

Dr. Wolfram Viefhues (Hrsg.)

Elektronischer Rechtsverkehr

Künstliche Intelligenz auf dem Vormarsch

eBroschüre

Elektronischer Rechtsverkehr

Künstliche Intelligenz auf dem Vormarsch

Hrsg. von

Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

Zitiervorschlag:

Viefhues, Elektronischer Rechtsverkehr Ausgabe 5/2019, Rn 1

Copyright 2019 by Deutscher Anwaltverlag, Bonn

Künstliche Intelligenz auf dem Vormarsch

Inhalt

	Rdn		Rdn
A. Einleitung	1	3. Tätigkeit im Rahmen einer Inkassoli- zenz.	41
B. Anwalt muss beA bedienen können	5	II. Legal Tech in Großkanzleien	42
I. Passive Nutzungspflicht seit 3.9.2018. . .	6	III. Weitere Einsatzmöglichkeiten?	44
II. Elektronische Empfangsbekennnisse au- tomatisch erkennen.	8	D. Künstliche Intelligenz im Kampf gegen Kinderpornographie	46
III. Empfangsbekennnis.	15	I. Einleitung	46
1. Anzeigen	15	II. Ausgangssituation.	47
2. Ablehnung erstellen	17	III. Ein neuer Weg.	54
3. Abgabe erstellen	18	1. Rechtliche Fragen	56
IV. Hilfsmittel für den schnellen Überblick: Etiketten	22	2. Technische Herausforderung	58
V. Eingänge ohne eEB	27	3. Aktueller Zwischenstand	60
VI. Wann beginnt die aktive Nutzungspflicht?	29	4. Nächste Schritte.	61
VII. Was erwartet Anwaltskanzleien ab 2020?	30	E. Künstliche Intelligenz in der JVA	63
VIII. Neuigkeiten vom EDV-Gerichtstag zum beA.	32	F. KI und die Gerichte	67
IX. Schwachstelle Drucker, Fax und Multi- funktionsgeräte	33	G. EDVGT-Nachlese	75
X. Kein Backup – Kein Mitleid!	35	H. E-Government-Monitor 2019	80
C. Legal Tech in Deutschland	38	I. Monitor „Digitale Verwaltung“ des Nationalen Normenkontrollrats	82
I. Legal-Tech-Anbieter.	38		
1. Ausnutzung des „rationalen Desinte- resses“	39		
2. Automatisierung	40		

A. Einleitung

Verfasser: Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D.

Natürlich hat auch in dieser Ausgabe wieder das beA seinen wichtigen Platz. Diesmal ist der Beitrag von **1**
Ilona Cosack überschrieben mit der dringenden Aufforderung „Anwalt muss beA bedienen können“.

Im Mittelpunkt steht aber diesmal die „Künstliche Intelligenz“, die auch in Justiz in Anwaltschaft – dort vor allem unter dem Begriff „Legal Tech“ – immer größere Bedeutung gewinnt.

Isabelle Désirée Biallaß gibt einen Überblick über Legal Tech in Deutschland. *Dieter Kesper* erläutert **2**
detailliert das vom Justizministerium des Landes Nordrhein-Westfalen eingeleitete Projekt mit dem Ziel, die Strafverfolgung von Kinderpornographie künftig mit Analysemethoden künstlicher Intelligenz zu unterstützen, über das wir bereits in der letzten Ausgabe kurz berichtet hatten. Weiter wird ebenfalls vom Ministerium der Justiz des Landes NRW der Einsatz Künstlicher Intelligenz (KI) im Justizvollzug geprüft; auch darüber wird kurz informiert.

Durchaus nachdenklich machen sollte uns der Beitrag „KI und die Gerichte“, in dem *Ralf Köbler* anschaulich **3**
zeigt, wie weit künstliche Intelligenz und dadurch entwickelte Algorithmen bereits unser Alltagsleben beeinflussen.

Die Ausgabe schließen kurze Berichte vom diesjährigen EDV-Gerichtstag, den E-Government-Monitor **4**
2019 und den Monitor „Digitale Verwaltung“ des Nationalen Normenkontrollrats ab.

Wir wünschen Ihnen eine angenehme und nutzbringende Lektüre unserer e-Broschüre.

B. Anwalt muss beA bedienen können

Verfasserin: Ilona Cosack

Fachbuchautorin und Inhaberin der ABC AnwaltsBeratung Cosack, Fachberatung für Rechtsanwälte und Notare

Rechtsanwälte können sich nicht darauf berufen, dass sie wegen Problemen mit der beA-Bedienung nicht **5**
in der Lage sind, gerichtliche Dokumente zur Kenntnis zu nehmen. Hierzu lautet der Leitsatz des LAG Schleswig-Holstein¹ am 19.9.2019:

*„Ein Rechtsanwalt ist als Inhaber eines beA nicht nur verpflichtet, die technischen Einrichtungen zum Empfang von Zustellungen und Mitteilungen über das beA lediglich vorzuhalten, **vielmehr ist der Rechtsanwalt zugleich verpflichtet, sich die Kenntnisse zur Nutzung dieser technischen Einrichtungen anzueignen**, damit er die über beA zugestellten Dokumente auch gemäß § 31a Abs. 6 BRAO zur Kenntnis nehmen kann. Die Gerichte sind nicht verpflichtet, den Rechtsanwälten Handlungsanweisungen zum Öffnen der über beA zugesandten Dokumente zu erteilen.“*

¹ Beschluss des LAG Schleswig-Holstein vom 19.9.2019 – 5 Ta 94/19.

I. Passive Nutzungspflicht seit 3.9.2018

Trotz der seit über einem Jahr bestehenden passiven Nutzungspflicht² haben sich immer noch nicht alle Rechtsanwälte im beA registriert und sind daher außerstande, Nachrichten in ihrem beA zur Kenntnis zu nehmen. Allein unter der PLZ der Autorin haben 10 % der dort zugelassenen Anwälte ihr beA bislang ignoriert. Da neben den Gerichten auch alle Anwälte das beA für Zustellungen nach § 174 Abs. 3 ZPO nutzen können, kann diese Ignoranz zu einem Haftpflichtfall für den Anwalt führen, für den keine Berufshaftpflichtversicherung Deckungsschutz gewährt.

6

Achtung:

„Es gibt Sachen, die muss man mitmachen, etwa das beA. Das geht nur in der ganzen Branche“.³

7

II. Elektronische Empfangsbekanntnisse automatisch erkennen

Gerichte beklagen, dass Rechtsanwälte elektronische Empfangsbekanntnisse (eEB) nicht zur Kenntnis nehmen und erst auf Nachfrage feststellen, dass die Nachricht mit eEB eingegangen ist. Hier kann man im beA Abhilfe schaffen:

8

Stellen Sie in der **Nachrichtenübersicht** unter dem Bereich

9

- **Sonstige Funktionen das**
- **Hervorheben von Nachrichten**

ein.

Achten Sie darauf, dass unterhalb des Postfachs der Ordner **Posteingang** angezeigt wird. Klicken Sie auf das Feld + **Neue Hervorhebung** und vergeben Sie einen Namen, z.B. eEB.

10

Wählen Sie eine Farbe aus. Da mit dieser Farbe die Nachrichten hinterlegt werden, hat sich z.B. die Farbe „Golden“ bewährt, da dies in etwa der Markierung mit einem gelben Textmarker entspricht.

Stellen Sie mit + **Filter hinzufügen** beim Filterkriterium „**Nachrichten, die ein Empfangsbekanntnis erfordern**“, Operator „**gleich**“, Wert „**Ja**“ ein und bestätigen mit Klick auf das **Häkchen**. Schließen Sie die Speicherung mit „**Speichern und zurück**“ ab.

11

Danach werden von beA alle Nachrichten mit elektronischem Empfangsbekanntnis (auch die bereits empfangenen Nachrichten), die im Ordner Posteingang stehen, automatisch „**golden**“ markiert. So ist direkt ersichtlich, dass diese Nachricht ein eEB enthält (die erste und die letzte Nachricht in unserem Beispiel).

12

<input type="checkbox"/>	Löschdatum	Etiketten
<input type="checkbox"/>	31.10.2019	■ ■
<input type="checkbox"/>	31.10.2019	■
<input type="checkbox"/>	07.11.2019	
<input type="checkbox"/>	07.11.2019	■ ■

13

² § 31a Abs. 6 BRAO.

³ Rechtsanwalt Professor Dr. Stephan Ory, Vorsitzender des EDV-Gerichtstages in: Cosack, Digitalisierung erfolgreich umsetzen – Ein Leitfaden für jede Anwaltskanzlei.

Beim Öffnen der Nachricht findet man dann den Hinweis, dass ein Empfangsbekanntnis angefordert wurde: 14

Empfangsbekanntnis angefordert

Anzeigen
Abgabe erstellen
Ablehnung erstellen

III. Empfangsbekanntnis

1. Anzeigen 15

Mit Klick auf „Anzeigen“ wird der Strukturdatensatz entschlüsselt und es öffnet sich ein Viewer, der für den Menschen das eEB lesbar anzeigt. Prüfen Sie, ob die im Feld aufgeführten Dokumente auch tatsächlich angehängt sind:

ist mir eine Aufforderung zur Abgabe des Empfangsbekanntnisses für die Entgegennahme des/der elektronischen Dokumente(s) 16

Typ	Dokumentendatum	Anzeigename
Beschluss		Uebersendg_Beschluss
Beschluss		BESCHLUSS Fristverlängerung

übermittelt worden

2. Ablehnung erstellen 17

Sollten die Dokumente unvollständig sein oder ein anderer Ablehnungsgrund vorliegen, kann die Abgabe des eEB abgelehnt werden:

Klicken Sie auf „Ablehnung erstellen“.

Ablehnungsgrund: * Bitte auswählen

Erläuterung: *

Bitte auswählen

Inhalt der Sendung unklar oder unvollständig

Zertifikatsprüfung fehlgeschlagen

Zustellungsempfänger nicht am Verfahren beteiligt

Wählen Sie einen der drei vorgegebenen Ablehnungsgründe aus. Danach müssen Sie das als Pflichtfeld (*) ausgestaltete Feld „Erläuterung“ ausfüllen.

Erläuterung: *

Strukturdatensatz signieren
Strukturdatensatz-Signatur entfernen

Wenn der Mitarbeiter die Ablehnung des eEB versenden soll, muss zwingend der Rechtsanwalt mit einem Klick auf „**Strukturdatensatz signieren**“ die elektronische Signatur (PIN-Eingabe) vornehmen. Versendet der Rechtsanwalt die Ablehnung des eEB selbst, so kann er dies nach § 130a Abs. 3 ZPO auch ohne eine qualifizierte elektronische Signatur tun und direkt auf „**Senden**“ klicken.

3. Abgabe erstellen

Der Rechtsanwalt entscheidet, wann er das Dokument zur Kenntnis nimmt. Nach § 53 BRAO muss er für eine Vertretung sorgen: 18

1. wenn er länger als eine Woche daran gehindert ist, seinen Beruf auszuüben;
2. wenn er sich länger als eine Woche von seiner Kanzlei entfernen will.

Die weit verbreitete Übung, das eEB am Tage des Eingangs in der Kanzlei als empfangen entgegenzunehmen, obwohl der Anwalt den Eingang noch nicht zur Kenntnis genommen hat, ist also auch im elektronischen Rechtsverkehr nicht erforderlich.

Klicken Sie auf „Abgabe erstellen“. Beim Feld „**Datum der Bestätigung**“ klicken Sie auf das Kalenderblatt, es öffnet sich eine Monatsübersicht: 19

The image shows a web form with three input fields: "Datum der Bestätigung: *", "Betreff: *", and "Aktenzeichen Sender:". A calendar pop-up is open over the first field, displaying the month of October 2019. The calendar grid shows days from 1 to 31, with the 28th highlighted in blue, indicating it is the selected date.

Das System schlägt das Tagesdatum vor, es kann aber auch ein Datum in der Vergangenheit ausgewählt werden.

Praxistipp:

Geben Sie das eEB immer dann ab, wenn Sie das Dokument zur Kenntnis genommen haben. 20

Auch hier gilt: Wenn der Mitarbeiter das abgegebene eEB versenden soll, muss zwingend der Rechtsanwalt mit einem Klick auf „**Strukturdatensatz signieren**“ die elektronische Signatur vornehmen. Ver-

sendet der Rechtsanwalt das abgegebene eEB selbst, so kann er dies nach § 130a Abs. 3 ZPO auch ohne eine qualifizierte elektronische Signatur tun und direkt auf „**Senden**“ klicken.

Achten Sie darauf, dass der Mitarbeiter zum Versenden zwingend das **Recht Nr. 14 EBs versenden** bzw. ggf. das **Recht Nr. 17 EBs versenden (persönlich/vertrauliche Nachrichten)** benötigt. Prüfen Sie diese Voraussetzungen in den **>Einstellungen >Benutzerverwaltung >Mitarbeitername auswählen >Rechte-Zuordnungen eines Benutzers verwalten** und vergeben Sie diese Rechte.

21

IV. Hilfsmittel für den schnellen Überblick: Etiketten

Leider sieht man der eingegangenen Nachricht nicht an, dass das eEB abgegeben wurde, denn diese befindet sich im Ordner „**Gesendet**“. Für einen schnellen Überblick sind **Etiketten** hilfreich. Mit diesen können Nachrichten markiert werden, so dass man sofort sieht, ob das eEB abgegeben wurde:

22



- Etiketten können an mehreren Stellen im beA verwaltet oder vergeben werden.
- Zunächst muss die Etiketete erstellt werden. Das kann in der **Nachrichtenübersicht** oder unter **>Einstellungen >Postfachverwaltung >Etiketten verwalten** erfolgen.
- Klicken Sie auf + **Neues Etikett** und wählen Sie das Postfach aus.
- Geben Sie danach die **Bezeichnung** ein, z.B. eEB abgegeben. Wählen Sie dann eine Farbe (z.B. „**Purpur**“) aus.

Dann erkennen Sie in der Nachrichtenübersicht auf einen Blick:

<input type="checkbox"/>	Löschdatum	Etiketten
<input type="checkbox"/>	31.10.2019	■ ■
<input type="checkbox"/>	31.10.2019	■
<input type="checkbox"/>	07.11.2019	
<input type="checkbox"/>	07.11.2019	■ ■

- 1.) Die Nachricht ist mit eEB gekommen.
- 2.) Das eEB wurde abgegeben und
- 3.) die Nachricht wurde exportiert.
- 4.) Die Nachricht wird vom System am 31.10.2019 automatisch in den Papierkorb verschoben.

beA unterscheidet zwischen „**Löschdatum**“ (automatisches Verschieben in den Papierkorb) und „**Endgültigem Löschdatum**“ (endgültigem Löschen aus beA).

23

Nur im Ordner „**Papierkorb**“ steht das „**Endgültige Löschdatum**“ automatisch am Ende der Zeile. Wenn Sie sich in der Nachrichtenübersicht beim Ordner „**Posteingang**“ und im Ordner „**Gesendet**“ das Löschdatum wie in unserem obigen Beispiel anzeigen lassen wollen, gehen Sie wie folgt vor:

- Klicken Sie in der **Nachrichtenübersicht** auf **>Sonstige Funktionen >Spaltenauswahl**, links **>Alle Spalten**, 24
- dort **>Löschdatum** (Achtung: nicht „Endgültiges Löschdatum“ wählen) anklicken
- und mit dem Rechtspfeil in die **>aktuelle Auswahl** schieben.

Danach steht das Löschdatum am Ende der Zeile.

Wollen Sie das Löschdatum an den Anfang der Nachrichtenübersicht stellen, so klicken Sie es an und schieben es mit den Doppelpfeiltasten nach oben. Ebenso kann man mit den Etiketten, die standardmäßig nicht in der Nachrichtenübersicht enthalten sind, verfahren.

Praxistipp:

Drucken allein genügt nicht!

Nur mit der Funktion „**Exportieren**“, die man **nur in der geöffneten Nachricht** unter „**Sonstige Funktionen**“ findet, wird der vollständige Nachweis elektronisch gesichert. 25

Achtung:

Derzeit können sämtliche Anwaltssoftwarehersteller mit der beA-Schnittstelle diese Aufgabe noch nicht vollständig erfüllen, da der beA-Schnittstelle wesentliche Funktionen in dieser Hinsicht fehlen. Die Version 2.2 enthielt – im Gegensatz zur Ankündigung der BRAK – diese Funktionen noch nicht und auch in der Version 2.3.2, die am 15.10.2019 online ging, steht dieses Update noch nicht zur Verfügung. Allen Nutzern von Anwaltssoftware sei daher geraten, nur in der Webanwendung Nachrichten zu exportieren. 26

V. Eingänge ohne eEB

Zu beachten ist, dass für Eingänge, die ohne eEB verschickt werden, das Datum, des Eingangs im beA maßgeblich ist. Wann die Nachricht geöffnet oder gelesen wird, ist unbeachtlich. 27

Praxistipp:

Beantragen Sie Fristverlängerung, wenn die Nachricht nicht innerhalb der vorgegebenen Schriftsatzfrist erledigt werden kann. Anders als bei einem eEB enthalten die ohne eEB verschickten Nachrichten keine Notfristen. 28

VI. Wann beginnt die aktive Nutzungspflicht?

Jedes Bundesland kann selbst entscheiden, ob es die aktive Nutzungspflicht⁴ durch Rechtsverordnung auf den 1.1.2020 oder 1.1.2021 vorzieht. Derzeit wird diskutiert, ob Schleswig-Holstein⁵ im Bereich der Arbeitsgerichtsbarkeit von dieser Möglichkeit Gebrauch macht. 29

⁴ ERVGerFöG vom 10.10.2013, Artikel 24, Absatz 2.

⁵ <https://www.lto.de/recht/justiz/j/elektronischer-rechtsverkehr-schleswig-holstein-nutzungspflicht-2020-rechtsanwaelte-behoerden/>.

Jeder Nutzer ist also gehalten, vor dem Versand zu prüfen,⁶ ob ein Bundesland und ggf. in welchem Bereich, bereits die aktive Nutzungspflicht eingeführt hat.

VII. Was erwartet Anwaltskanzleien ab 2020?

Das beA wird ab Januar 2020 einen neuen Betreiber bekommen. Die Firma **Westernacher Solutions** wird gemeinsam mit der **rockenstein AG** als Internet-Service-Provider die Weiterentwicklung, den Betrieb und den Support des besonderen elektronischen Anwaltspostfachs übernehmen. 30

Westernacher Solutions hat bereits vielfältige Erfahrungen⁷ mit dem elektronischen Rechtsverkehr. Die Erwartung, dass beA, vor allem was die Performance⁸ anbelangt, stabiler werden wird, ist hoch. Mit zunehmender Nutzung des beA ist es unzumutbar, dass permanente Fehlermeldungen die Arbeit mit beA beeinträchtigen.



Praxistipp:

Auch wenn es lästig ist und alle viel Arbeit haben: Melden Sie Fehler an die bis Ende des Jahres 2019 noch geltende E-Mail-Adresse: bea-servicedesk@atos.net. Nur dann ist gewährleistet, dass allen Fehlern nachgegangen werden kann. 31

⁶ Z.B. auf <https://bea-abc.de/lexikon/landesverordnung/>.

⁷ Ausführlich dazu siehe *Cosack*, Blogbeitrag vom 2.9.2019: <https://bea-abc.de/blog/quo-vadis-bea/>.

⁸ <https://bea.brak.de/category/aktuelle-meldungen/>.

VIII. Neuigkeiten vom EDV-Gerichtstag zum beA

Auch beim 28. EDV-Gerichtstag im September 2019 kam das beA immer wieder zur Sprache. Während die Justiz bis Ende 2025 die Baustellen am Wegesrand, die noch auf dem Weg zur digitalen Akte „Justiz 2026“ liegen, beseitigen muss, dämpfte Rechtsanwalt *Christoph Sandkühler*, Westfälische Notarkammer und Vorstandsmitglied des EDV-Gerichtstages, beim vielbesuchten Arbeitskreis⁹ für beA, beN und beBPo die Erwartungen.

32

Nach der Übernahme von Westernacher Solutions und rockenstein AG zum Jahresanfang 2020 könne er nichts Verbindliches sagen, aber nach der Systemstabilität würde eine Weiterentwicklung „betrachtet werden“: Im Bereich E2E-Verschlüsselung, Open Source, mobiler Einsatz, Usability und der Einrichtung von optionalen Kanzleipostfächern.

IX. Schwachstelle Drucker, Fax und Multifunktionsgeräte

Bereits vor dem Bekanntwerden des Eindringens des Trojaners „Emotet“ beim Berliner Kammergericht¹⁰ am 25.9.2019 wies der Sicherheitsexperte *Holger Junker* vom Bundesamt für Sicherheit in der Informationstechnologie (BSI), eindrucksvoll beim EDV-Gerichtstag darauf hin, dass alle diese Geräte ein Einfallstor seien, um ganze Unternehmensnetzwerke anzugreifen. Man solle die Firmware-Version überprüfen, häufig würden auch neue Geräte mit einer alten Version ausgeliefert. Auch Drucker hätten eine Festplatte, die angreifbar ist, wenn ein Mitarbeiter, z.B. über sein Handy, per WLAN etwas ausdruckt. Generell solle man die Anbindungen an das Internet nur mit einer Virtual Privat Network-Verbindung (VPN) realisieren. Auch die lokale Bedienung solle nur mit PIN erfolgen.

33

Praxistipp:

Sensibilisieren Sie alle Personen, die in Ihrer Kanzlei mit dem Computer arbeiten. Stellen Sie klare Regeln für den Umgang mit beA, mit E-Mails und allen Anhängen sowie der Nutzung von fremden Datenträgern (z.B. USB-Sticks) in Ihrer Kanzlei auf. beA selbst macht keine Virenprüfung. Diese kann erst dann erfolgen, wenn die Nachricht exportiert wurde und sich auf dem Kanzleirechner befindet. Oftmals ist nicht auf den ersten Blick erkennbar, dass der „bekannte Absender“ gehackt wurde und man sich beim Öffnen einen Trojaner einfängt.

34

X. Kein Backup – Kein Mitleid!

beA ist kein Archiv, daher sind alle empfangenen und gesendeten Nachrichten auf den eigenen Server zu exportieren. Nur mit dem unter Rdn 25 beschriebenen Praxistipp ist gewährleistet, dass alle notwendigen Dateien gesichert werden.

35

Überprüfen Sie Ihr Sicherheitskonzept.

36

- Wären Sie in der Lage, im Fall des Datenverlustes eine Rücksicherung vorzunehmen, damit Ihre Daten erhalten bleiben?

Je nach Art der Datensicherung kann auch das Backup von einem Virus oder Trojaner befallen werden, so dass dieses dann wertlos ist.

Auch wenn mittlerweile manche Berufshaftpflichtversicherung eine Cyberversicherung anbietet: Diesen GAU sollten Sie Ihrer Kanzlei ersparen, denn er blockiert Ihre Kanzlei womöglich eine lange Zeit. Stellen

37

⁹ Ausführlich dazu *Cosack* am 15.10.2019 auf: <https://www.legal-tech.de/edv-gerichtstag-2019/>.

¹⁰ <https://www.tagesspiegel.de/berlin/trojaner-angriff-berliner-kammergericht-nicht-vor-2020-wieder-am-netz/25146868.html>.

Sie sich vor, die ganze Kanzlei hätte über einen längeren Zeitraum nicht gearbeitet und müsste jetzt alles von vorne und doppelt bearbeiten, alle Diktate und sonstigen Arbeiten wären weg, so, als ob diese Zeit nie gewesen wäre. Treffen Sie Vorkehrungen, dass Ihnen ein solcher Albtraum erspart bleibt!

C. Legal Tech in Deutschland

Verfasserin: Isabelle Désirée Biallaß

Richterin am Amtsgericht, Essen

I. Legal-Tech-Anbieter

In den letzten Jahren nahmen auch auf dem deutschen Markt immer mehr Legal-Tech-Anbieter ihre Tätigkeit auf. Sie ermöglichen eine automatisierte Prüfung von Ansprüchen und bieten den Verbrauchern eine Alternative zur klassischen Rechtsberatung. Während sie sich zu Beginn vor allem auf die Geltendmachung von Ansprüchen nach der EU-Fluggastrechteverordnung spezialisiert hatten, existieren nunmehr auch Anbieter für zahlreiche weitere Rechtsgebiete. **38**

1. Ausnutzung des „rationalen Desinteresses“

Die Legal-Tech-Anbieter machen sich das so genannte „rationale Desinteresse“ der Bürger zunutze. Niedrige Ansprüche werden von den meisten Geschädigten nicht verfolgt. Nach einer Umfrage des Alvensbach-Instituts für den Roland Rechtsreport 2014 beträgt der durchschnittliche Streitwert, ab dem Bürger in Deutschland für einen finanziellen Schaden vor Gericht ziehen würden, 1.950 EUR. Wenn sie die Rechtsdurchsetzung jedoch ohne Kostenrisiko und mit geringem Zeitaufwand über ein Portal im Internet einem Dritten überlassen können, ändert sich die Einstellung der Bürger. Sie verfolgen auch niedrigere Ansprüche. Zum Geschäftsprinzip der Legal-Tech-Anbieter gehört, dass der Sachverhalt in wenigen Minuten eingegeben werden kann. Kosten fallen nur im Erfolgsfall an. **39**

2. Automatisierung

Ein weiteres Geschäftsprinzip der Legal-Tech-Anbieter ist es, die Möglichkeiten der Automatisierung zu nutzen. Sie versuchen, möglichst viele gleichartige Mandate zu erlangen. Dies ermöglicht eine Bündelung von Ressourcen. Die Fallbearbeitung erfolgt computergestützt. Die Portale bearbeiten nur ein klar begrenztes Rechtsgebiet, auf dem sie eine Expertise aufgebaut haben. **40**

3. Tätigkeit im Rahmen einer Inkassolizenz

Die Legal-Tech-Anbieter werden in der Regel aufgrund einer Inkassolizenz tätig. Je nachdem für welches Rechtsgebiet sie ihre Leistung erbringen, stellt sich jedoch die Frage, ob ihre Tätigkeit eine mit einer entsprechenden Registrierung zulässige Inkassodienstleistung ist oder es sich um eine der Anwaltschaft vorbehaltene unzulässige Rechtsberatung handelt. In Bezug auf einen Legal-Tech-Anbieter, der sich auf die Geltendmachung von Verstößen gegen die Mietpreisbremse spezialisiert hatte, ist diese Frage sogar innerhalb des Landgerichts Berlin umstritten. Drei Zivilkammern bejahten die Wirksamkeit der der Forderung an den Legal-Tech-Anbieter (Urt. v. 20.6.2018 – 65 S 70/18; v. 13.8.2018 – 66 S 18/18; v. 22.8.2018 – 65 S 83/18; v. 10.10.2018 – 65 S 131/18; v. 15.1.2019 – 15 O 60/18; v. 31.7.2019 – 65 S 18/19); zwei Kammern verneinten sie (Beschl. v. 26.7.2018 – 67 S 157/18 und Urt. v. 28.8.2018 – 63 S 1/18). Ein Urteil **41**

des Bundesgerichtshofs zu dieser Frage soll am 27.11.2019 verkündet werden und wird mit Spannung erwartet.

II. Legal Tech in Großkanzleien

Auch der Trend in den Großkanzleien geht in Richtung des Einsatzes von KI und Legal Tech. Es kommt zu einer Automatisierung von Standardaufgaben. Während beispielsweise in der Vergangenheit im Rahmen der Due-Diligence-Prüfung die Inhalte von zahlreichen Leitz-Ordnern gesichtet werden mussten, werden heutzutage die Dokumente in einem virtuellen Datenraum hochgeladen. Die Erstauswertung erfolgt nicht mehr durch Anwaltsgehilfen und Associates, sondern durch eine KI. Die Anwälte konzentrieren sich dann darauf, die durch die KI als relevant erkannten Verträge oder Vertragsteile zu prüfen. Die Due-Diligence-Prüfung wird hierdurch schneller und kostengünstiger. **42**

Weiterer Druck in Richtung eines verstärkten KI-Einsatzes wird durch die Mandanten ausgeübt. Schließt ein Unternehmen immer wieder eine Vielzahl ähnlicher Verträge ab, besteht nicht mehr die Bereitschaft, jeden einzelnen dieser Verträge durch einen Rechtsanwalt, der nach Stunden abrechnet, prüfen zu lassen. Stattdessen besteht das Bedürfnis nach einer Software, die automatisiert Sachverhalte, die standardisiert und formalisiert abgebildet werden können, prüft. Beispielsweise könnte eine solche Anwendung einen Vertrag im Hinblick auf eine konkrete, häufig vorkommende Rechtsfrage auswerten. Ein neuer Markt für Großkanzleien ist es, derartige Anwendungen ihren Mandanten zur Verfügung zu stellen. Durch die Lizenzierung derartiger Softwareprodukte werden neue Vergütungsmodelle geschaffen. In Standardfällen erfolgt eine Rechtsberatung zu Festpreisen. Es ist zu erwarten, dass die Bereitstellung derartiger Software ein Zukunftsmarkt ist. **43**

III. Weitere Einsatzmöglichkeiten?

Die Frage, ob sich die aus dem aktuellen Einsatz von KI gewonnenen Erfahrungen verwenden lassen, um den Einsatz von KI in der Justiz zu fördern, wurde in einem durch den EDV-Gerichtstag veranstalteten „Workshop über die Möglichkeiten des Einsatzes von künstlicher Intelligenz (KI) im Bereich der Justiz“ erörtert, der am 15.5.2019 stattfand. Einen Überblick über die Ergebnisse dieses Workshops finden Sie in einer der Folgeauflagen. **44**

Hinweis:

Am 12.1.2020 organisiert der EDV-Gerichtstag e.V. in der Landesvertretung Nordrhein-Westfalens in Berlin einen zweiten Workshop zu den Einsatzmöglichkeiten von künstlicher Intelligenz (KI) in der Justiz. Nähere Informationen finden Sie in Kürze unter www.edvgt.de. **45**

Hinweis: Isabelle Désirée Biallaß ist Referentin im Ministerium der Justiz Nordrhein-Westfalen. Der Beitrag gibt ausschließlich ihre persönliche Auffassung wieder.

D. Künstliche Intelligenz im Kampf gegen Kinderpornographie

Verfasser: Dieter Kesper,

Oberstaatsanwalt a.D., Bonn

I. Einleitung

Am 5.8.2019 hat der Minister der Justiz des Landes Nordrhein-Westfalen ein Projekt vorgestellt, das federführend von der bei der Staatsanwaltschaft Köln angesiedelten Zentral- und Ansprechstelle Cybercrime des Landes Nordrhein-Westfalen betrieben wird. Hieran beteiligt sind wichtige Kooperationspartner wie die Microsoft Deutschland GmbH, verschiedene Wissenschaftler, u.a. der Universität des Saarlandes sowie der Deutsche EDV-Gerichtstag e.V. 46

Ziel des Projekts ist es, die Strafverfolgung von Kinderpornographie künftig mit Analysemethoden künstlicher Intelligenz zu unterstützen.

II. Ausgangssituation

Nach der Polizeilichen Kriminalstatistik (PK) und Feststellungen des Ministeriums der Justiz des Landes Nordrhein-Westfalen hat die Polizei in NRW 2018 Tausende Terabyte kinder- und jugendpornographischer Bilder und Filme sichergestellt. Ende März 2019 waren insgesamt 1.895 diesbezügliche Ermittlungsverfahren anhängig. In nur 228 Verfahren seien Beweismittel durch die Polizeibehörden ausgewertet worden. 557 Durchsuchungsbeschlüsse seien noch gar nicht vollstreckt worden. Nach Hochrechnungen des Landeskriminalamts Nordrhein-Westfalen soll ein Ermittler für die Auswertung von einem Terabyte sichergestellter Daten ca. neun Monate und für die Sichtung des bereits sichergestellten Materials rund 2.000 Jahre brauchen. 47

Eine nicht nur körperlich, sondern auch psychisch belastende Aufgabe für die Ermittler!

Da es sich bei der Sicherstellung von Rechnern und Speichermedien um einen Grundrechtseingriff handelt, kann deren Beschlagnahme zum Zwecke der Auswertung auch unter Berücksichtigung der Belastung der Polizeibeamten und eines möglichen Personalmangels nicht unbegrenzt aufrechterhalten werden. Können Datenträger also nicht innerhalb einer angemessenen Zeitspanne ausgewertet werden, sind sie mit dem vermuteten inkriminierten Datenmaterial zurückzugeben. 48

Diesem Problem kann durch eine personelle Aufstockung bei der Polizei nur bedingt entgegengetreten werden. Daher bitten viele Staatsanwaltschaften professionelle Firmen um Unterstützung bei der Auswertung der sichergestellten Rechner oder Datenträger, indem sie ihnen diese übersenden mit dem Auftrag, die Daten zu sichern und nach kinder-/jugendpornografischen Schriften sowie im Hinblick auf Kommunikation betreffend den Austausch von Kinder-/Jugend-/Tier-/Gewaltpornografie auszuwerten. Als Ergebnis erhalten die Staatsanwaltschaften gegen bis zu fünfstelligen Beträge Hinweise auf mögliche, strafrechtlich relevante Dateihalte und Kommunikation. 49

Dem Bedenken, dass auf den Datenträgern regelmäßig auch strafrechtlich irrelevante, aber datenschutzrechtlich bedeutsame Daten wie Steuererklärungen, Schriftwechsel mit Behörden und Anwälten oder Privatpost und -bilder des Beschuldigten gespeichert sind, kann dabei mit einer Vertraulichkeitsvereinbarung entgegengetreten werden. 50

Prozessual stellen sich allerdings zwei Fragen, die mit dem Charakter der Tätigkeit der externen Firmen zusammenhängen. Zum einen entfaltet nur die Beauftragung eines Sachverständigen, nicht aber ein Unterstützungsauftrag an jedweden Dritten, eine die Verfolgungsverjährung unterbrechende Wirkung im 51

Sinne § 78c Abs. 1 Satz 1 Nr. 3 StGB. „Sachverständig“ ist aber nur eine Person, die „aufgrund besonderer Sachkunde eine Bewertung von Anknüpfungs- oder Befundtatsachen anhand wissenschaftlicher Erkenntnisse oder Erfahrungssätze vornehmen soll. Diese Voraussetzungen liegen nicht vor, wenn ein Unternehmen ersucht wird, der ermittelnden Polizeibehörde“ technische Unterstützung zu leisten (BGH, Beschl. v. 2.3.2011 – 2 StR 275/10, juris).

Handelt es sich bei der Tätigkeit der beauftragten Firma aber nicht um die eines Sachverständigen, gibt es aus Sicht des Schleswig-Holsteinischen Oberlandesgerichts auch keine Norm, nach der dem Beschuldigten die durch die Beauftragung einer solchen Firma angefallenen Kosten im Falle seiner Verurteilung auferlegt werden können (Schleswig-Holsteinisches Oberlandesgericht, Beschl. v. 10.1.2017 – 2 Ws 441/16 (165/16), juris). **52**

Bisher besteht die technische Unterstützung weitgehend darin, sogenannte Hashwerte (vergleichbar mit einem eindeutigen Fingerabdruck) von den sichergestellten Dateien zu erstellen und mit denjenigen von bereits identifizierten inkriminierten Dateien zu vergleichen. Damit lassen sich bekannte Bilder computergestützt identifizieren; nicht identifizieren lassen sich neue oder veränderte Bilder. **53**

III. Ein neuer Weg

Ziel des im Sommer 2017 gestarteten Projekts ist es, das sichergestellte Datenmaterial künftig mit Hilfe Künstlicher Intelligenz auszuwerten. Erste Versuche mit nicht inkriminiertem Material haben gezeigt, dass die Zeiten für eine solche Auswertung pro Bild im Millisekunden-Bereich liegen. Filme werden dabei in einzelne Bilder zerlegt. **54**

Ob die hierfür erforderliche Rechenleistung und die entsprechende Software künftig unter wirtschaftlichen Gesichtspunkten bei jeder Strafverfolgungsbehörde vorgehalten werden können, wird nach Abschluss der weiteren Tests zu entscheiden sein.

Auf dem Weg zum cloudbasierten Training einer künstlichen Intelligenz waren verschiedene rechtliche und technische Hürden zu überwinden. **55**

1. Rechtliche Fragen

Die §§ 184b ff. StGB statuieren ein umfassendes Umgangsverbot mit kinder- und jugendpornographischen Schriften. Damit besteht auch bei den eng auszulegenden Ausnahmeregelungen für das Strafverfahren in den §§ 184b Abs. 5 und 184c Abs. 6 StGB das Problem, dass auch Verschlüsselungen oder Transformationen in andere Dateiformate nichts an dem Umstand ändern, dass es sich um verbotenes Material handelt, das nicht – auch nicht zu Auswertungszwecken – in eine Cloud gelegt werden kann. Dies selbst dann nicht, wenn es sich um eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher gegen Angriffe von außen eingestufte (Deutsche) Cloud handelt, auf deren rechtlichen Status die Europäische Datenschutzgrundverordnung anwendbar ist und bei der ein Zugriff von US-Behörden auf im Ausland liegenden Daten nach dem CLOUD-Act (Clarifying Lawful Overseas Use of Data Act) verhindert werden könnte. **56**

Denn hierbei wären Fragen des internationalen Rechts zu klären, nämlich ob und in welchem Umfang die Länder, in denen der Cloud-Server und der Auswertungsrechner stehen, den Umgang mit inkriminiertem Material verbieten und ob sie ähnliche Ausnahmeregelungen wie das Strafgesetzbuch kennen. **57**

2. Technische Herausforderung

Die technische Herausforderung bestand nun darin, die Bilder so zu „dekonstruieren“ (anonymisieren und abstrahieren), dass es sich nicht mehr um pornographische Darstellungen handelt. Dies kann allerdings nicht erst in der Cloud erfolgen, sondern muss schon bei den Strafverfolgungsbehörden geschehen. **58**

Gemeinsam mit der Firma Microsoft und dem Lehrstuhl für Rechtsinformatik der Universität des Saarlandes wurde die Idee entwickelt, die sichergestellten Daten durch ein neuronales Netz so zu verändern, dass sie nicht mehr als pornographische Bilder zu erkennen sind und aus dem „Produkt“ auch nicht mehr auf solches Material „zurückgerechnet“ werden kann. Dieser Veränderungsprozess erfolgt in immer gleicher Weise über eine Vielzahl von sogenannten „Abstraktions-Layern“, durch die die Bilder schrittweise dekonstruiert und in Bestandteile aufgelöst werden. Da dieser Prozess mangels Rechenleistung und Verfügbarkeit relevanter neuronaler Netze nicht vollständig auf Rechnern der Strafverfolgungsbehörden ablaufen kann, war eine weitere Herausforderung zu untersuchen, ob diese Arbeit teils auf Rechnern der Justiz, teils in der Cloud erfolgen kann. **59**

3. Aktueller Zwischenstand

Versuche mit strafrechtlich unkritischem Material (Tierbildern) haben zu folgendem Ergebnis geführt: **60**

- Eine Verteilung der Abstraktions-Layer zwischen Justizrechnern und Cloud ist möglich; der Gesamtprozess des Dekonstruierens wird hierdurch nicht beeinträchtigt.
- Das Ergebnis der Schritte auf Justizseite reicht aus, um das Ausgangsbild nicht mehr erkennen oder aus dem Ergebnis auf das Ausgangsbild zurückrechnen zu können.
- Rechtlich gesehen ist das an die Cloud übergebene „Bild“ daher keine kinder- oder jugendpornographische Schrift mehr.
- Nach entsprechender Anlernung konnte in der Cloudlösung eine künstliche Intelligenz entwickelt werden, die speziell darauf trainiert ist, anzugeben, mit welcher Wahrscheinlichkeit es sich um das Bild welchen Tieres handelt.

4. Nächste Schritte

In den kommenden Monaten soll die Künstliche Intelligenz „angelernt“ werden. Hierzu werden bereits als strafrechtlich bedeutsam erkannte Bilder und entsprechendes Negativmaterial auf dem zuvor beschriebenen Weg modifiziert und an die Cloud übergeben, um dieser genügend Vergleichsmaterial für die zukünftige Auswertung unbekannter Bilder zu liefern. Anschließend Testläufe müssen zeigen, ob sich die Auswertung mit Hilfe Künstlicher Intelligenz als schnellerer Weg zur Bekämpfung der Kinder- und Jugendpornographie eignet. **61**

Am Ende eines vollständigen Analyseprozesses wird eine Aussage erwartet, mit welcher Wahrscheinlichkeit es sich bei welcher Datei um inkriminiertes Material handelt. Da der Dateiname beim Dekonstruieren nicht verändert wird, wird es künftig nur noch Aufgabe der Ermittler sein, diesen Hinweisen zu folgen und die Dateiinhalte auf ihre strafrechtliche Relevanz zu prüfen. **62**

E. Künstliche Intelligenz in der JVA

Verfasser: Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

Am 22.10.2019 hat das Ministerium der Justiz des Landes Nordrhein-Westfalen in einer Pressekonferenz mitgeteilt, dass der Einsatz Künstlicher Intelligenz (KI) im Justizvollzug geprüft wird. In einem in der Bundesrepublik Deutschland einmaligen Forschungsprojekt soll die Suizidprävention in den Justizvollzugsanstalten verbessert werden. Neben der Ernennung von Suizidpräventionsbeauftragten und der Einführung zusätzlicher Screenings zur Erkennung von Suizidgefährdungen soll als weiterer Baustein zur Verbesserung der Suizidprävention zukünftig Künstliche Intelligenz im Justizvollzug genutzt werden. Im Rahmen einer ereignisgesteuerten Videoüberwachung von Gefangenen sollen kritische Situationen in den Hafträumen frühzeitig erkannt werden. Die in den Zellen angebrachten Kameras übermitteln den Vollzugsbeamten aber nur Bilder von gefährlich erscheinenden Situationen, um die Persönlichkeitsrechte der Häftlinge zu schützen. **63**

Nach einer europaweiten Ausschreibung des Projekts hat die Zentrale Beschaffungsstelle für den Justizvollzug den Zuschlag an ein sächsisches Unternehmen aus Chemnitz (Fusion Systems GmbH) erteilt. Das Unternehmen soll im ersten Schritt das Forschungsprojekt gemeinsam mit dem Justizvollzug durchführen und eine Software entwickeln. 160.000 EUR lässt sich das Justizministerium das Projekt kosten. **64**

Bei der ereignisgesteuerten Videoüberwachung sollen auf der Grundlage von Erfahrungen bei der Suizidprävention Situationen erfasst werden, die auf ein geplantes Suizidvorhaben hindeuten. Als relevante Merkmale sind beispielsweise auffällige Verhaltensweisen wie Bewegungsmuster bei einem Strangulationsversuch oder der Einsatz gefährlicher Objekte wie Messer zu nennen. Auf der Grundlage von entsprechendem Expertenwissen erfolgt aus den Situationsbeschreibungen eine Einstufung des Suizidrisikos. Das Assistenzsystem soll die Justizvollzugsbediensteten rechtzeitig alarmieren. **65**

An die Entwicklung des Systems wird sich eine Testphase anschließen. Erweist sich das entwickelte System als hilfreich, sollen zunächst in einem Pilotvorhaben in einer Justizvollzugsanstalt suizidgefährdete Gefangene mit Videokameras überwacht werden. **66**

F. KI und die Gerichte

Dr. Ralf Köbler, Präsident des Landgerichts Darmstadt

Wir leben längst mit künstlicher Intelligenz, auch wenn wir nicht wissen, dass manche Phänomene darauf beruhen. Im weitesten Sinne gehören bereits die im Rechtsleben und bei allen deutschen Gerichten zu Recht sehr gerne genutzten Rechtsinformationssysteme dazu, die von unseren Schreibtischen nicht wegzudenken sind. Sie produzieren Ergebnisse wie: „Kunden, die nach dem Urteil des BGH vom 15.5.2015 suchten, bekamen auch die folgenden Ergebnisse vorgeschlagen.“ Oder so ähnlich jedenfalls. Dies setzt voraus, frühere fremde Suchergebnisse auf eine neue Suche zu übertragen und mit anderen Informationen zu verknüpfen. Aber wer von uns weiß schon, ob der Algorithmus des Fachinformationssystems tatsächlich alle derzeit einschlägigen richterlichen Entscheidungen gefunden hat oder ob Schwächen und Stärken dieser Systeme nicht mir nichts dir nichts immer mal soeben ein Stück deutscher Rechtsgeschichte schreiben? Ein Stück weit haben wir uns voller Vertrauen in die (bewährten) Hände der Anbieter begeben. **67**

- Viel deutlicher aber ist die Wirkung von KI-Systemen beim online-Shopping. Hier bekommt der Suchende tatsächlich auch die Suchergebnisse und vor allem abweichende Kaufentscheidungen anderer Kunden als Vorschlag mitgeteilt. Mit anderen Worten: Die Systeme hinter den großen (amerikanischen) Internet-Kaufportalen merken sich alles, was Millionen Kunden tun, und sind in der Lage diese mannigfachen Information zu verknüpfen und zu neuen Vorschlägen zu verarbeiten. Wir nehmen diese Vorschläge gerne an, aber: Ist das nicht schon ein durchaus irritierendes Stück „Big Brother is watching you“? Die Technik ist dabei mit Sicherheit inhaltsneutral: In China kann man so gewiss Kaufverhalten mit Sozialverhalten verknüpfen. **68**
- Ob all das nun definitorisch (schon) künstliche Intelligenz ist oder nicht, kann dahinstehen: Jede Suchanfrage, jeder Kauf werden gespeichert und weiterverarbeitet, alles ist in Echtzeit verknüpfbar. Wenn das der Staat oder die Polizei nur ansatzweise täten (könnten...), wäre der Protest groß. **69**
- (Internet-)Freiheit, die ich meine...!**
- Und alles über die zustimmenden Klicks zu den (nicht gelesenen oder nicht lesbaren) Allgemeinen Geschäftsbedingungen mit Einwilligung der Nutzer: take it or leave it. An dieser Stelle wäre gewiss hier und da aufsichtsrechtlich oder gesetzgeberisch über die Wirkweise und die zulässige Reichweite des Operierens mit solchen „Einwilligungen“ nachzudenken. **70**
- Zugleich unternehmen einige der großen Portale sehr erfolgreiche Anstrengungen, Streitfälle, die den abgewickelten Fernabsatzgeschäften entspringen, den Gerichten vorzuenthalten. **71**
- Sie schreiben für Streitigkeiten einen integrierten Streitschlichtungsdienst (online-dispute Verfahren) vor, der verpflichtend ist, und Vorrang vor staatlichen Streitentscheidungsmechanismen hat. Ein Schelm, der Böses dabei denkt. Es findet gewiss ein unparteiliches und neutrales Verfahren statt, bei dem regelmäßig der Anbieter dem wohlverstandenen Kundeninteresse nachgibt, will er weiterhin Anbieter auf der Plattform bleiben.
- Dies mag vordergründig verbraucherfreundlich erscheinen. Aber auch nicht jeder Verbraucher, der reklamiert, ist ein Engel. Daher sollten gerade in einer marktwirtschaftlich und privatautonom ausgestalteten Wirtschafts- und Rechtsordnung staatliche Gerichte mit unabhängigen Richtern über die Einhaltung der Gesetze und damit neutral über die Interessen der Vertragsparteien entscheiden können. **72**
- Wenn sie nicht angerufen werden (können), hat dies zwei Aspekte: Die deutschen Gerichte und auch die Staatsanwaltschaften sind für die modernen digitalen Massenphänomene, ob Mängelstreit, ob Hassbotschaft, weder personell noch technisch aufgestellt. Man wird froh sein, die bis 2026 zu leistende Einführung (funktionierender) elektronischer Akten zu bewältigen, die mehr oder weniger die digitale Verbesserung einer Papierakte darstellen. **73**
- Wenn wir uns aber darüber klar sind, dass die Phänomene der modernen digitalen Welt das Potenzial haben, den Rechtsstaat ein wenig auszuhöhlen, dann wäre über moderne online-Gerichtsverfahren mit wenigen Maus-Klicks nachzudenken. Natürlich ist das technisch nicht einfach, wenn man rechtlich dem 19. Jahrhundert verhaftet ist. Aber vielleicht könnte man bei der Programmierung solcher KI-gestützter Verfahren ja Aufträge an einige amerikanische (oder auch chinesische?) Unternehmen vergeben, die mit derlei Technik offensichtlich Erfahrung haben. **74**

G. EDVGT-Nachlese

Verfasser: Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

Der diesjährige EDV-Gerichtstag, der mit über 900 Teilnehmern einen Rekord aufgestellt hat, bot ein breites Fachprogramm zum Tagungsthema „Digitalisierung und Recht – Herausforderungen und Visionen“. Auch dort wurde schwerpunktmäßig über Künstliche Intelligenz sowie deren Möglichkeiten und Risiken diskutiert. Als zentrale aktuelle Herausforderungen für Justiz und Anwaltschaft wurden die Themen IT-Sicherheit und Datenschutz ausgemacht. Dabei mussten sich die Juristen von den IT-Fachleuten sagen lassen, dass sie diese Herausforderungen bislang nicht gut bewältigen. Das Fax, des Juristen liebstes Kommunikationsmittel, ist beispielsweise keinesfalls so sicher, wie viele glauben. Auch die in Kanzleien und Gerichten zur Standardausrüstung gehörenden Multifunktionsgeräte, die Druck-, Kopier-, Scan- und Fax-Funktion vereinen, sind ein Sicherheitsrisiko. Ganz ausschließen lässt sich dieses aus Sicht der IT-Experten nur, indem man den alten Übertragungsweg komplett abschafft. Über die entsprechende Auftaktveranstaltung des EDV-Gerichtstag, „IT-Sicherheit in der Justiz – Neue Gefahren für die Gerichte?“ ist ein Bericht von *Lena Leffer, Karin Potel* im Internet als JurPC Web-Dok. 133/2019, Abs. 1 – 27 verfügbar. 75

Wie wichtig der Sicherheitsaspekt ist, zeigte sich am 25.9.2019. An diesem Tag mussten die Rechner des Kammergerichts Berlin vom Netz genommen werden, weil der Trojaner Emotet in das System eingedrungen ist. Man rechnet damit, dass erst Anfang 2020 das Problem beseitigt sein wird und das Kammergericht wieder Online erreichbar ist. 76

Bei diesem Trojaner Emotet handelt es sich nach Einschätzung von Fachleuten um einen Virus, der zurzeit deutschlandweit wütet und mit dem auch andere Unternehmen oder Behörden kämpfen. Die Berliner Justiz ist also nicht das Opfer eines speziell auf sie gerichteten Angriffs geworden. Allerdings war offenbar die Abwehrbereitschaft der Justiz nicht hoch genug. Als Risiko für einen Virenangriff werden z.B. die Standardeinstellungen bei Word angesehen. Sind Makros aktiviert, kann es schnell passieren, dass sich beim Öffnen eines E-Mail-Anhangs Schadsoftware auf einem Rechner installiert und sich – einmal eingedrungen – dann von da aus im internen IT-System weiter ausbreitet. 77

Es bleibt nach diesen Erfahrungen zu hoffen, dass die zahlreichen unterschiedlichen IT-Systeme in den Anwaltskanzleien einem solchen Virenangriff standhalten würden. 78

Kritik kam auf dem EDV-Gerichtstag auch zum Datenschutz. Aus Sicht des Bundesbeauftragten für den Datenschutz Ulrich Kelber tut sich insbesondere die Anwaltschaft noch schwer mit dem Thema.

Der nächste EDV-Gerichtstag findet vom 23. – 25.9.2020 in Saarbrücken statt. 79

E-Government-Monitor 2019",6,32>H. E-Government-Monitor 2019

Verfasser: Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

Aus dem diesjährigen E-Government Monitor 2019, der von der Initiative D21 und Fortiss erstellt wird, geht hervor, dass 48 % der deutschen Bürgerinnen und Bürger von digitalen Verwaltungsangeboten Gebrauch machen. Dies bedeutet im Vergleich zum Vorjahr einen Anstieg um acht %. Im Vergleich zu den 80

deutschsprachigen Nachbarstaaten Österreich (70 %) und Schweiz (58 %) ist aber dennoch ein erheblicher Rückstand zu verzeichnen. Auch im Langzeitvergleich ist kein deutlicher Zuspruch ersichtlich – schon 2012 lag die hiesige Nutzungsrate bei 42 %. Es lässt sich nicht leugnen, dass trotz vieler Bemühen, mehr digitale Verwaltungsleistungen anzubieten und vor allem auch bekannt zu machen, Deutschland beim E-Government europaweit weiterhin im hinteren Feld verharret. *Klaus Vitt*, Staatssekretär im Bundesministerium des Innern, für Bau und Heimat und Beauftragter der Bundesregierung für Informationstechnik gesteht zwar im Vorwort der Studie ein, dass bei der Nutzung und Akzeptanz von digitalen Behördenleistungen in Deutschland noch Verbesserungsbedarf vorhanden ist, sieht uns aber bei der Verwaltungsdigitalisierung auf einem sehr guten gemeinsamen Weg und verweist dabei auch auf die laufenden Arbeiten im Rahmen des Online-Zugangsgesetzes.

Der Monitor richtet den Focus seiner Betrachtungen auch auf die Diskrepanz zwischen digitalen Angeboten und deren Bekanntheit. Während die elektronische Steuererklärung (ELSTER) nahezu allen Befragten bekannt ist und von immerhin 32 % genutzt wird, ist die Situation bei der elektronischen Identifizierung durch den elektronischen Personalausweis eher desillusionierend. Nur bei einem Viertel der Ausweishalter ist die eID-Funktion freigeschaltet, genutzt wird sie lediglich von gerade einmal sechs %. Die Ausweisinhaber, bei denen die Funktion nicht aktiviert ist, haben von der eID-Funktion nie gehört (11 %), haben kein Vertrauen (10 %) oder sehen keinen wahrnehmbaren Mehrwert (10 %) oder kennen keine Anwendungsmöglichkeiten (9 %). Ein Kommunikationsproblem ist hier unverkennbar vorhanden.

81

I. Monitor „Digitale Verwaltung“ des Nationalen Normenkontrollrats

Verfasser: Dr. Wolfram Viefhues

Weiterer Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

Der dritte „Monitor Digitale Verwaltung“ des Nationalen Normenkontrollrats (NKR) ist unter dem Beigleittitel „Fortschritte bei der Digitalisierung der Verwaltung transparent machen“ erschienen. Auch die Botschaft dieser vierteljährigen Berichtsreihe lautet einmal mehr: Tempo zulegen. Um die Ziele des Online-Zugangsgesetzes (OZG) zu erfüllen, müssten Zwischenziele definiert, das Monitoring geschärft und die Datenschutzfrage bis Ende 2019 geklärt sein. Es wird ausdrücklich klargestellt, dass es angesichts dieser komplexen Aufgabe nicht ausreicht, nur das „Enddatum 2022 im Blick zu haben“. Denn Deutschland belegt im internationalen Ranking nach wie vor hintere Plätze, wobei die Bundesrepublik im aktuellen Digital Economy and Society Index (DESI) der EU im Vergleich zum Vorjahr sogar noch weiter abgerutscht ist – von Platz 19 auf Platz 24. Um spürbar aufzuholen, müssen – so die Forderung des NKR – vergleichbar gute digitale Verwaltungsangebote für Bürger und Wirtschaft entwickelt werden – genauso wie in den führenden Ländern Europas und der Welt.

82