Flächennutzungsmonitoring VI
Innenentwicklung – Prognose – Datenschutz

IÖR Schriften Band 65 · 2014

ISBN: 978-3-944101-65-1

Datenschutz bei kleinräumigen Auswertungen – Anforderungen und Grenzwerte

Sven Hermerschmidt

Hermerschmidt, Sven (2014): Datenschutz bei kleinräumigen Auswertungen – Anforderungen und Grenzwerte. In: Gotthard Meinel, Ulrich Schumacher, Martin Behnisch (Hrsg.): Flächennutzungsmonitoring VI. Innenentwicklung – Prognose – Datenschutz. Berlin: Rhombos-Verlag, 2014, (IÖR-Schriften; 65), S. 251-259

Datenschutz bei kleinräumigen Auswertungen – Anforderungen und Grenzwerte

Sven Hermerschmidt

Zusammenfassung

Wissenschaft, Wirtschaft und Verwaltung sind in zunehmendem Maße auf georeferenzierte Informationen angewiesen. Dabei wächst auch der Bedarf an möglichst kleinräumigen Auswertungen, sei es zu Planungszwecken, zur Optimierung von Geschäftsmodellen oder zur Verbesserung wissenschaftlicher Analysen.

Die Informationstechnik sowie das vorhandene Datenmaterial an Geobasis- und Geofachdaten versetzen datenverarbeitende Unternehmen in die Lage, derartige Auswertungen mit überschaubarem Aufwand durchzuführen. Dabei sind die Möglichkeiten, ganz unterschiedliche georeferenzierte Informationen aus verschiedenen Quellen zusammenzuführen, miteinander zu verschneiden, daraus neue Erkenntnisse zu gewinnen und die so gewonnenen Informationen wiederum mit weiteren Daten zu verknüpfen, scheinbar unbegrenzt.

Die unendlichen technologischen Möglichkeiten treffen jedoch auf ein vorhandenes Umfeld rechtlicher Rahmenbedingungen, in das sie eingebettet werden müssen. Geht es um die Verarbeitung georeferenzierter Informationen, bildet das Datenschutzrecht einen wichtigen regulatorischen Rahmen, in dem sich kleinräumige Auswertungen bewegen müssen. Dabei fällt auf, dass ungeachtet des hohen Datenschutzbewusstseins in Deutschland im Zusammenhang mit der Verarbeitung geografischer Informationen eine eher geringe Sensibilität für den Datenschutz vorhanden ist. Öffentliche Debatten, z. B. zu Panoramadiensten wie Google Street View, haben auf der anderen Seite für eine gewisse Verunsicherung gesorgt. Schnell steht der Vorwurf im Raum, die datenschutzrechtlichen Regeln behindern die technologische Entwicklung.

Der folgende Beitrag soll deshalb einige wichtige datenschutzrechtliche Fragen im Zusammenhang mit der Verarbeitung georeferenzierter Informationen beleuchten.

1 Was haben Geodaten mit Datenschutz zu tun?

Geodaten sind in erster Linie Sachdaten. Sie treffen eine Aussage über bestimmte Eigenschaften eines Punktes oder einer Fläche auf der Erdoberfläche. Der Datenschutz beschäftigt sich nicht mit Sachdaten, sondern mit personenbezogenen Daten. Deshalb muss man sich die Frage stellen, wann Geodaten zu personenbezogenen Daten werden und welche Folgen dies hat.

Bedenkt man die weitreichende öffentliche Verfügbarkeit von Geoinformationen ist zudem fraglich, ob deren weitere Verarbeitung Persönlichkeitsrechte tangiert oder nicht, unabhängig davon, ob die Daten als personenbezogen betrachtet werden oder nicht.

1.1 Sachdaten oder personenbezogene Daten

Gegenstand der Betrachtung sind zunächst die Geodaten. Geodaten werden im Geodatenzugangsgesetz des Bundes, das auf der INSPIRE-Richtlinie beruht, als Daten mit direktem oder indirektem Bezug zu einem Standort oder einem geografischen Gebiet definiert.

Personenbezogene Daten sind nach der Definition in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Kombiniert man beide Definitionen miteinander, erhält man eine Definition für personenbezogene Geodaten: Einzelangaben über (persönliche oder) sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person mit direktem oder indirektem Bezug zu einem Standort oder geografischen Gebiet.

Die praktische Bedeutung dieser notwendigerweise abstrakten Beschreibung lässt sich am besten anhand der einzelnen Elemente der Definition erläutern.

1.1.1 Einzelangaben

Eine Einzelangabe ist jede Information, die sich singulär auf einen bestimmten Gegenstand bezieht. Sie verknüpft also die einzelne Information, das einzelne Merkmal mit einem Gegenstand, der noch nicht notwendigerweise einer Person zugeordnet sein muss. Handelt es sich um zusammengefasste oder aggregierte Angaben, kann dementsprechend nicht mehr von Einzelangaben gesprochen werden.

Für die Geodaten bedeutet dies, dass Informationen, die großräumige geografische Gebiete darstellen und sich auf Phänomene wie z. B. Klima, Topographie oder Böden beziehen, regelmäßig keine Einzelangaben sind. Dies gilt auch dann, wenn sie als Merkmal einem bestimmten Punkt der Erdoberfläche zugeordnet werden können, Beispiel: „Die Stadt Dresden befindet sich in der gemäßigten Klimazone“.

Kleinräumige Informationen, die sich auf ein bestimmtes Grundstück beziehen, sind in der Regel Einzelangaben. Dabei kann es sich um Informationen zu Art und Maß der baulichen Nutzung, zur Verkehrserschließung oder auch zu konkreten Umwelteigenschaften handeln, Beispiel: „Grundstück X befindet sich in einem hochwassergefährdeten Gebiet mit dem Hochwasserrisiko Y“.

1.1.2 Persönliche oder sachliche Verhältnisse

Einzelangaben sind nur dann personenbezogen, wenn sie etwas über die persönlichen oder sachlichen Verhältnisse einer Person aussagen.

Eine Differenzierung zwischen sachlichen und persönlichen Verhältnissen ist schwierig, da die sachlichen Verhältnisse (z. B. bauliche Eigenschaft eines Grundstücks) auch eine Aussage über persönliche Verhältnisse (z. B. Alter oder Gesundheitszustand) treffen können. Da beide Merkmale gleichberechtigt nebeneinander stehen, ist diese Unterscheidung von untergeordneter Bedeutung.

Die sachlichen oder persönlichen Verhältnisse sind der Bezugsgegenstand der Einzelangabe, welche nicht für sich steht, sondern immer eine bestimmte Aussage trifft. Gleichzeitig stellen sie das verbindende Merkmal zwischen Einzelangabe und Person dar.

So treffen konkrete Informationen über die Hochwassergefährdung eines bestimmten Grundstücks (auch) eine Aussage über die sachlichen Verhältnisse einer Person, nämlich über den Wert des Grundstücks und damit über das Vermögen des Eigentümers des Grundstücks.

1.1.3 Bestimmte oder bestimmbare natürliche Person

Wichtigstes Merkmal eines personenbezogenen Datums ist, dass sich die Einzelangaben auf eine bestimmte oder bestimmbare natürliche Person beziehen. Dies bedeutet zunächst, dass nur lebende natürliche Personen vom Datenschutz erfasst werden. Die datenschutzrechtlichen Bestimmungen schützen also in der Regel weder juristische Personen noch verstorbene Personen, sofern nicht ausnahmsweise gesetzlich etwas anderes angeordnet wird.

Wie die Gleichsetzung von „bestimmt“ und „bestimmbar“ zeigt, hat sich der Gesetzgeber für einen weiten Begriff des Personenbezugs entschieden: Informationen sind also nicht nur dann personenbezogen, wenn aus ihnen, etwa durch Nennung eines Namens in Verbindung mit einer Anschrift, eindeutig und für jedermann erkennbar der Bezug zu einer bestimmten Person hergeleitet werden kann.

Personenbezug wird vielmehr auch schon dann angenommen, wenn die Informationen einer natürlichen Person zugeordnet werden können. Demzufolge entfällt ein Personenbezug erst dann, wenn diese Zuordnung nicht mehr möglich ist. Dies ist erst dann der Fall, wenn die Daten anonym sind. Das Gesetz legt dabei einen relativen Ansatz zugrunde: Daten werden schon dann als anonym angesehen, wenn sie nur noch mit unverhältnismäßig hohem Aufwand an Kosten, Zeit und Arbeitskraft einer natürlichen Person zugeordnet werden können.

Das Gesetz trifft unmittelbar keine Aussage darüber, für wen die Person bestimmbar sein muss. Es wird daher vertreten, dass nur dann von einem Personenbezug auszugehen sei, wenn die verantwortliche Stelle selbst in der Lage ist, die Informationen einer Person zuzuordnen. Dies würde bedeuten, dass die Daten für diejenigen, die selbst nicht unmittelbar die Informationen einer natürlichen Person zuordnen können, u. U. als anonymisiert angesehen werden könnten. Damit könnte ein und dasselbe Datum sowohl personenbezogen als auch nicht personenbezogen sein, je nachdem, von wem es verarbeitet wird.

Dieser sog. relative Begriff des Personenbezugs wird von den Datenschutzaufsichtsbehörden überwiegend abgelehnt und stattdessen ein absoluter Begriff des Personenbezugs vertreten. Demnach sind Daten erst dann als anonym zu betrachten, wenn niemand mehr in der Lage ist, die Informationen einer natürlichen Person zuzuordnen.

Diese Unterscheidung ist nicht allein theoretischer Natur, sondern hat durchaus gravierende Konsequenzen: Legt man den absoluten Begriff des Personenbezugs zugrunde sind auch solche Daten als personenbezogen anzusehen, bei denen die potenzielle Möglichkeit der Herstellung eines Personenbezugs besteht, auch wenn die verantwortliche Stelle vielleicht selbst gar kein Interesse am Personenbezug hat. So sind z. B. Daten über eine Internetnutzung, die lediglich mit einer IP-Adresse verknüpft sind, als personenbezogene Daten zu betrachten, da – etwa mithilfe des Access Providers – eine Zuordnung zur Person des Internetnutzers in vielen Fällen ohne unverhältnismäßig großen Aufwand möglich sein wird.

Ein solches weites Verständnis des Personenbezugs ist durchaus geboten, da anderenfalls ein wirksamer und umfassender Grundrechtsschutz für den Einzelnen nicht gewährleistet wäre.

Für die Geoinformationen bedeutet das, dass solche Informationen, die sich auf ein konkretes Grundstück beziehen, grundsätzlich als personenbezogene Daten anzusehen sind, sofern es sich bei dem Eigentümer oder sonst dinglich oder schuldrechtlich Berechtigten (z. B. Inhaber eines Nießbrauchrechts oder Mieter) um eine natürliche Person handelt. Dies gilt unabhängig davon, ob sich die Identität des Eigentümers unmittelbar aus den Informationen ergibt oder nicht. Denn es ist in der Regel nicht mit einem unverhältnismäßigen Aufwand an Kosten, Zeit und Arbeitskraft verbunden, die Person des Eigentümers/Berechtigten zu ermitteln.

1.2 Was bedeutet der Personenbezug grundstücksbezogener Informationen?

Aufgrund der Systematik des deutschen und europäischen Datenschutzrechts ist die Verarbeitung personenbezogener Daten verboten, sofern sie nicht aufgrund der Einwilligung des Betroffenen oder auf der Grundlage gesetzlicher Bestimmungen erlaubt ist.

Dies bedeutet aber nicht automatisch, dass die Verarbeitung grundstücksbezogener Informationen weitgehend unzulässig wäre, nur weil es sich hier regelmäßig um personenbezogene Daten handelt. Der Personenbezug führt (lediglich) dazu, dass bei der Verarbeitung grundstücksbezogener Informationen die datenschutzrechtlichen Rahmenbedingungen zu beachten sind.

Die Einwilligung des Betroffenen wird bei der Verarbeitung von personenbezogenen Geodaten häufig als Legitimation nicht in Betracht kommen, da gerade bei der Einbeziehung von Daten einer größeren Zahl von Grundstücken der hierfür zu leistende Aufwand sehr hoch wäre.

Sofern die Einwilligung nicht in Betracht kommt, bedarf die Verarbeitung personenbezogener Geodaten daher einer rechtlichen Grundlage in den Datenschutzgesetzen von Bund und Ländern. Dabei wird in Deutschland zwischen der Verarbeitung personenbezogener Daten durch Behörden oder anderen öffentlichen Stellen einerseits und der Verarbeitung durch Unternehmen, Freiberufler, Vereine und anderer sog. nicht-öffentlicher Stellen andererseits unterschieden.

Öffentliche Stellen dürfen – vereinfacht gesagt – personenbezogene Daten dann verarbeiten, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Das bedeutet, dass sie sich auf dasjenige beschränken müssen, was zur Erfüllung ihrer Aufgaben tatsächlich notwendig ist. Reine Zweckmäßigkeitsgesichtspunkte vermögen Eingriffe in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung nicht zu rechtfertigen.

Nicht-öffentliche Stellen dürfen – abgesehen von der Einwilligung – personenbezogene Daten grundsätzlich dann zu eigenen geschäftlichen Zwecken verarbeiten, wenn dies zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist oder sie ein berechtigtes Interesse an der Verarbeitung haben. Im letzteren Falle müssen die berechtigten Interessen mit den schutzwürdigen Interessen der Betroffenen abgewogen werden; eine Verarbeitung darf nur erfolgen, wenn die berechtigten Interessen überwiegen.

Handelt es sich um Daten aus allgemein zugänglichen Quellen, so wird der Verarbeiter privilegiert. Seine berechtigten Interessen überwiegen nur dann nicht, wenn die schutzwürdigen Interessen des Betroffenen offensichtlich überwiegen. Dies ist für die Verarbeitung personenbezogener Geodaten von großer Bedeutung, da aufgrund der Umsetzung der INSPIRE-Richtlinie eine Vielzahl von Geodaten, auch personenbezogenen Geodaten, allgemein zugänglich ist.

Darüber hinaus ist auch die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung erlaubt und dies u. U. auch dann, wenn die Daten ursprünglich zu einem anderen Zweck erhoben und verarbeitet worden sind.

1.3 Zwischenfazit

Georeferenzierte Daten sind in jedem Falle immer dann als personenbezogene Daten im Sinne der datenschutzrechtlichen Bestimmungen anzusehen, wenn sie sich auf einzelne Grundstücke beziehen. Die Person des Eigentümers oder eines anderen Berechtigten an dem einzelnen Grundstück ist in der Regel ohne unverhältnismäßig hohen Aufwand an Kosten, Zeit und Arbeitskraft ermittelbar.

Deshalb sind bei der Erhebung, Verarbeitung und Nutzung grundstücksbezogener Daten und damit auch bei deren kleinräumiger Auswertung die datenschutzrechtlichen Bestimmungen zu beachten.

2 Lösungsansätze

Wie bereits angedeutet, bedeutet die weitreichende Einordnung georeferenzierter Daten als personenbezogene Daten nicht automatisch, dass deren Verarbeitung nicht mehr erfolgen kann.

Angesichts der hohen Komplexität der datenschutzrechtlichen Vorschriften stehen einzelne Verarbeiter jedoch häufig vor der Schwierigkeit einschätzen zu können, was erlaubt ist und an welcher Stelle ggf. mit Einschränkungen oder gar der Unzulässigkeit der Datenverarbeitung zu rechnen ist. Dies beginnt bei der hier skizzierten Frage, ob es sich überhaupt um personenbezogene Daten handelt und setzt sich fort mit dem Finden der notwendigen rechtlichen Grundlagen und deren Auslegung.

2.1 Beratung durch die Aufsichtsbehörden

Die Aufsichtsbehörden – seien es die für die Datenschutzaufsicht im Bereich der Privatwirtschaft zuständigen Aufsichtsbehörden der Länder oder die für die öffentliche Verwaltung in Bund und Ländern jeweils zuständigen Bundes- bzw. Landesdatenschutzbeauftragten – haben nicht nur den gesetzlichen Auftrag, die verantwortlichen Stellen im Rahmen ihrer Zuständigkeit zu kontrollieren. Sie sind vielmehr auch gehalten, die verantwortlichen Stellen bei der Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen zu beraten.

2.2 Selbstregulierung der geodatenverarbeitenden Wirtschaft

2.2.1 Ziel der Selbstregulierung und Verfahren

Seit einigen Jahren sind im Bereich der geodatenverarbeitenden Wirtschaft Bestrebungen zu beobachten, für den Umgang mit georeferenzierten personenbezogenen Daten im Wege der Selbstregulierung für mehr Rechtssicherheit und faire Wettbewerbsbedin-

gungen zu sorgen. Das Bundesdatenschutzgesetz sieht in § 38a die Möglichkeit vor, dass beispielsweise Verbände, die datenverarbeitende Unternehmen vertreten, im Wege der Selbstregulierung zur Verbesserung des Datenschutzes beitragen können.

Selbstregulierungsmechanismen (Codes of Conduct) nach § 38a BDSG können keine eigenständigen Befugnisse zur Verarbeitung personenbezogener Daten begründen. Diese grundsätzlichen Entscheidungen bleiben dem Gesetzgeber vorbehalten. Insofern verbleibt es auch bei einem bestehenden Code of Conduct bei den oben skizzierten grundsätzlichen datenschutzrechtlichen Rahmenbedingungen.

Der Zweck eines Codes of Conduct besteht vielmehr darin, die notwendigerweise sehr abstrakt gehaltenen datenschutzrechtlichen Vorschriften zu konkretisieren und für typische Anwendungen in einer bestimmten Branche mit Leben zu erfüllen. Insofern bietet sich die geodatenverarbeitende Branche als Beispiel für die Etablierung von Selbstregulierungsmechanismen in Form eines Codes of Conduct geradezu an.

Um sicherzustellen, dass ein Code of Conduct mit dem Datenschutzrecht vereinbar ist, muss er vom verantwortlichen Verband der zuständigen Aufsichtsbehörde vorgelegt werden, die die Vereinbarkeit mit dem Datenschutzrecht prüft. Kommt sie zu einem positiven Ergebnis, wird die Vereinbarkeit mit einem feststellenden Verwaltungsakt bestätigt.

2.2.2 Möglicher Inhalt: Festlegung von Schwellenwerten

Ein Code of Conduct könnte einerseits verfahrensmäßige bzw. technische und organisatorische Sicherungen enthalten, die zu einer Verbesserung des Datenschutzniveaus und gleichzeitig für gleiche Bedingungen im Wettbewerb sorgen könnten. Vorstellbar wäre etwa die standardisierte Akkreditierung von bestimmten Geschäftsmodellen oder die Vorgabe, ein Datenschutzmanagement zur Einhaltung bestimmter Standards im technischen und organisatorischen Datenschutz einzuführen.

Darüber hinaus können aber auch die rechtlichen Anforderungen in einer Weise konkretisiert werden, dass ein Code of Conduct auch in dieser Weise einen echten Mehrwert darstellt. In diesem Zusammenhang wird bei der Verarbeitung von personenbezogenen Geodaten über bestimmte Schwellenwerte diskutiert, bei deren Unterschreiten im Regelfall nur noch von einer geringen persönlichkeitsrechtlichen Relevanz ausgegangen wird. Dies ist vor allem immer dann von Bedeutung, wenn die gesetzlichen Bestimmungen eine Abwägung verschiedener Interessen vorsehen, so wie dies insbesondere bei der Abwägung des berechtigten Interesses eines Verarbeiters mit den schutzwürdigen Interessen des Betroffenen der Fall ist. Zudem hat diese Herangehensweise den Vorteil, dass über die im Einzelfall regelmäßig umstrittene Frage, ob es sich um personenbezogene Daten handelt, nicht zwingend entschieden werden muss. Denn dieser Ansatz unterstellt grundsätzlich den Personenbezug, trägt jedoch der unterschiedlichen Eingriffstiefe Rechnung.

Konkret werden hier folgende Schwellenwerte diskutiert:

- Auflösung ≥ 20 cm pro Bildpunkt (bei Satelliten- bzw. Luftbildinformationen)
- Maßstab ≤ 1:5 000 (bei Kartendarstellungen)
- Darstellung auf einer gerasterten Fläche ≥ 100 m x 100 m
- Aggregierung auf mindestens 4 Haushalte

Werden diese Schwellenwerte unterschritten, so geht die Mehrzahl der Aufsichtsbehörden von einer geringen persönlichkeitsrechtlichen Relevanz aus mit der Folge, dass Abwägungsprozesse in der Regel zugunsten der verantwortlichen Stelle ausgehen. Dies gilt ungeachtet der Frage, dass auch bei einem Unterschreiten dieser Schwellenwerte häufig noch von einem Personenbezug auszugehen ist.

Diese Schwellenwerte sind keine verbindliche gesetzliche Regelung. Sie sind jedoch ein starkes Indiz für die Frage der Zulässigkeit der Verarbeitung personenbezogener Geodaten.

2.2.3 Weiterverarbeitung zulässig erhobener und verarbeiteter Geodaten

Sind Geodaten auf zulässige Weise erhoben und werden sie für einen bestimmten (primären) Zweck nach den o. g. Kriterien in zulässiger Weise verarbeitet, stellt sich die Frage nach der Zulässigkeit der Weiterverarbeitung dieser Daten für andere Zwecke.

Auch hierfür gelten selbstverständlich die datenschutzrechtlichen Rahmenbedingungen. Es bedarf also wiederum einer Einwilligung oder einer Rechtsgrundlage im Datenschutzrecht. Vorrangig ist jedoch immer zu prüfen, ob die Daten in einer Weise aggregiert oder sonst verändert werden können, dass von einer Anonymität der Daten ausgegangen werden kann. Dies folgt schon aus dem übergreifenden datenschutzrechtlichen Prinzip von Datenvermeidung und Datensparsamkeit (§ 3a BDSG).

Die Daten unterliegen zudem einer Zweckbindung, d. h. der Primärzweck haftet den Daten in einer Weise an, dass sie grundsätzlich nur für diesen Zweck weiterverarbeitet werden dürfen. Dies dient der Transparenz für den Betroffenen, der grundsätzlich nachvollziehen können soll, wer was wann bei welcher Gelegenheit über ihn weiß. Die Datenschutzgesetze erlauben allerdings unter bestimmten Bedingungen ein Abweichen von der Zweckbindung; so ist z. B. die wissenschaftliche Forschung hierbei privilegiert.

Ein besonderes Problem ist die Verknüpfung und Verschneidung zunächst eher „harmloser" personenbezogener Daten zu neuen Daten, aus denen völlig neue, für den Betroffenen u. U. sehr sensible, Erkenntnisse gewonnen werden können. Die Nutzung von Big-Data-Technologien ermöglicht hier die Bildung umfassender Profile über identifizierbare Personen. Aufgrund der nicht unerheblichen Gefahren für die Datenschutzrechte des Einzelnen, sind derartige Datenverarbeitungen nur unter sehr engen Voraussetzungen zulässig.

3 Literatur

BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2011): Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010. 23. Tätigkeitsbericht, 41-47.

BMI – Bundesministerium des Innern (2012): Vorsprung durch Geoinformationen – Dritter Bericht der Bundesregierung über die Fortschritte zur Entwicklung der verschiedenen Felder des Geoinformationswesens im nationale, europäischen und internationalen Kontext. 3. Geo-Fortschrittsbericht der Bundesregierung, 30-31.

Forgó, N.; Krügel, T. (2010): Der Personenbezug von Geodaten – Cui bono, wenn alles bestimmbar ist? Multimedia und Recht, 17.

IMAGI – Interministerieller Ausschuss für Geoinformationswesen (2014): Behördenleitfaden zum Datenschutz bei Geodaten und -diensten.

Karg, M. (2010): Datenschutz für Geodaten. Datenschutz und Datensicherheit, 824.

Karg, M. (2012): Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes? Zeitschrift für Datenschutz 2012, 255.

Lindner, C. (2010): Persönlichkeitsrecht und Geo-Dienste im Internet – z. B. Google Street View/Google Earth, Zeitschrift für Urheber- und Medienrecht, 292.

Martini, M.; Damm, M. (2014): Der Zugang der Öffentlichkeit zu hochauflösenden Satellitenbildern. Neue Juristische Wochenschrift, 130.

Moos, F.; Zeiter, A. (2013): Vorabwiderspruch bei Geodatendiensten – Gesetz oder Geste? – Zwischenbilanz anhand erster Gerichtsentscheidungen zu Google Street View. Zeitschrift für Datenschutz, 178.

RatSWD – Rat für Sozial- und Wirtschaftsdaten (2011): Endbericht der AG „Georeferenzierung von Daten" des RatSWD.

Weichert, T. (2007): Der Personenbezug von Geodaten. Datenschutz und Datensicherheit, 113.