Kleine Anfrage

Risiken der Digitalisierung (eID)

Frage von	Landtagsabgeordneter Martin Seger
Antwort von	Regierungschefin Brigitte Haas

Frage vom 03. September 2025

Die Digitalisierung entwickelt sich in rasantem Tempo und hält Einzug in allen Lebensbereichen. Diese Schnelligkeit führt unter anderem dazu, dass Gesetze fehlen beziehungsweise Gesetzesanpassungen ins Hintertreffen geraten. Hackerangriffe sind allgegenwärtig. Ein digitaler Identitätsdiebstahl beziehungsweise Identitätsmissbrauch kann beispielsweise gravierende Folgen für Betroffene haben. Die strafrechtliche Verfolgung der Täter im digitalen Raum ist schwierig und teils erfolglos. Das sind erhebliche Risiken, die nebst den Chancen dieser Entwicklung zu beachten sind.

Ein Kleinstaat wie Liechtenstein ist mit derartigen Herausforderungen besonders gefordert. Alternativen zu einem ausschliesslich digitalen Verwaltungsweg sind unter anderem vor diesem Hintergrund wichtig und können als angemessene Risikodiversifikation gesehen werden, so wie es bei der Vermögensverwaltung des Landes als Grundsatz gilt. Der kürzlich im «Vaterland» veröffentlichte Beitrag «Ohne Microsoft steht die Landesverwaltung still» spricht ein digitales Klumpenrisiko an.

* Wie beurteilt die Regierung die Risiken bezüglich digitalem Identitätsdiebstahl beziehungsweise Identitätsmissbrauch generell und explizit in Bezug auf die eID?
* Welche Massnahmen existieren beziehungsweise sind geplant, um vor digitalem Identitätsmissbrauch zu schützen?
* Wird aufgrund der Digitalisierung eine Vielzahl neuer Digitalgesetze nötig sein und wie wird sichergestellt, dass Polizei, Staatsanwaltschaft, Gerichte und so weiter nicht überlastet werden?
* Welche Möglichkeiten bestehen, Täter von digitalem Identitätsdiebstahl beziehungsweise Identitätsmissbrauch zu ermitteln sowie strafrechtlich zur Verantwortung zu ziehen und wie hoch ist die Erfolgsquote bei derartigen Ermittlungen?

* Welche Risiken birgt die Microsoft-Dominanz in der Landesverwaltung bezüglich der kritischen Infrastruktur des Landes und des Tagesgeschäfts in der Verwaltung?

Antwort vom 05. September 2025

zu Frage 1:

Bei regulierten und mit hohen Sicherheits- und Datenschutzstandards umgesetzten elektronischen Identitäten ist das Risiko eines digitalen Identitätsdiebstahles oder Missbrauchs sehr gering. Die Einhaltung dieser Standards sorgt dafür, dass persönliche Daten zuverlässig geschützt sind und unbefugter Zugriff nahezu ausgeschlossen werden kann.

Die liechtensteinische eID, aber auch die gemäss der sogenannten eIDAS-Verordnung der EU im EWR verpflichtend anzuerkennenden europäischen Identifikationsmittel, unterliegen alle einem sehr hohen Sicherheitsstandard.

zu Frage 2:

Um einen digitalen Identitätsdiebstahl bei der eID.li wirksam zu verhindern, wurden auf mehreren Ebenen umfangreiche Sicherheits- und Datenschutzmassnahmen implementiert. Die Massnahmen umfassen ein mehrschichtiges Sicherheitskonzept aus High-Security-Hardware, state-of-the-art Kryptografie, strengen organisatorischen Kontrollen und klaren rechtlichen Vorgaben.

Konkret werden in der eID.li-App kryptografische Schlüssel und technische Informationen verwaltet, um einen sicheren Anmeldevorgang zu garantieren. In der eID.li-App sind mit Ausnahme der digitalen Nachweise, die sogar bei einem Netzausfall verfügbar sein müssen, keine Personendaten gespeichert. So werden die Privatsphäre und persönlichen Daten vor Missbrauch geschützt. Sämtliche Daten, welche im Zusammenhang mit der eID.li verwaltet und eingesetzt werden, befinden sich auf IT-Systemen der Landesverwaltung oder im EWR. Zur Gewährleistung eines hohen Sicherheitsniveaus werden zudem regelmässig Sicherheitsüberprüfungen und Penetrationstests durchgeführt. Es besteht somit ein grösstmöglicher Schutz vor Identitätsmissbrauch.

zu Frage 3:

Der Übergang in die digitale Welt wird seit vielen Jahren - auch in der Gesetzgebung - konsequent verfolgt, auch um so die vielfältigen Chancen zu nutzen. Die Digitalisierung ist ein fortlaufender Prozess, der schon lange die Gesellschaft, Wirtschaft und Verwaltung prägt und durch das E-Government-Gesetz als Rahmengesetz geregelt ist. Die Digitalisierung macht nicht automatisch eine Vielzahl neuer Digitalgesetze notwendig. Stattdessen wird es weiterhin - wie bisher schon - gezielte Gesetzesanpassungen oder Gesetzeserlasse geben – dann, wenn sie tatsächlich erforderlich sind.

Die Landespolizei, die Staatsanwaltschaft und die Gerichte fallen ebenfalls unter den Behördenbegriff des E-Government-Gesetzes. Im Rahmen der Digitalisierung der Strafverfolgungsbehörden ist daher das E-Government-Gesetzes anwendbar. Auch in diesem Bereich wird im Zuge von einzelnen Projektumsetzungen die Rechtslage jeweils spezifisch zu analysieren und im Einzelfall die Notwendigkeit der Schaffung weiterer Rechtsgrundlagen aus Gründen der Rechtssicherheit und Rechtsklarheit zu prüfen sein. Die Digitalisierung soll zu einer Entlastung der Strafverfolgungsbehörden führen.

zu Frage 4:

Bei der Landespolizei gibt es ein Kommissariat «Digitale Kriminalität», welches bei der Kriminalpolizei angesiedelt ist. Wie der Name schon sagt, ist dieses Kommissariat auf die Ermittlung strafbarer Handlungen spezialisiert, die als «Cyberkriminalität» bezeichnet und zusammengefasst werden. Es geht dabei insbesondere um die Nutzung moderner Informations- und Kommunikationstechnologien zur Begehung strafbarer Handlungen, die von Betrügereien über Identitätsdiebstahl bis hin zu Angriffen auf Computersysteme reichen. Im Strafgesetzbuch sowie in Nebengesetzen gibt es zahlreiche Tatbestände, welche diese strafbaren Handlungen unter Strafe stellen. Zu Cyberdelikten publiziert die Landespolizei jedes Jahr eine Statistik in der polizeilichen Kriminalstatistik. Identitätsdiebstahl beziehungsweise Identitätsmissbrauch sind keine eigenständigen Straftatbestände, sondern spezielle Vorgehensweisen im Bereich Cyberbetrug und werden daher nicht separat erfasst und ausgewiesen.

zu Frage 5:

Im Rahmen der Planung und Risikoanalyse für das Projekt «Modern Workplace» der Liechtensteinischen Landesverwaltung wurden gezielte Massnahmen getroffen, um die Risiken einer strategischen Abhängigkeit von einem Anbieter möglichst gering zu halten sowie auch um die Sicherstellung der Datensouveränität zu wahren.

Auch ein Ausstieg aus der Microsoft-Umgebung wurde im Rahmen der Risikoanalyse und Projektplanung grundsätzlich mitgedacht. Es wurde bewusst darauf geachtet, technische Abhängigkeiten zu begrenzen und kritische Prozesse nicht vollständig an Microsoft-Dienste zu binden.

Zentraler Bestandteil dieser strategischen Vorsorge ist die Vorgabe, dass geschäftsrelevante Daten nicht dauerhaft in Microsoft 365 gespeichert, sondern weiterhin in den sogenannten On-Premise-Fachanwendungen der Liechtensteinischen Landesverwaltung abgelegt und gespeichert werden. Zudem betreibt die LLV ein mehrstufiges Backup- und Wiederherstellungskonzept für Cloud-Daten, das eine kontrollierte und vollständige Rückführung von Daten unterstützt.