Stellungnahme

Referentenentwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen
18. Dezember 2014

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Pablo Mentzinis
Bereichsleiter Public Sector
Tel.: +49.30.27576-130
Fax: +49.30.27576-51130
p.mentzinis@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

BITKOM begrüßt nachdrücklich, dass mit dem Referentenentwurf zur Einführung der elektronischen Akte in Strafsachen eine gesetzliche Grundlage für eine elektronische Aktenführung in Strafverfahren geschaffen und ausgestaltet werden soll.

Die Vorteile einer digitalisierten Akte sind offenkundig:

- Nachhaltige Prozessbeschleunigung und –vereinfachung. Die elektronische Aktenführung erlaubt automatisierte Verarbeitung personenbezogener Daten und ermöglicht damit im Vergleich zur Papierakte eine wesentlich einfachere und schnellere Durchsuchung, Filterung oder Verknüpfung von Daten. Die Bearbeitung der Akten wird durch die Strukturierung etwa nach Zeugenaussagen oder Verfahrensanträgen deutlich einfacher. Dies wird nachhaltig zur Beschleunigung von Strafverfahren beitragen.

- Die Digitalisierung kann vielfach auch unmittelbare wirtschaftliche Vorteile, da Verfahrenskosten insbesondere für die Vervielfältigung der Unterlagen deutlich gesenkt werden können. Welche extremen Kosten hierbei entstehen können, verdeutlicht exemplarisch ein Verfahren beim Oberlandesgericht Düsseldorf vom September 2014. Bei diesem Verfahren hatte ein Auslagen in Höhe von bis zu 67.000 € pro für den Ausdruck von knapp 380.000 Seiten aus elektronischen Datenträgern (erfolglos) geltend gemacht.[i] Sinnvoll strukturierte und ergonomische Datenaufbereitung helfen hier künftig, dass entsprechende Vervielfältigungen nicht mehr erforderlich und auch nicht mehr sinnvoll sind, da sich strukturierte elektronische Dokumente einfacher und schneller bearbeiten lassen.

- Durch die elektronische Aktenführung werden sich „die Akten“, auf die sich die Strafprozessordnung in verschiedenen Vorschriften bezieht in ihrer Form verändern: Sie sind nicht mehr ein physisches Objekt, das heißt im Wesentlichen miteinander verbundenes Papier, sondern ein definiertes System elektronisch gespeicherter Daten.

Daher begrüßt Bitkom nachdrücklich, dass das Bundesministerium für Justiz mit dem vorliegenden Referentenentwurf das Modernisierungspotential im Justizsektor nutzen will. Der Entwurf ist grundsätzlich geeignet, diesem Ziel gerecht zu werden. Zu einzelnen Bestimmungen möchte Bitkom dennoch Empfehlungen unterbreiten.

1 § 32 StPO-E – Verbindliche Einführung

§ 32 StPO-E schafft die Rechtsgrundlage für die verbindliche Einführung der elektronischen Akte in Strafsachen. Die Vorschrift ermächtigt zudem den Verordnungsgeber, technische und organisatorische Rahmenbedingungen zu regeln.

§ 32 Absatz 1 StPO-E verpflichtet alle am Strafverfahren beteiligten Behörden und Strafgerichte in Bund und Ländern dazu, Strafakten elektronisch zu führen. Die Regelung betrifft die elektronische Akte als maßgebliche (das heißt „führende“) Akte, die an die Stelle der bislang in Papierform geführten Akte tritt und sie ersetzt. Die Pflicht zur elektronischen Aktenführung umfasst das gesamte Strafverfahren vom Ermittlungsverfahren bis zum Vollstreckungsverfahren und schließlich die Ablage der Akten.

Zu Recht weicht § 32 Absatz 1 StPO-E von den Regelungen ab, die mit dem Justizkommunikationsgesetz vom 22. März 2005 in andere Verfahrensordnungen eingefügt wurden[ii] (u. a. § 298a Absatz 1 Satz 1 der Zivilprozessordnung [ZPO], § 110b Absatz 1 Satz 1 OWiG). Diese Regelungen hatten die Einführung der elektronischen Aktenführung insgesamt in das Ermessen der Verordnungsgeber der Länder gestellt. Wie das Ministerium selbst feststellt, hat sich diese Einführungsstrategie in der Praxis nicht als wirksam erwiesen: Von den seit dem 29. März 2005 bestehenden Möglichkeiten der Einführung elektronischer Akten ist in den anderen Verfahrensordnungen – von einzelnen Pilotierungen abgesehen – bisher kein Gebrauch gemacht worden. Der nun vorliegende Gesetzesentwurf schafft daher zu Recht mehr Verbindlichkeit.

2 § 32 StPO-E – Kohärente Fristengestaltung zu ERV-Gesetz

Der Gesetzesentwurf ermöglicht dem Landesgesetzgeber eine sogenannte Opt-Out-Befugnis. Den Landesregierungen wird die Möglichkeit eröffnet, die Pflicht zur elektronischen Aktenführung durch Rechtsverordnung bis zu einem Zeitpunkt vor dem 1. Januar 2024 ganz oder teilweise aufzuschieben.

Demgegenüber erweitert das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013[iii] den elektronischen Zugang zur Justiz durch bundeseinheitliche Regelungen in der Zivilprozessordnung und den anderen Verfahrensordnungen: Innerhalb eines Zeitraums von vier Jahren kann jedes Land durch Rechtsverordnung selbst bestimmen, wann der elektronische Zugang zu den Gerichten erweitert wird. Spätestens zum 1. Januar 2022 treten die Regelungen bundesweit und dann für Rechtsanwälte verpflichtend in Kraft.

Demgegenüber sieht § 32d StPO-E kein Vorziehen durch die Länder vor und ermöglicht umgekehrt einen Aufschub bis zum 1. Januar 2024. Die Einführung der elektronischen Strafakte und die Einführung elektronischer Akten in den

anderen Verfahrensordnungen sollten möglichst kongruent erfolgen. Daher sollte die Opt-out-Regelung zugunsten der Länder entsprechend angepasst werden, um sicherzustellen, dass spätestens zum 1. Januar 2022 alle gerichtlichen Akten elektronisch geführt werden können.

3 Keine hybriden Akten

Zu Recht verfolgt der Entwurf das Ziel, eine ausnahmslos elektronische Aktenführung in Strafsachen zu erreichen. Eine nur teilweise („hybride“) Führung der Akten in elektronischer Form soll in Strafsachen unzulässig sein. Bei einer hybriden Aktenführung könnten zeitliche und logistische Vorteile einer elektronischen Aktenführung, etwa im Rahmen der elektronischen Akteneinsicht und Aktenübermittlung, nicht realisiert werden.

4 § 497 StPO-E - Auftragsdatenverarbeitung

§ 497 StPO-E schafft für die Auftragsdatenverarbeitung von Strafverfahrensdaten eine bereichsspezifische Sonderregelung. Diese Sonderregelung wird mit dem besonderen Schutzbedarf dieser Daten begründet. Die Regelung geht den allgemeinen Vorschriften des Bundesdatenschutzgesetzes (namentlich § 11 BDSG) und den jeweils anwendbaren Landesdatenschutzgesetzen vor. Die Vorschrift soll es ermöglichen, eine andere als die aktenführende Stelle mit der Datenverarbeitung bei der elektronischen Aktenführung zu beauftragen („Auftragsdatenverarbeitung“).

Gegenüber dem Diskussionsentwurf des BMJ zur Einführung einer elektronischen Strafakte aus dem Jahr 2012 (dort § 496 StPO-E) sieht § 497 StPO-E vor, dass grundsätzlich auch eine Datenverarbeitung durch nicht-öffentliche Stelle zulässig ist, so ausdrücklich die Begründung zu § 297 Abs. 1 StPO-E.

§ 496 StPO-E in der Fassung des Diskussionsentwurfs von 2012 sah in Abs. 3 nur vor:

> Mit der Datenverarbeitung können andere Stellen oder juristische Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform beauftragt werden.

Eine Beauftragung nicht-öffentlicher Stellen war nicht vorgesehen.

Die Neuregelung in § 297 StPO-E erlaubt nun unter sehr engen Voraussetzungen auch die Beauftragung anderer nicht-öffentlicher Stellen:

> „Nicht-öffentliche Stellen können mit der Datenverarbeitung nur beauftragt werden, wenn
> 1. die Daten in Anlagen verarbeitet werden, bei denen eine öffentliche Stelle den Zutritt, Zugang und Zugriff tatsächlich und ausschließlich kontrolliert, und
> 2. ein Zugriff auf die Daten durch die mit der Datenverarbeitung beauftragten nichtöffentlichen Stellen aus der Ferne und eine Datenübermittlung an den Auftragnehmer oder an unbefugte Dritte ausgeschlossen sind.
> Die Begründung von Unterauftragsverhältnissen durch nicht-öffentliche Stellen ist unzulässig.“

Zur Begründung führt der Gesetzentwurf aus:

> „Durch die Möglichkeit der Einbeziehung nicht-öffentlicher Stellen (natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen, die keine öffentlichen Stellen sind; vgl. § 2 Absatz 4 Satz 1 BDSG) in Satz 2 soll dem wirtschaftlichen Interesse der Länder an einer Auslagerung von IT-Dienstleistungen auf Privatunternehmen Rechnung getragen werden. Jedoch handelt es sich bei der Führung der elektronischen Strafakte um eine hoheitliche Kernaufgabe der Staatsanwaltschaften und Gerichte. In den Strafakten werden nicht nur höchst sensible personenbezogene Daten für Zwecke des Strafverfahrens gespeichert, sondern darüber hinaus auch – etwa in Staatsschutzverfahren – Daten von hohem nationalem Geheimhaltungsinteresse.
>
> Deshalb müssen die entsprechenden Daten unbedingt im unmittelbaren staatlichen Einflussbereich verbleiben, um dem Risiko einer unbefugten Herausgabe der Daten an Dritte – insbesondere auch an ausländische Regierungen – so weit wie möglich entgegenzuwirken. Namentlich ein Zugriff ausländischer Ermittlungsbehörden auf Daten, die bei einem Privatunternehmen mit ausländischem Hauptsitz gespeichert sind (vgl. unter anderem Kapitel 4 des britischen Data Retention and Investigatory Powers Act 2014 oder die Auslegung des Electronic Communications Privacy Act durch den United States District Court Southern District of New York vom 25. April 2014 (Az 13 Mag. 2814), aufrechterhalten durch Entscheidung vom 31. Juli 2014 des Chief United States District Judge, nach der dieses Gesetz auch den extraterritorialen Datenzugriff erlaube) soll dadurch verhindert werden, dass sich die Datenverarbeitungsanlagen (Server) und damit auch die Daten selbst nicht im Besitz eines privaten Unternehmens befinden dürfen, sondern diesen lediglich ein temporärer Zugang zu den Daten gewährt wird.
>
> Die Anlagen zur Datenspeicherung und - verarbeitung müssen sich demnach auch physisch vollständig im Bereich der öffentlichen Hand befinden. Ausgeschlossen ist damit jede Datenverarbeitung in einem Rechenzentrum eines Privatunternehmens beziehungsweise in einer nicht ausschließlich von öffentlichen Stellen betriebenen „Cloud“.
>
> Bei Akten in Strafsachen ist grundsätzlich von einem besonders hohen Schutzbedarf auszugehen: Diese enthalten regelmäßig hochsensible personenbezogene Daten, die zu großen Teilen ohne Einwilligung der Betroffenen auf Grundlage dazu ermächtigender Vorschriften erhoben wurden. Oft handelt es sich bei diesen Daten um „besondere Arten personenbezogener Daten“ im Sinne von § 3 Absatz 9 BDSG, also um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Ihr Bekanntwerden würde, gerade auch wegen des Zusammenhangs mit einem Strafverfahren, eine erhebliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung des Betroffenen darstellen. Auch beziehen sich personenbezogene Daten in Strafakten nicht allein auf den jeweils Beschuldigten, sondern auch auf Zeugen, Opfer von Straftaten und gänzlich unbeteiligte Dritte.

BITKOM teilt diese Begründung nicht. Denn es gibt zahlreiche technisch-organisatorische Möglichkeiten, einen Datenzugriff ausländischer Dienste zu unterbinden. Keineswegs kann aus der gegebenenfalls bestehenden Verpflichtung einzelner Unternehmen zur Weitergabe von Daten darauf geschlossen werden, dass alle Unternehmen gleichermaßen zur Herausgabe verpflichtet sind. Der faktische Ausschluss privater Betreiber für die IT-Infrastruktur ist nicht verständlich und aus den genannten sicherheitsrelevanten Gründen sachlich nicht begründbar. Zudem bedeutet der § 497 StPO-E in der vorliegenden Fassung letztendlich auch einen Ausschluss von der Entwicklung von Software, denn dabei ist es auch erforderlich, auf Daten zuzugreifen, vor allem beim Support.

In der Begründung wird zu § 497 StPO-E die Vorsorge vor ausländischem Zugriff auf die Daten angeführt. Der Ausschluss des Zugriffs auf die Daten aufgrund ausländischer Gerichtsbeschlüsse kann durch entsprechende Regelungen in der Ausschreibung geregelt werden.

Vergleichbare Projekte im juristischen Umfeld haben ähnlich hohe Anforderungen für Anwendungen für den Elektronischen Rechtsverkehr definiert; eine ähnliche Beschränkung bestand hier nicht.

Die Sicherung gegen unautorisierte Zugriffe setzt bei einem vergleichbaren Projekt im juristischen Umfeld schon auf der Ebene der Software ein. Sie wird durch Maßnahmen wie die Verschlüsselung der Daten bei Transport und Speicherung, Schutz aller technischen Aufzeichnungen gegen Manipulation und technische Maßnahmen für die umfassende Implementierung des Vier-Augen-Prinzips gewährleistet.

Es ist nicht nachvollziehbar, weshalb die Daten in Strafsachen nicht durch vergleichbare Maßnahmen gegen unautorisierte Zugriffe geschützt werden könnten. Ein Betrieb durch nicht-öffentliche Stellen ist auf höchstem Sicherheitsniveau möglich. Zumal Dienstleister zum Beispiel Dienste zur Zahlungsabwicklung von Kreditkarten betreiben, deren Sicherheitsanforderungen denen in Strafsachen in nichts nachstehen.

Schließlich lässt die Regelung vollständig außer Acht, dass in den meisten Fällen ein sogenannter Innentäter vertrauliche Daten zur Verfügung stellt. Gegen entsprechende Innentäter schafft die restriktive Regelung in § 497 StPO-E keinen Schutz. Sinnvoller wär stattdessen eine verbindliche Verpflichtung auf die Nutzung von Analysewerkzeugen, die anhand von Mustererkennung auffällige Zugriffsmuster und andere Formen des Missbrauchs von Daten erkennen und offenlegen können. Damit ließe sich ein effektiver und zudem auch effizienter Schutz gegen Risiken von außen ebenso wie gegen Innentäter erreichen.

Zusammenfassend muss daher festgehalten werden, dass die Regelung des § 497 StPO-E den Wettbewerb zwischen öffentlichen und nicht-öffentlichen IT-Dienstleistern einseitig einschränkt und zudem nicht geeignet ist, einen wirksamen Schutz der Daten vor sogenannten Innentätern zu erreichen.

5 § 49d OWiG-E – Auftragsdatenverarbeitung

Zum Schutz personenbezogener Daten in einer elektronischen Akte verweist der Gesetzesentwurf auf die Regelungen in der Strafprozessordnung.

Allerdings ist nicht im Ansatz nachvollziehbar, inwieweit die Gründe, die bei Strafverfahren für einen weitgehenden Ausschluss privater Dienstleister führen sollen, sich tatsächlich auch auf Ordnungswidrigkeitenverfahren übertragen lassen.

Tragende Gründe in den Erläuterungen zu § 497 StPO-E sind:

- Die Führung einer elektronischen Strafakte ist eine hoheitliche Kernaufgabe der Staatsanwaltschaften und der Gerichte. Dies lässt sich auf das Ordnungswidrigkeitenverfahren als Verwaltungsstrafrecht nicht übertragen.
- Die Begründung weist darauf hin, dass in Strafverfahren höchst sensible personenbezogene Daten für Zwecke der Strafverfahren gespeichert werden. In der Begründung zu § 496 Abs. 2 StPO-E wird ausdrücklich Bezug genommen auf besondere Arten personenbezogener Daten im Sinne von § 3 Abs- 9 BDSG also um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Sämtliche der vorgenannten Informationen spielen in Ordnungswidrigkeitenverfahren keine Rolle. Damit geht auch dieser Begründungsansatz ins Leere.

- Zudem nimmt die Begründung zu § 497 StPO-E Bezug auf den NSA-Skandal und die hiermit für bestimmte IT-Häuser angenommene Verpflichtung zur Weiterleitung von Daten an ausländische Geheimdienste. Ein Interesse ausländischer Geheimdienste an Ordnungswidrigkeitenverfahren scheint eher abwegig, gänzlich unhaltbar wird diese Annahme jedenfalls insoweit wie die Begründung ausdrücklich auf Staatsschutzverfahren und dem hierbei bestehenden hohen nationalen Geheimhaltungsinteresse hinweist. Eine entsprechende Interessenlage kann definitiv bei Ordnungswidrigkeitenverfahren ausgeschlossen werden.

Zusammenfassend muss daher im Interesse eines funktionierenden Wettbewerbs und mit Rücksicht auf die wirtschaftlichen Interessen der Länder daher eine Klarstellung erfolgen, dass die Auftragsdatenverarbeitung keineswegs im Ordnungswidrigkeitenverfahren den gleichen Beschränkungen unterliegt wie im Strafverfahren.

---

[i] http://www.justiz.nrw.de/JM/Presse/presse_weitere/PresseOLGs/23_09_2014_1/index.php

[ii] http://www.egvp.de/pdf/rechtsvorschriften/JKomG.pdf

[iii] http://www.bgbl.de/banzxaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%2527bgbl113s3786.pdf%2527]#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl113s3786.pdf%27]__1418911902642