Bayerischer Landtag

18. Wahlperiode 30.08.2019 **Drucksache** 18/**3433**

Schriftliche Anfrage

des Abgeordneten **Christoph Maier AfD**
vom 18.07.2019

Abhörmaßnahmen im „Smart Home“

Vor dem Hintergrund der zunehmenden Digitalisierung im häuslichen Wohnbereich mittels Sprachassistenten wie „Alexa“ frage ich die Staatsregierung:

1. Welche Kenntnisse hat die Staatsregierung über die Speicherfunktionen und Übertragungswege von Geräten und Medien, mit deren Hilfe später und unverzüglich Beweismittel gewonnen werden können (z. B. Handy, Smart-Home-Geräte wie Kühlschränke, Amazon Echo mit Alexa Voice Service, Rechner, Fernseher, Radiogeräte, Feuermelder, elektronische Wasserzähler, Stromzähler, Heizungsmessgeräte etc.)?

2.1 Welche Geräte sind nach Auffassung der Staatsregierung geeignet, um als Speicher- und Übertragungsmedium für Beweismaterial genutzt zu werden (bitte jeweils detailliert mit Funktionsweisen erläutern)?
2.2 Welche Software ist nach Ansicht der Staatsregierung geeignet, um die Daten zu erheben, zu speichern und zu übermitteln?
2.3 Bestehen Pläne, Hersteller zur Änderung ihrer Software und Sicherheitsstrukturen zu zwingen, um auf die Geräte in einer Wohnung zugreifen zu können?

3.1 Sollen Geräte, die heute schon mit einer konzeptionellen Reinheit gestaltet worden und sicher sind, unsicher gemacht werden?
3.2 Sollen private Schlüssel auf Geräten an offizielle Stellen übergeben werden?
3.3 Wie soll verhindert werden, dass durch diese Aufweichung der Sicherheitsstrukturen die Daten vor Manipulation Dritter sicher sind?

4.1 Auf welche Weise sollen die Behörden in Zukunft Zugriff auf das gespeicherte, erhobene und übermittelte Datenmaterial aus Geräten innerhalb der Wohnung erhalten?
4.2 Haben die Behörden schon zum heutigen Zeitpunkt Zugriff auf das gespeicherte, erhobene und übermittelte Datenmaterial aus Geräten innerhalb der Wohnung?

5.1 Welche Geräte können zur Erhebung von Daten und Beweismitteln in der Wohnung genutzt werden, die außerhalb der Wohnung installiert sind?
5.2 Wie fälschungssicher sind die gespeicherten, erhobenen und übertragenen Daten, die als Beweismittel genutzt werden könnten?

6.1 Inwiefern können sich betroffene Bürger darüber versichern, dass die aus ihrer Wohnung gewonnenen Daten definitiv fälschungssicher erhoben, gespeichert und übermittelt wurden?
6.2 Welche Auswirkungen haben mögliche Fälschungen von gespeicherten, erhobenen und übermittelten Daten auf die Beweiskraft vor Gericht?

7. Ab welchem Zeitpunkt müssen Bürger damit rechnen, dass die Behörden über elektronische Geräte innerhalb und außerhalb der Wohnung Zugriff auf ihre Privatsphäre haben?

8.1 Inwiefern sind die Pläne zur Beweismittelerhebung mit Art. 13 Grundgesetz und Art. 106 Bayerische Verfassung vereinbar?
8.2 Welche Position vertritt die Staatsregierung in der Frage einer möglichen Beweiskraft von erhobenen, gespeicherten und übermittelten Daten, die innerhalb und von außerhalb der Wohnung gewonnen werden?

Antwort

des Staatsministeriums des Innern, für Sport und Integration im Einvernehmen mit dem Staatsministerium der Justiz
vom 13.08.2019

1. Welche Kenntnisse hat die Staatsregierung über die Speicherfunktionen und Übertragungswege von Geräten und Medien, mit deren Hilfe später und unverzüglich Beweismittel gewonnen werden können (z. B. Handy, Smart-Home-Geräte wie Kühlschränke, Amazon Echo mit Alexa Voice Service, Rechner, Fernseher, Radiogeräte, Feuermelder, elektronische Wasserzähler, Stromzähler, Heizungsmessgeräte etc.)?
2.1 Welche Geräte sind nach Auffassung der Staatsregierung geeignet, um als Speicher- und Übertragungsmedium für Beweismaterial genutzt zu werden (bitte jeweils detailliert mit Funktionsweisen erläutern)?

Potenziell sind alle technischen Geräte mit Speicherfunktion geeignet, um als Beweismittel im Strafverfahren eingebracht zu werden. Eine abschließende Auflistung ist aufgrund der Vielzahl der weltweit verfügbaren Geräte nicht möglich.

2.2 Welche Software ist nach Ansicht der Staatsregierung geeignet, um die Daten zu erheben, zu speichern und zu übermitteln?

Aufgrund der Vielzahl an weltweiten Anbietern von Beweissicherungs- und Analysesoftware, die ein ähnliches Leistungsspektrum abdecken, wird von einer namentlichen Nennung und/oder Priorisierung der entsprechenden Produkte Abstand genommen.

2.3 Bestehen Pläne, Hersteller zur Änderung ihrer Software und Sicherheitsstrukturen zu zwingen, um auf die Geräte in einer Wohnung zugreifen zu können?
3.1 Sollen Geräte, die heute schon mit einer konzeptionellen Reinheit gestaltet worden und sicher sind, unsicher gemacht werden?
3.2 Sollen private Schlüssel auf Geräten an offizielle Stellen übergeben werden?

Im Hinblick auf die zunehmende Digitalisierung aller Lebensbereiche nimmt die Spurensicherung in der digitalen Welt eine immer größere Bedeutung ein. Die Sicherheits- und Strafverfolgungsbehörden müssen in der Lage sein, digitale Spuren zu erkennen, zu sichern und auszuwerten. Keineswegs sollen jedoch strenge Anforderungen (an z. B. die Wohnraumüberwachung) durch neue Regelungen aufgeweicht oder unsichere Produkte (infolge von sog. backdoors) in Umlauf gebracht werden.

3.3 Wie soll verhindert werden, dass durch diese Aufweichung der Sicherheitsstrukturen die Daten vor Manipulation Dritter sicher sind?

Auf die Ausführungen zu 2.3 bis 3.2 wird verwiesen.

Ungeachtet dessen ist der Schutz des höchstpersönlichen Lebensbereichs der Staatsregierung ein wichtiges Anliegen. Dies wird nicht zuletzt durch die hohen rechtlichen Voraussetzungen der bestehenden Befugnisnormen sowie die dort gesetzlich festgeschriebenen technischen Schutzvorkehrungen deutlich (vgl. etwa Art. 45 Polizeiaufgabengesetz – PAG).

4.1 Auf welche Weise sollen die Behörden in Zukunft Zugriff auf das gespeicherte, erhobene und übermittelte Datenmaterial aus Geräten innerhalb der Wohnung erhalten?

4.2 Haben die Behörden schon zum heutigen Zeitpunkt Zugriff auf das gespeicherte, erhobene und übermittelte Datenmaterial aus Geräten innerhalb der Wohnung?

5.1 Welche Geräte können zur Erhebung von Daten und Beweismitteln in der Wohnung genutzt werden, die außerhalb der Wohnung installiert sind?

Eine pauschale Beantwortung ist losgelöst vom Einzelfall und ohne eingehende Beurteilung sowie Zuordnung des jeweiligen Geräts und dessen Funktionen sowie eines möglichen Zugriffs nicht möglich.

Die rechtlichen Grundlagen unterscheiden grundsätzlich nicht zwischen „smarter“ und „normaler“ Technik oder zwischen digitalen und analogen Beweismitteln. Im Rahmen von Strafverfahren können technische Geräte grundsätzlich vor Ort auf Grundlage von richterlichen Durchsuchungsbeschlüssen sichergestellt/beschlagnahmt und ausgewertet werden, wobei es unbeachtlich ist, ob es sich hierbei um ein älteres Mobiltelefon, ein Smartphone oder ein digitales Assistenzsystem (Amazon Echo mit Alexa, Apple Homepod mit Siri, Google Home etc.) handelt. Anders verhält es sich, wenn Daten nicht lokal gespeichert sind und auch kein entsprechender Zugriff durch das jeweilige Gerät erfolgen kann. Hier kommt es wesentlich auf den Speicherort dieser Daten an. Dieser befindet sich oftmals nicht in Deutschland und ein entsprechender Zugriff steht den deutschen Strafverfolgungsbehörden nur im Rahmen von internationalen Rechtshilfeersuchen zur Verfügung.

Auch im präventivpolizeilichen Bereich können vor diesem Hintergrund im Einzelfall bestimmte Zugriffe in engen rechtlichen Grenzen und unter Einhaltung gesetzlich festgeschriebener technischer Schutzvorkehrungen möglich sein.

Im Übrigen wird auf die Ausführungen zu den Fragen 2.3 bis 3.2 verwiesen.

5.2 Wie fälschungssicher sind die gespeicherten, erhobenen und übertragenen Daten, die als Beweismittel genutzt werden könnten?

6.1 Inwiefern können sich betroffene Bürger darüber versichern, dass die aus ihrer Wohnung gewonnenen Daten definitiv fälschungssicher erhoben, gespeichert und übermittelt wurden?

Digitale Spuren können – ebenso wie Spuren in der analogen Welt – selbst- oder fremdmanipuliert werden. Eine Aufdeckung etwaiger Manipulationen obliegt der digitalen Forensik. Die Feststellung digitaler Spuren wird in der Regel in einem Bericht oder Gutachten der digitalen Forensik dokumentiert und in das Ermittlungsverfahren eingebracht.

6.2 Welche Auswirkungen haben mögliche Fälschungen von gespeicherten, erhobenen und übermittelten Daten auf die Beweiskraft vor Gericht?

Abhängig von der Entdeckung der Manipulation der Daten fließen diese in die Beweiswürdigung des jeweiligen Gerichts ein.

Sollte beispielsweise gutachterlich festgestellt werden, dass Daten manipuliert worden sind, so könnten diese für sich selbst Beweiskraft in diverse Richtungen erlangen oder aber ihre Beweiskraft teilweise oder vollständig verlieren.

7. Ab welchem Zeitpunkt müssen Bürger damit rechnen, dass die Behörden über elektronische Geräte innerhalb und außerhalb der Wohnung Zugriff auf ihre Privatsphäre haben?

Eine pauschale Beantwortung ist losgelöst vom Einzelfall und ohne eingehende Beurteilung und Zuordnung des jeweiligen Geräts und dessen Funktionen sowie des möglichen Zugriffs nicht möglich. Die bestehenden – von der Art des Zugriffs abhängigen – möglichen Befugnisnormen sehen Zugriffe nur in engen rechtlichen Grenzen und unter Einhaltung gesetzlich festgeschriebener technischer Schutzvorkehrungen vor.

8.1 Inwiefern sind die Pläne zur Beweismittelerhebung mit Art. 13 Grundgesetz und Art. 106 Bayerische Verfassung vereinbar?

Gesetzliche Regelungen sind stets so auszugestalten, dass sie mit den verfassungsrechtlichen Vorgaben in Einklang stehen.

8.2 Welche Position vertritt die Staatsregierung in der Frage einer möglichen Beweiskraft von erhobenen, gespeicherten und übermittelten Daten, die innerhalb und von außerhalb der Wohnung gewonnen werden?

Digitale Spuren sind mit zunehmender Digitalisierung der Lebenswirklichkeit von hoher Bedeutung für eine effektive Strafverfolgung. Die Strafverfolgungsbehörden müssen in der Lage sein, digitale Spuren zu erkennen, zu sichern und auszuwerten. Dazu brauchen sie auch in der digitalen Welt geeignete Werkzeuge. Eine Sicherung digitaler Spuren findet nur auf gesetzlicher Grundlage statt. Die bestehenden gesetzlichen Regelungen müssen aber kontinuierlich beobachtet und an die Lebenswirklichkeit angepasst werden.