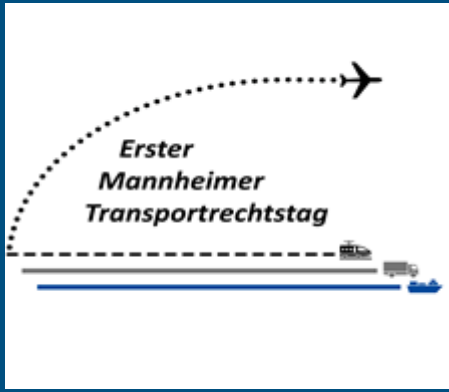
Bundesministerium
für Verkehr und
digitale Infrastruktur



1. Mannheimer Transportrechtstag

24. Juni 2016

Rechtliche Fragen zum Schutz und zur Verwertbarkeit von Daten aus elektronischen Erfassungssystemen

RDir Norman Gerhardt (BMVI)

Bundesministerium
für Verkehr und
digitale Infrastruktur

Übersicht

I. Einführung anhand aktueller Beispiele

II. Welche elektronischen Erfassungssysteme gibt es?

III. Wer nutzt die AIS-Daten?

IV. Wie sind AIS-Daten geschützt?

V. Erfahrungen mit der Strafverfolgung

VI. Blick nach Brüssel

VII. Schlussfolgerungen

I. Einführung anhand aktueller Beispiele

✓ Schiffsunfalldatenbank (WSV – GDWS)

- Betrieb startet vrstl. Ende 2016; SchUnfDatG in Kraft ab 1.1.2014

✓ Schiffsbestandsdatenbank (Europäische Kommission)

- ZBBD liefert gem. § 9 BinSchAufgG seit 2016 Schiffsdaten an EU-Datenbank

✧ Binnenschifffahrtsaufgabengesetz

- Datenschutzrechtliche Novellierung läuft seit 2014

IVR-Register (privatrechtlicher Verein)

- IVR-Rechtsgutachten 2013 bestätigt: internationale Teilnahmeverpflichtung und nationale Rechtsgrundlage sind Voraussetzungen für Datenlieferung

II. Welche elektronischen Erfassungssysteme gibt es?

Im Wesentlichen sind dies Radar, Meldepflichten und AIS:

- Radarpflicht bei unsichtigem Wetter; Radarbilder werden von WSV aber nur punktuell zur Verkehrsüberwachung aufgezeichnet.
- Meldepflicht zur Unfallvorsoge für Container-, Tank-, Kabinen- und Gefahrgutschiffe
- AIS-Pflicht auf dem Rhein seit 1.12.2014, auf der Mosel seit 1.1.2016, auf den übrigen nationalen Binnenwasserstraßen 2016/17
- AIS-Pflicht in anderen Staaten (u.a. AUT, BEL u. NLD seit 1.1.2016)

⇨ Einführung einer AIS-Nutzungspflicht führt(e) zu datenschutz-rechtlichem Regelungsbedarf, da nur AIS Positions- und Ladungsdaten in Echtzeit liefert.

III. Wer nutzt die AIS-Daten? (1)

Hauptzweck der Einführung von AIS: die Nutzung Schiff-Schiff

<u>Unterstützung der Selbstwahrschau</u>, insbesondere wenn AIS in Verbindung mit Inland ECDIS im Informationsmodus genutzt wird.

Begegnungen und Überholungen können besser und frühzeitiger koordiniert werden.

Die Sicherheit und Leichtigkeit der Binnenschifffahrt wird erhöht.

Datenschutzrechtliche Einschätzung:

Keine große Relevanz, da bei Datenübermittlung Schiff-Schiff von gegenseitigem Einvernehmen der Binnenschiffer ausgegangen wird und keine Dritten oder öffentliche Stellen beteiligt sind.

III. Wer nutzt die AIS-Daten? (2)

WSV will AIS-Daten nutzen für:

- Verkehrsberatung durch Revierzentralen
- Abgabenerhebung
- Verkehrsstatistik
- Unfallprävention und Havariemanagement
- Schleusen- und Liegestellenmanagement
- Str.: Unterstützung der Logistikbranche (Transportinformationen)
- Str.: Verfolgung von Ordnungswidrigkeiten (pro: AG Kiel)

Erforderlich:

- Aufbau einer AIS-Landinfrastruktur (in Arbeit)
- Änderung des Binnenschifffahrtsaufgabengesetzes (in Arbeit)

WSP will AIS-Daten nutzen für:

- Gefahrenabwehr und schifffahrtspolizeilichen Vollzug
- Erforschung und Verfolgung von Straftaten und schifffahrtspolizeilichen OWi‘s.

III. Wer nutzt die AIS-Daten? (3)

Dritten wollen AIS-Daten auf folgende Weise nutzen:

- Kommerzieller Gebrauch der AIS-Daten durch Schiffsverfolgungsdienste wie z.B. Vesseltracker, AIS-Live oder MarineTraffic findet statt.
  MarineTraffic wirbt neben Echtzeitdaten mit 20 Mrd.(!) historischen Schiffspositionen.
  „Wettbewerber lassen sich überwachen“ (DtSeeSch 2016, H. 5/6, S. 22 f.)
- Kommerzieller Gebrauch der Daten zu Logistikzwecken durch Transportbeteiligte (Verlader, Reeder, Häfen wollen wissen, wo ihr Schiff ist bzw. wann es ankommt).
- Ideeller Gebrauch der AIS-Daten durch Privatpersonen im Internet. Hierunter fallen auch die Privaten, die entgeltlose „Datenzulieferer“ der Unternehmen sind.
- Krimineller Missbrauch der AIS-Daten denkbar
  Siehe Spiegel-Online vom 16.10.2013 – „Hacker können Positionsdaten von Schiffen manipulieren“; bisher noch nicht vorgekommen, aber technisch machbar (z.B. Fehlauslösen von Kollisionsalarm)

IV. Wie sind AIS-Daten geschützt? (1)

Was sind die Hauptsorgen der Binnenschiffer?

Die Schifffahrtstreibenden haben im Verhältnis Staat – Bürger Sorgen vor

- Einer uferlosen Verwendung ihrer Daten durch die WSV
- Mehr Straf- und Bußgeldverfahren bei Nutzung ihrer Daten durch die WSP
- Minimierung des Eingriffs steht im Vordergrund
- Aktuelle Beispiele

Die Schifffahrtstreibenden haben im Verhältnis Bürger – Bürger Sorgen vor

- Ausspähung ihrer Geschäftsgeheimnisse durch Vertragspartner oder Konkurrenten
- Ausspähung ihrer Privatsphäre („der gläserne Binnenschiffer“)
- Staat nur zum Interessenausgleich und zum Schutz des Kerngehalts des R.i.S. verpflichtet

IV. Wie sind AIS-Daten geschützt? (2)

Lösung im Verhältnis Staat – Binnenschiffer de lege ferenda im BinSchAufgG:

- WSV bekommt die Daten zweckgebunden für Verkehrsmanagement, Abgaben etc.
- Datenübermittlung an die WSP für Gefahrenabwehr und schifffahrtspolizeilichen Vollzug
- Kein „Total“-Beweisverwertungsverbot analog §§ 4 III, 7 II BFStrMG
- Umfassendes Verwertungsverbot bzgl. Owi‘s
- Eingeschränktes Verwertungsverbot bei Straftaten

„Leitlinie“ LG Magdeburg zum ABMG (= BFStrMG):

„Die Kammer übersieht nicht, dass diese strenge Handhabung des ABMG zu teils schwerlich nachvollziehbaren Ergebnissen führen kann. Beispiele…, bei denen etwa die Auswertung der bereits erhobenen Daten aus dem Mauterfassungssystem (also nicht einmal die zusätzliche Datenerhebung) möglicherweise sogar zur Aufklärung von durch Lkw-Fahrern begangenen Tötungsdelikten hätte führen können, geben Anlass, über eine zumindest bereichsweise Ausnahme von der Zweckbindung im ABMG zur Aufklärung erheblichster Straftaten nachzudenken. Insoweit ist allerdings der Gesetzgeber gefordert.“

IV. Wie sind AIS-Daten geschützt? (3)

Lösung im Verhältnis WSV – Binnenschiffer – Logistik de lege ferenda im BinSchAufgG

schwierig, weil:

- Kein einheitlicher Standpunkt im Gewerbe (BDB vs. BDS)
- EU-Projekte pushen den „digitalen Binnenschifffahrtsraum“
- Bessere Integration der Binnenschifffahrt in die multimodalen Logistikketten
- Druck zur Umsetzung EU-finanzierter Forschungsprojekte
- Überarbeitung der EU-RL zum Thema RIS in Vorbereitung

Zielrichtung:

- WSV darf ausgewählte AIS-Daten den Transportbeteiligten zur Verfügung stellen.
- Hoffnung, damit Internetdienste zurückzudrängen
- Verbot der Nachnutzung für Transportbeteiligte
- Löschungspflicht nach Abschluss des Warentransports

Offen: Einwilligung erforderlich? Von wem ggf.? Wie technisch realisierbar? Sanktionen?

IV. Wie sind AIS-Daten heute geschützt? (4)

Wie ist Rechtslage de le lata im Verhältnis Binnenschiffer – Dritte?

- AIS-Daten enthalten personenbezogene Daten gemäß § 3 Abs. 1 BDSG
  - ✓ „bestimmte oder bestimmbare natürliche Person“, da über allgemein zugängliche Quellen (Internet oder Schiffsregister) herauszufinden ist, wer sich auf einem Binnenschiff befindet.
  - ✓ „Einzelangaben über persönliche oder sachliche Verhältnisse“, da durch die Veröffentlichung der Schiffsposition Rückschlüsse auf den Aufenthaltsort der Besatzung ermöglicht werden

- § 29 BDSG, der geschäftsmäßiges Erheben personenbezogener Daten für Werbung, Adresshandel u.ä. zulässt, ist nicht einschlägig, weil
  - ✓ die Betroffenen ein schutzwürdiges Interesse (Recht auf informationelle Selbstbestimmung) an dem Ausschluss der Erhebung haben,
  - ✓ das in der Abwägung die wirtschaftlichen Interessen der datenerhebenden Unternehmen überwiegt („Niemand soll unfreiwillig ein Bewegungsprofil von sich im Internet fürchten müssen“),
  - ✓ die Daten nicht allgemein zugänglich sind.

⇨ Rechtswidriges Erheben und Nutzen der Daten ist OWi nach § 43 Abs.2 Nr.1 BDSG (bis 300.000 € Geldbuße) und bei Bereicherungsabsicht Straftat nach § 44 Abs.1 (bis zwei Jahre Freiheitsstrafe oder Geldbuße). Antragsdelikt.

IV. Wie sind AIS-Daten geschützt? (5)

Wie ist Rechtslage de le lata im Verhältnis Binnenschiffer – Dritte?

- § 202b **StGB** schützt die AIS-Daten vor unbefugtem Abfangen, da
  - ✓ die AIS-Daten nach dem maßgeblichen Willen der Berechtigten nicht für schifffahrtsfremde Dritte bestimmt sind (sondern nur für die Selbstwahrschau und das Verkehrsmanagement) und
  - ✓ es sich beim AIS-Datenfunk um eine nichtöffentliche Datenübermittlung handelt, da AIS-Daten nur über UKW-Funkkanäle übertragen werden, die speziell für den AIS-Datenaustausch reserviert sind und deren Frequenzen von der Bundesnetzagentur zugeteilt wurden. Analog dem Sprechfunk ist der AIS-Datenfunk ein nichtöffentlicher Funkdienst.

⇨ Eine Tat nach § 202b wird mit Geldstrafe oder zwei Jahren Freiheitsstraße bestraft, allerdings in der Regel nur auf Antrag eines Betroffenen.

- § 202a StGB (–), da AIS-Daten nicht „gegen unberechtigten Zugang besonders gesichert“ sind.
- § 89 TKG (–), da AIS-Signale nicht abgehört werden können (so VG Köln, str.).

V. Erfahrungen mit der Strafverfolgung

2009 Strafantrag der WSD Nordwest über die BNetzA einen gegen www.aislive.com.

- StA Aurich stellte Verfahren mit dem Hinweis ein, dass der Tatort in GB liege.
- Es wurde aber von allen Beteiligten ausschließlich ein Verstoß gegen das TKG in Betracht gezogen.
- Nicht geprüft wurde ferner die Strafbarkeit der Privatleute, die die AIS-Daten „abgreifen“ und aislive zur Verfügung stellen.

⇨ Der Fall zeigt die praktischen Schwierigkeiten beim Schutz von AIS-Daten. Aber kein Präzedenzfall, da das Problem nur unvollständig erfasst wurde

Zurzeit läuft ein neues Ermittlungsverfahren. Bei Hausdurchsuchung konnte ein AIS-Empfangsgerät sichergestellt werden. Auswertung läuft.

VI. Blick nach Brüssel

- Am 25. Mai 2018 tritt die neue Datenschutz-Grundverordnung in Kraft, die die geltende DatenschutzRL ablösen wird.
- Mit einer Verordnung kommt es innerhalb der EU zu mehr Rechtsvereinheitlichung.
- Aber Schwierigkeiten das deutsche bereichsspezifische Datenschutzrecht zu „retten“.
- Viel Arbeit, die Öffnungsklauseln der EU-VO mit Leben zu füllen.

VII. Schlussfolgerungen

- Das Thema Schutz von Daten im Allgemeinen und AIS-Daten im Besonderen ist aktuell.
- Die Datennutzung zur Selbstwahrschau und durch die WSV wird weitgehend akzeptiert.
- Für die Datennutzung durch die WSP zeichnet sich eine ausgewogene Lösung ab.
- Schwieriger ist die Regelfindung für die logistische Datennutzung.
- Die kommerzielle Datennutzung durch schifffahrtsfremde Dritte ruft Besorgnis hervor.
- ZKR hat mit Einführung der AIS-Pflicht 2013 die frei zugängliche Veröffentlichung von AIS Daten ohne Einwilligung der Betroffenen missbilligt.
- Schutz ist hier bereits auf Basis der geltenden Rechtslage gewährleistet.
- Es besteht eher ein Vollzugsdefizit bei Staatsanwaltschaften, Gerichten und Polizei.
- Schifffahrtstreibende und deren Interessenvertreter sind aufgerufen, Strafanträge zu stellen!
- EU-Datenschutz-Grundverordnung ist noch nicht eingearbeitet.

Vielen Dank für ihre Aufmerksamkeit!

Hinweis: Vortrag am 28.06.2016 in Hamburg beim Maritimen Cluster Norddeutschland
„Wem gehören Schiffsdaten?
Rechtliche Aspekte zur Datenerhebung und -nutzung in der Schifffahrt“
(RA‘in Dr. Caroline Rupp)

Kontakt

Bundesministerium für Verkehr und digitale Infrastruktur
Referat: WS 25
Robert-Schuman-Platz 1
53175 Bonn

Norman.Gerhardt@bmvi.bund.de
www.bmvi.de

Bundesministerium
für Verkehr und
digitale Infrastruktur

§ 9e Seeaufgabengesetz

(*1) Soweit es zur Erfüllung einer Aufgabe nach diesem Gesetz erforderlich ist, darf die für die Durchführung dieser Aufgabe zuständige Stelle folgende Daten erheben: …*

(2) … Die Daten dürfen an andere öffentliche Stellen übermittelt werden, wenn dies zur Erfüllung von Aufgaben nach diesem Gesetz oder zur Gefahrenabwehr erforderlich oder durch eine bereichsspezifische Ermächtigungsgrundlage erlaubt ist.

§ 4 Bundesfernstraßenmautgesetz

(3) … *Diese Daten dürfen ausschließlich zum Zweck der Überwachung der Einhaltung der Vorschriften dieses Gesetzes verarbeitet und genutzt werden. Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig.*

§ 163 StPO

(1) Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

§ 202b StGB

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, …

§ 6b BDSG

3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.