3751/J XXVII. GP

Eingelangt am 14.10.2020

Anfrage

der Abgeordneten Dr. Nikolaus Scherak, MA, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesminister für Inneres

betreffend Jedes Video kann eine Lüge sein: Deepfakes bei Videoüberwachung

Jedes Video kann heute eine Lüge sein. Deepfakes wirken wie realistische Aufnahmen - sind aber gefälscht. Inzwischen kann jeder mit entsprechender Software täuschend echt wirkende Videos herstellen, in denen Gesichter von Menschen vertauscht werden, Personen Dinge sagen, die sie nie gesagt haben oder Handlungen vornehmen, die sie nie vollzogen haben. Deepfakes können inzwischen selbst Laien mit kostenlosen Apps produzieren.

Vertrauen genießen heute in der Regel nur noch Live-Videos, etwa von Videoüberwachungsanlagen. Aber nicht immer zu Recht, denn auch hier bestehen Möglichkeiten der Manipulation. So können etwa Objekte oder Personen in das Bild eingefügt werden, ohne dass dies als Fälschung erkennbar wäre. Auch in Hackerkreisen wird öfter debattiert, wie Videoaufnahmen mittels Deepfakes unbrauchbar gemacht werden können. Mittels spezieller Software, die etwa die Schatten im Bild überprüft, können Deepfakes als solche erkannt werden. Jedoch kann dadurch nur aufgezeigt werden, ob Aufnahmen bearbeitet wurden. Nicht feststellbar ist mit dieser, ob es auch wirklich von der Kamera aufgenommen wurde, von der es stammen solle.

Insofern stellt sich die Frage, wie bei Videoüberwachung im öffentlichen Raum festgestellt werden kann, ob eine Aufnahme echt oder gefälscht ist und welche Konsequenzen daraus zu ziehen sind.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Ist Ihnen bewusst, dass es sich bei Videoüberwachungen im öffentlichen Raum um Fälschungen handeln kann?
2. Trifft Ihr Ressort Vorkehrungen, um derartige Deepfakes zu erkennen bzw. zu vermeiden?

a. Wenn ja, welche?
b. Wenn nein, warum nicht?

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