3799/AB
vom 14.12.2020 zu 3751/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.672.085

Wien, am 14. Dezember 2020

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Dr. Nikolaus Scherak, MA, Douglas Hoyos-Trautt-mansdorff, Kolleginnen und Kollegen haben am 14. Oktober 2020 unter der Nr. **3751/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Jedes Video kann eine Lüge sein: Deepfakes bei Videoüberwachung“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

- *Ist Ihnen bewusst, dass es sich bei Videoüberwachungen im öffentlichen Raum um Fälschungen handeln kann?*

Ja. Zur Analyse der politischen gesellschaftlichen und wirtschaftlichen Risiken durch Deepfakes wurde durch das BMI in Umsetzung der Entschließung vom 14. Oktober 2020 betreffend Entwicklung einer Strategie zur Thematik und Risiken von Deepfakes, eine interministerielle Arbeitsgruppe eingerichtet.

Zur Frage 2:

- *Trifft Ihr Ressort Vorkehrungen, um derartige Deepfakes zu erkennen bzw. zu vermeiden?*
  a. *Wenn ja, welche?*
  b. *Wenn nein, warum nicht?*

Prinzipiell ist zu unterscheiden, ob es sich bei der Videoüberwachung im öffentlichen Raum um ressorteigene Kameras, Übertragungs- und Aufnahmegeräte handelt oder um digitale Medien (Bild, Video, Audio) Dritter.

Die ressorteigenen Kameras, Übertragungs- und Aufnahmegeräte sind mit entsprechenden Sicherheitsmaßnahmen versehen.

Digitale Medien Dritter werden bei Verdacht auf Manipulation mittels forensischer Methoden auf deren Nachbearbeitung überprüft.

Zur Frage 3:

- *Stellt Ihr Ressort fest, ob Videoraufnahmen tatsächlich von der Kamera stammen, von der sie vorgeben zu stammen?*
  a. *Wenn ja, wie?*
  b. *Wenn nein, warum nicht?*

Die ressorteigenen Kameras, Übertragungs- und Aufnahmegeräte verfügen über zusätzliche Sicherheitseinrichtungen, um einen Zugriff von Unbefugten nahezu unmöglich zu machen. Eine Manipulation wäre durch das korrekte Interpretieren der Log- und Videodaten feststellbar.

Bei digitalen Medien Dritter wird bei Zweifel an der Herkunft einer Aufnahme mittels forensischer Methoden geprüft, ob diese tatsächlich vom aufzeichnenden Gerät stammen.

Zur Frage 4:

- *Verfügt Ihr Ressort über Software, um Deepfakes zu erkennen?*
  a. *Wenn ja, um welche Software handelt es sich?*
  b. *Wenn ja, wie ist die Funktionsweise der Software?*

c. Wenn nein, warum nicht?
d. Wenn nein, wie sollen Deepfakes sonst erkannt werden?
e. Wenn nein, ist die Anschaffung einer solchen angedacht?
i. Wenn ja, welche Software soll angeschafft werden und wie ist deren Funktionsweise?

Das Bundesministerium für Inneres verfügt über unterschiedliche forensische Programme. Die Auswahl der zur Anwendung kommenden Programme richtet sich dabei nach dem jeweiligen Anwendungsfall sowie der individuellen Aufgabenstellung. Die Beantwortung der Fragen bezüglich der Nennung der für forensische Zwecke zur Anwendung kommenden Programme sowie deren Funktionsweise kann aus sicherheitspolizeilichen Erwägungen nicht erfolgen.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2020-12-14T15:15:51+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-12-14T15:19:25+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	