
5827/J XXVII. GP

Eingelangt am 17.03.2021

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

Anfrage

**der Abgeordneten Dr. Stephanie Krisper, Kolleginnen und Kollegen
an den Bundesminister für Inneres**

**betreffend "Ibiza"-Videos - gesetzeswidrige exzessive Klassifizierung für
"Ibiza"-Untersuchungsausschuss versus ministerieninterne Handhabung**

Auf Grund entsprechender Aufforderungen nach § 27 Abs 4 VO-UA der Abgeordneten Krisper, Krainer, Kolleginnen und Kollegen wurden seitens des BMJ mit Lieferung vom 18. Dezember 2020 dem "Ibiza"-Untersuchungsausschuss die "Ibiza"-Videos, d.h. alle sich in Akten zum "Ibiza"-Verfahrenskomplex befindlichen Video- und Audio-dateien, ohne Schwärzungen samt Transkript übermittelt.

Dabei erfolgte seitens des BMJ die Einstufung in die Klassifizierungsstufen "STRENG GEHEIM (4)" nach § 4 Abs 1 InfOG.

Hinsichtlich der Lieferung der "Ibiza"-Videos samt Transkript wurde am 27. Jänner 2021 seitens der Abgeordneten Krisper und Krainer bereits eine Herabstufung in Sicherheitsstufe 1 nach § 6 Abs 1 InfOG angeregt. Die diesbezügliche Entscheidung von Nationalratspräsident Wolfgang Sobotka steht zum Zeitpunkt der Einbringung gegenständlicher Anfrage weiterhin aus.

Bei der gewählten Sicherheitsstufe „STRENG GEHEIM“ handelt es sich um die höchste Sicherheitsstufe nach dem InfOG.

Eine solche Einstufung ist nach § 4 Abs 1 Z 4 InfOG vorgesehen, wenn das Bekanntwerden der Informationen eine schwere Schädigung der in Z 1 genannten Interessen wahrscheinlich machen würde (Stufe 4).

Bei den genannten Interessen handelt es sich nach § 4 Abs 1 Z 1 InfOG um folgende:

Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen, den wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder dem überwiegenden berechtigten Interesse der Parteien zuwiderlaufen würde und die Informationen eines besonderen organisatorischen Schutzes bedürfen.

Im Ausschussbericht zum InfOG wurden als Beispiele für die berechtigte Einstufung einer Information als „STRENG GEHEIM“ genannt:

- unmittelbarer Verlust zahlreicher Menschenleben
- unmittelbare Gefährdung der inneren Stabilität Österreichs oder von Drittstaaten oder internationalen Organisationen

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

- schwere und langfristige Schädigung der österreichischen Wirtschaft

Zur Herstellung des entsprechenden Schutzniveaus ist u.a. vorgesehen (vgl. §§ 6, 8, 9 11 InfoV):

Sicherheitsstufe "STRENG GEHEIM":

- **Aufbewahrung:** nur in besonders geschützten Bereichen (d.h. solchen die einer ständigen, doppelten Zutrittskontrolle unterliegen) in einem Sicherheitsbehältnis mit ständiger Bewachung oder Kontrolle oder mit zugelassener Einbruchsmeldeanlage in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst oder einem mit einer Einbruchsmeldeanlage ausgestatteten Tresorraum in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst;
- **Bearbeitung:** nur in einem besonders geschützten Bereich
- **mündliche Übermittlung:** nur in geschützten Bereichen und in Anwesenheit von Personen, die für die jeweilige Stufe berechtigt sind; zusätzlich Maßnahmen gegen Abhören nötig
- **Telefongespräche:** ebenfalls nur bei Maßnahmen gegen Abhören möglich
- Dokumente dürfen **nicht elektronisch verarbeitet** werden
- Verbot der Herstellung von **Notizen**
- Anfertigung von **Kopien** ist unzulässig

Gemäß § 27 Abs. 6 VO-UA ist der Untersuchungsausschuss über den Zeitpunkt und die Gründe der Klassifizierung schriftlich zu unterrichten. Der Ausschussbericht führt dazu aus, dass diese Bestimmung sicherstellen soll, dass „bestimmte Informationen **nicht erst aufgrund der Einsetzung eines Untersuchungsausschusses klassifiziert werden**“ (AB 440 BlgNR XXV.GP). Sie entspricht daher einem Verbot einer solchen Höherstufung. Ziel des InfoG (vgl AB 441 BlgNR XXV.GP) ist, ein einheitliches Schutzniveau auf Seiten der Organe der Gesetzgebung und der Vollziehung zu gewährleisten. Eine Erhöhung der erforderlichen Schutzmaßnahmen durch Einstufung gemäß InfoG im Vergleich zum gewährten Schutzniveau auf Seite der Organe der Vollziehung stellt daher eine unzulässige Höherstufung aus Anlass der Vorlage von Akten und Unterlagen an einen Untersuchungsausschuss dar.

Klassifizierungen haben außerdem gemäß § 5 InfoG nur in jenem Ausmaß und Umfang zu erfolgen, als dies unbedingt notwendig ist.

Für den Bereich des BMI gilt hinsichtlich des Umgangs mit klassifizierten Informationen die **Geheimchutzordnung des Bundes**. Für den Umgang mit Unterlagen der Klassifizierungsstufe 4 gilt dort (Auswahl):

- **Aufbewahrung:** ausschließlich in Tresoren (entsprechend der Zuordnung durch die Informationssicherheitskommission). Die Schlüssel dieser Behältnisse sind kontrolliert zu verwahren. Ab der Klassifizierungsstufe VERTRAULICH ist über die Ausgabe dieser Schlüssel (Zugangsmittel, Codes) ein Protokoll zu führen.
- **mündliche Übermittlung:** Bei der mündlichen Weitergabe und bei Besprechungen mit einem Inhalt ab der Klassifizierungsstufe VERTRAULICH ist dafür Sorge

zu tragen, dass die Teilnehmer entsprechend sicherheitsüberprüft und belehrt sind. Aufzeichnungen sind entsprechend zu klassifizieren. Bei der mündlichen Darlegung von Informationen, die als GEHEIM oder STRENG GEHEIM klassifiziert sind, sind soweit vorhanden abhörsichere Räume bzw. entsprechend geschützte Lokationen zu verwenden.

- **Telefongespräche:** Die Weitergabe von klassifizierten Informationen mittels Kommunikationsdiensten wie Telefon und Fax ist durch adäquate Schutzmechanismen abzusichern, die dem technischen Standard entsprechen. Für VERTRAULICH, GEHEIM und STRENG GEHEIM sind entsprechende durch die ISK zugelassene kryptographische Methoden einzusetzen.
- **Elektronische Verarbeitung:** Klassifizierte Informationen dürfen nur mit IKT-Systemen, Algorithmen und in Arbeitsprozessen verarbeitet, gespeichert und übermittelt werden, welche für die jeweiligen Klassifizierungsstufen geeignet sind. Die Beurteilung der Eignung ist vom jeweiligen Ressort in Abstimmung mit den Vorgaben der ISK zu treffen, wobei eine regelmäßige Überprüfung in Bezug auf geänderte Rahmenbedingungen durchzuführen ist. Die Übermittlung von klassifizierten Informationen (elektronischer Transport klassifizierter Informationen oder Transport klassifizierter Informationen auf externen Datenträgern außerhalb gesicherter Bereiche bzw. kontrollierter Umgebungen) hat grundsätzlich mittels kryptographischer Produkte und Verfahren, die auf die jeweilige Klassifizierungsstufe abzustimmen und von der ISK zugelassen sind, zu erfolgen. Unverschlüsselte Dateinamen, Überschriften und Beschriftungen etc. dürfen dabei keine Rückschlüsse auf die klassifizierten Inhalte zulassen. Klassifizierte Informationen ab der Klassifizierungsstufe GEHEIM dürfen nur auf Geräten verarbeitet werden, die als abstrahlungsarm deklariert sind. Werden anstelle dessen andere Schutzmaßnahmen ergriffen, kann von einer Verarbeitung auf abstrahlarmen Geräten abgesehen werden. Klassifizierte Informationen der Klassifizierungsstufe STRENG GEHEIM dürfen überdies nicht auf vernetzten Geräten verarbeitet werden
- **Kopien:** Werden Kopien oder Abschriften von Dokumenten der Klassifizierungsstufe VERTRAULICH oder GEHEIM angefertigt, so ist dies in geeigneter Weise festzuhalten und die Kopie als solche zu kennzeichnen und zu registrieren. Jede Kopie ist durch einen geeigneten Zusatz zu individualisieren. Die Anfertigung von Kopien von Informationen der Klassifizierungsstufe STRENG GEHEIM durch Empfänger ist unzulässig. Kopien dürfen ausschließlich unter der unmittelbaren Verantwortung des/der jeweiligen Leiters/Leiterin der Organisationseinheit angefertigt werden. Dokumente der Klassifizierungsstufe EINGESCHRÄNKT, VERTRAULICH oder GEHEIM dürfen nur von solchen Personen kopiert, abgeschrieben, gescannt, archiviert oder verarbeitet werden, welche die Voraussetzungen des § 6 Abs. 1 und 2 erfüllen.

Aufgrund der Lieferung vonseiten des BMJ an den Untersuchungsausschuss in der Klassifizierungsstufe "streng geheim" stellt sich die Frage, wie innerhalb des BMI und BMJ mit denselben Beweismitteln seit deren Sicherstellung umgegangen wurde.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Welche gesetzlichen und sonstigen rechtlichen Bestimmungen sind im Umgang mit Beweismitteln in Ihrem Haus einschlägig?
2. In welchen Fällen werden Beweismittel in jeweils welcher Form unterschiedlich klassifiziert?
 - a. Auf Basis welcher gesetzlichen und sonstigen rechtlichen Bestimmungen geschieht dies jeweils?
3. Wie wird in diesen Fällen jeweils mit den Beweismitteln verfahren?
 - a. Auf Basis welcher gesetzlichen und sonstigen rechtlichen Bestimmungen geschieht dies jeweils?
 - b. Welche Schutzmaßnahmen sehen diese Bestimmungen jeweils vor?
4. Inwiefern werden diese Bestimmungen jeweils in der Praxis umgesetzt?
5. Wann wurden die in der Begründung genannten Akten und Unterlagen ("Ibiza"-Videos samt Transkript) vonseiten des BMI an das BMJ übergeben?
 - a. Durch wen an wen?
6. Nach welchen Bestimmungen wurden die in der Begründung genannten Akten und Unterlagen ("Ibiza"-Videos samt Transkript) klassifiziert?
7. Wer nahm die Klassifizierung aufgrund eines Auftrages von wem wann vor?
8. Welchen organisatorischen Schutzmaßnahmen unterliegen die in der Begründung genannten Akten und Unterlagen ("Ibiza"-Videos samt Transkript) seit wann jeweils?
9. Wer entschied über das Setzen dieser organisatorischen Schutzmaßnahmen aufgrund eines Auftrages von wem jeweils wann?
10. Befinden sich diese Unterlagen in einem besonders geschützten (d.h. solchen die einer ständigen, doppelten Zutrittskontrolle unterliegen) Bereich in einem Sicherheitsbehältnis oder Tresorraum?
11. Werden diese Unterlagen ausschließlich in einem besonders geschützten (d.h. solchen die einer ständigen, doppelten Zutrittskontrolle unterliegen) Bereich bearbeitet?
12. Erfolgt die mündliche Übermittlung von Inhalten nur in geschützten Bereichen und in wie weit ist der Personenkreis, der potentiell Zugang zu diesen Informationen hat in einer den Bestimmungen des InfOG für die Sicherheitsstufe 4 vergleichbaren Art und Weise beschränkt?
13. Erfolgen bei (fern-)mündlicher Übermittlung von Inhalten dieser Dokumente Maßnahmen zum Abhörschutz?
 - a. Wenn ja, welche?
 - b. Werden dabei entsprechende durch die ISK zugelassene kryptographische Methoden angewendet?
14. Werden die Akten und Unterlagen auch elektronisch verarbeitet?

- a. Wenn nein, besteht ein diesbezügliches Verbot?
- 15. Besteht ein Verbot der Anfertigung von Notizen betreffend der Akten und Unterlagen?
- 16. Ist die Anfertigung von Kopien generell unzulässig?
 - a. Wenn nein, unter welchen Bedingungen ist die Anfertigung von Kopien zulässig?
- 17. Hinsichtlich der Fragen 8 bis 16: seit wann gelten die jeweiligen Regularien jeweils?
 - a. Auf welcher Rechtsgrundlage beruhen diese?
 - b. Wer verfügte diese Regularien?
- 18. Welcher Einstufung nach der Geheimschutzordnung des Bundes unterliegen diese Akten und Unterlagen?
 - a. Seit wann unterliegen diese Akten und Unterlagen der genannten Einstufung?
 - b. Kann bestätigt werden, dass sämtlichen in der Geheimschutzordnung des Bundes normierten Regularien für die entsprechende Sicherheitsstufe eingehalten werden?