Professor Dr. Kai von Lewinski

Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht

UNIVERSITÄT PASSAU
Juristische Fakultät

An Herrn
Dominic Spreitz

Telefon 0851 509-2221

Telefax 0851 509-2222

E-mail kai.lewinski@uni-passau.de

Zeichen

Datum 06.03.2015

Ihre Anfrage an unsere Law Clinic

Sehr geehrter Herr Spreitz,

zunächst möchten wir uns bei Ihnen bedanken, dass Sie uns bei unserem neuen Format, der studentischen Rechtsberatung in Form einer Law Clinic, durch Ihre juristische Frage und Ihr entgegengebrachtes Vertrauen unterstützt haben.
Ihnen verdanken die Studenten einen anspruchsvollen Fall „aus der Wirklichkeit", und uns haben Sie damit geholfen, ein Format zu gestalten, das den Studenten im ansonsten theorielastigen Studium bereits einen Einblick in die Praxis und die tatsächliche Umsetzung rechtlicher Fragestellungen ermöglicht.

Umso mehr freut es uns, Ihnen mitteilen zu können, dass die Bearbeitung Ihres Falles abgeschlossen ist und „Ihr Beraterin", Frau Hentrich, Ihnen in den kommenden Tagen, soweit nicht ohnehin bereits geschehen, ihre Erarbeitung zukommen lassen wird.

Bei der Arbeit handelt es sich um eine, die als deutlich überdurchschnittliche Leistung einzuschätzen ist.

In rechtlicher Hinsicht möchten wir Sie jedoch ergänzend noch auf nachfolgende Aspekte hinweisen:

Allgemein geht Frau Hentrich mit einer sehr vom Einwilligungsverständnis geprägten Sicht des Datenschutzrechtes an die Materie heran. Gesetzliche Erlaubnistatbestände – insbesondere die Privilegierung allgemein zugänglicher Daten – werden hier sehr restriktiv gesehen, hingegen extensiv-streng werden die Strafvorschriften der §§ 202a ff. StGB angewandt.
Für Sie bedeutet das, dass mit entsprechender Argumentation die vorliegenden Fragen partiell und durchaus auch im Ergebnis anders gesehen werden können; Verfechtern der Rechtswidrigkeit der Handlungen kann also unter Berufung auf Erlaubnistatbestände und der Auslegung der strafbewehrten Handlungen auch eine andere, liberalere Sicht entgegengehalten werden.

Konkret fehlt es noch an der Abgrenzung der Anwendbarkeit des § 1 V BDSG bezüglich einer Verdrängung durch die Rom-II-Verordnung, sowie Art. 40 EGBGB.

Auch bei der Prüfung der §§ 88 f. TKG wäre im Hinblick auf die Besonderheiten des Drei-Personen-Verhältnisses (Emittent, Rezipient und Telekommunikationsdiensteanbieter) ein anderes Ergebnis jedenfalls vertretbar.

Hinsichtlich der Betreiber von Bodenstationen fehlt eine Diskussion über den Personenbezug der Daten, da diese jene regelmäßig nur empfangen und weiterleiten, jedoch (noch) nicht personenbezogen verknüpfen; dies dürfte generell erst auf dem Server, also zu einem späteren Zeitpunkt, geschehen.

Auch die ausschließliche Anwendbarkeit deutschen Rechts im Hinblick auf die Veröffentlichung der Daten auf der Internetseite ist im Kontext einer europarechtskonformen Auslegung nicht ohne weiteres möglich.

Ihrer Bitte, die Arbeit im Internet veröffentlichen zu dürfen, steht – vorbehaltlich des Einverständnisses von Frau Hentrich – unsererseits nichts entgegen.
Leider können wir die Ausarbeitung nicht auf die Lehrstuhl- und oder Universitätsserver stellen. Konkrete Rechtsgutachten sind generell weniger für eine Lehrstuhlseite geeignet; eine Veröffentlichung auf der Seite der Universität würde zudem der Universität zugerechnet werden, die rechtlich aber nur durch den Präsidenten vertreten werden kann.

Wir hoffen, für Sie ist der Mehrwert, Ihren Fall in unsere Law Clinic gegeben zu haben, ähnlich groß, wie er es für uns und die Studenten war.

Mit bestem Dank und herzlichen Grüßen

- Prof. Dr. Kai von Lewinski -

- Johannes Hoffmann -

Rechtliche Aspekte des Open Glider Networks

Law-Clinic

an der

Universität Passau

Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht

Prof. Dr. Kai von Lewinski

von: Rebecca Hentrich

E-Mail: rebeccahentrich@online.de

Passau, im Januar 2015

Inhaltsverzeichnis

Seite

Literaturverzeichnis

Autor	Werk
Bauer, Martin Bernhard	„Strafbarkeit der unerlaubten Nutzung eines offenen WLANs- Kommentar“, MMR-Aktuell, 2010, 311321
Beyvers, Eva/ Herbrich, Tilman	„Das Niederlassungsprinzip im Datenschutzrecht- am Beispiel von Facebook- Der neue Ansatz des EuGH und die Rechtsfolgen“, ZD 2014, 558 ff. Zitiert: Beyvers/ Herbrich: „Das Niederlassungsprinzip im Datenschutzrecht“
Dreier, Thomas/ Schulze, Gernot	Urheberrechtsgesetz, Kommentar, 3. Auflage 2008, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Dreier/ Schulze, UrhG
Fechner, Frank	„Medienrecht- Lehrbuch des gesamten Medienrechts unter besonderen Berücksichtigung von Presse, Rundfunk und Multimedia“, 15. Auflage 2014, Mohr-Siebeck, Tübingen; Zitiert: Fechner, Medienrecht
Geppert, Martin/ Schütz, Raimund	Beck’scher TKG-Kommentar, Geppert/ Schütz (Hrsg.), 4. Auflage 2013, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Beck’scher TKG-Kommentar
Grabitz, Eberhard/ Hilf, Meinhard	Das Recht der Europäischen Union, Nettesheim, Martin (Hrsg.), 40. Auflage 2009, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Grabitz/ Hilf, Das Recht der Europäischen Union.
Gola, Peter/ Schomerus, Rudolf	BDSG- Bundesdatenschutzgesetz-Kommentar, Gola/ Schomerus (Hrsg.), 11. Auflage 2012,Verlag C.H. Beck; Zitiert: Bearbeiter in Gola/ Schomerus, BDSG
Hauschka, Christoph E.	Corporate Compliance- Handbuch der Haftungsvermeidung in Unternehmen, Hauschka (Hrsg.), 2. Auflage 2010, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Hauschka, Corporate Compliance
Heckmann, Dirk	Juris- Praxiskommentar Internetrecht, Heckmann (Hrsg.), 3. Auflage 2011, juris GmbH, Saarbrücken; Zitiert: Bearbeiter in jurisPK- Internetrecht

Heynen, Ulli	„Wir sehen uns! glidernet.org“ in segelfliegen, 1/2015, 58 ff.
Karg, Moritz	„Anwendbares Datenschutzrecht bei Internet-Diensteanbietern- TMG und BDSG vs. Konzernstrukturen?“, ZD 2013, 371 ff. Zitiert: Karg: „Anwendbares Datenschutzrecht bei Internet-Diensteanbietern“
Kilian, Wolfgang/ Heussen, Benno	Computerrecht, Kilian/ Heussen (Hrsg.), 32. Ergänzungslieferung 2013, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Kilian/ Heussen: Computerrecht
Kindhäuser, Urs/ Neumann, Ulfrid/ Paeffgen, Hans-Ullrich	Strafgesetzbuch, Paeffgen (Hrsg.) 4. Auflage 2013, Nomos Zitiert: Bearbeiter in Kindhäuser/ Neumann/ Paeffgen, StGB
Maunz, Theodor/ Dürig, Günter	Grundgesetz- Kommentar, Maunz/ Dürig (Hrsg.), 63. Lieferung 2011, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Maunz/ Dürig, GG
Rauschhofer, Hajo	„Haftung für Links auf Twitter zu rechtswidrigen Inhalten“, MMR-Aktuell 2010, 302790
Roßnagel, Alexander	Beck’scher Kommentar zum Recht der Telemediendienste, Roßnagel (Hrsg.), 2013, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Roßnagel, Recht der Telemediendienste
Simitis, Spiros	Bundesdatenschutzgesetz, Simitis (Hrsg.), 8. Auflage 2014, Nomos; Zitiert: Bearbeiter in Simitis, BDSG
Spindler, Gerald/ Schuster, Fabian	Recht der elektronischen Medien-Kommentar, Spindler/ Schuster (Hrsg.), 2. Auflage 2011, Verlag C.H. Beck, München; Zitiert: Bearbeiter in Spindler/ Schuster, Recht der elektronischen Medien
Willi, Ernst	„FLARM- was zeigt die Zukunft?“ in segelfliegen 5/2013, 40 ff.
Wolff, Heinrich Amadeus/ Brink, Stefan	Beck’scher Online-Kommentar Datenschutzrecht, Wolff/ Brink (Hrsg.), 10. Edition, Stand 01.11.2014, Verlag C. H. Beck, München; Zitiert: Bearbeiter in Beck’scher Online-Kommentar Datenschutzrecht

Verzeichnis der Internetquellen

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Allgemeinzuteilungen/2014_69_SRD_pdf.pdf?__blob=publicationFile&v=1; abgerufen am 13.01.2015, 13.04 Uhr.

http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.31 Uhr.

http://wiki.glidernet.org/, abgerufen am 14.01.2015, 19.01 Uhr.

http://wiki.glidernet.org/faq#toc0 , abgerufen am 14.01.2015, 19.02 Uhr.

http://wiki.glidernet.org/about#toc2, abgerufen am 13.01.2015, 13.17 Uhr.

http://flarmrange.onglide.com/#EDMD,max,all,48.2287_11.426,9,#00990000:#009900ff,circles;, abgerufen am 09.01.2015, 10.30 Uhr.

http://wiki.glidernet.org/links#toc5, abgerufen am 16.01.2015, 12.14 Uhr.

http://wiki.glidernet.org/about, abgerufen am 09.01.2015, 10.12 Uhr.

http://wiki.glidernet.org/about#toc2, abgerufen am 13.01.2015, 13.19 Uhr.

http://live.glidernet.org/#c=47.31921,8.51575&z=9, abgerufen am 09.01.2015, 10.35 Uhr.

http://www.bazl.admin.ch/experten/luftfahrzeuge/luftfahrzeugregister/index.html?&lfrSucheDetailKnz=HB-XFQ, abgerufen am 09.01.2015, 10.57 Uhr.

https://www.google.de/search?nfpr=1&q=%22D-6346%22&gws_rd=cr&ei=M6avVKnJI4LC7gb9woGQAQ, abgerufen am 09.01.2015, 10.58 Uhr.

http://wiki.glidernet.org/list-of-receivers#toc10, abgerufen am 13.01.2015, 13.37 Uhr.

http://www.flarm.de/disclaimer/index.html, abgerufen am 16.01.2015, 12.24 Uhr.

http://www.flarm.de/support/Flarm_Competitions_de.pdf, abgerufen am 14.01.2015, 20.45 Uhr.

http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 14.01.2015, 21.06 Uhr.

http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 14.01.2015, 21.08 Uhr.

http://flarmnet.org/index.php/en/register-now, abgerufen am 14.01.2015, 20.58 Uhr.

http://wiki.glidernet.org/links#toc5, abgerufen am 16.01.2015, 12.14 Uhr.

https://github.com/glidernet/rtlsdr-flarm, abgerufen am 21.01.2015, 16.17 Uhr.

http://www.flarm.de/disclaimer/index.html, abgerufen am 16.01.2015, 12.24 Uhr.

https://github.com/glidernet/rtlsdr-flarm, abgerufen am 21.01.2015, 16.19 Uhr.

http://wiki.glidernet.org/links#toc5, abgerufen am 21.01.2015, 16.20 Uhr.

http://wiki.glidernet.org/downloads, abgerufen am 21.01.2015, 16.30 Uhr.

http://flarmnet.org/index.php/en/faqs-and-answers, abgerufen am 21.01.2015, 21.25 Uhr.

http://flarmnet.org/index.php/en/faqs-and-answers, abgerufen am 21.01.2015, 21.25 Uhr.

http://flarmnet.org/index.php/en/impressum, abgerufen am 23.01.2015, 11.51 Uhr.

http://wiki.glidernet.org/about#toc2, abgerufen am 24.01.2015, 17.57 Uhr.

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164, abgerufen am 28.01.2015, 15.23 Uhr.

http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 28.01.2015, 16.23 Uhr.

http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.32 Uhr.

http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.33 Uhr.

http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.32 Uhr.

Abkürzungsverzeichnis

Gebraucht werden die üblichen Abkürzungen, vgl. Kirchner, Hildebert: Abkürzungsverzeichnis der Rechtssprache, 7. Auflage, Berlin.

Ausgegebener Sachverhalt

Viele Segelflieger (ca. 80% der aktiv am Luftverkehr teilnehmenden Maschinen) sind auf freiwilliger Basis mit einem Antikollisionssystem (sog. Flarm http://www.flarm.com) ausgestattet. Dieses System sendet permanent die Position Geschwindigkeit, eine Geräte-ID, des Segelflugzeugs auf einer öffentlichen Frequenz.
Andere Segelflugzeuge mit Flarm-Gerät können diese Information empfangen und daraus mögliche Kollisionskurse detektieren und Ausweichempfehlungen geben. Dieses System funktioniert in der Luft relativ zuverlässig und hat schon viele Leben gerettet. Soweit zum primären Einsatzzweck der Flarm-Geräte.
In letzter Zeit hat sich europaweit eine sekundäre Nutzung dieser Flarm-Geräte mehr und mehr etabliert. Ein von Privatpersonen betriebenes Netz von bodengebundenen Flarm Empfangsstationen (Open Glider Network http://wiki.glidernet.org) empfängt die von Flugzeugen auf öffentlichen Frequenzen gesendeten Signale und kommuniziert diese Information via Internet an Server (glidernet.org; Standort Frankreich). Dort werden diese Informationen ausgewertet, visualisiert und veröffentlicht. Siehe http://live.glidernet.org/#c=49.34295.11.91615&z=7&l=r

Mit Hilfe der Daten der Flarm-Sender werden so Flugspuren/ Bewegungsprofile in Echtzeit erstellt. Dies geschieht jedoch ohne explizite Zustimmung des jeweiligen Piloten. Eine Zuordnung von Flarm-ID zu Pilot ist jedoch nur über freiwillige Pilotenangaben möglich (siehe http://www.flarmnet.org/index.php.en/). Es besteht weder die Pflicht ein Flarm-Gerät mitzuführen, noch die Pflicht die Flarm-ID mit personenbezogenen Daten oder dem Flugzeugkennzeichen zu verknüpfen. (vgl. Zuordnung KFZ-Kennzeichen zu Halter). Wie Sie sich vorstellen können, wird diese Praxis von einigen Piloten abgelehnt und als gesetzwidrig eingestuft. Eine juristische Bewertung der verschiedenen Aspekte des Systems liegt jedoch bisher nicht vor.

I. Problemaufriss

1. Flarm und das Open Glider Network

„Flarm“ ist ein technisches Hilfsmittel, um Kollisionen im Segelflugverkehr verhindern oder verschwundene Flugzeuge auffinden zu können. Das System besteht aus Hard- (dem Flarm-Gerät oder einem Flarm-kompatiblen Gerät*)* und Software (Flarm). In Europa sind über 20.000 Flarm-Systeme im Einsatz.[1]

Die Kollisionsvermeidung baut sich aus drei Elementen auf: Erstens werden aus dem Segelflugzeug, das mit Flarm ausgestattet ist, kontinuierlich Bewegungsinformationen gesendet: dieses Profil umfasst die Geräte-ID des Flarm-Systems, Bewegungsrichtung und –geschwindigkeit, die aktuelle Position im Raum, Steigwerte etc. Gesendet wird auf einer öffentlichen, zulassungsfreien Frequenz: 868, 3 MHz.[2]
Zweitens werden Flarm-Informationen, die alle auf derselben Frequenz gesendet werden, von anderen Segelfliegern empfangen. Drittens wertet die Software die eigenen und die empfangenen Bewegungsprofile aus und errechnet daraus Kollisionsgefahren. Die Reichweite der Kollisionskommunikation zwischen den Flugzeugen beträgt bis zu fünf Kilometer.[3] Die Flarm-Daten werden verschlüsselt gesendet. [4]

Weil die Informationen regelmäßig aus dem Segelflugzeug gesendet werden, ist es möglich, langfristige Bewegungsanalysen zu erstellen. Dabei kann die Bewegung des Flugzeugs im Raum anhand der gesendeten Daten verfolgt und aufgezeichnet werden.

Die Flarm-Daten machen sich insbesondere zwei Institutionen zu Nutze: *Flarmnet.org* und *openglidernetwork.org*.[5]

Auf beiden Webseiten sind Segelflugbewegungen nachvollziehbar. Das hat außer einem gewissen spielerischen Reiz den Vorteil, dass der Pilot sich vor dem Start schon über den Verkehr am Himmel informieren kann. Auch Bewegungen auf dem Rollfeld oder Flugzeugschlepps werden von Flarm erkannt. Zudem können Flugsituationen, etwa vor Unfällen oder anderen Problemaufkommen, zu einem späteren Zeitpunkt nachvollzogen werden. So bietet nicht nur Flarm selbst, sondern auch die Visualisierung der gesammelten Flarm-Daten hervorragende Möglichkeiten, die Flugsicherheit zu verbessern.

---

[1] Ernst: „ FLARM-Was zeigt die Zukunft?“ in segelfliegen 5/ 2013, 43.

[2] Diese Frequenz liegt im Funkband für Short Range Devices (SRD; Kurzstreckenfunk). Siehe Amtsblattverfügung 30/2014 der BNetzA, zuletzt geändert mit der Amtsblattverfügung 69/2014, abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Allgemeinzuteilungen/2014_69_SRD_pdf.pdf?__blob=publicationFile&v=1; abgerufen am 13.01.2015, 13.04 Uhr.

[3] http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.31 Uhr.

[4] Um die Flarm-Daten auslesen zu können, müssen sie erst decodiert werden, s. http://wiki.glidernet.org/, abgerufen am 14.01.2015, 19.01 Uhr; http://wiki.glidernet.org/faq#toc0 , abgerufen am 14.01.2015, 19.02 Uhr (Frage: Is OGN an open source project?).

[5] Weitere Webseiten mit Flugbewegungen: flightradar24.com, skylines.aero, stanlytrack2.dfs.de, glidertracking.com.

Stein des Anstoßes ist in der Segelfluggemeinde -trotz aller Nützlichkeit- die private Initiative Open Glider Network (OGN). Bei OGN handelt es sich nicht um eine Open Source Code- Bewegung im klassischen Sinne. Es ist auch keine rechtliche Körperschaft darunter zu verstehen. Stattdessen setzt es sich lose aus international agierenden Privatpersonen zusammen, die durch Eigeninitiative und auf eigene Kosten tätig werden.[6]

Das eigentliche Netzwerk besteht aus mehreren Bodenempfangsstationen, die die Flarm-Informationen von Segelfliegern in einem Radius von maximal 25 km empfangen.[7] Ein OGN-Receiver besteht aus einer Antenne, einem DVB-T-Stick und einem Computer mit entsprechender Software.[8] Es können auch ganz normale Flarm-Geräte dazu verwendet werden, davon geht diese Arbeit aber nicht aus.[9] Die einzelnen Bodenstationen sind nicht direkt[10], sondern über das Internet miteinander verbunden.[11] Im Anschluss an den Datenempfang werden die Informationen an zwei Server[12] in Frankreich übertragen. Die französischen Server werten die Informationen aus, visualisieren und veröffentlichen sie unter *live.glidernet.org*.[13] Auf dieser Webseite kann man verschiedene Flugobjekte auf einer Weltkarte verfolgen. Klickt man auf eines der Symbole für einzelne Flugobjekte, erscheint ein Fenster mit Informationen über die Registerkennung des Fluggeräts, die Flarm-ID[14], den Fluggerättyp (z.B. Glider, Motorglider, Helicopter,…), den Eigentümer, den Flugplatz, das Modell, Längen- und Breitengrad der Position, Höhe, Geschwindigkeit und Steigwerte. Farbige Linien stellen die Spuren der Flugzeuge auf der Karte dar. Außerdem wird die empfangende Bodenstation angezeigt.

In diesem Infofenster gibt es auch die beiden Link- Buttons „Infos“ und „Pictures“. Der Pictures-Link verweist auf eine Google-Bilder-Suche zur Registerkennung. Der Infos-Link verweist auf eine Google-Web-Suche zur Registerkennung. Die Google-Suche liefert Hintergrundinformationen.[15]

---

[6] http://wiki.glidernet.org/about#toc2, abgerufen am 13.01.2015, 13.17 Uhr.

[7] http://flarmrange.onglide.com/#EDMD,max,all,48.2287_11.426,9,#00990000:#009900ff,circles, abgerufen am 09.01.2015, 10.30 Uhr.

[8] http://wiki.glidernet.org/links#toc5, abgerufen am 16.01.2015, 12.14 Uhr.

[9] Heynen: „Wir sehen uns! glidernet.org“ in segelfliegen 1/2015, 63.

[10] http://wiki.glidernet.org/about, abgerufen am 09.01.2015, 10.12 Uhr.

[11] Heynen: “Wir sehen uns! glidernet.org“ in segelfliegen 1/2015, 59f.

[12] „glidern1.glidernet.org“ und „glidern2.glidernet.org“; Die Informationen aus der Client-Schicht sind ohne Zugangsbeschränkungen gehalten; http://wiki.glidernet.org/about#toc2, abgerufen am 13.01.2015, 13.19 Uhr.

[13] http://live.glidernet.org/#c=47.31921,8.51575&z=9, abgerufen am 09.01.2015, 10.35 Uhr.

[14] Die Piloten können selbsttätig ihre Flarm-ID ändern und z.B. ihre internationale Flugzeugkennung benutzen. Da sie das aber nur dann machen werden, wenn sie öffentlich im OGN auftreten wollen, wird diese Fallkonstellation nicht berücksichtigt.

[15] Bei in der Schweiz registrierten Flugzeugen erschien in der Google-Suche mehrmals der Link auf die Webseite des Bundesamts für Zivile Luftfahrt mit der Detailauskunft zum entsprechenden Flugzeug; bei deutschen Flugzeugen war das Google-Ergebnis eher von fragwürdigem Erkenntniswert, denn die deutsche Luftfahrzeugrolle, in der z.B. der Eigentümer eines Segelflugzeugs eingetragen ist, ist ein nicht-öffentliches Register, vgl. § 64 LuftVG. Auskünfte oder Übermittlungen aus der Luftfahrzeugrolle sind nur unter den Voraussetzungen der § 63 Abs. 6-10 LuftVG möglich. § 18 LuftVZO, nachdem jedermann Einsicht in die Luftfahrzeugrolle nehmen konnte, ist weggefallen.
Schweizer Beispiel:
http://www.bazl.admin.ch/experten/luftfahrzeuge/luftfahrzeugregister/index.html?&lfrSucheDetailK

Die Webseite ist in englischer Sprache abrufbar. Der erklärende „?“-Link ist auf französisch, englisch und deutsch abrufbar.

Jede einzelne Funktion für sich, ja sogar schon das Empfangen und Verwerten der Flarm-Informationen könnte das Persönlichkeitsrecht der Segelflugpiloten und Flugzeugeigentümer beeinträchtigen.[16] Das Empfangen und Verwerten der Daten durch Dritte berührt das informationelle Selbstbestimmungsrecht der Piloten. Denn grundsätzlich steht es dem Einzelnen selbst zu, über die Erhebung, Verarbeitung und Speicherung seiner Daten zu bestimmen. Besondere Brisanz haben personenbestimmte Bewegungsprofile (Tracks), wenn sie minutiös Aufschluss über den Aufenthaltsort und das Handeln der beobachteten oder beobachtbaren Person geben.

2. Herangehensweise

Um die Verwendung der Flarm-Daten durch das OGN zu beurteilen, werden die verschiedenen Stufen der Datennutzung durch Flarm und das OGN einzeln betrachtet: erst das Verarbeiten der Daten im Segelflugzeug, dann die Kommunikation mit Flarm-Geräten in anderen Segelflugzeugen, anschließend das Empfangen der Datensätze von der öffentlichen Frequenz und abschließend das Verarbeiten der Daten und das Veröffentlichen der aufbereiteten Daten im Internet.

Grundlegend ist jeweils die Frage zu stellen, welcher (Rechts-) Natur die Daten sind und ob der Anwendungsbereich des Datenschutzrechts eröffnet ist: handelt es sich um nur sachbezogene, personenbeziehbare oder personenbezogene Daten?

Der verfassungsrechtliche Unterbau des Datenschutzrechts und allgemeine Erläuterungen sind zum besseren Verständnis im **Anhang** nachzulesen.

3. Anwendbarkeit des deutschen Rechts auf vorliegende Fallkonstellation

Die Anwendbarkeit der deutschen Datenschutznormen[17] richtet sich grundsätzlich nach § 1 Abs. 5 BDSG. § 1 Abs. 5 BDSG setzt die Vorgaben der Richtlinie 95/46/EG (Datenschutzrichtlinie, DS-RL) um. Aus Art. 4 Abs. 1 a) der DS-RL ergibt sich das Niederlassungs- oder Sitzlandprinzip: solange eine datenverarbeitende Stelle eine Niederlassung innerhalb der EU oder des EWR hat, kommt einzelstaatliches Recht zur Anwendung.[18] Gelangt Art. 4 Abs. 1 a) DS-RL nicht zur Anwendung, weil der Verantwortliche keine Niederlassung innerhalb der EU oder des EWR hat, gilt das Territorialprinzip aus Art. 4 Abs. 1 c) DS-RL: Nationales Datenschutzrecht ist anzuwenden, wenn der Verantwortliche auf Mittel zurückgreift, die in dem Mitgliedsstaat belegen sind.[19] § 1 Abs. 5 S. 1 Hs. 1 BDSG weicht im Wortlaut von

---

nz=HB-XFQ, abgerufen am 09.01.2015, 10.57 Uhr
Deutsches Beispiel: https://www.google.de/search?nfpr=1&q=%22D-6346%22&gws_rd=cr&ei=M6avVKnJI4LC7gb9woGQAQ, abgerufen am 09.01.2015, 10.58 Uhr.

[16] Im Folgenden werden der Einfachheit halber stets nur die Segelflugpiloten genannt. Nur wenn eine Differenzierung zwischen Piloten und Eigentümern notwendig ist, wird darauf hingewiesen

[17] Dies gilt für BDSG und TMG. Die Anwendbarkeit des TMG leitet sich über § 3 Abs. 3 Nr. 4 TMG i.V.m. § 1 Abs. 5 BDSG her.

[18] Beyvers/ Herbrich: „Das Niederlassungsprinzip im Datenschutzrecht“, ZD 2014, 558.

[19] Beyvers/ Herbrich: „Das Niederlassungsprinzip im Datenschutzrecht“, ZD 2014, 558.

Art. 4 I a) DS-RL ab. Die Vorschriften des BDSG sind europarechtskonform auszulegen.

Zunächst ist also nach Art. 4 Abs. 1 a) DS-RL und § 1 Abs. 5 Abs. 1 BDSG festzustellen, ob die Datenverarbeitung durch das OGN in einem anderen Mitgliedsstaat der EU oder des EWR erfolgt und dort eine Niederlassung des OGN zu finden ist. Die OGN-Bodenstationen, die die Daten empfangen und verschlüsseln, stehen in vielen Nationen. Hier soll es nur auf die Bodenstationen auf deutschem Grund ankommen.

a) Die Bodenstationsbetreiber

Mit Blick auf das Auftreten des OGN ist zunächst unklar, wer überhaupt verantwortliche Stelle sein kann. Nach dem deutschen Datenschutzrecht ist verantwortlich, wer personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, § 3 Abs. 7 BDSG. Nach Art. 2 d) DS-RL ist diejenige natürliche oder juristische Person oder Stelle verantwortlich, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Zusätzlich zu den deutschen Kriterien kommt somit noch die Entscheidungsmacht hinzu.[20]
Das OGN ist jedenfalls keine juristische Person. Aus der Struktur des OGN ergibt sich, dass es lediglich ein loser, ideell verbundener Interessenkreis ist. Es sind natürliche Personen, die gemeinsam Flarm-Daten verwenden.[21] Jeder Bodenstationsbetreiber empfängt und übermittelt die Flarm-Daten selbstverantwortlich und nicht etwa nach Weisung einer zentralen Stelle. Für diesen ersten Arbeitsschritt im OGN gibt es folglich unzählige datenschutzrechtlich Verantwortliche. Für den Empfang, das Verarbeiten und Aussenden der Daten auf deutschem Boden gilt für alle Verantwortlichen gem. § 1 Abs. 2 Nr. 3 BDSG das deutsche Datenschutzrecht.

b) Die Server in Frankreich und die Webseite

Die deutschen Bodenstationen übermitteln die Daten anschließend weiter nach Frankreich (EU). Dort werden sie auf zwei Servern weiterverarbeitet und dort wird auch die Webseite *live.glidernet.org* gehostet.[22] Nun reicht es für die Anwendbarkeit französischen Rechts nicht aus, dass nur die Datenverarbeitung auf französischem Staatsgebiet stattfindet, sondern es müsste sich auch eine Niederlassung in Frankreich befinden. Für die Bestimmung einer Niederlassung als verantwortliche Stelle kommt es auf die effektive und tatsächliche Ausübung einer Tätigkeit an, die mittels einer festen Einrichtung vollzogen wird. Die Stelle muss die tatsächliche Entscheidungsbefugnis innehaben.[23] Die Server sind eine feste Einrichtung. Problematisch ist, dass kein personaler Überbau zu diesen Servern erkennbar ist, zumal auf die dort gespeicherten Daten frei zugegriffen werden kann. Man weiß nicht, von wo die Serverinhalte genutzt werden. Allein der Serverstandpunkt ist kein hinreichendes Indiz für die Existenz einer Niederlassung, denn die Klassifizierung

---

[20] Vgl. Dammann in Simitis, BDSG, § 3 Rn. 224 ff.

[21] Eine Liste der deutschen Bodenstationen, teilweise mit Kontaktdaten, ist unter http://wiki.glidernet.org/list-of-receivers#toc10 abrufbar, abgerufen am 13.01.2015, 13.37 Uhr.

[22] siehe Sachverhalt.

[23] Beyvers/ Herbrich: „Das Niederlassungsprinzip im Datenschutzrecht“, ZD 2014, 558, 559.

als verantwortliche Stelle dient nicht zuletzt auch der Sicherung der Betroffenenrechte. Diese würden leerlaufen, wenn man bei der Subsumtion nur auf die technische Einrichtung abzielen würde.
Letztendlich gibt der Sitz der entscheidenden Personen den Ausschlag. Die Betreiber der Webseite bearbeiten die ihnen zugesandten Daten und nutzen sie für ihr Projekt. Sie sind die verantwortliche Stelle. Geht man davon aus, dass ihr Sitz in Frankreich ist, ist französisches (Datenschutz)Recht für das Veröffentlichen der Daten anwendbar.

Weil die persönlichkeitsrechtlichen Gefährdungen durch das Internet grenzüberschreitende Ausprägungen bekommen haben, könnte man auch ein anderes Kollisionsprinzip anlegen: das Markt- oder Zielortprinzip. In der Google-Spain-Entscheidung des EuGH[24] erfolgt die Auslegung von „Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung“ so weit[25], dass schon fast von einem Marktortprinzip gesprochen werden kann. Denn der EuGH hat nicht nur die Datenverarbeitung an sich betrachtet, sondern auch die sinnhafte Verbundenheit zwischen Datenverarbeitung, finanziellem Nutzen und Konzernstrukturen. Danach wäre zu fragen: Mit welchen Tätigkeiten oder Zwecken ist die Datenverarbeitung inhaltlich und logisch so eng verknüpft, dass keines von beidem alleine stehen kann?

Die Webseite *live.glidernet.org* soll es weltweit ermöglichen, den Segelflugverkehr nachvollziehen zu können und bezweckt die Verbesserung der Flugsicherheit. Die Seite ist von Deutschland aus abrufbar, bildet den Flugverkehr auf deutschem Staatsgebiet ab und ist teilweise in deutscher Sprache gehalten. Die Webseite richtet sich demzufolge auch an deutsches Publikum. Die Datenverarbeitung ist von ihrem Zweck kaum zu trennen. Nach dem Markt- oder Zielortprinzip wäre deutsches Datenschutzrecht anzuwenden. Problematisch bleibt, dass das Markt- oder Zielortprinzip keine Kollisionsregel im eigentlichen Sinne ist, da es auch zu dem Schluss führen kann, dass mehrere Rechtsordnungen gleichzeitig auf denselben Sachverhalt anzuwenden sind. Das würde zur Rechtsunsicherheit beitragen statt sie zu reduzieren und im Endeffekt das Vorkommen von international ausgerichteten Internetangeboten, und damit den europäischen Binnenmarkt, behindern.

Für die Veröffentlichung der Daten durch die Webseite ist deutsches Datenschutzrecht nicht anwendbar.

c) Zivilrechtliche Ansprüche

Damit ist aber noch nicht ausgeschlossen, dass deutsche Staatsbürger bei Verletzungen ihres Persönlichkeitsrechts nicht doch Ansprüche gegen die Webseitenbetreiber haben könnten. Nach Art. 1 Abs. 2 g) Rom-II-VO sind deliktische Ansprüche aus Verletzungen des Persönlichkeitsrechts aus dem Anwendungsbereich der Verordnung ausgenommen, weswegen gem. Art. 3 a) a.E. EGBGB Art. 40 Abs. 1 EGBGB zum Tragen kommen kann. Nach Satz 1 unterliegen deliktische Ansprüche zwar grundsätzlich dem Recht des Staates, in dem die Handlungen vorgenommen wurden, nach Satz 2 kann der Geschädigte aber selbst bestimmen, dass das Recht des Staates gelten soll, in dem der Erfolg eingetreten ist. Der Erfolg i.S.d. Art. 40 Abs. 1 EGBGB ist der erlittene Schaden. Bei Verletzungen

[24] EuGH, Urteil vom 13.05.2014, Az. CR 131/ 12.

[25] Kritisch dazu Beyvers/ Herbrich, die darin eine vom Gesetzgeber unbeabsichtigte Erweiterung des Anwendungsbereichs sehen, „Das Niederlassungsprinzip im Datenschutzrecht“, ZD 2014, 558, 560.

des allgemeinen Persönlichkeitsrechts durch Internetinhalte kann der schädigende Erfolg potenziell überall dort eintreten, von wo aus die Internetseite bestimmungsgemäß abgerufen werden kann.[26] Ein zusätzlicher Hinweis für den Erfolgsort kann sein, wieviel Inlandsbezug die Internetseite aufweisen kann.[27] Die *live.glidernet.org*- Webseite ist von Deutschland aus abrufbar, bildet Flugverkehr über deutschem Staatsgebiet ab und ist teilweise in deutscher Sprache gehalten. Sie soll also in Deutschland bestimmungsgemäß abgerufen werden und weist zusätzlich noch Inlandsbezug auf.

d) Ergebnis

Für die Tätigkeiten der Bodenstationsbetreiber ist deutsches Datenschutzrecht anwendbar. Für die Veröffentlichung der Daten im Internet ist wenigstens deutsches zivilrechtliches Deliktsrecht anwendbar.

II. Flarm erhebt und verarbeitet die Daten im Segelflugzeug

Erste Frage muss sein, welche Daten erhoben werden und ob sie personenbezogene Daten sind. Anschließend wird festgelegt, welchem Regelungsregime die Datenverarbeitung im Flugzeug unterfällt.

Flarm sammelt ausschließlich über eigene Sensoren Informationen über die Bewegung des Flugzeugs. Diese werden von der Software so umgerechnet, dass sie dem Piloten im Cockpit sinnvoll wahrnehmbar dargestellt werden können. Die Informationen sind mit einer Geräte-ID verknüpft. Optional kann der Pilot seinen Namen hinzufügen. Es ist möglich, Flarm mit einem PC zu verbinden, etwa um es zu konfigurieren und Updates hoch- oder Flugaufzeichnungen herunterzuladen.

1. Ist Datenschutzrecht einschlägig?

Der Personenbezug ist die Schlüsselfigur des Datenschutzrechts. Eine persönliche oder sachliche Information oder Einzelangabe ist dann personenbezogen, wenn sie einer bestimmten oder bestimmbaren Person (Betroffener) zugeordnet werden kann, § 3 Abs. 1 BDSG. Eine Einzelangabe umfasst jede Information, gleich welche Darstellungsform sie hat.[28] Dazu gehören auch Beziehungen einer Person zu ihrer Umwelt, sofern sie Rückschlüsse auf Eigenschaften der Person zulassen. Der Begriff der Angabe über persönliche oder sachliche Lebensverhältnisse ist außerordentlich weit zu verstehen, es sollen alle Informationen, die über eine Bezugsperson etwas aussagen, erfasst werden.[29] Dazu gehören auch Beziehungen einer Person zu ihrer Umwelt, sofern sie Rückschlüsse auf Eigenschaften der Person zulassen. Das heißt, dass auch die Verknüpfung z.B. eines Namens mit den zunächst nur sachbezogenen Flugdaten personenbezogene Daten entstehen lässt. Hat der Pilot seinen Namen angegeben, sind auch schon die Daten im Flarm-System personenbezogen.

---

[26] Vgl. LG München I: Internationale Zuständigkeit bei unberechtigter öffentlicher Zugänglichmachung eines urheberrechtlich geschützten Werks im Internet, NJOZ 2010, 449, 450.

[27] Heckmann in jurisPK, Kap. 1 Rn. 159.

[28] Dammann in Simitis, BDSG, § 3 Rn. 7.

[29] Dammann in Simitis, BDSG, § 3 Rn. 7; Gola/ Schomerus in Gola/ Schomerus, BDSG, § 3 Rn. 5.

Die Daten werden im Flarm-System gesammelt, aufbereitet und an den Piloten ausgegeben. Dabei liegt kein Telekommunikationsvorgang oder ein zwischengeschaltetes Telemedium vor, so dass das BDSG anwendbar ist.[30]

Es ist im nächsten Schritt allgemein zu bestimmen, wer verantwortliche Stelle ist. Diese Position hat derjenige inne, der die tatsächliche Entscheidungsgewalt über die Datenverarbeitung trägt. Zwar kann man anmerken, dass der Pilot nicht immer in jeder Sekunde weiß, welche Daten sein Flarm exakt erhebt, trotzdem hat er die volle Verfügung darüber, ob er sein Flugzeug mit Flarm ausstattet oder nicht, ob er das System in Betrieb nimmt, welche Speicherabstände er auswählt, usw. Der Pilot wäre die verantwortliche Stelle für die Datenverarbeitung im Flugzeug.

Der Pilot ist der Herr seiner eigenen Flugdaten. Er nutzt sie während des Fluges zur Kollisionsvermeidung und kann sie auch danach langfristig speichern. Nach § 1 Abs. 2 Nr. 3 a.E. BDSG finden die Rechten und Pflichten aus dem Datenschutzrecht keine Anwendung, wenn die Daten nur für persönliche oder familiäre Zwecke erhoben werden. Der Pilot erhebt die Daten nur für seine persönlichen Zwecke und unterliegt deswegen nicht als verantwortliche Stelle dem Datenschutzrecht.

2. Zwischenergebnis

Die Verwendung von Flarm im Flugzeug unterliegt keinen datenschutzrechtlichen Vorschriften.

III. Flarm kommuniziert mit anderen Segelfliegern

1. Ist Datenschutzrecht einschlägig?

Für die Kollisionswarnungen sendet Flarm kontinuierlich die aktuellen Flugdaten. Gleichzeitig empfängt und verarbeitet es die Daten anderer Flarm-Systeme. Den ausgesandten Datenpaketen ist ausschließlich die Geräte-ID[31] beigefügt, die über kein öffentlich zugängliches Register mit personenbezogenen Daten verknüpft ist.[32] Die Datenpakete enthalten ausschließlich sachbezogene Daten, die von empfangenden Segelfliegern auch höchstens über Sichtkontakt zum Flugzeugkennzeichen[33] o.ä. Zusatzwissen (weil man z.B. alle Segelflugzeuge in der eigenen Flugregion kennt) mit Personen verknüpft werden können. Die rechtliche Frage ist, ob die Person hinter den Datensätzen bestimmbar i.S.d. Datenschutzrechts ist. Zur Bestimmbarkeit einer Person kann es ausreichen, vormals rein sachbezogene Datensätze zusammenzuführen, um dadurch präzisierende Angaben über die dahinterstehende Person zu erlangen. Kernproblem ist, ob alle überhaupt existierenden Verknüpfungsmöglichkeiten bei der Subsumtion zu betrachten sind, oder nur diejenigen Verknüpfungsmöglichkeiten beachtet werden müssen, die der datenverarbeitenden Stelle offensichtlich gerade zur Verfügung stehen. Nach europarechtskonformer Auslegung[34] müssen alle Mittel berücksichtigt werden, die

---

[30] Zur Abgrenzungsdogmatik siehe Anhang.

[31] Die IGC-Datei mit Namen des Piloten wird nicht über Funk ausgesendet. IGC steht für die International Gliding Commission.

[32] Unter FlarmNet.org kann man freiwillig persönliche Angaben mit seiner Flarm-ID verknüpfen. Um diese Angaben einsehen zu können, ist eine Registrierung bei FlarmNet.org nötig.

[33] Nach den §§ 14 und 19 und der Anlage 1 LuftVZO muss jedes Luftfahrzeug sein Kennzeichen deutlich sichtbar führen.

[34] Art. 2 a) RL 95/46/EG: „(…)als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann (…).“

von der verantwortlichen Stelle vernünftigerweise herangezogen werden könnten, um den Personenbezug der Daten herzustellen. Dabei ist es unerheblich, ob die Zuordnung durch den Verantwortlichen selbst oder nur im Zusammenwirken mit einem Dritten erfolgen kann, der im Besitz eines weiteren Zuordnungsmerkmals ist.[35] Das Zusatzwissen, das der empfangende Pilot haben kann beschränkt sich auf das mentale, persönliche Wissen. Während des Fluges steht auch nicht zu befürchten, dass der Pilot sich anderweitig Zusatzwissen verschafft. Auch im Nachhinein ist dies nicht ohne weiteres möglich: Die Zuordnung von Luftfahrzeugkennzeichen zum Halter sind für Privatpersonen aus der Luftfahrzeugrolle nicht zu entnehmen.[36]

Bei rein mentalem Zusatzwissen handelt es sich allerdings nicht um ein Mittel, mit dem vernünftigerweise gerechnet werden kann, sondern um persönlich abhängiges, zufälliges Wissen. Solches Zusatzwissen hat keinen Einfluss auf die Definition einer Information als personenbezogenes Datum. Die Daten sind sachbezogen, datenschutzrechtliche Vorschriften greifen nicht.

2. Sind andere Schutzvorschriften einschlägig?

In Betracht kommt insbesondere das Fernmeldegeheimnis aus § 88 TKG.[37] Der Schutzbereich ist deckungsgleich mit dem Schutzbereich aus Art. 10 Abs. 1 GG: jede individuelle Übermittlung von Signalen über Fernmeldetechnik ist geschützt.[38] Für den Schutz durch das Fernmeldegeheimnis muss ein Telekommunikationsvorgang vorliegen, § 88 Abs. 1 TKG. Das Aussenden der Flarm-Signale ist unzweifelhaft unter Telekommunikation zu subsumieren.[39] § 88 Abs. 1 TKG verpflichtet allerdings nur die Telekommunikationsdiensteanbieter, § 88 Abs. 2 TKG. Diensteanbieter ist nach § 3 Nr. 6 TKG jeder, der Telekommunikationsdienste ganz oder teilweise geschäftsmäßig erbringt oder an der Erbringung mitwirkt. Nach § 3 Nr. 10 TKG genügt für das „geschäftsmäßige Erbringen“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Zu fragen ist, wer hier Diensteanbieter ist. Die Piloten nutzen Flarm zwar nachhaltig (kontinuierlich), bieten es aber gerade nicht für Telekommunikation mit Dritten an, es geht ihnen nur um die Kommunikation mit dem Gegenüber, nämlich dem fremden Flugzeug. Es handelt sich bei Flarm um eine reine Maschine-zu-Maschine-Kommunikation, so dass nicht verallgemeinernd von einer einseitigen Leistungserbringung durch einen Diensteanbieter gesprochen werden kann. Für automatisierte Telekommunikationsvorgänge gilt, dass die hinter den kommunizierenden Anlagen stehenden Betreiber sich auf § 88 TKG berufen können.[40] Insofern können die Piloten[41] den Schutz ihrer Kommunikation doch auf § 88 TKG stützen, sind aber gleichzeitig auch Verpflichtete des Fernmeldegeheimnisses und müssen es (im Umgang mit den Daten anderer) wahren.

---

[35] Brühann in Grabitz/ Hilf, Das Recht der Europäischen Union, A 30. RL 95/46/EG Art. 2, Rn. 8.

[36] Luftfahrzeugkennzeichen haben aus sich selbst heraus nicht dieselbe datenschutzrechtliche Brisanz wie Kraftfahrzeugkennzeichen; zu Kraftfahrzeugkennzeichen vgl: BVerfG, Urteil vom 11.3.2008 - 1 BvR 2074/05 und 1 BvR 1254/07, MMR 2008, 308.

[37] § 88 TKG ist lex specialis zu Art. 10 Abs. 1 GG und wird deswegen hier zuerst, und wenn er einschlägig ist ausschließlich, geprüft.

[38] Eckhardt in Spindler/Schuster, TKG, § 88, Rn. 4.

[39] Die Definition von Telekommunikation ist in § 3 Nr. 22 TKG zu finden.

[40] Bock in Beck’scher TKG-Kommentar, § 88, Rn. 20.

[41] In den persönlichen Schutzbereich fällt jeder an der Telekommunikation Beteiligte, § 88 Abs. 1 S.1 TKG; Eckhardt in Spindler/Schuster, TKG, § 88, Rn. 14.

Durch die Verschlüsselung der Flarm-Daten, die nur durch andere Flarm-Geräte entschlüsselt werden kann, handelt es sich bei den Flarm-Signalen um eine individuelle Kommunikation, denn der Empfängerkreis ist abgegrenzt: nicht jedermann, sondern nur jeder mit einem Flarm-Gerät kann die Daten auslesen/ kommunizieren. Flarm selbst ist so konzipiert, dass Kommunikation nur mit anderen Flarm-Geräten und Flarm-kompatiblen Systemen stattfinden kann (/können soll).[42] Durch diese Flarm-eigenen Sicherheitsmaßnahmen wahren die Piloten untereinander das einfachgesetzliche Fernmeldegeheimnis.

Verstöße gegen § 88 TKG können zivilrechtliche Schadens- und Unterlassungsansprüche gem. § 44 TKG nach sich ziehen.

IV. Die Bodenstation empfängt und verarbeitet die Flarm-Daten

1. Ist Datenschutzrecht einschlägig?

a) Empfang

Empfangen werden alle ausgesendeten Flugdaten, die Flarm-ID und ggf. die Stealth-ID.[43] Der Stealth-Modus[44] beschränkt das „sehen und gesehen werden" mit anderen Flugzeugen auf sehr nahe, kollisionswahrscheinliche Entfernungen.[45] Die Information, nicht gesehen werden zu wollen, also die Stealth-ID, wird trotzdem ausgesendet und von anderen Flarm-Geräten empfangen.

Für den Empfang der Daten gilt das zuvor gesagte: die Daten sind (noch) nur sachbezogen. Damit sind klassische Datenschutzvorschriften außen vor.

Der Überlegung, den Inhalt der Übertragung als Telemedium zu werten, steht entgegen, dass die Informationsübermittlung bei Übertragungsende ebenfalls abgeschlossen ist, so dass ein telekommunikationsgestützter Dienst nach § 3 Nr. 25 TKG vorliegt und der Vorgang in den Regelungsbereich des TKG fällt.

Näher zu betrachten sind Vorschriften, die die Übermittlung von Signalen und Daten betreffen. Dies sind die §§ 88, 89, 148 TKG, §§ 202a, 202b, 202c StGB.

b) Verarbeitung und Weitersendung

Die Verarbeitung der Daten in den Bodenstationen umfasst das Entschlüsseln der Flarm-Codierung und ggf. die Verknüpfung der Flarm-ID mit dem *FlarmNet*-

---

[42] „FLARM verwendet für die Funkkommunikation zwischen den einzelnen Geräten ein proprietäres und urheberrechtlich geschütztes Protokoll in regional unterschiedlichen Frequenzbändern [ ], zudem ist die Funkübertragung gesondert gegen unberechtigten Zugang gesichert.[...] Das Protokoll ist nicht öffentlich zugänglich, es wird jedoch im Rahmen eines Lizenzvertrags von FLARM Technology GmbH in der Form eines kompatiblen Kerndesigns integrierbar in kompatible[n] Systemen verwendet. Diese Systeme sind entsprechend als FLARM-kompatibel bezeichnet." http://www.flarm.de/disclaimer/index.html, abgerufen am 16.01.2015, 12.24 Uhr.

[43] Heynen: „Wir sehen uns! glidernet.org" in segelfliegen 1/2015, 61.

[44] stealth (engl.)= Heimlichkeit; frei übersetzt als Tarnkappen-Modus.

[45] http://www.flarm.de/support/Flarm_Competitions_de.pdf, abgerufen am 14.01.2015, 20.45 Uhr.

Eintrag[46]. Flarm-IDs, die mit einer Stealth-ID verbunden sind, werden nicht weiterverarbeitet.[47]

Die Daten sind bis zu dem Moment sachbezogen, in dem sie mit ausreichenden Zusatzinformationen verknüpft werden, um die Person hinter den Sachdaten ermitteln zu können.[48] Auf *FlarmNet* sind Flarm-ID, Name des Piloten, Flugzeugtyp, Kennzeichen, Region und E-Mail-Adresse hinterlegt. Optional anzugeben sind der Heimatflugplatz, die Wettbewerbs-ID und die genutzte Frequenz.[49] Wird die Flarm-ID mit den *FlarmNet*- Daten verknüpft und anschließend die *FlarmNet*-Kennung verwendet, so sind die Flarm-Daten ab diesem Zeitpunkt personenbezogene Daten. Für diesen Fall sind datenschutzrechtliche Vorschriften anwendbar. Parallel können trotzdem Vorschriften zum Schutz der technischen Übertragung greifen, s.o. (VI. 1. a).

Ist die Flarm-ID nicht auf *FlarmNet* registriert, werden die Informationen nicht mit personenbezogenen Daten verknüpft. Dann bleiben die Daten auch weiterhin sachbezogen und es greifen nur die Vorschriften zum Schutz der Datenübertragung.

2. Rechtmäßigkeit des Empfangs

a) § 88 TKG (Fernmeldegeheimnis)

§ 88 TKG schützt die Vertraulichkeit nur gegen denjenigen, dessen Telekommunikationsleistung man nutzt.[50] Wie oben (s. V.2.) bereits ausgeführt, genießen die Piloten für „ihre“ Flarm-Daten den Schutz des Fernmeldegeheimnisses und sind gleichzeitig als Flarm-Betreiber für die Wahrung des § 88 TKG verantwortlich.

Bemerkenswert ist, dass auf den Schutz aus § 88 TKG durch Einwilligung beider Telekommunikationsteilnehmer verzichtet werden kann.[51] Grundsätzlich kann von der Einwilligung zur Flarm-Flarm-Kommunikation ausgegangen werden.

Handelte es sich bei der Bodenstation um ein Flarm-Gerät, so ist zu erwarten, dass die Piloten ihre Einwilligung zur Kommunikation mit dem Gerät gegeben haben. Das Open Glider-Netzwerk allerdings ist aus andersartigen Bodenstationen zusammengesetzt: Ein OGN-Receiver besteht aus einer Antenne, einem DVB-T-Stick und einem Computer mit entsprechender Software.[52] Zwar sind auch die Receiver an Kommunikation beteiligt und die dahinter stehenden Betreiber Berechtigte des Fernmeldegeheimnisses, sie als Diensteanbieter zu bezeichnen, würde den Wortlaut des § 88 TKG hingegen überstrapazieren. Systematisch betrachtet schützt § 88 TKG die Nachricht vor den Diensteanbietern, also an der Telekommunikation Beteiligten. Die speziellere Norm für den Schutz vor Dritten, an der Telekommunikation eigentlich Unbeteiligten, ist § 89 TKG.

---

[46] Heynen: „Wir sehen uns! glidernet.org“ in segelfliegen 1/2015, 61; http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 14.01.2015, 21.06 Uhr.

[47] http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 14.01.2015, 21.08 Uhr.

[48] s.o. unter V.1.; dazu unter dem Stichwort „Geodaten“: Heckmann in jurisPK-Internetrecht, Kap. 9, Rn. 569 ff.

[49] http://flarmnet.org/index.php/en/register-now, abgerufen am 14.01.2015, 20.58 Uhr.

[50] Eckhardt in Spindler/Schuster, TKG, § 88, Rn. 3.

[51] Eckhardt in Spindler/Schuster, TKG, § 88 Rn. 15

[52] http://wiki.glidernet.org/links#toc5, abgerufen am 16.01.2015, 12.14 Uhr.

b) §§ 148 Abs. 1 Nr. 1 i.V.m. 89 TKG (Strafbarkeit des Abhörens und Mitteilens von Nachrichten)

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 89 TKG nicht für die Allgemeinheit bestimmte Nachrichten abhört oder anderen mitteilt. Fraglich ist, ob der Empfang durch die OGN-Receiver unter § 89 TKG zu subsumieren ist.

aa) OGN-Receiver als Funkanlage

Funkanlagen sind elektrische Sende- oder Empfangseinrichtungen, zwischen denen die Informationsübertragungen oder Verbindungsleitungen stattfinden können.[53] Die OGN-Receiver sind sowohl Sende-, als auch Empfangseinrichtungen, die untereinander und mit anderen Einrichtungen Informationen austauschen können. OGN-Receiver sind Funkanlagen i.S.d. § 89 TKG.

bb) Flarm-Signale als Nachrichten

Informationen in Form von Zeichen, Sprache, Bildern oder Tönen sind Nachrichten. Auch private Funksendungen sind geschützt.[54] Die Flarm-Signale können in Zeichen, Sprache und Bilder umgesetzt werden, sind aber erstmal nur als rein technische, codierte Signalübermittlungen zu sehen. Der Code ist eine verabredete Zeichenfolge[55], die für die Kommunikationsteilnehmer Informationsgehalt hat. Die Flarm-Signale sind Nachrichten.

cc) Für den Betreiber der OGN-Receiver oder die Allgemeinheit bestimmt

Die Flarm-Nachrichten sind grundsätzlich weder für den Betreiber des OGN-Receivers, noch für die Allgemeinheit bestimmt. Sie sollen nur zwischen Flarm-Geräten ausgetauscht werden (s. V.2.).

dd) Abhören

Die Tathandlung „Abhören“ soll das „akustische Wahrnehmen“ der Nachricht sein.[56] Darunter fallen das unmittelbare Zuhören und das unmittelbare Hörbar-Machen einer Nachricht.[57] Dieses ausschließliche Abstellen auf die Akustik scheint höchst widersinnig: wenn auch ein Bild-Signal eine Nachricht i.S.d. § 89 TKG sein, also auch vom Schutzbereich umfasst sein soll, wie verträgt sich das mit dem ausschließlich untersagten „Hören“? Zwar ist zu bedenken, dass § 89 TKG strafbewährt ist und deswegen das Analogieverbot aus Art. 103 Abs. 2 GG gilt, doch steht dem gegenüber, dass das TKG entwicklungsoffen und technologieneutral formuliert sein soll, § 1 TKG. Schon lange werden nun nicht mehr nur Sprachnachrichten durch den Äther geschickt, sondern auch technische Codes, Befehle (z.B. von einer Fernbedienung an das Garagentor), etc.

---

[53] Vgl. § 3 Nr. 4 TKG-1996; Bock in Beck’scher TKG-Kommentar, § 89, Rn. 4.

[54] Bock in Beck’scher TKG-Kommentar, § 89, Rn. 5.

[55] Bock in Beck’scher TKG-Kommentar, § 89, Rn. 5.

[56] So Bock in Beck’scher TKG-Kommentar, § 89, Rn. 6.

[57] So Bock in Beck’scher TKG-Kommentar, § 89, Rn. 6.

Ein weiteres Kriterium ist das bewusste Auswerten der Daten.[58] Die Bodenstationsbetreiber wollen die Daten gezielt für ihre Zwecke weiterverwenden, daran würde die Subsumtion nicht scheitern.

Will man den Wortlaut aber nicht überstrapazieren, muss man zu dem Ergebnis kommen, dass der Empfang der Flarm-Daten nicht unter „abhören“ zu fassen ist.[59]

ee) Zwischenergebnis

Die OGN-Bodenstationsbetreiber sind nicht nach den §§ 148 Abs. 1 Nr. 1 i.V.m. 89 TKG strafbar.

c) § 202 a Abs. 1 StGB (Ausspähen von Daten)

Die OGN-Bodenstationsbetreiber könnten sich strafbar machen, wenn sie sich unbefugt Zugang zu Daten verschaffen, die nicht für sie bestimmt und besonders vor Zugang gesichert sind und sie dafür die Zugangssicherung überwinden.

Geschützt sind das individuelle Geheimhaltungsinteresse und das formelle Verfügungsbefugnis des Verfügungsberechtigten.[60] Verfügungsberechtigter „Herr der Daten“ ist der übermittelnde Pilot.[61]

aa) Daten

Darunter sind alle Darstellungen von Informationen, die sich als Gegenstand oder Mittel der Datenverarbeitung für eine Datenverarbeitungsanlage codieren lassen oder die das Ergebnis eines Datenverarbeitungsvorgangs sind, zu verstehen.[62] Es kommt nicht darauf an, ob die Daten selbst Geheimnisse (z.B. personenbezogene Daten) sind. [63] Die Daten dürfen nach § 202 a Abs. 2 StGB nicht unmittelbar wahrnehmbar gespeichert sein oder unmittelbar wahrnehmbar übermittelt werden. Die sachbezogenen, per Funk übertragenen und codierten Flarm-Daten erfüllen den Tatbestand des § 202 a StGB.

bb) Nicht für den Täter bestimmt

Es kommt auf das tatsächliche Vorliegen des Einverständnisses an: Ist der Pilot mit der Datensichtung einverstanden, sind die Daten auch für den Täter, also den OGN-Bodenstations-Betreiber bestimmt. Gibt der Pilot nicht sein Einverständnis dazu, sind sie nicht für den Täter bestimmt. Es ist irrelevant, ob der Täter von einem Einverständnis ausgeht oder nicht.[64] Für die weitere Prüfung wird davon ausgegangen, dass der Pilot sein Einverständnis **nicht** gegeben hat.

---

[58] Bauer: „Strafbarkeit der unerlaubten Nutzung eines offenen WLANs- Kommentar“, MMR-Aktuell 2010, 311321.

[59] Bock sieht Netzwerksignale, die über WLAN übertragen werden, als „abhörbar“ i.S.d. § 89 TKG an (Der von ihm angenommene Fall, dass der Router an alle Netzteilnehmer Informationen schickt, scheitert an dem Merkmal der Bestimmtheit der Nachrichten). Bock in Beck’scher TKG-Kommentar, § 89, Rn. 6.

[60] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 7, 14; Kargl in Kindhäuser/ Neumann/ Paeffgen, StGB, § 202 a Rn.3.

[61] Die übermittelnde Stelle ist Berechtigter, BayObLG JR 1994, 477 f.

[62] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 14; so auch Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 4.

[63] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 7.

[64] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 21.

cc) Zugangssicherung und deren Überwindung; fehlende Berechtigung

Die Sicherung muss geeignet sein, den Zugang wenigstens zu erschweren. Es muss erkennbar sein, dass der Berechtigte die Daten geheim halten wollte.[65] Die Verschlüsselung genügt als Zugangssicherung.
Das Überwinden wiederum ist schwieriger festzustellen, denn die OGN-Receiver verfügen über die Decodierungs-Formeln, müssen also die Schranke nicht „überwinden", sondern können sie einfach öffnen. Die Zugangsschranke muss aber nicht ausnahmslos jedem entgegenstehen, für den die Daten nicht bestimmt sind[66], weil es auf das manifestierte Geheimhaltungsinteresse des Datenherrn ankommt. Insofern ist das „Überwinden" nicht ohne die „fehlende Berechtigung" zu prüfen. Da die Bodenstationsbetreiber hier insgesamt ohne Berechtigung handeln, ist das Überwinden der Zugangssperre schon in der (unberechtigten) Benutzung des Entschlüsselungscodes zu sehen.

dd) Tathandlung

Es wäre nicht notwendig, dass der Täter sich tatsächlich die Daten verschafft, also Macht über sie ausübt. Es genügt, dass der Täter sich den Zugang oder den Zugangsschlüssel[67] verschafft. Der Zugangsschlüssel zu den Flarm-Daten ist in der OGN- Software enthalten.[68] Das Installieren der Software ist gleichzeitig die Verschaffung des Zugangsschlüssels. D.h. schon mit der Installation, erst recht aber mit der Überwindung der Verschlüsselung ist die Tathandlung erfüllt.

ee) Der objektive Tatbestand ist erfüllt.

ff) Die Bodenstations-Betreiber wissen um und wollen den Flarm-Datenempfang und die Weiterverarbeitung. Die Betreiber könnten einem vorsatzausschließenden Tatbestandsirrtum dahingehend unterliegen, dass sie die Daten für sich bestimmt glauben.[69] Dem steht allerdings entgegen, dass der Flarm-Disclaimer ausdrücklich darauf hinweist, dass die Flarm-Daten gegen unberechtigten Zugang geschützt sein sollen[70] und jeder Betreiber erst eine spezielle Software installieren muss um die Flarm-Daten lesen zu können[71]. Der subjektive Tatbestand ist erfüllt.

gg) Unbefugt handelt auch, wer sich nicht auf einen Rechtfertigungsgrund berufen kann.[72] Rechtfertigungs- oder Entschuldigungsgründe sind nicht ersichtlich.

hh) Ergebnis: Die Bodenstationsbetreiber sind nach § 202 a Abs. 1 StGB strafbar. Die Tat wird grundsätzlich nur auf Antrag des Verfügungsberechtigten, also des Piloten, verfolgt, § 205 Abs. 1 S. 1 StGB.

---

[65] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 24.

[66] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 11.

[67] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 12.

[68] = „rtlsdr-flarm", hier der Einfachheit halber OGN-Software genannt; https://github.com/glidernet/rtlsdr-flarm, abgerufen am 21.01.2015, 16.17 Uhr.

[69] Cornelius in Kilian/ Heussen: Computerrecht, Rn. 33.

[70] http://www.flarm.de/disclaimer/index.html, abgerufen am 16.01.2015, 12.24 Uhr.

[71] https://github.com/glidernet/rtlsdr-flarm, abgerufen am 21.01.2015, 16.19 Uhr; http://wiki.glidernet.org/links#toc5, abgerufen am 21.01.2015, 16.20 Uhr.

[72] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 16.

d) § 202 b StGB (Abfangen von Daten)

Die Bodenstations-Betreiber könnten sich durch die unbefugte Verschaffung der Flarm-Daten unter Anwendung der OGN-Stationen strafbar machen.

aa) Daten aus einer nicht-öffentlichen Datenübermittlung

Für den Datenbegriff des § 202 b StGB bestehen im Vergleich zu § 202 a StGB einige Einschränkungen: Die Daten müssen aus einer nicht-öffentlichen Datenübermittlung oder einer elektromagnetischen Abstrahlung stammen. Die nicht-öffentliche Datenübermittlung ist technologieneutral zu verstehen, sie muss nicht leitungsgebunden sein.[73] Trotzdem muss die Übertragung[74] zielgerichtet sein, also einen bestimmten Adressaten haben.[75] Der nur bestimmbare, aber nicht bestimmte Personenkreis der Flarm-Nutzer erfüllt das Kriterium der Zielgerichtetheit nicht.

Fraglich ist auch, ob der Übertragungsweg der Flarm-Daten „nicht-öffentlich" ist. Zwar sind die Daten verschlüsselt (also nicht für jedermann auslesbar), wohl sind sie aber von jedermann mit dem entsprechenden Empfangsgerät empfangbar. Der Aufwand, der für den Empfang getrieben werden muss, kann Aufschluss über die Nicht-Öffentlichkeit der Übertragung geben. Bei Daten, die mit einem unmanipulierten Empfangsgerät, das legal zu erwerben ist, abgefangen werden können, ist die Datenübermittlung öffentlich,[76] auch weil sie an die Allgemeinheit gerichtet ist.[77] Die Bestandteile der OGN-Bodenstationen sind legal zu erwerben, der Flarm-Übertragungsweg ist öffentlich.

bb) Die Bodenstations-Betreiber sind nicht nach § 202 b StGB strafbar.

e) § 202 c Abs. 1 Nr. 2 StGB (Vorbereiten des Ausspähens und Abfangens der Daten)

Die OGN-Programmierer[78] könnten durch das Bereithalten der Software zum Download[79] strafbar sein.

aa) Die Verwendung der Software zum Empfang der Flarm-Daten ist nach § 202a StGB strafbar (s. VI.2.c).

bb) OGN-Software als Computerprogramm

Ein Computerprogramm ist eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind, zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt.[80] Der objektive Zweck des

---

[73] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 b, Rn. 4.

[74] Zu betonen ist, dass es allein auf den Übertragungsvorgang, nicht auf den Inhalt der Nachricht ankommt, vgl. auch Cornelius in Kilian/ Heussen: Computerrecht, § 202 b, Rn. 43.

[75] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 4.

[76] Kargl in Kindhäuser/ Neumann/ Paeffgen: StGB, §202 a, Rn. 5;

[77] Spindler/ Schuster, Recht der elektronischen Medien, § 202 b StGB, Rn. 4.

[78] Der Begriff OGN-Programmierer ist verallgemeinernd: hier soll nur derjenige darunter fallen, der tatsächlich an der Entwicklung und Veröffentlichung der Software mitwirkt.

[79] http://wiki.glidernet.org/downloads, abgerufen am 21.01.2015, 16.30 Uhr.

[80] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 3; Vgl. dazu auch OLG Hamburg, CR 1998, 333 f.; Dreier in: Dreier/Schulze, UrhG, § 69 a StGB Rn. 12.

Programms muss die Begehung einer Computerstraftat sein.[81] Die OGN-Software befähigt den OGN-Receiver, die Flarm-Daten entschlüsseln zu können, ist also ein Computerprogramm. Der objektive Zweck des Programms ist das Empfangen der Flarm-Daten, was nach § 202 a StGB strafbar ist.

cc) In Betracht kommende Tathandlungen: herstellen, anderen überlassen, verbreiten oder sonst zugänglich machen

Herstellen ist die Programmierung der Software.[82] Überlassen liegt vor, wenn der Täter einem Dritten zu dessen Verfügung Gebrauch und Besitz ermöglicht.[83] Unter Verbreiten versteht man das Auftreten der Software auf mehreren Rechnern, ausgelöst durch die Tathandlung.[84] Zugänglichmachen ist die Ermöglichung des Zugriffs auf das Tatobjekt, also die Software.[85]

Die Software wird hergestellt, überarbeitet und erneuert. Sie wird einer unbestimmten Menge an Downloadern überlassen, wodurch die Software verbreitet wird. Der objektive Tatbestand ist erfüllt.

dd) Es ist gerade gewollt, dass die Software hergestellt, überlassen und verbreitet wird. Die OGN-Programmierer handeln vorsätzlich. Zudem ist wichtig, dass sie die Software bewusst als Vorbereitung des Flarm-Empfangs (also der Haupttat) herstellen, überlassen und verbreiten. Auch das ist der Fall. Der subjektive Tatbestand ist erfüllt.

ee) Rechtfertigungs- oder Entschuldigungsgründe sind nicht ersichtlich.

ff) Die OGN-Programmierer sind gem. § 202 c Abs. 1 Nr. 2 StGB strafbar.

f) Zwischenergebnis

§ 88 TKG ist für den Empfang der Flarm-Signale durch die OGN-Bodenstationen nicht einschlägig.

Es ergibt sich keine Strafbarkeit der Bodenstationsbetreiber aus §§ 148 Abs. 1 Nr. 1 i.V.m. 89 TKG, ebenso wenig aus § 202 b StGB.

Stattdessen machen sie sich durch das Verwenden der OGN-Software nach § 202 a Abs. 1 StGB strafbar.

Die OGN-Programmierer sind nach § 202 c Abs. 1 Nr. 2 StGB strafbar.

3. Rechtmäßigkeit der Verarbeitung

Bei der Verarbeitung werden die Daten entschlüsselt, die Flarm- und Stealth-ID werden wahrgenommen und gegebenenfalls mit den Informationen aus dem *FlarmNet* gekoppelt.

---

[81] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 3.

[82] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 4.

[83] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 4.

[84] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 4.

[85] Gercke in Spindler/ Schuster, Recht der elektronischen Medien, StGB § 202 c, Rn. 4.

a) Fall 1: ohne Personenbezug

Für die Verarbeitung der Daten ohne Personenbezug gilt das unter VI.2. festgestellte fort, da sich die Qualität der Daten nach dem Empfang nicht ändert und auch die Verarbeitung der Daten von den §§ 202 a, 202 b, 202c StGB mitumfasst ist.

b) Fall 2: mit Personenbezug

Anders ist der Fall ab dem Moment gelagert, in dem die Flarm-Daten mit den *FlarmNet*-Daten verknüpft werden. Die zu verarbeitenden Daten sind jetzt personenbezogene Daten. Werden personenbezogene Daten verarbeitet, sind die Rechte und Pflichten aus dem Datenschutzrecht zu beachten. Es gilt der Grundsatz aus § 4 Abs. 1 BDSG: Die Verarbeitung ist nur erlaubt, wenn eine Einwilligung oder eine gesetzliche Grundlage vorliegt.

aa) Ausnahme: § 1 Abs. 2 Nr. 3 a.E. BDSG

Den Bodenstationsbetreiber würden keine Pflichten aus dem BDSG treffen, wenn er die Daten ausschließlich zu persönlichen oder familiären Zwecken verwenden würde. Der Stationsbetreiber nutzt den OGN-Receiver in seiner Freizeit, nicht für berufliche oder erwerbsmäßige Zwecke. Trotzdem muss man fragen, wer mit den Daten in Berührung kommt, denn daraus lässt sich entweder eine ausschließlich persönliche oder weitreichendere Verwendung erkennen. Die Daten werden hauptsächlich zum Zwecke der Weiterleitung erhoben. Weitergeleitet werden sie an Server in Frankreich, was nicht der persönlichen oder familiären Sphäre des Bodenstationsbetreibers zuzurechnen ist. Die Ausnahme greift nicht.

bb) Gibt es eine Einwilligung?

OGN verknüpft die Flarm-Daten automatisch mit *FlarmNet*-Daten. Die Frage ist, ob der Pilot genau zu dieser Verknüpfung vorher[86] eingewilligt hat. Die Einwilligung in die Datenverarbeitung muss vor allem informiert und bestimmt abgegeben werden. Informiert ist der Betroffene, der alle entscheidungsrelevanten Informationen kennt und Risiken und Vorteile der Einwilligung abwägen kann.[87] Dafür ist es zwingend notwendig, dass der Betroffene den genauen Verwendungszweck der Daten erkennen kann, § 4a Abs. 1 S. 2 BDSG.

(1) Einwilligung bei der Registrierung auf *FlarmNet*[88]

Über eine Button-Leiste auf der Startseite von *FlarmNet* gelangt man auf die FAQ-Seite.[89] Dort findet man unter dem Stichpunkt „Am I always visible, if I register at FlarmNet“ folgende Ausführungen:

“FlarmNet supports the stealth-mode, which is integrated in every FLARM®-device. FlarmNet authorized devices don't show any FlarmNet-data of aircraft with enabled stealth-mode. To make it

---

[86] Die Einwilligung ist eine vorherige Zustimmung, Kühling in Beck’scher Online-Kommentar Datenschutzrecht, § 4a, Rn. 32.

[87] Kühling in Beck’scher Online-Kommentar Datenschutzrecht, § 4 a BDSG, Rn. 43.

[88] Über den Registrierungsvorgang selbst kann keine Aussage getroffen werden. Für den Registrierungsvorgang ist die Eingabe einer Flarm-ID notwendig. Es kann nur anhand der öffentlich bereitgehaltenen Informationen geprüft werden.

[89] http://flarmnet.org/index.php/en/faqs-and-answers, abgerufen am 21.01.2015, 21.25 Uhr.

short: Only who wants to be seen is displayed.
Be careful, some other devices may have the ability to display FlarmNet data without this restriction, therefore only submit data if your are willing to allow others to see these. Also some Web-Projects displaying traffic data may publicly display FLARM-Data and use FlarmNET to identify you, if you register."[90]

Fraglich ist, ob der Zusatz "if you are willing to allow others to see [your data]", genügt, um von einer informierten Einwilligung der *FlarmNet*-Nutzer in die OGN-Datennutzung auszugehen. Die schwammige Formulierung lässt gerade nicht den genauen Verwendungszweck der Datenverarbeitung, und die damit zu erwartende Verbreitung der Daten, erkennen.
Dazu kommt noch die Erweiterung, dass „einige Web-Projekte" die Daten öffentlich anzeigen werden, was die Verwendung der Daten noch undurchsichtiger und unvorhersehbarer macht, jedenfalls aber nicht auf die Verwendung durch das OGN hinweist.
Die tendenzielle Verbreitungsgeneigtheit der Daten im Internet dürfte heute allgemein bekannt sein, so dass der obenstehenden Erklärung kein weitergehender Informationsgehalt zu entnehmen ist.

Auf der Impressumsseite[91] ist zum Thema Datenschutz ausgeführt:

„4. Datenschutz
Sofern innerhalb des Internetangebotes die Möglichkeit zur Eingabe persönlicher oder geschäftlicher Daten (Emailadressen, Namen, Anschriften) besteht, so erfolgt die Preisgabe dieser Daten seitens des Nutzers soweit möglich stets auf freiwilliger Basis. Die Nutzung der Angebote und Dienste ist, soweit möglich, stets ohne Angabe personenbezogener Daten möglich. ***Wir weisen darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.*** *Der Nutzung von im Rahmen der Impressumspflicht veröffentlichten Kontaktdaten durch Dritte zur Übersendung von nicht ausdrücklich angeforderter Werbung und Informationsmaterialien wird hiermit ausdrücklich widersprochen. Die Betreiber der Seiten behalten sich ausdrücklich rechtliche Schritte im Falle der unverlangten Zusendung von Werbeinformationen, etwa durch Spam-Mails, vor."*

Auch daraus ist nicht ersichtlich, dass das OGN Zugriff auf die *FlarmNet*-Daten hat und sie mit Flugbewegungen verknüpft.
Grundsätzlich sind drei Fälle sind denkbar:

- Der Pilot registriert sich bei *FlarmNet*, weiß von OGN und ist einverstanden mit der Datennutzung durch OGN.
- Der Pilot registriert sich auf *FlarmNet* und weiß nicht um die Existenz des OGN.
- Der Pilot registriert sich auf *FlarmNet* und ist gegen die Datennutzung durch das OGN.

Wegen der unpräzisen Erklärung kann nur derjenige informiert einwilligen, der schon vor der Registrierung weiß, dass OGN die Daten verwenden wird. Doch auch der Wissende müsste seine Einwilligung schriftlich, wahlweise elektronisch[92]

---

[90] http://flarmnet.org/index.php/en/faqs-and-answers, abgerufen am 21.01.2015, 21.25 Uhr.

[91] http://flarmnet.org/index.php/en/impressum, Hervorhebung nachträglich hinzugefügt, abgerufen am 23.01.2015, 11.51 Uhr.

[92] schriftlich: § 4 a Abs. 1 S. 3 BDSG, elektronisch nach den Vorgaben des § 13 Abs. 2 TMG.

abgeben. Dies geschieht nicht. Auf der Webseite *FlarmNet* kann kein Pilot in die Datenverarbeitung durch das OGN einwilligen.

(2) Erklärungen auf der OGN-Webseite

Das OGN selbst legt seine Struktur offen. Dem OGN-Internetauftritt kann man entnehmen, dass die Daten nach Frankreich gesendet werden.[93] Der Internetauftritt ist aber in keiner Weise mit dem Verarbeitungsvorgang der Daten verknüpft, wird auf *FlarmNet* nicht erwähnt und dürfte deswegen vielen Piloten unbekannt sein. Die Erläuterungen haben keine datenschutzrechtliche Relevanz.

(3) Einwilligung durch Deaktivierung der Stealth-Funktion

Ist der Stealth-Modus aktiviert, verwendet das OGN die Daten nicht weiter. Im Umkehrschluss könnte die Deaktivierung der Stealth-Funktion der Einwilligung in die Veröffentlichung der Daten gleichkommen.

Das hieße, eine konkludente Einwilligung anzunehmen. Nach § 4a Abs. 1 S. 3 BDSG bedarf die Einwilligung grundsätzlich der Schriftform, nur unter besonderen Umständen kann eine andere Form angemessen sein. Das Schriftformerfordernis schließt eine Einwilligung durch konkludentes Handeln aus.

Auch die Deaktivierung der Stealth-Funktion ist keine Einwilligung in die Datenverarbeitung durch das OGN.

(4) Zwischenergebnis: Es liegen keine Einwilligungen vor.[94]

bb) Gibt es eine gesetzliche Grundlage?

Möglich ist, dass der OGN-Bodenstationsbetreiber für die Verknüpfung der *FlarmNet*-Daten mit den Flugbewegungen auf eine gesetzliche Grundlage zurückgreifen kann.

Die Verknüpfung der Datensätze kommt der Erhebung[95] gleich. Einschlägig ist § 28 BDSG.

(1) Verwendung für eigene Geschäftszwecke

Datenverarbeitung ist geschäftsmäßig, wenn sie mit Wiederholungsabsicht betrieben wird und auf eine gewisse Dauer angelegt ist, auf eine Gewinnerzielung (oder die Absicht dazu) kommt es nicht an.[96] Die Betreiber nutzen die Bodenstationen für eigene Zwecke und arbeiten nicht etwa nach Weisung. Die OGN-Bodenstationen haben einen nur geringen Energieverbrauch, was den ganztägigen Betrieb für Privatpersonen ermöglicht. Zweck der Bodenstationen ist, den Flugverkehr möglichst großflächig und genau „auszulesen“. Die Datenverarbeitung erfolgt naturgemäß nur dann, wenn ein entsprechendes Segelflugzeug in den Empfangsbereich kommt, der Betrieb der datenverarbeitenden Anlage ist aber unzweifelhaft auf Dauer angelegt.

---

[93] http://wiki.glidernet.org/about#toc2, abgerufen am 24.01.2015, 17.57 Uhr.

[94] Hier sei nochmal darauf hingewiesen, dass es durchaus möglich ist, dass während des FlarmNet-Registrierungsvorgangs genügend auf die OGN-Nutzung hingewiesen werden könnte. Dabei müssten das Koppelungsverbot (§ 4a Abs. 1 S. 1 BDSG) beachtet und genügend Informationen über den Umfang der Datenverarbeitung durch das OGN bereitgestellt werden, so dass der FlarmNet-Nutzer sich umfassend ein Bild der Lage machen kann.

[95] Erheben ist das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG.

[96] Ehmann in Simitis, BDSG, § 29, Rn. 58, Rn. 110 f.

(2) Zulässigkeit

Die verantwortliche Stelle muss bei, bzw. vor der Erhebung der Daten den Verwendungszweck konkret festlegen und erläutern, §§ 28 Abs. 1 S. 2, 4 Abs. 3 S. 1 Nr. 2 BDSG. Es mag sein, dass die Bodenstationsbetreiber den Verwendungszweck der Daten im Vorhinein festgelegt haben. Erläutert haben sie ihn den Betroffenen aber nicht. Schon deswegen ist die Erhebung unzulässig.[97]

Keiner der Zulässigkeitstatbestände des § 28 BDSG ist für die OGN-Mitglieder einschlägig: sie stehen in keinem Schuldverhältnis mit den Piloten, haben kein eigenes berechtigtes Interesse[98] an der Erhebung und die Daten sind nicht allgemein zugänglich.

cc) Ergebnis: Der OGN-Bodenstationsbetreiber verknüpft die Datensätze in unzulässiger Weise zu personenbezogenen Daten.

dd) Rechtsfolgen und weitere Pflichten des Datenverarbeiters

Gleichzeitig verstößt die Verknüpfung der Daten gegen den Grundsatz der Direkterhebung, § 4 Abs. 2 BDSG.

Es ist davon auszugehen, dass die Daten des betroffenen Piloten wenigstens im Zwischenspeicher des PCs abgelegt werden, womit die Benachrichtigungspflicht aus § 33 BDSG zum Tragen kommt: Der OGN-Bodenstationsbetreiber müsste den Piloten über seine Identifizierung (das Erheben personenbezogener Daten), die erste Übermittlung und den Empfänger informieren, § 33 Abs. 1 BDSG. Missachtet er diese Vorschrift kann ihm ein Bußgeld bis zu 50.000 € auferlegt werden, §§ 43 Abs.1 Nr. 8 i.V.m. Abs. 3 S. 1 Hs. 1 BDSG.

Nach §§ 43 Abs. 2 Nr. 1 i.V.m. Abs. 3 S. 1 Hs. 2 BDSG kann die unzulässige Erhebung personenbezogener Daten mit einer Geldbuße bis zu 300.000 € geahndet werden.

Die unzulässig erhobenen Daten müssen von den Bodenstationsbetreibern gelöscht werden.[99]

ee) Rechte des Betroffenen

Der betroffene Pilot kann nach § 34 BDSG Auskunft über seine Daten und nach § 35 Abs. 2 S. 1 Nr. 1 BDSG ihre Löschung verlangen.

Ist ihm wegen der unzulässigen Erhebung ein Schaden entstanden, kann er unter den Voraussetzungen des § 7 BDSG Schadensersatz einklagen

ff) Ansprüche aus dem allgemeinen Persönlichkeitsrecht

(1) Der Pilot könnte gegen den Bodenstationsbetreiber einen Unterlassungsanspruch gem. §§ 1004 Abs. 1 analog i.V.m. 823 Abs. 1 BGB

i) Geschütztes Rechtsgut

Das allgemeine Persönlichkeitsrecht ist ein absolut schützendes Recht. Die Normen des BDSG sind die einfachgesetzliche Ausprägung des Rechts auf informationelle Selbstbestimmung.

---

[97] Simitis in Simitis, BDSG, § 28, Rn. 46.

[98] Öffentliche Belange- wie das abstrakte OGN-Ziel „Flugsicherheit“- sind keine berechtigten Interessen, vgl. Simitis in Simitis, BDSG § 28, Rn. 103 ff.

[99] Simitis in Simitis, BDSG, § 28, Rn. 338.

ii) Widerrechtliche Verletzung

Das allgemeine Persönlichkeitsrecht wird durch die unzulässige Erhebung personenbezogener Daten widerrechtlich verletzt. (s. VI. 3. B) cc).

iii) Bodenstationsbetreiber als Anspruchsgegner

Anspruchsgegner des § 1004 BGB analog ist derjenige, der die Verletzung des Rechtsguts kausal zurechenbar herbeigeführt hat oder dessen Verhalten die Beeinträchtigung zumindest vermuten lässt. Die Installation der Bodenstation lässt die (zukünftige) Beeinträchtigung des Persönlichkeitsrechts der Piloten vermuten.

iv) Erstbegehungs- oder Wiederholungsgefahr

Ist die Station erstmal in Betrieb, besteht akut die Gefahr der Rechtsgutsverletzung.

v) Ergebnis: Der betroffene Pilot hat einen Unterlassungsanspruch gegen den OGN-Bodenstationsbetreiber.

(2) Der Pilot könnte nach § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG einen Schadensersatzanspruch gegen den Bodenstationsbetreiber haben.

i) Verletztes Rechtsgut ist das allgemeine Persönlichkeitsrecht

ii) Verschulden trifft den Bodenstationsbetreiber, sobald er die Bodenstation mind. fahrlässig in Betrieb nimmt.

iii) Materieller Schaden des Piloten ist nicht völlig ausgeschlossen, muss aber kausal auf die Verletzung des allgemeinen Persönlichkeitsrechts zurückzuführen sein. Bei immateriellen Schäden ist § 253 BGB zu beachten. Die Verletzung des Persönlichkeitsrechts ist als ein Fall des § 253 Abs. 1 BGB anerkannt.[100] Weiteres Kriterium für die Geldentschädigung ist dann die schwere Verletzung des allgemeinen Persönlichkeitsrechts.

iv) Ergebnis: Je nach Schadenseintritt kann der Pilot Schadensersatz verlangen.

(3) Der Pilot könnte nach § 823 Abs. 2 BGB i.V.m. § 4 BDSG einen Schadensersatzanspruch gegen den Bodenstationsbetreiber haben.

i) § 4 BDSG ist eine drittschützende Norm.[101]

ii) Die Bodenstationsbetreiber verstoßen gegen § 4 BDSG, indem sie unzulässigerweise, also ohne Einwilligung oder gesetzliche Ermächtigung, die Daten der Piloten erheben.

iii) Der Schaden muss kausal auf die Erhebung zurückzuführen sein.

iv) Die Bodenstationsbetreiber erheben die Daten vorsätzlich.

---

[100] Soraya-Beschluss, BVerfGE 34, 269.

[101] OLG Hamburg, Urteil vom 2. August 2011, Az. 7 U 134/10; auch in BGH: Urteil vom 27. Februar 2007 – Az. XI ZR 195/05;

v) Ergebnis: Je nach Schadenseintritt kann der Pilot Schadensersatz verlangen.

(4) Ergebnis: Der Pilot hat einen Unterlassungsanspruch gegen den Bodenstationsbetreiber. Je nach Fallgestaltung kann er den Bodenstationsbetreiber auch auf Schadensersatz in Anspruch nehmen.

4. Ergebnis für VI.

Der Empfang der Flarm-Daten mit den OGN-Bodenstationen ist strafbar. Das Herstellen und Verbreiten der OGN-Software ist strafbar.
Die Verknüpfung der Datensätze zu personenbezogenen Daten steht nicht im Einklang mit dem Datenschutzrecht und kann mit Bußgeldern geahndet werden.
Der Pilot kann die Bodenstationsbetreiber auf Unterlassung der Verknüpfung seiner Daten verklagen. Je nach Fall können Schadensersatzansprüche geltend gemacht werden.

V. Die Bodenstation sendet die Daten an die Server in Frankreich

1. Welches Datenschutzrecht ist anwendbar?

Es geht um die Übertragung von personenbezogenen Daten mittels Fernmeldetechnik, was in den Anwendungsbereich des TKG oder des BDSG fallen könnte. Die §§ 91 ff. TKG sind anwendbar, wenn der Schutz von Kommunikationsdaten bei der Erhebung und Verwendung durch Telekommunikationsunternehmen in Frage steht, § 91 Abs. 1 S. 1 TKG.
Das BDSG ist anwendbar, wenn das bereichsspezifische Datenschutzrecht (in diesem Falle das TKG) nicht einschlägig ist.

Bei diesem Übertragungsvorgang geht es nicht um das Schutzverhältnis vom Telekommunikationsunternehmen zum Betroffenen, also nicht um die Übertragungsebene, sondern um den Inhalt der Übertragung. Die Vorschriften des BDSG sind anzuwenden.

2. Zulässigkeit der Übermittlung

a) Besondere Problematik

Die Daten werden von Deutschland nach Frankreich gesendet. Nach § 4b Abs. 1 Nr. 1 BDSG gilt weiterhin deutsches Recht: Die §§ 15, 16, 28-30a BDSG sind die bestimmenden Regeln für Übermittlungen von Deutschland in andere Mitgliedsstaaten der EU.

b) Einwilligung

Für die Faktenlage zur Einwilligung gilt das oben (VI.3.b) Gesagte. Eine andere Informationsquelle als die *FlarmNet*-Seite, die speziell auf die Übermittlung der Daten hinweist, ist nicht bekannt. Es liegen keine Einwilligungen vor.

c) Gesetzliche Grundlage

Für Datenübermittlungen gilt § 29 Abs. 2 BDSG. Soll die Datenübermittlung zulässig sein, darf der Betroffene kein schutzwürdiges Interesse am Ausschluss der

Übermittlung haben und der Dritte muss ein berechtigtes Interesse an der Kenntnis der Daten darlegen können. Dritter ist der Betreiber der Server.

aa) Glaubhafte Darlegung des berechtigten Interesses

Für die glaubhafte Darlegung müsste der Serverbetreiber Dokumente vorlegen können, die sein Interesse bestätigen. Dazu gehören z.B. behördliche Bescheinigungen oder bereits angelegte Akten.[102] Dergleichen wird der Serverbetreiber wohl nicht vorweisen können.

bb) Schutzwürdiges Interesse des Betroffenen

Der Betroffene hat ein schutzwürdiges Interesse daran, dass die unzulässig erhobenen Daten nicht weiterversendet werden.

cc) Hinweispflicht

Aus §§ 29 Abs. 4 i.V.m. 28 Abs. 5 S. 3 BDSG folgt die Hinweispflicht gegenüber dem Datenempfänger, ihm die Zweckbindung der Daten bekanntzugeben.

3. Ergebnis

Das Übermitteln der Daten nach Frankreich ist unzulässig. Bußgelder können nach § 43 Abs. 2 Nr. 1 BDSG drohen. Der betroffene Pilot kann nach § 34 BDSG Auskunft über seine Daten und nach § 35 Abs. 2 S. 1 Nr. 1 BDSG ihre Löschung verlangen.

Ist ihm wegen der unzulässigen Übermittlung ein Schaden entstanden, kann er unter den Voraussetzungen des § 7 BDSG Schadensersatz einklagen.

VI. Die Daten werden unter *live.glidernet.org* veröffentlicht

1. Zivilrechtliche Ansprüche

a) Unterlassung, §§ 1004 Abs. 1 analog i.V.m. 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Wird das Persönlichkeitsrecht der Piloten durch die Veröffentlichung der Flugdaten verletzt, haben sie einen Unterlassungsanspruch gegen die Webseitenbetreiber.

aa) Verletzung eines absolut geschützten Rechtsguts

Das Recht auf Selbstdarstellung ist Teil des allgemeinen Persönlichkeitsrechts. Jedermann darf grundsätzlich selbst und allein bestimmen, ob und inwieweit andere sein Lebensbild oder bestimmte Vorgänge aus seinem Leben öffentlich darstellen dürfen.[103] Ausprägung davon ist das Recht auf informationelle Selbstbestimmung. Durch die ungefragte Veröffentlichung der identifizierbaren Flugdaten umgehen die Webseitenbetreiber diese Verfügungsrechte der Betroffenen[104]. Sie verletzen das allgemeine Persönlichkeitsrecht.

bb) Rechtswidrigkeit der Verletzung

---

[102] Ehmann in Simitis, BDSG, § 29, Rn. 224.

[103] Vgl. Fechner, Medienrecht, 4. Kap., Rn. 25.

[104] Werden die Daten der Flugzeugeigentümer angezeigt, sind auch sie Betroffene und können Ansprüche geltend machen.

Die Webseitenbetreiber könnten ein von der Rechtsordnung gebilligtes Interesse an der Veröffentlichung haben. So könnte die Veröffentlichung z.B. der allgemeinen Handlungsfreiheit oder der Meinungsfreiheit unterfallen.

Vom Schutzbereich der Meinungsfreiheit ist grundsätzlich auch die elektronische Veröffentlichung von Tatsachenbehauptungen erfasst. Die Tatsachenbehauptungen müssen der öffentlichen Meinungsbildung dienlich sein.[105] Die Veröffentlichung der Segelflugdaten steht der Behauptung gleich, dass zu einem bestimmten Zeitpunkt an einem bestimmten Ort ein bestimmtes Flugzeug unterwegs war. Dies kann zwar zur Flugsicherheit beitragen, der Beitrag zur öffentlichen Meinungsbildung ist dagegen als gering einzuschätzen. Jedenfalls überwiegt dieser Beitrag nicht das allgemeine Persönlichkeitsrecht der Piloten.

Die allgemeine Handlungsfreiheit ist durch Rechte anderer oder die verfassungsmäßige Ordnung, also durch das Grundgesetz, einfache Gesetze und andere verfassungsmäßige Rechtssetzungsakte einschränkbar, Art. 2 Abs. 1 Hs. 2 GG. Das Recht auf informationelle Selbstbestimmung ist zum einen das Recht eines Anderen und zum anderen Teil der verfassungsmäßigen Ordnung, kann die allgemeine Handlungsfreiheit folglich einschränken. Im konkreten Fall überwiegt das tatsächlich verletzte allgemeine Persönlichkeitsrecht der Piloten die allgemeine Handlungsfreiheit der Webseitenbetreiber.

Wägt man die Interessen der Webseitenbetreiber mit denen der Piloten ab, kommt man zum Schluss, dass die Verletzung des Persönlichkeitsrechts als Rahmenrecht tatsächlich rechtswidrig ist.

cc) Anspruchsgegner

Die Rechtsgutsverletzung müsste den Webseitenbetreibern adäquat kausal zurechenbar sein. In Anlehnung an die (deutsche) Unterscheidung der Diensteanbieter in den §§ 7-10 TMG kann hier festgehalten werden, dass die Webseitenbetreiber die Inhalte als eigene nutzen (§ 7 Abs. 1 TMG). Die Veröffentlichung der Daten sind ihnen vollumfänglich zuzuschreiben, ihre Verantwortung muss nicht auf irgendgeartete Prüfpflichten reduziert werden.

dd) Erstbegehungs- oder Wiederholungsgefahr

Die Gefahr der Verletzung muss konkret bevorstehen. Falls die Verletzung schon stattgefunden hat, muss für die Verwirklichung des Unterlassungsanspruchs eine Wiederholungsgefahr bestehen. Der Eingriff steht konkret bevor, wenn die Daten den Webseitenbetreibern vorliegen. Wiederholungsgefahr besteht ab der ersten Veröffentlichung der Daten.

ee) Die Piloten können Unterlassungsansprüche gegen die Webseitenbetreiber nach den vorstehenden Bedingungen geltend machen.

b) Schadensersatz, § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

aa) Verletzung des allgemeinen Persönlichkeitsrechts

Das allgemeine Persönlichkeitsrecht der Piloten ist verletzt (s.o.).

bb) Rechtswidrigkeit

---

[105] BVerfGE 90, 1, 14; BVerfGE 99, 185, 197.

Die Webseitenbetreiber können der Verletzung keine eigenen Rechte entgegenhalten.

cc) Verschulden

Sie wissen um die Veröffentlichung der Daten und wollen sie auch veröffentlichen, handeln also vorsätzlich, § 276 BGB.

dd) Kausal zurechenbarer, materieller Schaden

Inwiefern den Piloten materieller Schaden entstehen kann, hängt vom Einzelfall ab.

ee) Ergebnis: Schadensersatzansprüche sind nicht grundsätzlich ausgeschlossen.

c) Anspruch auf Geldentschädigung, § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Für den Anspruch auf Geldentschädigung müsste eine schwerwiegende Beeinträchtigung des allgemeinen Persönlichkeitsrechts vorliegen.

In der vorliegenden Fallkonstellation ist dies schwer vorstellbar.[106]

2. Bestimmungen zur Gestaltung der Webseite

Im Rahmen dieser Arbeit kann keine Überprüfung des französischen Internetrechts erfolgen. Es sei jedoch darauf hingewiesen, dass für französische Webseiten eine Impressumspflicht besteht. Die Umsetzung der E-Commerce-Richtlinie erfolgte im „Loi pour la confiance dans l'économie numérique" (LCEN). In. Art 19 Abs. 1 LCEN wird gefordert (vergleichbar dem deutschen § 5 Abs. 1 TMG), dass das Impressum leicht erkennbar, unmittelbar erreichbar und ständig verfügbar ist. [107] Ebenso müssen nach Art. 19 Abs. 1 Nr. 1-6 LCEN die Kontaktdaten der Webseitenbetreiber bereitgehalten werden.

VII. Zusammenfassung und Lösungsansätze

1. Zusammenfassung

Das Projekt Open Glider Network steht zum jetzigen Zeitpunkt nicht mit deutschem Recht in Einklang. Die Überwindung der Flarm-Codierung nach den §§ 202 a und 202 c StGB strafbar. Das betrifft den Betrieb der Bodenstationen und die Verbreitung der Software. Für die weitere Datenverarbeitung durch das OGN muss zwischen den personenbezogenen und sachbezogenen Datensätzen unterschieden werden. Für die sachbezogenen Datensätze ergeben sich keine Probleme. Sobald die Daten aber Personenbezug haben, werden sie rechtswidrig verarbeitet. Es sind keine gesetzlichen Grundlagen einschlägig und rechtswirksame Einwilligungen liegen nicht vor. Daraus folgen Löschungs-, Unterlassungs- und je nach Fall auch Schadensersatzansprüche der Betroffenen.
Außerdem sind wegen der Rechtswidrigkeit der Datenverarbeitung Bußgeldtatbestände erfüllt.

---

[106] Der BGH klassifizierte z.B. die Unterstellung oder unsachgemäße Berichterstattung zu einem Pädophilie-Vorwurf als schwere Persönlichkeitsverletzung, BGH, Urteil vom 17.12.2013, VI ZR 211/12, K&R 2014, 265 ff.

[107] Das LCEN ist abrufbar unter: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164, abgerufen am 28.01.2015, 15.23 Uhr.
Im Anhang zur Arbeit findet sich eine kurze Prüfung zum Impressum nach deutschem Recht.

Die Veröffentlichung der personenbezogenen Daten unter *live.glidernet.org* verletzt das allgemeine Persönlichkeitsrecht der Betroffenen und kann Unterlassungs- und Schadensersatzansprüche nach sich ziehen.

2. Lösungsansätze

Das Anliegen des Open Glider Networks ist grundsätzlich unterstützenswert. Die Verbesserung der Flugsicherheit kann Menschenleben retten und tragische Unglücksfälle vermeiden.

Die Strafbarkeit des Flarm-Datenempfangs ließe sich vermeiden, indem die OGN-Receiver offiziell in die Reihen der Flarm-kompatiblen Geräte aufgenommen werden würden. Die individuelle Kommunikation, die über die Verschlüsselung gesichert wird, würde dann auch die OGN-Receiver miteinschließen. Sie müssten die Zugangssicherung nicht erst umgehen, so dass die Betreiber der Stationen und die Softwareprogrammierer die Straftatbestände nicht mehr erfüllen würden.

Der Umgang mit den personenbezogenen Daten bedarf weitreichender Verbesserungen, wenn nicht alle Daten grundsätzlich anonymisiert werden sollen. Die vollständige Anonymisierung der Daten würde aber nicht nur der Idee des OGN zuwiderlaufen, sondern auch dessen Potenzial ungenutzt lassen.

Grundsätzlich muss die Möglichkeit einer datenschutzrechtlich wirksamen Einwilligung geschaffen werden. Dies könnte z.B. mit entsprechenden Eingabefenstern auf *FlarmNet* verwirklicht werden. In ihnen müsste der Nutzer ausdrücklich und ausführlich über die Datenverwendung durch das OGN informiert werden.

Dabei darf aber nicht vergessen werden, dass die Nutzung des *FlarmNet* nicht von der Einwilligung in die OGN-Datenverarbeitung abhängen darf. Es ist also auch Raum für eine Opt-Out-Option zu schaffen. Die Vorschläge des OGN, auf *FlarmNet* zu verzichten oder das eigene Flarm-Gerät stets im Stealth-Modus zu verwenden[108], genügen dem nicht.
Begrüßenswert wäre eine technische Datenvermeidungslösung: Entweder die *FlarmNet*-Datensätze oder die Flarm-Daten selbst könnten mit der Information „Keine Weiterverarbeitung durch OGN gewünscht“ gekoppelt werden. In beiden Fällen muss das OGN sicherstellen, dass die zwar empfangenen, aber von der Verarbeitung ausgeschlossenen Daten unverzüglich wieder gelöscht werden.

Den Betreibern der Webseite ist zu raten, ihre Impressumspflichten genau zu überprüfen und ihre Identität dementsprechend offen zu legen. Das wird den erforderlichen Dialog zwischen allen Beteiligten erleichtern und sicherlich zur Akzeptanz des OGN beitragen.

[108] http://wiki.glidernet.org/opt-in-opt-out, abgerufen am 28.01.2015, 16.23 Uhr.

Schlusserklärung

Ich versichere, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Anhang

I. Das Persönlichkeitsrecht der Piloten und andere verfassungsrechtlich geschützte Positionen

1. Feststellung der mittelbaren Drittwirkung der Grundrechte zwischen Privaten

Grundsätzlich sind die Grundrechte Abwehrrechte gegen staatliches Handeln. Gleichzeitig sind sie aber auch Ausdruck einer objektiven Wertordnung, die in alle Bereiche des Rechts ausstrahlt.[109] Die Wirkung der Grundrechte offenbart sich zum einen in spezialgesetzlich ausgestalteten Regelungen (z.B. dem 3. Abschnitt des BDSG), zum anderen müssen sie bei jeder Auslegung des einfachen Rechts als Maxime gelten. Diese abstrahlende Sphäre der Grundrechte wird als mittelbare Drittwirkung bezeichnet.

2. Art. 2 Abs. 1 i.V.m. 1 A bs. 1GG: das Allgemeine Persönlichkeitsrecht

Das Bedürfnis persönliche Informationen zu schützen, ist in unserer Gesellschaft fest verankert. Das Verfassungsrecht hat dieses Bedürfnis konkretisiert: das Allgemeine Persönlichkeitsrecht dient der Abgrenzung zwischen Privatem und Öffentlichem. Das Grundrecht leitet sich aus der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG und einem Menschenwürdegehalt aus Art. 1 Abs. 1 GG ab.

Für die Piloten sind die nachstehenden Fallgruppen relevant:

Das **Recht auf Privatheit** schafft dem Einzelnen einen von der Öffentlichkeit abgrenzbaren Raum, einen Rückzugsort, an dem er sich frei entfalten und zu sich selbst finden kann. Daraus ergibt sich die wegweisende Unterscheidung zwischen der grundsätzlich unberührbaren Intimsphäre, der einschränkbaren Privatsphäre und der öffentlich wahrnehmbaren Sozialsphäre. Das technische Verfolgen einer Flugzeugbewegung kann zumindest die Privat- und Sozialsphäre der Piloten berühren. Vergleichbar mit einer altertümlichen Observierung oder dem modernen GPS-Tracking können durch die virtuellen Spuren Rückschlüsse auf das Verhalten der Piloten gezogen werden, obwohl sie selbst sich fernab der Öffentlichkeit glauben.

Das **Recht auf informationelle Selbstbestimmung** gibt jedem, also auch den Piloten, das Recht, selbst über die Erhebung, Verarbeitung und Speicherung seiner Daten zu verfügen. Die personenbezogenen Daten sind unabhängig von ihrer Thematik geschützt, denn in den Zeiten der automatisierten Datenverarbeitung kann es kein belangloses Datum mehr geben.[110]

Das Abgreifen der Flugdaten durch das OGN und die anschließende Verarbeitung und Visualisierung ist jedenfalls ein datenverarbeitender Vorgang. Sind die Daten bestimmt oder bestimmbar personenbezogen, ist dieser Vorgang nur erlaubt, wenn die betroffenen Piloten eingewilligt haben oder eine gesetzliche Grundlage vorliegt.

Das **IT-Grundrecht** schützt informationstechnische Systeme, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder ein aussagekräftiges Persönlichkeitsbild zu erhalten.[111] Das System muss als eigenes genutzt werden, wobei es

---

[109] Lüth-Urteil, BVerfGE 7, 198

[110] Volkszählung-Urteil, BVerfGE 65, 1.

[111] Online-Durchsuchung, BVerfGE 120, 274.

nicht auf die rechtliche Zuordnung zu einer Person aufkommt, sondern auf die Widmung durch den Nutzer. Verletzt ist dieses Recht, wenn die Integrität des Systems angetastet wird, indem so auf das System zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.[112] Es ist zu fragen, ob das Flarm-System überhaupt ein IT-System i.S.d. IT-Grundrechts ist.

Das Flarm-Gerät und die dazugehörige Software stellt unzweifelhaft ein informationstechnisches System dar. Der Pilot nutzt es auch regelmäßig als eigenes. Dass der Pilot dem Flarm-System allerdings wesentliche Teile seiner Lebensgestaltung anvertraut und dem System Daten einspeist, die zu einem aussagekräftigen Persönlichkeitsbild führen können, ist zunächst fragwürdig.

Der allergrößte Teil der Daten sind flugbezogene Daten. Damit haben sie nur einen Sachbezug, noch nicht aber Personenbezug.[113]

Das Flarm-System selbst bietet die Möglichkeit, Flugdaten in einem nicht-flüchtigen Speicher zu konservieren. Je nach Aufzeichnungsintervall (1-4 Sekunden) sind 20-40 Stunden Flug speicherbar. Über ein spezielles Programm[114] können zusätzlich auch Piloten- und Flugzeugdaten konfiguriert werden.[115] Die Flugdaten werden automatisch überschrieben, wenn der Speicherplatz voll ist. Die Daten können entweder mit entsprechender Software[116] oder im Falle eines Unfalls von Flarm Technology ausgelesen werden.[117] Der Pilot kann seinen Namen mit diesen Daten verknüpfen. Die Informationen insgesamt liegen dann als IGC-Datei vor.[118]

Das den Bewegungsprofilen immanente Risiko ist also schon im Flarm-System selbst angelegt.

Hat der Pilot seinen Namen in der IGC-Datei im Flarm-Gerät hinterlegt, so sind diese Daten eindeutig ihm eindeutig zuzuordnen. Auch in anderen Fällen sind die Flarm-Daten als persönliche Daten erkennbar, etwa wenn zur Rekonstruktion eines Unfallhergangs die Daten ausgelesen werden. Ergo ist Flarm ein grundrechtlich geschütztes IT-System.

3. Art. 10 Abs. 1 GG: das Fernmeldegeheimnis

Das Fernmeldegeheimnis ist lex specialis zu den allgemeineren Vertraulichkeitsrechten aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Das Telekommunikationsgeheimnis schützt jede unkörperliche Informationsvermittlung, die mittels Fernmeldetechnik übertragen wird.[119] Auch geschützt sind die Umstände der Kommunikation. Es ist einerlei, auf welchem

---

[112] Vgl. zum Schutzbereich auch Brink in Wolff/ Brink, Datenschutzrecht, Verfassungsrecht, XII: Rn. 146 ff. und Schmidl in Hauschka, Corporate Compliance, § 29, Rn. 318 ff.

[113] Flarm versteht sich auch als Kommunikationskanal, Ernst: „FLARM- Was zeigt die Zukunft?“ in segelfliegen 5/2013, 41. Gemeint ist damit allerdings eine reine Maschine-zu-Maschine-Kommunikation. Die Schnittstellen der Flarm-Geräte (u.a. USB (im PowerFlarm), RS-232-Schnittstellen).

[114] FlarmSoft PC-Applikation.

[115] http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.32 Uhr.

[116] Die Daten liegen im FAI/ IGC-Flugdatenformat vor, http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.33 Uhr.

[117] http://flarm.de/support/faq/index.html, abgerufen am 13.01.2015, 16.32 Uhr.

[118] IGC steht für die International Gliding Commission.

[119] BVerfGE 130, 151, 179, NJW 2012, 1419, 1421- „Zuordnung dynamischer IP-Adressen“; BVerfGE 125, 260, 309, NJW 2010, 833, 835 - „Vorratsdatenspeicherung“.

speziellen Übermittlungsweg die Information übertragen wird.[120] Der Schutz reicht vom Aussenden der Nachricht bis zum Abschluss des Übermittlungsvorgangs. Geschützt ist die Vertraulichkeit des Nachrichtenaustauschs zwischen Privaten, also die Individualkommunikation.[121].

Damit erscheint zunächst das Aussenden der Flarm-Signale über die öffentliche Frequenz (an eine unbestimmte Anzahl von Empfängern) als nicht unter den Schutzbereich fallend. Der Begriff Individualkommunikation ist aber weiter zu konkretisieren: zugangsgesicherte Kommunikationsformen unterfallen stets Art. 10 Abs. 1 GG.[122] Die Flarm-Signale werden verschlüsselt ausgesendet. Die Verschlüsselung dient als Sicherung, um den Empfängerkreis bestimmen zu können. Die Aussendung von Flarm-Signalen über die öffentliche Frequenz ist deswegen trotzdem als Individualkommunikation zu werten und unterfällt dem Schutzbereich von Art. 10 Abs. 1 GG.

Eingriffe in das Fernmeldegeheimnis können durch formelle Gesetze rechtfertigt sein, Art. 10 Abs. 2 GG. Die einfachgesetzliche Ausgestaltung des Fernmeldegeheimnisses erfolgte im TKG.

4. Wirtschaftsgrundrechte

Sofern die Segelflugzeuge kommerziell betrieben werden, kommen bei Beeinträchtigungen durch das OGN die Wirtschaftsgrundrechte aus Art. 12 und 14 GG in Betracht (Berufs- und Eigentumsfreiheit).

II. Einfachgesetzliche Regelungen zum Schutz der Persönlichkeit, insbesondere das Datenschutzrecht

1. Das Datenschutzrecht

Das deutsche Datenschutzrecht gliedert sich in das allgemeine Datenschutzrecht, das BDSG, und die bereichsspezifischen Regelungen auf. Die bereichsspezifischen Regelungen gehen auf die Besonderheiten bestimmter Datenverarbeitungen ein und sind dementsprechend in TKG, TMG und RStV zu finden.

Um die Anwendungsräume der einzelnen Gesetze gegeneinander abzugrenzen, bietet sich das 3-Schichten-Modell an: Hierbei wird ein inhaltlich zusammengehörender Gesamtvorgang in die einzelnen Datenübertragungsarten unterteilt: für die Übertragungsschicht gilt das TKG, für die Interaktionsschicht können je nach Ausgestaltung TKG, TMG oder RStV einschlägig sein, für die Inhaltsschicht gelten dann die allgemeingesetzlichen Bestimmungen aus BDSG, BGB, UrhG, etc.

2. Grundlagen

Im Datenschutzrecht gelten einige allgemeine Prinzipien, die den Zweck und das Ziel des Datenschutzes klar skizzieren.
Das **Verbot mit Erlaubnisvorbehalt,** § 4 Abs. 1 BDSG, soll dem Einzelnen bestmögliche Kontrolle über seine Daten bieten. Aus derselben Erwägung ergibt sich auch das Gebot der **Direkterhebung**: personenbezogene Daten sollen direkt beim Betroffenen erhoben werden. Zudem unterliegt jede Datenverarbeitung dem **Zweckbindungsgrundsatz**. Rechtmäßig erhobene Daten dürfen nur für die Zwecke verwendet werden, die bei oder vor der Erhebung

[120] BVerfGE 115, 166, 183, NJW 2006, 976- „Ermittlung von Verbindungsdaten“.

[121] BVerfGE 100, 313, 358.

[122] Durner in Maunz/ Dürig, GG, Art. 10, Rn. 94.

bekannt gegeben wurden. Jede Zweckänderung bedarf einer erneuten Einwilligung des Betroffenen. Zudem muss jede Datenerhebung für den Zweck **erforderlich** sein.

Um den unnötigen Umgang mit personenbezogenen Daten zu vermeiden, gilt das Gebot der **Anonymisierung und Pseudonymisierung**. Fehlt den Daten von Anfang an der Personenbezug unterliegt der Umgang nicht mehr den strengen Anforderungen des Datenschutzrechts. Diese beiden Werkzeuge dienen **der Datenvermeidung und der Datensparsamkeit**, § 3a BDSG.

Noch zu erwähnen ist die Verpflichtung, die **Datensicherheit** durch technische und organisatorische Maßnahmen zu gewährleisten, § 9 BDSG mit Anlage.

Um die Rechte des Betroffenen (§ 6 BDSG) zu stärken gilt ein allgemeiner Grundsatz der **Transparenz**.

III. Prüfung § 5 TMG

Geschäftsmäßig angebotene Telemedien bedürfen einer Anbieterkennzeichnung (Impressum), § 5 Abs. 1 TMG.

Fraglich ist, ob die Webseite live.glidernet.org ein geschäftsmäßig angebotenes Telemedium ist. Im Sinne des TMG ist für die Geschäftsmäßigkeit eines Angebots keine Gewinnerzielungsabsicht notwendig. Es genügt eine „nachhaltige Tätigkeit“.[123]

Zudem muss der Dienst in der Regel gegen Entgelt angeboten werden. Ausnahmen und Einzelfälle in denen gleichartige Dienste ohne Entgelt angeboten werden, schließen die Anwendung des § 5 TMG nicht aus.[124]

Die Webseite ist auf eine dauerhafte, also nachhaltige Tätigkeit ausgelegt. Vergleichbare Angebote werden in der Regel gegen Entgelt erbracht[125], so dass es nicht darauf ankommt, ob die Darstellung der Flugrouten auch entgeltlich erfolgt.

Die Webseite unterfällt der Impressumspflicht. Der Inhalt des Impressums ist dem § 5 Abs. 1 Nr. 1-7 TMG zu entnehmen. Hervorzuheben ist aber, dass die Anbieter ihre Namen und Kontaktmöglichkeiten bereithalten müssen. Die Voraussetzungen für die Rechtmäßigkeit ist, dass sie dies leicht erkennbar, unmittelbar erreichbar und ständig verfügbar tun.

Leicht erkennbar bedeutet, dass das Impressum, oder der Link dorthin, deutlich als solches gekennzeichnet sein muss. Unmittelbar erreichbar ist das Impressum, wenn man von jeder Unterseite einer Webseite mit zwei Klicks dorthin gelangen kann. Die ständige Verfügbarkeit bezieht sich auf die tatsächliche Wahrnehmbarkeit des Impressums. Ziel ist, den Anbieter problemlos identifizieren zu können.[126]

Auf der Webseite findet sich kein Link, der deutlich als Impressum gekennzeichnet ist. Einzig in Betracht kommen könnte der kleine Schriftzug am oberen rechten Bildschirmrand: „Powered by GliderNet.Org“. Der Link verweist auf die Wiki-Seite des OGN. Dort sind weder die Namen der Verantwortlichen noch direkte Kontaktdaten bereitgehalten.

---

[123] Brönneke in Roßnagel, Recht der Telemediendenste, § 5 TMG, Rn. 40.

[124] Brönneke in Roßnagel, Recht der Telemediendenste, § 5 TMG, Rn. 42 ff.

[125] z.B. von flightradar24.

[126] Vgl. Brönneke in Roßnagel, Recht der Telemediendienste, § 5 TMG, Rn. 78 ff.

Würde die Webseite von Deutschland aus betrieben, würden die Verantwortlichen die Impressumspflicht verletzen und sich den drohenden Bußgeldern aus § 16 Abs. 2 TMG aussetzen.

Es könnten deswegen Unterlassungsklagen aus dem UWG oder Schadensersatzklagen nach den §§ 280 Abs. 1 oder 823 Abs. 2 BGB angestrengt werden.[127]

[127] Rauschhofer, MMR-Aktuell 2010, 302790; Micklitz/ Schirmbacher in: Spindler/Schuster, § 5 TMG Rn. 13a.