EU-Richtlinie - Datenschutz bei der Strafverfolgung

Laut EU-Kommission erfordere der besondere Charakter der polizeilichen und justiziellen Tätigkeiten in Strafsachen differenzierte Regeln für den Schutz personenbezogener Daten, um den freien Datenverkehr zu erleichtern und die Zusammenarbeit zwischen den Mitgliedstaaten in diesen Bereichen zu fördern.

Aus diesem Grund wurde die Richtlinie (EU 2016/680) über den Schutz personenbezogener Daten, die zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten verarbeitet werden, erlassen und am 5. Mai 2016 in Kraft gesetzt. In den Mitgliedstaaten sollte die Richtlinie bis zum 6. Mai 2018 in nationales Recht umgesetzt werden.

Die Kommission bezeichnet die Richtlinie zum Datenschutz bei der Strafverfolgung als das erste Instrument, mit dem ein umfassender Ansatz für den Datenschutz im Bereich der Strafverfolgung verfolgt werde, insbesondere durch die Regelung der „innerstaatlichen" Datenverarbeitung. Im Vergleich zu dem früheren Rahmenbeschluss, der lediglich die Datenübermittlung zwischen Mitgliedstaaten regele und durch die Richtlinie aufgehoben und ersetzt würde, stelle die Richtlinie mithin eine bedeutende Weiterentwicklung dar.

Die Mitgliedstaaten hatten nun durch eine Konsultation der EU-Kommission die Möglichkeit, zu der Richtlinie und der Umsetzung Stellung zu beziehen. Die Deutsche Polizeigewerkschaft (DPolG) hat diese Möglichkeit ergriffen.

In ihrer Stellungnahme betont die DPolG, dass das Spannungsfeld zwischen dem legitimen Anspruch jeder EU-Bürgerin und jedes EU-Bürgers auf Schutz der personenbezogenen Daten und gleichzeitig auf ein hohes Maß an öffentlicher Sicherheit, immer wieder neu austariert werden müsse.

Für die Polizeigewerkschaft gehe es aktuell vor allem um zwei Bereiche, die notwendig seien, um die Kriminalitätsbekämpfung adäquat zu ermöglichen und größtmögliche Sicherheit für die Bevölkerung zu gewährleisten – unter Wahrung datenschutzrechtlicher Bestimmungen.

Bei der Vorratsdatenspeicherung beziehungsweise Mindestspeicherfrist von Verbindungsdaten bestünden derzeit für die Erhebung und dauerhafte Speicherung personenbezogener Daten hohe Hürden. Dabei gehe es nicht um die Speicherung von Inhalten, sondern um das Erfassen der Verkehrsdaten. Nur über diese kann die Zuordnung von IP-Adressen zu konkreten Personen erfolgen. Das sei unerlässlich, zum Beispiel im Bereich der Strafverfolgung von Kinderpornographischen Inhalten.

Der Spielraum, den das aktuelle Urteil des Europäischen Gerichtshofs (EuGH) für die EU-Mitgliedstaaten eingeräumt hat, müsse hier nach Ansicht der DPolG genutzt werden. Das sorge in der Folge für Rechtsfrieden – nicht zuletzt für den persönlichen Frieden der Opfer.

Ein zweiter Bereich sei die Nutzung von intelligenter Videoaufklärung im öffentlichen Raum. Ein solcher Eingriff in Grundrechte müsse natürlich nicht nur in angemessenem Verhältnis zu den zu schützenden Rechtsgütern stehen, sondern auch so gering wie möglich gehalten werden. Moderne Videotechnik mache es möglich, sämtliche Personen für die unmittelbar vor dem Bildschirm sitzende Sicherheitskraft unkenntlich zu machen und trotzdem das Gesamtgeschehen zu betrachten.

Der Zugriff auf die entschlüsselnden Aufnahmen sollten rechtlich einer höheren Zugriffsebene, zum Beispiel einer polizeilichen Führungskraft, der Staatsanwaltschaft oder sogar einem Gericht übertragen werden. Damit wäre sichergestellt, dass nur in Fällen mit beweisbarem Grund tatsächlich auf diese sensiblen Daten zugegriffen werden kann. Die „Eingriffstiefe" in die Grundrechte würde drastisch verringert.

Intelligente Videosoftware sei außerdem für die Kriminalitätsbekämpfung und –prävention notwendig, um verdächtige oder gefährliche Situationen, häufig schon im Entstehungsprozess, zu erkennen und damit zu ermöglichen, dass Kräfte der Polizei oder des Ordnungsamtes alarmiert werden und eingreifen könnten.