Datenschutzfragen im Geoinformationsbereich

Karin DOLLINGER

Datenschutz ist eine bislang hauptsächlich juristisch dominierte Materie, die sich kaum mit konkreten Fragestellungen aus dem Geoinformationsbereich beschäftigt hat. Entsprechend gering ist auch die Literatur und Rechtsprechung zu dieser Thematik.

Umgekehrt wurden im technisch dominierten und anwendungsorientierten Geoinformationsbereich kaum grundlegende Rechtsfragen beleuchtet. Diese gewinnen nun durch die – aber immer noch sehr technisch bestimmte – INSPIRE-Richtlinie 2007/2/EG samt ihren Durchführungsverordnungen an Bedeutung. Davon zeugt auch die für 25. Juni 2009 in Neustrelitz, Mecklenburg-Vorpommern, angesetzte Fachtagung „Privatsphäre – gefangen im Netz der Koordinaten“. In Amerika finden sich wissenschaftliche Arbeiten zu diesem Themenkreis unter den Schlagworten „Geospatial Privacy“ bzw. „Spatial Confidentiality“.

Gemäß Artikel 1 Abs. 1 der Datenschutz-Richtlinie 95/46/EG haben die Mitgliedstaaten den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Artikel 2 beinhaltet die zugehörigen Begriffsbestimmungen, so etwa für „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „Datei mit personenbezogenen Daten“ etc. Artikel 3 Abs. 2 dieser Richtlinie (RL) nennt Ausnahmen vom Anwendungsbereich: Dazu gehören u. a. die Verarbeitung personenbezogener Daten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich.

Handelt es sich aber um besondere Kategorien personenbezogener Daten, so regelt Artikel 8 Abs. 1, dass die Mitgliedstaaten die Verarbeitung personenbezogener Daten untersagen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. Diesbezügliche Ausnahmefälle sind nur gegeben bei ausdrücklicher Einwilligung der betroffenen Person, bei Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person (sofern diese außerstande ist, ihre Einwilligung zu geben) oder, wenn sich die Verarbeitung auf Daten bezieht, die die betroffene Person offenkundig öffentlich gemacht hat.

Trotz dieser einheitlichen Richtlinie kam es zur Schaffung sehr verschiedener Datenschutzgesetze und Datenschutzbehörden in der Gemeinschaft. Die Handhabung und Auslegung erfolgen entsprechend unterschiedlich, obwohl das ursprüngliche Ziel der RL in der Ermöglichung des freien Datenverkehrs in der EU lag.

Datensammlungen vom Staat und von Privaten fanden schon seit langem statt (z. B. gibt es Volkszählungen seit 2000 Jahren). Die Gefährdung der elektronischen Privatsphäre erhielt aber durch den Einsatz von EDV eine neue Dimension. Die Entwicklung erfolgte ausgehend von einem Recht, das in den 1970er Jahren als Abwehrrecht gesehen wurde, zu einem Gestaltungsrecht, sodass die europäische Datenschutzentwicklung der 1980er Jahre bereits das Grundrecht auf informationelle Selbstbestimmung als Leitmotiv verfolgte.

Bereits 1980 gab es in Österreich ein Bundes-Datenschutzgesetz. Da es aber durch die Datenschutz-Richtlinie zu einer Aufnahme von Regelungen über die manuelle Verarbeitung von Daten kam, erhielten die Länder Gesetzgebungskompetenz für manuelle Dateien in Landesangelegenheiten, also für bestimmte Dateien, die nach wie vor manuell geführt werden (z. B. manuelle Register im Bereich des Fischerei- und Jagdrechts). Die Datenschutz-RL wurde daher in Österreich durch ein Bundes- und neun Länder-Datenschutzgesetze umgesetzt, entsprechend gering ist die Bedeutung der Landes-Datenschutzgesetze.

Mit dem Datenschutzgesetz 2000 (DSG 2000) wurden alle bisherigen Regelungen zum Datenschutz in Österreich tief greifend revisioniert und die Forderungen der Datenschutz-RL mehr als erfüllt. Unter das Datenschutzrecht fallen nämlich in Österreich neben den Daten natürlicher Personen auch die Daten von Unternehmen, womit sich die Normierungen von jenen der meisten anderen Staaten der EU unterscheiden.

Das Datenschutzrecht ist in Österreich ein verfassungsrechtlich gewährleistetes Grundrecht mit unmittelbarer Drittwirkung. § 1 Abs. 1 DSG 2000 regelt den Anspruch auf Geheimhaltung, Abs. 3 normiert das Auskunftsrecht sowie das Recht auf Richtigstellung und Löschung. Das Grundrecht auf Datenschutz umfasst demnach vier verschiedene Rechte.

§ 1 Abs. 5 DSG 2000 regelt, dass das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen ist. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, wenn nicht Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind. Die Datenschutzkommission verfügt weiters über ein umfassendes Kontrollrecht und über Genehmigungskompetenzen für den internationalen Datenverkehr. Im Vergleich zu anderen Datenschutzbehörden in der Union verfügt sie über wenig Personal, sodass sich eine Verlängerung der Verfahrensdauer ergibt, die im schnelllebigen Informationszeitalter für Unternehmen problematisch ist.

Knyrim weist auf eine Vielzahl von Problemen im Datenschutzrecht hin, u. a. seien in Österreich kaum Strafen zu befürchten und das Beschreiten des normalen Zivilrechtsweges bei Miniverstößen zu beschwerlich. Der Klagsweg sei oftmals überhaupt unbekannt, sodass die Datenschutzthemen über den Umweg des Wettbewerbsrechts zur Behandlung kämen. Hauptpunkt sei aber die Nicht-Wissens-Problematik, womit in der Folge durch uninformierte Akteure es entweder zur „Vogel-Strauß-Politik“ (Kopf in den Sand stecken und hoffen, dass nichts passiert) komme oder die „Datenschutzkeule“ geschwungen werde, um unliebsame Projekte zu erschlagen, anstatt rechtlich mögliche Lösungen zu suchen.

Datenschutzrechtliche Sonderbestimmungen finden sich weiterhin in Materiengesetzen, z. B. im Telekommunikationsgesetz 2003 oder im E-Governmentgesetz. Viele Normen weisen auch darauf hin, dass die datenschutzrechtlichen Bestimmungen unberührt bleiben sollen, z. B. das E-Commerce-Gesetz oder das Informationsweiterverwendungsgesetz (Umsetzung der PSI-RL durch den Bund).

In den vergangenen Jahren vergrößerte sich der Anwendungsbereich des Datenschutzrechtes durch v. a. technische Entwicklungen immens. Einerseits sind hier politische Vorhaben zu nennen, wie die Videoüberwachung an öffentlichen Plätzen und die Einführung der elektronischen Gesundheitskarte (E-Card) durch den Hauptverband der Sozialversicherungsträger. Andererseits ergeben sich zahlreiche Datenschutzbelange im wirtschaftlichen Bereich durch die Anbindung österreichischer Unternehmen an internationale Konzerne.

Die Berührungspunkte zwischen Geodaten und Geoinformationen und dem Themenkreis des Datenschutzes sind vielfältig, da jede natürliche Person prinzipiell durch die Adresse, an der sie gemeldet ist, verortet werden kann. Alle Informationen, die somit zu dieser Person an dieser Adresse gespeichert werden, stellen Geoinformationen dar. Es ist letztlich nur eine rechtliche Frage, welche dieser Daten zulässigerweise gespeichert, verknüpft und wieder verwendet werden dürfen. Es könnten beispielsweise in Österreich durch Verbindung von geokodierter Adresse, Nummer des Zentralen Melderegisters (ZMR-Nummer) und Gesundheitsdaten via E-Card Geodatenbanken geschaffen werden, die in der Folge Karten zur Verteilung spezifischer Krankheitsfälle erstellen ließen.

Für statistische Einheiten gelten bestimmte Mindestgrößen, sodass auf Einzelpersonen keine Rückschlüsse gemacht werden können, doch auch hier ist ein steigender Genauigkeitsbedarf zu verzeichnen: Wurden früher Regionalstatistiken auf Gemeindebasis dargestellt, so finden sich heute Kartendarstellungen auf verfeinerter Rasterbasis mit Rastern von bis zu 125 × 125 m² Untersuchungsgebiet.

Umgekehrt werden bewusst Geodatensätze zu personenbezogenen Inhalten angelegt. So wurden etwa ab 1991 spezielle Karten für das steirische Fehlbildungs-Register erstellt. Auch die INSPIRE-RL zählt in ihren Anhängen Themen auf, die unter diesem Gesichtspunkt zu betrachten sind. So sind etwa zum Thema „Gesundheit“ folgende Geodaten unionsweit zu sammeln, harmonisieren, mit Metadaten auszustatten und mittels verschiedener Dienste anzubieten: „Geografische Verteilung verstärkt auftretender pathologischer Befunde (Allergien, Krebserkrankungen, Erkrankungen der Atemwege usw.), Informationen über Auswirkungen auf die Gesundheit (Biomarker, Rückgang der Fruchtbarkeit, Epidemien) oder auf das Wohlbefinden (Ermüdung, Stress usw.) der Menschen in unmittelbarem Zusammenhang mit der Umweltqualität (Luftverschmutzung, Chemikalien, Abbau der Ozonschicht, Lärm usw.) oder in mittelbarem Zusammenhang mit der Umweltqualität (Nahrung, genetisch veränderte Organismen usw.)“.

Wenn auch Erwägungsgrund 24 der INSPIRE-RL lautet: „Die Bereitstellung von Netzdiensten sollte unter uneingeschränkter Beachtung der Grundsätze des Schutzes personenbezogener Daten nach der Richtlinie 95/46/EG ... erfolgen.“, so dürften doch viele offenen Fragen bestehen. Auch in Deutschland wurde im Zusammenhang mit dem Aufbau der nationalen Geodateninfrastruktur festgestellt, dass die Bestimmungen zum Datenschutz in Zusammenhang mit Geoinformationen noch nicht im Speziellen geregelt sind und hier Handlungsbedarf besteht.

Die INSPIRE-RL selbst führt lediglich in Artikel 13 an, dass die Mitgliedstaaten den Zugang der Öffentlichkeit zu Geodatensätzen und -diensten beschränken können, wenn dieser Zugang nachteilige Auswirkungen hätte auf: „ ... f) die Vertraulichkeit personenbezogener Daten und/oder Akten über eine natürliche Person, sofern diese der Bekanntgabe dieser Informationen an die Öffentlichkeit nicht zugestimmt hat und sofern eine derartige Vertraulichkeit nach einzelstaatlichem oder gemeinschaftlichem Recht vorgesehen ist; g) die Interessen oder den Schutz einer Person, die die angeforderte Information freiwillig zur Verfügung gestellt hat, ohne dazu gesetzlich verpflichtet zu sein oder verpflichtet werden zu können, es sei denn, dass diese Person der Herausgabe der betreffenden Informationen zugestimmt hat; ... “ Die Gründe für eine solche Zugangsbeschränkung sind dabei eng auszulegen und die Anforderungen der Richtlinie 95/46/EG sind einzuhalten.

Datenschutzbestimmungen können dort greifen, wo sich die staatliche Souveränität erstreckt, also im Staatsgebiet, das ist ein Teil der Erdoberfläche, der Untergrund und der Luftraum darüber. Konkret ließe sich eine Erstellung und Verbreitung (z. B. mit Online-Diensten von Behörden oder Google) von Orthofotos mit einer Genauigkeit detaillierter als 40 cm Pixel reglementieren, wenn dies tatsächlich, wie der deutsche Bundesverfassungsgerichtshof in seinem Mallorca-Urteil angesprochen hat, den Schutz personenbezogener Daten gefährden könnte. Es bestehen aber Probleme der Grenzziehung u. a. in der Luft gegenüber den Anrainerstaaten und gegenüber Räumen, die nicht anzeigenbar sind bzw. zum gemeinsamen Erbe der Menschheit gehören. Zur letzt genannten Kategorie zählt auch der Weltraum, in dem inzwischen Satelliten Fernerkundungsbildmaterial von im militärischen Bereich bis unter 10 cm Pixelgenauigkeit erzeugen. Dies wirft bisher wenig diskutierte Datenschutzfragen auf. Zumindest hat Deutschland diesen Problemkreis erkannt und 2007 ein „Bundesgesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten“ beschlossen.

Unabhängig von völkerrechtlichen Fragestellungen im Zusammenhang mit Fernerkundungsdaten ist die Verbreitung von hochauflösenden, entzerrten Farbluftbildern, deren Standardgenauigkeit derzeit bei 20-25 cm Pixel liegt, u. a. in Kombination weiterer in „GIS-Online-Systemen“ darüber legbarer Schichten (z. B. Grundstückskataster, Adressdaten – diese wiederum in Kombination mit elektronischen Telefonbüchern und Google-Schagwortsuchen) diskussionswürdig. Insbesondere naht nun der nächste technische-organisatorische Meilenstein, nämlich die Verfügbarkeit noch genauerer, flächendeckender Orthofotos auf Basis von Laserscanbefliegungen im öffentlichen Bereich. Zeitungsberichte sprechen davon, dass Einbrüche verstärkt und verbessert mit Online-Diensten in Kombination mit Luftbilddaten planbar seien, was die Brisanz des Themas unterstreicht. Medienberichten zufolge haben in England die Bewohner jene Fahrzeuge gestoppt, die für die Firma Google die Straßenzüge für die Anwendung „Street View“ fotografieren sollten, da durch eine solche Invasion auf die Privatsphäre nicht nur die Sicherheit gefährdet sei.

Neue Technologien, wie sie die Location Based Services darstellen, bringen auch neue Datenschutzfragen. Auf Basis der Standortermittlung von Geräten wie von Mobiltelefonen, GPS-Geräten, Chips und anderen verortbaren Produkten, können zurückgelegte Wege dieser Produkte selbst, von Tieren oder auch Menschen, erhoben und überwacht werden. Für GIS-Techniker ist sicherlich die Benutzerfreundlichkeit ausschlaggebend, wenn sie Geodaten, wie Straßenverläufe, mittels mobiler Dienste erfassen. Gleichzeitig ist aber auch nachvollziehbar, wann sich die erhebenden Personen in den jeweiligen Straßen befunden haben. In der Folge könnten diese Daten nämlich auch zur Kontrolle der Arbeitsleistung der erhebenden Personen verwendet werden.

Die bei den Mobilfunkbetreibern vorliegenden Standortdaten werfen überhaupt eine Menge neuer Fragestellungen auf, nicht nur im Hinblick auf die bisher diskutierten strafprozessualen oder sicherheitspolizeilichen Auskunftsbegehren bzw. unter welchen Bedingungen (z. B. richterlicher Befehl) diese Auskünfte erteilt werden müssen/dürfen. Heutige GIS-Projekte beschäftigen sich bereits mit der Erstellung von Nutzungskarten aus diesen laufend vorliegenden Standortdaten und können in Siedlungsgebieten gebäudegenau auswerten, wo Wohngebäude (verstärkt nur nachts mit Mobiltelefonen belegt), Bürogebäude oder Nachtlokale sind bzw. wo PKW oder Busse (wandernde rechteckige Punktewolke) fahren sowie Menschen (langsame Einzelpunkte) gehen.

Es ist zu hoffen, dass im Rahmen der Ausarbeitung von Durchführungsbestimmungen zu INSPIRE auch Datenschutzfragen betreffend den Geoinformationsbereich unionsweite Vorgaben erhalten. Andernfalls ist jeder Einzelne aufgerufen, auch trotz mühsamer Rechtsschutzmaßnahmen durch rechtliche Einzelentscheidungen die gewünschte Einhaltung der Datenschutzgrundrechte einzufordern.

Literatur

ANONYMUS (2007): Architektur der Geodateninfrastruktur Deutschland. Version 1.0. Konzept zur fach- und ebenenübergreifenden Bereitstellung von Geodaten im Rahmen des E-Government in Deutschland. o. O., 82 S.

BKA – BUNDESKANZLERAMT (2009): Rechtsinformationssystem Bundesrecht. Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 i. d. F. BGBl. I Nr. 2/2008.

DOLLINGER, K. (2008): Die Richtlinie 2007/2/EG zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) und weitere rechtliche Aspekte zur Führung öffentlicher Geodateninfrastrukturen. Diplomarbeit Rechtswissenschaftliche Fakultät der Universität Salzburg. Salzburg.

EUR-LEX (2009): Der Zugang zum EU-Recht. 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 (Datenschutz-RL). ABl. L 281 vom 23. November 1995, S. 31-50.

EUR-LEX (2009): Der Zugang zum EU-Recht. Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE). ABl. L 108 vom 25. April 2007, S. 1-14.

GIS-STEIERMARK (2007): Meilensteine GIS-Steiermark. http://gis2.stmk.gv.at/gis2.stmk.gv.at/gis/content/20_Jahre/Meilensteine/flash/index.html abgerufen am 16. Dezember 2007.

JAHNEL, D. (2004): Datenschutzrecht in der Praxis. Grundbegriffe, Zulässigkeit, Meldepflicht, Datensicherung, Rechtsschutz und Spamming. Graz und Wien (= Schriftenreihe „Arbeitsmaterialien zur Kanzleiorganisation“, Bd. V), 71 S.

KNYRIM, R. (2005): 25 Jahre Datenschutzrecht in Österreich. Bestandsaufnahme und Lösungsansätze für aktuelle Probleme. – In: medien und recht, 7/05, S. 415-420.

KNYRIM, R. und V. HAIDINGER (2005): Datenschutzrecht in Österreich aus Sicht der anwaltlichen Praxis. – In: RDV 2005, H. 5, S. 208-212.