

Heidelberg, den 21. Februar 2016

Verwaltungsgericht Wiesbaden
Mainzer Str. 124
65189 Wiesbaden

**Verwaltungsstreitverfahren Markus D
land, -6 K 20/16.WI-**

./ Bundesrepublik Deutsch-

Ihr Schreiben vom 15.2.2016, Antrag des BKA vom 12.2.2016

In dem o.g. Verwaltungsstreitverfahren überlasse ich unten dem Gericht – wie in Ihrem Schreiben vom 15.2.2016 erbeten – die relevanten Schriftstücke, insbesondere die Bescheide des BKA. Die originale IFG-Anfrage wurde über die Plattform fragdenstaat.de gestellt, und ist online¹ verfügbar.

Ich möchte diese Gelegenheit nutzen, meine Klage zu präzisieren, auch auf das Risiko hin, mich gegenüber den dem Gericht vorliegenden Dokumenten zu wiederholen.

Ziel meiner Klage ist die Verpflichtung des BKA, mir nach dem Informationsfreiheitsgesetz Dokumente zu Errichtung und Betrieb der so genannten elektronischen Kriminalakte (eKA) zur Verfügung zu stellen, insbesondere die Errichtungsanordnung des diese implementierenden EDV-Systems nach §34 BKAG. Mit diesem Dokument würde ich eine minimale Auskunft nach IFG für gewährt ansehen, auch wenn zur Beurteilung der datenschutzrechtlichen Implikationen der Migration von Papierakten zu automatisierten Dateien weitere Dokumente natürlich willkommen wären, insbesondere die DDL der entsprechenden Datenbank-Tabellen oder vergleichbare Details im Falle von Volltextdatenbanken. Obwohl ich jedoch eine VS-NfD-Einstufung entsprechender Dokumente persönlich für klar missbräuchlich halte, will ich diese mit der vorliegenden Klage *nicht* angreifen.

Zur Begründung:

(1) Der Bescheid des BKA vom 13.7. ist schon deshalb anfechtbar, weil er fälschlicherweise angibt, dem Antrag sei teilweise stattgegeben worden. Dies ist nicht der Fall – die Errichtungsanordnungen der *Nachweissysteme* KAN und BKA-AN sind vom Gegenstand her nicht einschlägig; sie beschreiben Indexsysteme, die schon deshalb keinen ohne weitere Informationen erkennbaren Zusammenhang mit der eKA

¹ <https://fragdenstaat.de/anfrage/dokumente-zur-elektronischen-kriminalakte/>

haben können, weil sie bestenfalls in gleicher Weise auf Papier- wie auf elektronische Akten anzuwenden sind. In der Tat ist aber z.B. in 5.2 der Errichtungsanordnung für das BKA-AN explizit von einer „Kriminalaktennummer“ die Rede – wäre das BKA-AN angepasst auf eine Infrastruktur mit Integration der eKA, so hätte ich hier vielmehr mit einem Fremdschlüssel oder eventuell einem Hyperlink gerechnet. Insofern würde ich ohne nähere Kenntnis der BKA-Verwaltungsverfahren mutmaßen, dass die Errichtungsanordnungen sogar noch den Zustand vor der Einführung der eKA reflektieren.

Die Überlassung weitgehend beliebiger, allenfalls in losem Zusammenhang mit der Anfrage stehender und zudem bereits zuvor öffentlich gemachter Dokumente ist schlicht eine völlige Auskunftsverweigerung. Angesichts dieses doch recht durchsichtigen Versuches, einen für mich als Petenten günstigeren Ausgang vorzutäuschen, hätte ich den Bescheid wohl gleich nach §43 Abs. 1 VwVfG angreifen sollen. Andererseits konnte ich mit der behördlichen Intransigenz auch nur eingeschränkt rechnen.

(2) Selbst wenn die Nachweissysteme in der tatsächlichen Aktenführung eine Rolle spielten und mithin mein Punkt (1) hinfällig wäre, hat das BKA bei der Berufung auf §3 IFG im seinem Bescheid vom 13.8.2015 offensichtlich die Regelung aus §7 Abs. 2 IFG missachtet, nach der möglicherweise geheimhaltungsbedürftige Dokumente so zu redigieren seien, dass einer Anfrage ohne „Preisgabe der geheimhaltungsbedürftigen Informationen“ nachgekommen werden kann. Dass durchaus nicht der gesamte vorliegende Informationspool geheimhaltungsbedürftig ist, wird schon dadurch deutlich, dass im Bescheid des BKA vom 17.12.2015 immerhin ein Teil der angefragten Information enthalten ist, namentlich, dass die eKAen individuell, nicht aber global durchsuchbar sind.

Da diese Information im Rahmen eines Ablehnungsbescheides gegeben werden kann, ohne die Sicherheit der Bundesrepublik Deutschland aufs Spiel zu setzen, warum kann sie nicht im Rahmen einer Auskunft gegeben werden? Und natürlich ist, wie im Widerspruch und meinem Schreiben an das VG Wiesbaden schon ausgeführt, kein plausibles Szenario vorstellbar, in dem diese Auskunft einen wie immer gearteten Angriff auf die EDV des BKA erleichtern würde, es sei denn, das BKA würde bereits bürgerrechtliche Einwände gegen bestimmte Details seiner EDV-Nutzung als Angriff auffassen.

Ähnliches gilt ganz sicher für Fragen wie:

- Wie heißt das DV-System, in dem die eKAen geführt werden, und welchen Rechtsnormen unterliegt es nach Ansicht des BKA?
- Werden tatsächlich alle Kriminalakten des BKA digitalisiert?
- Welche Art Daten stehen in welcher Form in den eKA?
- Mit welcher Granularität kann in den eKA gesucht werden, welche technischen und organisatorischen Maßnahmen sind getroffen, um eine globale Volltextsuche zu unterbinden?
- Wie werden die eKAen gepflegt?
- Wie sieht es mit der Aussonderung von Informationen aus? Wenn etwa ein Tatbestand aus dem BKA-AN gelöscht wird, verschwindet er dann auch aus der eKA?

Ein Vergleich mit §34 BKAG zeigt, dass sich dieser Fragenkatalog recht weitgehend mit den für eine Errichtungsanordnung vorgesehenen Punkten deckt. Es ist umgekehrt kaum vorstellbar, dass für eine Vorbereitung auf einen technischen Angriff auf die EDV des BKA tatsächlich nützliche Informationen (das *könnten* Informationen zu Netzwerktopologie, eingesetzter Software, o.ä. sein; vgl. aber unten) in der Errichtungsanordnung zum eKA-System enthalten sein könnten. Und selbst wenn einzelne Passagen bei maximal bürgerrechtsfeindlicher Interpretation des IFG noch entsprechend klassifiziert werden könnten, wäre ihre Schwärzung ganz gewiss verhältnismäßig nach §7 Abs. 2 IFG.

(3) Nachgerade kafkaesk wird die Verweigerung durch die Angabe im Antrag des BKA vom 12.2.2016, schon die Benennung wenigstens eines plausiblen Angriffsszenarios, das einer Auskunft entgegensteht, stelle eine Gefährdung der EDV des BKA dar und müsse daher unterbleiben.

Geheimhaltungsgründe wiederum geheimzuhalten und so einer rechtlichen Überprüfung zu entziehen ist natürlich zunächst in einem Rechtsstaat jedenfalls außerhalb des engsten Geheimdienstbereichs inakzeptabel, da es einen effektiven Rechtsschutz ausschließt.

Im vorliegenden Fall ist die Argumentation aber auch sachlich äußerst angreifbar. Als jemand, der seit über 20 Jahren zahlreiche vernetzte Informationssysteme betreibt (im Übrigen trotz praktisch durchweg öffentlich verfügbarem Quellcode ohne einen erfolgreichen Einbruchversuch), traue ich mir in diesem Punkt eine gewisse Sachkenntnis zu. Der Versuch, „Security by Obscurity“ zu schaffen, technische Sicherheit also dadurch, dass organisatorische Details verschleiert werden, ist in der Fachwelt zumindest heiß umstritten (ich empfehle die entsprechende Abhandlung in der englischen Wikipedia für eine noch zurückhaltende Diskussion).

Die Implikation schließlich, die BKA-Systeme seien so verletzlich, dass jede Diskussion auch nur sehr abstrakter technischer Details mit einer Gefährdung einhergehe, die eine Verweigerung öffentlicher Rechte nach IFG rechtfertige, ist jedenfalls alarmierend, ob nun im Hinblick auf eine möglicherweise tatsächlich unzureichende Sicherung teils äußerst heikler Daten oder im Hinblick auf eine außer Kontrolle geratene (Un-)Kultur der Geheimhaltung.

Im konkreten Fall tritt hinzu, dass das BKA keinerlei Vertrauensvorschuss verlangen kann speziell, was technische Mittel des Datenschutzes angeht. Ich verweise nochmals auf den jahrelangen Einsatz des „Bundestrojaners“ der Firma Digitask offenbar unter den Augen des behördlichen Datenschutzbeauftragten. Obwohl sowohl diesem also auch der Behördenleitung hätte klar sein müssen, dass hier an der Grenze des überhaupt in einem Rechtsstaat Vorstellbaren operiert wurde und mithin äußerste Sorgfalt vonnöten gewesen wäre, fehlte der Software selbst eine so elementare Funktion wie das Löschen oder Sperren von den Kernbereich der persönlichen Lebensgestaltung betreffenden Gesprächspassagen. Spätestens nach dieser Episode muss sich das BKA Fragen aus der Öffentlichkeit gefallen lassen, ob etwa in einer eKA anderweitig nicht mehr speicherbare Sachverhalte wirklich gelöscht oder gesperrt werden sollen und ob dies in der Implementation auch stattfindet.

Dem BKA zu erlauben, die Antworten unter wolkigen Verweisen auf geheimgehaltene und jedenfalls bestenfalls abstrakte Gefährdungslagen zu verweigern, hieße, das

IFG zu entkernen. In diesem Sinn zitiere ich abschließend aus der Begründung zum IFG, Bt-Drucksache 15/4493:

Der Zugang zur Information und die Transparenz behördlicher Entscheidungen ist eine wichtige Voraussetzung für die effektive Wahrnehmung von Bürgerrechten. Dies gilt angesichts der wachsenden Informationsmacht des Staates heute mehr denn je. Lebendige Demokratie verlangt, dass die Bürger die Aktivitäten des Staates kritisch begleiten, sich mit ihnen auseinandersetzen und versuchen, auf sie Einfluss zu nehmen.

Mit freundlichen Grüßen,

Markus D