Beeinflussung des Verarbeitungsergebnisses festgestellt werden soll. Die sich sofort anschließende Frage wäre natürlich, in welches Verhältnis die überkommene Dogmatik Verarbeitungszweck und sachlichen Anwendungsbereich stellt.

[7] Die Artikel-29-Datenschutzgruppe benennt als diese: „alle Informationen", „über", „identifizierte/identifizierbare", „natürliche Person".

schlagen. Das betrifft insbesondere die Voraussetzungen, die für eine Verarbeiterin vorliegen müssen, um eine entsprechende Beurteilung der einzelnen Elemente für die Relation zwischen dieser und Datum zu plausibilisieren.

„ALLE INFORMATIONEN“

Zu Beginn einer näheren Begriffsbestimmung dieses Elementes wird häufig darauf hingewiesen, es sei nicht etwa der „mathematische“ Informationsbegriff zugrundezulegen, sondern vielmehr ein „geisteswisseschaftlicher“, der nämlich auch die „Bedeutung“ der „Information“ abzubilden im Stande sei[8]. Informationen im Sinne des Datenschutzrechtes seien daher alle sinnhaften Aussagen über natürliche Personen[9]. Damit wird freilich übersehen, dass auch die Sinnhaftigkeit von Nachrichten ihrerseits nur vor dem Hintergrund aller möglichen Sinnangebote, mithin vor einem Selektionshorizont festgestellt werden kann. Dies aber ist auch der Kern der mathematischen Informationstheorie, der es um die genaue Reproduktion einer Nachricht geht, für die die Annahme gilt, dass bereits diese aus einem Repertoire möglicher Nachrichten ausgewählt wurde. Die Reproduktion der Nachricht erfolgt dann vor dieser a priori gegebenen Menge möglicher Nachrichten an anderer Stelle. Der entscheidende Umstand ist der der Wahrscheinlichkeit, welche die Erwartungsunsicherheit der Empfängerin vor Empfang der Nachricht konstituiert. Information ist dann ein Maß, welches anzeigt, dass und „wieviel“[10] dieser Unsicherheit beseitigt wurde.

Für die Zwecke dieses Beitrages muss von der traditionellen Bestimmung nicht vollständig abgerückt werden. Der Vergleich mit den Grundannahmen der „mathematischen“ Informationstheorie macht aber deutlich, dass die Rede von Informationen darauf angewiesen ist, entsprechend offene Erwartungsstrukturen und damit Möglichkeitshorizonte anzugeben, deren Reduktion dann als Information bezeichnet werden kann. In dieser Hinsicht zwingt uns das Element „alle Informationen“ be-

[8] Der Nachweis der Ungeeignetheit erfolgt regelmäßig über ein Zitat aus der Einleitung des Artikels von Shannon, in der dieser das ingenieurwissenschaftliche Problem technisch vermittelter Kommunikation behandelt. Dort heißt es auf S. 379: „Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.“ (Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, July 1948, S. 379ff.).

[9] WP136, S. 7.

[10] Dieser Umstand ist aus technischer Sicht entscheidend, denn davon abhängig sind dann die Eigenschaften der zu konstruierenden Kommunikationskanäle. Eine genaue Messung der Beseitigung von Unsicherheit erfordert dann freilich auch eine genaue Quantifizierung der Unsicherheit, mithin eine genaue Angabe der erwartbaren Nachrichten. Zu einer Reflexion der Bedingungen einer solchen Möglichkeit in diesem Band Pohle, On Measuring Fundamental Rights Protection – Can and Should Data Protection Law Learn From Environmental Law?.

reits auf dieser Ebene, „personenbezogene Daten“ als systemrelativ[11] zu begreifen[12], denn andernfalls wären wir außerstande, eine entsprechende Erwartungsstruktur anzugeben. Offen bleibt allerdings ein die Menge der möglichen Systemrelationen limitierenden Merkmales. Diese Funktion liegt in einem anderen Definitionselement.

„IDENTIFIZIERTHEIT/IDENTIFIZIERBARKEIT“

Durch dieses Merkmal legt das Datenschutzrecht fest, welches Wissen und welche Fähigkeiten einer Verarbeiterin zurechenbar hinsichtlich der Frage ist, ob für diese eine konkrete Möglichkeit der Identifikation des in Rede stehenden Datums mit der Verarbeiterin bereits bekannten Angaben besteht, die diese auf eine realweltliche Entität[13] bezieht. Die Formulierung in Erwägungsgrund 26 der Verordnung macht dabei klar, dass es nicht nur auf aktuelles Wissen und Fähigkeiten der Verarbeiterin ankommt, sondern auch auf solches, das in der Person anderer Verarbeiterinnen vorliegt, für welche aber für die in Rede stehende Verarbeiterin eine angebbare Zugriffschance besteht. Zwar spricht der Wortlaut von Erwägungsgrund 26 von beliebigen „anderen Person[en]“, die dabei zu berücksichtigen sind, ohne diesen Kreis ausdrücklich einzuschränken. Aus rechtsstaatlicher Sicht dürfte dabei nur auf solche Personen abzustellen sein, zwischen denen und der Verarbeiterin eine reale Kommunikationschance besteht. Andernfalls wäre für die Verarbeiterin in ihrer Selbstbeobachtung nicht feststellbar, ob sie unter den Anwendungsbereich des Datenschutzrechtes fallen – ultra posse nemo obligatur.

Die juristische Diskussion der letzten Dekaden zum Problem des Personenbezuges war ganz maßgeblich von der praktischen Unsicherheit hinsichtlich der jeweils im konkreten Fall unterstellbaren Fähigkeiten und Mittel der Verarbeiterinnen begleitet, aus welchen diesen wenigstens die Möglichkeit der Identifikation der von in den Daten liegenden sinnhaften Aussagen betroffenen Personen zugesprochen werden konnte. Die Debatte unterschlägt dabei noch immer, dass jede Identifikation eine für diese Operation konstituierte Identität voraussetzt[14], und kann daher keine abstrakten Kriterien vorweisen, nach denen sie diese für die Identifikation erfor-

[11] Ohne freilich bereits eine spezifische Systemreferenz angeben zu müssen. Darin liegt dann die Funktion eines anderen Defintionselementes.

[12] So bereits Steinmüller, Stellenwert der EDV in der öffentlichen Verwaltung und Prinzipien des Datenschutzrechts, ÖVD 1972, S. 460; sowie Steinmüller/Ermer/Schimmel, Datenschutz bei riskanten Systemen, Berlin-Heidelberg 1978, S. 84.

[13] Konzeptuell kommen damit beliebige Einheiten in Betracht, die von der Verarbeiterin als solche zugrunde gelegt werden. Datenschutzrechtlich relevant sind freilich nur natürliche Personen, wie sich aus einem weiteren Merkmal ergibt. Zum Hintergrund dieser Annahmen aus dem Bereich der Datenmodellierung siehe Hölzel, European Data Protection Law Review 2019, S. 189; ders., DuD 2018, S. 504.

[14] Dazu aus sprachanalytischer Perspektive Tugendhat, Traditional and Analytical Philosophy, Cambridge 1982, S. 310ff., mit der Unterscheidung zwischen ursprünglicher Spezifikation und davon abhängiger Identifikation, sowie Kripke, Naming and Necessity, Cambridge 1980, S. 107, der die Herstellung der ursprünglichen Identität als „Taufe“ bezeichnet. Beide weisen darauf hin, dass es sich um eine unhintergehbare Voraussetzung handelt.

derliche Identität als hinreichend konstituiert ansieht. Eindrücklich sichtbar wird das insbesondere im parallel geführten technischen Anonymisierungsdiskurs, der durchgehend unter der Prämisse einer im Zusatzwissen der Verarbeiterin bereits hinreichend etablierten Identität geführt wird[15] und damit die Operation der Identifikation als Vorgang der „record linkage" über einen Ähnlichkeitsvergleich der Attributwerte eines angegriffenen Datensatzes bestimmen kann. Die Herstellung dieser ursprünglichen Identität wird damit als notwendige Voraussetzung begriffen, die im Wesentlichen im pragmatischen Belieben des Datenbankherstellers liegt[16]. Auch an dieser Stelle zeigt sich die notwendige Systemrelativität des Personenbezuges, denn jede Identifikation setzt eine ursprüngliche Identitätsherstellung voraus, die technisch durch eine bestimmte Kombination von Attributwerten innerhalb eines Attributschemas verwirklicht wird. Der Wortlaut des Datenschutzrechts in Artikel 4 Nr. 1 der Verordnung sieht an dieser Stelle nur eine beispielhafte Aufzählung von „insbesondere" in Betracht kommenden „Kennungen" vor, wie etwa Namen oder Kennnummern. Damit wird deutlich, dass das Datenschutzrecht von einem funktionalen Identitätsbegriff ausgeht, es also keineswegs auf Kategorien wie die des bürgerlichen Namens ankommt, sondern nur auf die Schaffung der Voraussetzung einer Beobachtungsverknüpfung in Form von sinnhaften Aussagen über eine designierte Entität.

Ein Beispiel dafür wäre etwa das sogenannte datr-Cookie, welches bei einem Besuch der Facebook-Webseite auf dem Rechner gespeichert wird, von dem der Zugriff mittels des Browsers stattfindet. Es handelt sich um eine Textdatei, die wenige Einträge wie etwa das Erzeugungs- und Ablaufdatum, eine eindeutige Buchstabenkette und Datum und Zeit des letzten Zugriffs enthält. Das Cookie besitzt einen Gültigkeitszeitraum von zwei Jahren und kann von Facebook etwa auch dann abgerufen werden, wenn sogenannte „Social Plugins" auf Drittseiten eingebunden und diese abgerufen werden. Es ist Facebook damit relativ einfach möglich, eine Surfhistorie anzufertigen[17]. Auf dieser Grundlage kann dann etwa spezifische Werbung über das Facebook-Werbenetzwerk ausgespielt werden. Diese Spezifizierung der ausgespielten Inhalte erfolgt anhand der von Facebook generierten Erwartungshorizonte hinsichtlich zukünftigen Surfhaltens; die Informativität der über das Cookie verknüpften Beobachtungen, die als strukturierte Daten vorliegen, besteht dann darin, diese Erwartungswerte in die eine oder andere Richtung zu beeinflussen.

[15] Nur selten so explizit wie bei Willenborg/Waal, Elements of Statistical Disclosure Control, New York 2001, S. 41: „A requirement of a target unit is that it be identfiable, that is that it has an associated identity.".

[16] Dazu und näher zu den technischen Hintergründen insgesamt Hölzel, DuD 2018, S. 502ff.

[17] So korrekt das OLG Düsseldorf im Vorlagebeschluss vom 19.01.2017, I-20 U 40/16. Der EuGH hat in der darauffolgenden Entscheidung vom 29.07.2019, C-40/17 – Fashion iD diese Prämisse übernommen, ohne diese selbst zu überprüfen.

„ÜBER“

Der traditionelle Ansatz qualifiziert über dieses Element den Aussagegehalt des Datums im Hinblick auf die zumindest identifizierbare Person. Innerhalb dieses Ansatzes werden drei mögliche Dimensionen unterschieden, nach denen dieser besondere Aussagegehalt beurteilt werden kann: nach Inhalt, nach Zweck und nach dem Ergebnis. Das Inhaltselement sei dann anzunehmen, wenn „Informationen über eine bestimmte Person gegeben werden“[18], das Zweckelement dann, wenn das Datum mit dem Zweck verwendet werden wird, eine Person einer aufgrunddessen differenzierten Behandlung zu unterziehen und das Ergebniselement schließlich dann, wenn sich die Verwendung des Datums auf Rechte und Interessen der Person auswirken könnte.

Das Verhältnis dieser durch den Wortlaut der Verordnung nicht induzierten Differenzierung in drei Unterelemente bleibte dabei über die Feststellung, es handele sich um alternative, nicht um kumulative Kriterien, unklar. So bleibt etwa offen, wie z.B. im Rahmen des Zweckelementes einer Person eine bestimmte Behandlung angediehen werden kann, ohne zugleich an einer ihr zugesprochenen Eigenschaft anzuknüpfen, die in Form einer Aussage über diese Person dargestellt werden kann. Die Einführung eines Inhaltselementes in der Bestimmung der Artikel-29-Gruppe ist auch logisch zirkulär insofern, als dieses immer dann bejaht werden soll, wenn „Informationen über eine bestimmte Person gegeben werden“. Genau diese Frage ist aber noch zu beantworten, sodass es sich bei diesem Element im Wesentlichen um eine tautologische Wiedergabe der Ausgangsfrage handelt. Deutlich wird dabei der objektivistische Interpretationshorizont, der der Analyse der Artikel-29-Gruppe zugrunde liegt, nach der versucht wird, das Kriterium des Personenbezuges ohne Rekurs auf ein kognitives System zu bestimmen. Erreicht wird damit freilich nur eine Verdunkelung der dann zugrundegelegten Interpretationskriterien, in der die Bestimmung dann gleichsam in der „Natur des Datums“ liegt[19].

Mit dem Zweck- und dem Ergebniselement ist hingegen einem systemrelativen Ansatz bereits der Weg geebnet, indem die Interpretation auf dem Datum selbst externe Bedingungen zurückgreift. Beide Elemente können dann auf die jeweiligen Entscheidungsprogramme der Verarbeiterinnen, in denen an Personenmodellen angeknüpft wird, zurückgeführt werden, indem das Zweckelement den Horizont der intendierten Folgen, das Ergebniselement den Horizont der nichtintendierten Nebenfolgen als Interpretationskriterien absteckt. Präzisierend sei für das Ergebnise-

[18] WP136, S. 11.

[19] Dabei dürften insbesondere aus Perspektive der Rechtsanwendung unabweisbare praktische Bedürfnisse eine Rolle spielen, um die in der Praxis kaum einmal erfüllbaren Anforderungen einer systemrelativen Beurteilung auf ein handhabbares Maß zu reduzieren. Die dann aber eigentlich sofort offenkundige Frage nach der prinzipiellen Geeignetheit eines so gestalteten Regulierungsmodells wird aber kaum einmal gestellt.

lement lediglich angefügt, dass es sich um für die Verarbeiterin reflektierbare Nebenfolgen handeln muss, sodass es sich bei der ex-post-Feststellung, ein bestimmtes Datum habe als Ursache einer differenzierten Behandlung gewirkt, für sich genommen nicht ausreicht, solange dieser Umstand für die Verarbeiterin nicht erkennbar war[20]. Festzuhalten ist, dass das Element „über" den Kreis der von der Verarbeitung in datenschutzrechtlich relevanter Weise Betroffenen konkretisiert. Daten beziehen sich damit dann auf identifizierbare Personen, wenn diese nach den Entscheidungsprogrammen der Verarbeiterinnen die Ursache[21] einer differenzierten Behandlung dieser Person darstellen.

FAZIT

Die vorstehenden Ausführungen sollten verdeutlichen, dass im Rahmen eines systemrelativen Ansatzes der Auslegung des Personenbezuges die kognitiv-normativen Strukturen – Erwartungen an Personen sowie Entscheidungsprogramme – der Verarbeiterinnen in den Mittelpunkt rücken. Es handelt sich um einen im Sinne der Schutzgüter des Datenschutzrechts[22] – die Grundrechte und Grundfreiheiten natürlicher Personen als Betroffene automatisierter Datenverarbeitungen – längst überfälligen Schritt[23], denn die Interpretationslinie der letzten 40 Jahre konnte die Unsicherheiten der praktischen Anwendung nicht überwinden. Aus rechtspolitischer Perspektive wäre schließlich die Konsequenz zu ziehen, das sachliche Anwendungskriterium „personenbezogene Daten" durch ein entsprechend explizit entscheidungsorientiertes Konzept zu ersetzen[24].

[20] Als Instrument für die Etablierung eines konkreten Erkennbarkeitsmaßstabes dürfte sich z.B. die Datenschutz-Folgeabschätzung in Artikel 35 der DS-GVO eignen.

[21] Das betrifft, wie eben ausgeführt zukünftige Ursachen, die anhand der Reflexion von intendierten Folgen und Nebenfolgen der Entscheidungsprogramme bezeichnet werden können, sowie vergangene Ursachen nur dann, wenn deren Ursächlichkeit für die Verarbeiterin bei Anwendung geeigneter Reflexionsmittel erkennbar waren.

[22] Des aktuell geltenden Datenschutzrechts, wohlgemerkt, und nicht der innerhalb der Datenschutzrechtstheorie beschreibbaren Schutzgüter.

[23] So auch Jörg Pohle, Personal Data Not Found, DANA – Datenschutz Nachrichten 1/2016, S. 14ff.; ders., Datenschutz und Technikgestaltung, Berlin 2018, insbes. S. 251ff.; Moritz Karg, Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes?, ZD 2012, S. 255ff.

[24] So ebenfalls die Forderungen von Pohle, ibid., der an personenbezogenen Entscheidungen anknüpfen will, und Karg, ibid., der von personenbezogenen Verfahren spricht.