LEITSÄTZE UND SCHAUBILDER NR. 8

8. Datenerhebung und Datenverarbeitung

Grundrechtserheblichkeit der Informationsverarbeitung

Die Polizei ist bei der Gefahrenabwehr auf die Erhebung und Verarbeitung von Daten angewiesen. Die Erhebung und Verarbeitung personenbezogener Daten sind Eingriffe in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I GG. Ihre verfassungsrechtliche Rechtfertigung setzt bereichsspezifische Datenschutzregelungen durch den parlamentarischen Gesetzgeber voraus. Das Polizeigesetz enthält daher umfassende Regelungen der polizeilichen Informationsgewinnung und –verarbeitung.

Das Recht auf Datenschutz schützt den Grundrechtsberechtigten gegen die Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten. Er kann über die Preisgabe und Verwendung seiner Daten grundsätzlich selbst bestimmen. Einschränkungen dieses Grundrechts sind nur zulässig, wenn sie einem überwiegenden Allgemeininteresse dienen. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem Verhältnismäßigkeitsgrundsatz und dem rechtsstaatlichen Gebot der Normenklarheit entspricht. Das Grundrecht ist durch organisatorische und verfahrensrechtliche Regeln abzusichern (BVerfGE 65, 1 – Volkszählung).

Personenbezogene Daten sind Daten, die in individualisierter, nicht anonymer Form erhoben werden. Hierzu zählt auch der sog. genetische Fingerabdruck, das DNA-Identifizierungsmusters eines Menschen. Ein Eingriff in das Recht auf Datenschutz ist durch ein legitimes Allgemeininteresse gerechtfertigt, wenn es die Aufklärung künftiger Straftaten von erheblicher Bedeutung erleichtert, einer an rechtsstaatlichen Garantien ausgerichteten Rechtspflege dient (BVerfGE 103, 21 – Genetischer Fingerabdruck).

Bei modernen Ermittlungsmethoden sind die Anforderungen an das Verfahren wegen des Gefährdungspotentials, das einem „additiven“ Grundrechtseingriff innewohnt, besonders zu beachten. Das gilt vor allem, wenn die Datenerhebung dem Betroffenen verborgen bleibt. Der Gesetzgeber muss die technische Entwicklung deshalb aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung und verfahrensrechtliche Vorkehrungen korrigierend eingreifen (BVerfGE 112, 304 – GPS-Überwachung).

Der Schutzbereich des Art. 10 GG erstreckt sich nicht nur auf die staatliche Kenntnisnahme von Telekommunikationskontakten, sondern auch auf den Informations- und Datenverarbeitungsprozess, der sich daran anschließt, sowie den Gebrauch, der von den erlangten Kenntnissen gemacht wird. Wenn der Gesetzgeber zu derartigen Eingriffen in das Fernmeldegeheimnis ermächtigt, verpflichtet ihn Art. 10 GG, Vorsorge gegen diejenigen Gefahren zu treffen, die sich aus der Erhebung und Verwertung personenbezogener Daten ergeben. Dazu gehört insbesondere, dass die Verwendung erlangter Kenntnisse an den Zweck gebunden werden, der die Erfassung

rechtfertigt. Die Übermittlung personenbezogener Daten an eine andere Behörde setzt voraus, dass sie für deren Zwecke erforderlich sind, die Anforderungen an Zweckänderungen beachtet werden und die gesetzlichen Übermittlungsschwellen dem Grundsatz der Verhältnismäßigkeit genügen (BVerfGE 100, 313 – Telekommunikationsüberwachung).

Das allgemeine Persönlichkeitsrecht (Art. 2 I i.V.m. Art. 1 I GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die heimliche Infiltration eines informationstechnischen Systems, durch das die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 I GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein (BVerfGE 120, 274 –Informationstechnische Systeme).

Die akustische Überwachung von Wohnraum setzt eine gesetzliche Ermächtigung voraus, die den Anforderungen des Art. 13 III GG entspricht. Darüber hinaus besteht ein durch Art. 1 I GG absolut geschützter Kernbereich privater Lebensgestaltung, in den bei der Überwachung von Wohnraum nicht eingegriffen werden darf. Insoweit darf nicht nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 I i.V.m. Art. 1 I GG) und dem Strafverfolgungsinteresse abgewogen werden. Werden bei der Überwachung gleichwohl Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung erhoben, muss sie abgebrochen werden. Die Aufzeichnungen sind zu löschen. Jede Verwertung solcher Informationen ist ausgeschlossen (BVerfGE 109, 279 – Akustische Wohnraumüberwachung).

Grundbegriffe der Datenverarbeitung

„Personenbezogene Daten“ sind nach § 3 I LDSG und § 3 I BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Die Datenverarbeitung bildet einen Oberbegriff, der auch die Datenerhebung umfasst. „Verarbeiten“ ist das Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen personenbezogener Daten (§ 3 II 1 LDSG, § 3 IV 1 BDSG). Grundlage der Informationsverarbeitung ist die Datenerhebung. „Erheben“ ist das Beschaffen von personenbezogenen Daten über den Betroffenen (§ 3 II Nr. 1 LDSG, § 3 III BDSG). Hierfür ist ein zielgerichtetes, aktives Handeln erforderlich. Unerheblich ist hingegen, wer Adressat der Maßnahme ist, mit welchen Mitteln und nach welcher Art und Weise Daten beschafft werden und ob bereits eine weitere Datenverarbeitung vorgesehen ist. Die Datenschutzgesetze des Bundes und der Länder enthalten auch Legeldefinitionen der weiteren Akte der Datenverarbeitung (vgl. § 3 II 2 LDSG, § 3 IV 2 BDSG).

Rechtsnatur polizeilicher Datenverarbeitungsmaßnahmen

Polizeiliche Maßnahmen der Datenverarbeitung sind als Verwaltungsakte zu qualifizieren, wenn sie eine rechtsverbindliche Regelung enthalten. Dies ist nicht der Fall, wenn Datenverarbeitungsmaßnahmen ohne Kenntnis des Betroffenen vorgenommen werden. Eine Regelung liegt auch dann nicht vor, wenn durch die Maßnahme keine Pflichten für den Betroffenen begründet werden.

Grundsätze der Datenerhebung

Nach dem Grundsatz der unmittelbaren Datenerhebung sind personenbezogene Daten, soweit sie nicht aus allgemein zugänglichen Quellen entnommen werden können, grundsätzlich beim Betroffenen mit dessen Kenntnis zu erheben (§ 19 I 1 PolG). Eine Ausnahme ist nur zulässig, wenn sonst die Wahrnehmung polizeilicher Aufgaben gefährdet werden würde oder die Daten nicht oder nur mit einem unverhältnismäßigen Aufwand erhoben werden könnten (§ 19 I 2 PolG). Nach dem Grundsatz der offenen Datenerhebung sind personenbezogene Daten grundsätzlich offen zu erheben (§ 19 II 1 PolG). Auch hier ist eine Ausnahme nur unter den oben genannten Voraussetzungen zulässig oder wenn anzunehmen ist, dass dies den überwiegenden Interessen des Betroffenen entspricht (§ 19 II 2 PolG).

Ermächtigungen für die Datenerhebung enthalten die §§ 20-25 PolG. § 19 PolG selbst bildet keine eigenständige Ermächtigungsgrundlage. § 20 II-V PolG sind allgemeine Ermächtigungsgrundlagen, die im Anwendungsbereich der speziellen Ermächtigungsgrundlagen der § 20 I und §§ 21-25 PolG sowie der Ermächtigungsgrundlagen in Spezialgesetzen verdrängt werden.

Weitere Datenverarbeitung
Jede Maßnahme der weiteren Verarbeitung personenbezogener Daten ist grundsätzlich ein Eingriff in das Recht auf Datenschutz, so dass auch hierfür bereichsspezifische Bestimmungen erforderlich sind. Die weitere Verarbeitung der erhobenen personenbezogenen Daten ist in §§ 37-48a PolG geregelt. Maßnahmen der Datenverarbeitung sind die Speicherung, Veränderung und Nutzung von Daten (§§ 37, 38 PolG), der Datenabgleich als spezielle Nutzungsart (§§ 39, 40 PolG), die Datenübermittlung (§§ 41-44 PolG) und die Löschung, Sperrung und Berichtigung von Daten (§ 46 PolG).