POSTULATSBEANTWORTUNG

DER REGIERUNG

AN DEN

LANDTAG DES FÜRSTENTUMS LIECHTENSTEIN

BETREFFEND

MASSNAHMEN GEGEN MISSBRAUCH DURCH DEEPFAKES

Behandlung im Landtag	
	Datum
Kenntnisnahme am:	

Nr. 34/2026

INHALTSVERZEICHNIS

Seite

ZUSAMMENFASSUNG

Der Landtag hat in seiner Sitzung vom 1. Oktober 2025 das Postulat «Massnahmen gegen Missbrauch durch Deepfakes» an die Regierung überwiesen. Die Regierung wurde mit diesem Postulat eingeladen, zu prüfen, wie in Liechtenstein verstärkt gegen die zunehmende Verbreitung nicht autorisierter Deepfakes und KI-generierter Inhalte vorgegangen werden kann. Zudem wurde sie gebeten, Massnahmen zu prüfen, um den Missbrauch von Deepfakes und KI-generierten Inhalten zu verhindern und die Bevölkerung sowie Institutionen vor den damit verbundenen Risiken zu schützen. Dabei sollen rechtliche, technische und präventive Massnahmen analysiert werden, um mögliche Handlungsspielräume aufzuzeigen. Insbesondere soll dargestellt werden, welche zusätzlichen rechtlichen und technischen Schritte geeignet wären, um Personen besser zu schützen, die ohne ihre Zustimmung in KI-erzeugten Bildern, Videos oder Audios erscheinen. Zudem ist zu prüfen, inwiefern Plattformen, die solche Inhalte verbreiten, zur Verantwortung gezogen werden können.

In der vorliegenden Postulatsbeantwortung wird nach einleitenden Ausführungen dargelegt, dass Liechtenstein bereits über ein breites nationales Rechtsinstrumentarium gegen missbräuchliche Deepfakes verfügt. Bestimmungen des Persönlichkeits-, Datenschutz-, Medien-, Straf- und Zivilrechts ermöglichen es schon heute, gegen Identitätsmissbrauch, Rufschädigung, Betrug oder politische Manipulation vorzugehen.

Auf europäischer Ebene bilden der Digital Services Act (DSA) und der AI-Act künftig die zentralen Regelwerke für den Umgang mit synthetischen Medien. Der AI-Act enthält erstmals eine einheitliche Legaldefinition von Deepfakes und verpflichtet Anbieter wie Betreiber generativer KI zu klaren Kennzeichnungs- und Transparenzpflichten. Der DSA verpflichtet Online-Plattformen zur Entfernung rechtswidriger Inhalte, zu Melde- und Abhilfeverfahren sowie zur Eindämmung systemischer Risiken wie Desinformation oder Wahlbeeinflussung. Nach der EWR-Übernahme werden diese beiden Rechtsakte auch in Liechtenstein unmittelbar gelten.

Die Regierung nimmt zudem jüngste Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung im Zusammenhang mit nicht einvernehmlichen Deepfake-Anwendungen sowie entsprechende rechtspolitische Diskussionen,

gerade auch innerhalb der Europäischen Union, zur Kenntnis und beobachtet diese fortlaufend; ein nationaler Vorgriff auf laufende europäische Gesetzgebungsprozesse erscheint gegenwärtig nicht angezeigt. Sobald sich gesetzliche Lösungswege in umliegenden Ländern abzeichnen, erwägt die Regierung eine zeitnahe Umsetzung von griffigen Strafbarkeitsnormen, um Betroffene in Liechtenstein schützen zu können.

Technische Schutz- und Erkennungsmethoden – etwa Wasserzeichen, Metadaten, Hash-Verfahren oder Deepfake-Detektoren – bieten zwar gewisse Abwehrmechanismen, ermöglichen aber keinen vollumfänglichen, dauerhaft verlässlichen Schutz. Sie können teilweise umgangen oder manipuliert werden und verlieren durch die rasche Weiterentwicklung generativer Modelle schnell an Wirkung.

Im präventiven Bereich verfügt Liechtenstein über gut ausgebaute Strukturen. Die Fachgruppe Medienkompetenz (FGMK), Schulen und weitere unterstützende Institutionen leisten bereits heute entsprechende Arbeit in den Bereichen Bildung, Sensibilisierung und Medienkompetenz. Schülerinnen und Schüler werden systematisch im kritischen Umgang mit digitalen Inhalten geschult; Eltern und Lehrpersonen erhalten praxisnahe Unterstützung.

Zur Stärkung des Vertrauens in staatliche Institutionen und die Demokratie könnten u.a. eindeutig erkennbare und verifizierte staatliche Kommunikationskanäle, proaktive Information bei Desinformation oder Deepfake-Vorfällen sowie technische Integritätsnachweise wie Signaturzertifikate für amtliche Medieninhalte Inhalte implementiert werden. Ein koordiniertes Zusammenspiel von Recht, Technik, Bildung und Kommunikation wird als zentral erachtet, um Deepfake-Risiken nachhaltig einzudämmen.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Präsidiales und Finanzen (Federführung)
Ministerium für Gesellschaft und Justiz
Ministerium für Inneres, Wirtschaft und Sport
Ministerium für Infrastruktur und Bildung

BETROFFENE STELLEN

Amt für Informatik
Amt für Justiz
Amt für Kommunikation
Landespolizei
Schulamt
Stabsstelle Cyber-Sicherheit
Stabsstelle für Digitale Innovation
Fachgruppe Medienkompetenz

Vaduz, 31. März 2026

LNR 2026-414

P

Sehr geehrter Herr Landtagspräsident,
Sehr geehrte Frauen und Herren Abgeordnete

Die Regierung gestattet sich, dem Hohen Landtag nachstehende Postulatsbeantwortung zu unterbreiten.

I. BERICHT DER REGIERUNG

1. ANLASS

1.1 Postulat vom 26. August 2025

Mit Datum vom 26. August 2025 reichten die Abgeordneten Dagmar Bühler-Nigsch, Tanja Cissé, Dietmar Hasler, Carmen Heeb-Kindle, Manfred Kaufmann, Stefan Öhri, Roger Schädler und Johannes Zimmermann das Postulat: «Massnahmen gegen Missbrauch durch Deepfakes» gestützt auf Art. 44 der Geschäftsordnung des Landtags vom 19. Dezember 2012[1] ein Postulat mit folgendem Wortlaut ein:

«Die Regierung wird gebeten zu prüfen, wie auch in Liechtenstein verstärkt gegen die zunehmende Verbreitung von nicht autorisierten Deepfakes und KI-generierten Inhalten vorgegangen werden kann. Die Regierung wird gebeten, Massnahmen zu

[1] Geschäftsordnung für den Landtag des Fürstentums Liechtenstein vom 19. Dezember 2012, LGBl. 2013 Nr. 9.

prüfen, um den Missbrauch von Deepfakes und KI-generierten Inhalten zu verhindern und die Bevölkerung sowie Institutionen vor den damit verbundenen Risiken zu schützen. Dabei sollen rechtliche, technische und präventive Massnahmen untersucht werden, um mögliche Handlungsspielräume aufzuzeigen. Insbesondere soll dargelegt werden, welche weiteren rechtlichen und technischen Massnahmen möglich sind, um betroffene Personen in Liechtenstein besser zu schützen, die ohne ihre Einwilligung in KI-generierten Inhalten wie Bildern, Videos oder Audios auftauchen. Zudem soll geprüft werden, inwiefern Plattformen, die solche Inhalte verbreiten, zur Verantwortung gezogen werden können.

Begründung:

Die Qualität KI-generierter Die Qualität KI-generierter Inhalte steigt rasant. Stimmen, Gesichter und Bewegungen lassen sich inzwischen so realistisch nachbilden, dass sie für viele kaum noch von echten Aufnahmen zu unterscheiden sind. Damit wächst zugleich das Missbrauchsrisiko: Kriminelle nutzen täuschend echte Stimmen, um insbesondere ältere Menschen am Telefon um ihr Geld zu bringen. In sozialen Netzwerken kursieren gefälschte Nacktbilder oder intime Videos, die ohne Zustimmung Betroffener erstellt werden, oft als Racheaktion nach gescheiterten Beziehungen. Auch die Politik ist nicht gefeit: 2024 sorgte etwa ein Deepfake-Video für Aufsehen, in dem die dänische Premierministerin angeblich Feiertage abschaffen und den Fleiss ihrer Landsleute infrage stellen wollte. In einer Berichterstattung des schweizerischen „Tagesanzeiger" vom 30. April 2024 wurde auch die Meinung von Jesper Taekke, Medienwissenschaftler von der Universität Aarhus wiedergegeben. Er ist der Ansicht, dass solcherlei täuschend echt wirkende Videos das Vertrauen in alle Politiker kategorisch untergraben, weil sie Zweifel daran säten, was und wem man überhaupt noch glauben könne. Um solchen Manipulationen wirksam zu begegnen, plant Dänemark laut verschiedenen Medienberichten ein neues KI-Gesetz. Es soll Betroffenen das Recht geben, die Löschung von Deepfakes, die

ohne ihre Zustimmung erstellt wurden, einzufordern. Plattformen, die solchen Forderungen nicht nachkommen, müssen künftig mit empfindlichen Strafen rechnen. Gemäss der Nachrichtenplattform heise.de sagte der dänische Kulturminister Jakob Engel-Schmidt der britischen Tageszeitung Guardian: "Mit dem Gesetzesentwurf einigen wir uns auf die eindeutige Botschaft, dass jeder das Recht auf seinen eigenen Körper, seine eigene Stimme und seine eigenen Gesichtszüge hat. Das aktuelle Gesetz schützt die Menschen jedoch offenbar nicht vor generativer KI."

Diese Problematik ist auch für Liechtenstein von Relevanz: Aufgrund der überschaubaren politischen Landschaft und der direkten Nähe zwischen Bürgern und Entscheidungsträgern könnten Deepfakes das Vertrauen in Institutionen besonders schnell erschüttern. Umso wichtiger ist es, dass Politik, Medien und Gesellschaft im Land frühzeitig Sensibilität für diese Gefahr entwickeln und Strategien im Umgang mit KI-generierten Inhalten erarbeiten.

Es ist den Postulanten dabei bewusst, dass Liechtenstein aufgrund der Marktgrösse eventuell schlechtere Karten gegenüber weltweit agierenden digitalen Plattformen hat, als beispielsweise ein Land wie Dänemark. Insofern wird die Regierung gebeten, die rechtlichen Möglichkeiten darzulegen und deren Durchsetzbarkeit einzuschätzen sowie allfällige Alternativen aufzuzeigen.»

Der Landtag hat das Postulat in seiner Sitzung vom 1. Oktober 2025 an die Regierung überwiesen.

1.2 Behandlung des Postulats im Landtag vom 1. Oktober 2025

Am 1. Oktober 2025 behandelte der Landtag das Postulat zur Bekämpfung des Missbrauchs durch Deepfakes. Die Debatte zeigte die Einigkeit unter den Abgeordneten: Alle Votanten begrüssten das Postulat und unterstrichen die Dringlichkeit, sich mit den Risiken und Herausforderungen von KI-generierten Inhalten auseinanderzusetzen.

Deepfakes – also künstliche erzeugte, täuschend echte Bilder, Videos und Stimmen – würden eine wachsende Bedrohung für Individuen, Institutionen und die Demokratie darstellen. In den Voten wurde geschildert, wie diese Technologie bereits heute missbraucht würde: Gefälschte Nacktbilder würden als Mittel der Rache verbreitet, täuschend echte Telefonanrufe mit geklonten Stimmen könnten insbesondere ältere Menschen um ihr Erspartes bringen, und manipulierte politische Inhalte würden das Vertrauen in demokratische Prozesse untergraben. In diesem Zusammenhang sei auf den Wahlkampf in Moldau zu verweisen, wo Deepfakes gezielt zur Desinformation und Destabilisierung eingesetzt worden seien.

Einige Abgeordneten betonten, dass Liechtenstein als Kleinstaat besonders anfällig für solche Manipulationen sei. Gerade die Nähe zwischen Bürgern und Politik mache das Vertrauen besonders verletzlich. Gleichzeitig wurde hervorgehoben, dass die Kleinheit des Landes auch eine Chance für schnelle und agile Reaktionen biete.

Inhaltlich deckten sich die Wortmeldungen in mehreren zentralen Bereichen:

Aus rechtlicher Perspektive wurde ausgeführt, dass bestehende Gesetze nur ansatzweise ausreichen würden, um Deepfakes wirksam zu regulieren. Es brauche neue bzw. angepasste rechtliche Grundlagen, insbesondere zum Schutz vor Identitätsdiebstahl und zur Löschung manipulierter Inhalte. Internationale Vorbilder wie Dänemark, Italien und der EU AI-Act (KI-Verordnung) wurden als Referenz genannt. Auch die Frage nach einer klaren Definition von Deepfakes und der Abgrenzung zu Satire und Kunst wurde als zentral erachtet.

Aus technischer Sicht wurde die globale Natur der Plattformen als Herausforderung für die Durchsetzbarkeit nationaler Regelungen erkannt. Dennoch wurde

betont, dass technische Massnahmen mit rechtlichen und gesellschaftlichen Ansätzen kombiniert werden müssten.

Präventiv und gesellschaftlich wurde die Bedeutung von Sensibilisierung und Medienkompetenz hervorgehoben. Besonders Kinder und Jugendliche seien gefährdet, da sie täglich mit KI-generierten Inhalten konfrontiert seien, ohne diese zuverlässig erkennen zu können. Bildungseinrichtungen und Eltern sollen gezielt unterstützt werden, und bestehende Strukturen wie die Stabsstelle Cyber-Sicherheit (SCS) und die Fachgruppe Medienkompetenz könnten ihre Informations- und Aufklärungskampagnen ansprechender und zielgruppenorientierter gestalten.

International und strategisch wurde die Notwendigkeit internationaler Kooperation betont. Zwar wurde anerkannt, dass Liechtenstein als Kleinstaat nur begrenzten Einfluss auf globale Plattformen habe, doch gerade die kurzen Wege und die Agilität des Landes könnten genutzt werden, um frühzeitig und gezielt zu reagieren. Die EU-Regelwerke wie der Digital Services Act und der AI-Act wurden als relevante Rahmenbedingungen genannt, deren Umsetzung in Liechtenstein noch bevorstehe.

In der Debatte wurde festgehalten, dass Deepfakes nicht nur eine technische, sondern auch eine gesamtgesellschaftliche Herausforderung darstellen würden. Es gehe um den Schutz der Menschenwürde.

Das Postulat wurde schliesslich mit 24 Ja-Stimmen an die Regierung überwiesen.

2. ALLGEMEINES

Die zunehmende Verbreitung von KI-generierten Inhalten, insbesondere sogenannter Deepfakes, stellt auch für Liechtenstein eine ernstzunehmende Herausforderung dar. Die Regierung ist sich der Wichtigkeit dieses Themas bewusst und erkennt die potenziellen Risiken, die mit dem Missbrauch solcher Technologien

einhergehen – sei es im Bereich der Cyberkriminalität, der Desinformation oder der Verletzung von Persönlichkeitsrechten.

Deepfakes können in vielfältiger Weise auftreten: manipulierte Videos, gefälschte Audiodateien oder realistisch wirkende Bilder, die Personen in kompromittierenden oder irreführenden Kontexten darstellen. Diese Bandbreite macht es notwendig, sowohl rechtlich als auch technisch und gesellschaftlich breit aufgestellt zu reagieren. Um die Bevölkerung vor dem vielfältigen Missbrauch von künstlich generierten Deepfakes zu schützen, spielen, neben juristischen und technischen Massnahmen, vor allem präventive und aufklärende Massnahmen eine wichtige Rolle.

In der vorliegenden Postulatsbeantwortung behandelt die Regierung die komplexen und vielschichtigen Fragestellungen im Zusammenhang mit KI-Systemen und möglichen Massnahmen gegen den Missbrauch von Deepfakes anhand verschiedener Betrachtungsweisen. Obwohl die Thematik vergleichsweise jungen Ursprungs ist, besteht bereits eine umfangreiche und stetig wachsende Literatur, welche die technische, gesellschaftliche und rechtliche Dimension dieses Themenfelds beleuchtet.

Aufgrund der dynamischen Entwicklung im Bereich der KI-Systeme kann insbesondere in technischer Hinsicht nicht ausgeschlossen werden, dass weitere, vor allem technische Massnahmen in dieser Beantwortung (noch) nicht berücksichtigt werden konnten. Dies ist darauf zurückzuführen, dass laufend neue Erkenntnisse publiziert werden und sich die zugrunde liegenden technologischen Mechanismen und Methoden fortlaufend verändern. Um den Umfang des Postulats in einem sachlich vertretbaren Rahmen zu halten, hat sich die Regierung daher darauf beschränkt, sich an den in der bestehenden Literatur am häufigsten genannten und als wesentlich erachteten Aspekten zu orientieren.

Auch in rechtlicher Hinsicht bestehen weiterhin Unklarheiten, insbesondere aufgrund der fortschreitenden Ausarbeitung der einschlägigen EU-Rechtsakte.[2] Zahlreiche Regelungsinhalte auf EU-Ebene sind noch in Ausarbeitung; weitere Leitlinien und Durchführungsrechtsakte werden erwartet. Zudem wurden die relevanten Rechtsakte bislang nicht in das EWR-Abkommen übernommen. Die Regierung stellt in dieser Postulatsbeantwortung deshalb jeweils den aktuellen Stand der Entwicklungen dar.

3. BEANTWORTUNG DES POSTULATES

Zur Prüfung entsprechender Massnahmen sowie zur Beantwortung der im Postulat und während der Landtagsdebatte aufgeworfenen Fragen ist zunächst zu klären, wie Deepfakes allgemein definiert werden. Danach werden die juristischen Fragestellungen behandelt, bevor sich der Bericht den technischen Aspekten annimmt. Anschliessend werden präventive und gesellschaftliche Massnahmen auf nationaler Ebene erörtert, bevor abschliessend strategische Überlegungen dargestellt werden.

3.1 Allgemeine Definition von Deepfakes

Der Begriff «Deepfake» wird als Überbegriff für verschiedene Formen der audiovisuellen Manipulation einschliesslich Bild, Video und Audio verwendet. Typischerweise wird zur Erstellung von Deepfakes eine auf Künstlicher Intelligenz (KI) basierte Technologie verwendet. Deepfakes sind gefälschte Videos, Bilder oder Audios, in denen Personen Aussagen in den Mund gelegt werden oder in denen sie scheinbar Handlungen begehen, die in Wirklichkeit nie stattgefunden haben. Mit

[2] An dieser Stelle wird auf die Ausführungen unter Punkt 3.6 zu den jüngsten Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung verwiesen, wonach ein Verbot bestimmter KI-Anwendungen, die die Erzeugung nicht einvernehmlicher pornografischer Deepfakes ermöglichen, in die KI-Verordnung aufgenommen werden soll.

leistungsfähigen Verfahren der KI lassen sich Medien in einer Weise manipulieren, sodass zumindest mit blossem Auge nicht mehr zu erkennen ist, ob sie echt sind oder manipuliert wurden. Der Begriff Deepfake setzt sich dabei aus den Begriffen «deep learning» und «fake» zusammen. «Deep learning» ist eine spezielle KI-Technik und «fake» steht für Fälschung oder Falschmeldung. Deepfakes fügen sich ein in eine lange Reihe der medialen Manipulationen zum Zweck der Falsch- oder Desinformation.[3]

3.2 Rechtliche Fragen

3.2.1 Bestehende nationale und staatsvertragliche Rechtsnormen

In der liechtensteinischen Rechtsordnung existiert derzeit keine ausdrückliche gesetzliche Definition des Begriffs «Deepfake». Weder das Strafgesetzbuch noch andere gesetzliche Regelungen enthalten eine Norm, die sich explizit auf KI-generierte oder manipulierte Inhalte bezieht. Gleichwohl bestehen verschiedene nationale und internationale Rechtsnormen bzw. Regelungen, die geeignet sind, die missbräuchliche Verwendung von Deepfakes zu adressieren.

Diese Regelungen umfassen insbesondere die verfassungs- und völkerrechtlich garantierten Persönlichkeitsrechte, das Medienrecht, das Datenschutzrecht, das Strafrecht sowie zivilrechtliche und urheberrechtliche Bestimmungen. Ergänzt werden diese bestehenden Normen durch die schrittweise Übernahme europäischer Digitalisierungsrechtsakte, die künftig ein erweitertes Instrumentarium zur Bekämpfung digitaler Manipulationen bereitstellen sollen.

---

[3] https://www.bmi.gv.at/bmi_documents/2779.pdf, Aktionsplan Deepfake, Bundesministerium für Inneres, S. 8, zuletzt geprüft am 09.03.2026.

Zentraler Ausgangspunkt für den Schutz der Menschenwürde bildet Art. 27bis der Landesverfassung.[4] Diese Bestimmung weist besondere Bezüge zu spezielleren Grundrechten und insbesondere zu den verfassungsrechtlichen Persönlichkeitsrechten auf.[5] Flankiert wird der nationale Grundrechtsschutz durch mehrere völkerrechtliche Instrumente. Die Europäische Menschenrechtskonvention[6] garantiert in Art. 8 das Recht auf Achtung des Privat- und Familienlebens. Der Internationale Pakt über bürgerliche und politische Rechte[7] enthält in Art. 17 einen umfassenden Schutz vor willkürlichen Eingriffen in das Privatleben sowie vor rechtswidrigen Beeinträchtigungen der Ehre und des Rufes. Für Minderjährige stellt die UN-Kinderrechtskonvention[8] mit Art. 8 und Art. 16 den Schutz der Identität und der Privatsphäre sicher und verpflichtet die Vertragsstaaten in Art. 17 zur Gewährleistung eines verantwortungsvollen Umgangs mit Medieninhalten. Diese Bestimmungen entfalten primär Wirkung gegenüber staatlichem Handeln, wirken aber über die zivilrechtlichen Normen der §§ 16 f. und 1328a ABGB[9] auch mittelbar im Privatrechtsverkehr.

Das Mediengesetz (MedienG)[10] enthält Vorschriften, mit denen das Phänomen Deepfake zumindest teilweise adressiert werden kann. So untersagt Art. 6 MedienG Medieninhalte, die die öffentliche Ruhe und Ordnung gefährden. Zudem bestehen nach Art. 82c MedienG Schutzpflichten insbesondere mit Blick auf den Schutz von Minderjährigen. Audiovisuelle Mediendienste und Video-Sharing-Plattform-Dienste müssen demnach angemessene Massnahmen treffen, um

---

[4] Verfassung des Fürstentums Liechtenstein vom 5. Oktober 1921, LGBl. 1921 Nr. 15.

[5] Bussjäger, Peter, Art. 27bis LV, in: Liechtenstein-Institut (Hrsg.): Online-Kommentar zur liechtensteinischen Verfassung, https://verfassung.li/Art._27bis, Ziff. 16 (Stand: 12. April 2017), zuletzt geprüft am 09.03.2026.

[6] Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten, LGBl. 1982 Nr.60/1.

[7] Internationaler Pakt über bürgerliche und politische Rechte vom 16. Dezember 1966, LGBl. 1999 Nr. 58.

[8] Übereinkommen über die Rechte des Kindes vom 20. November 1989, LGBl. 1996 Nr. 163.

[9] Allgemeines bürgerliches Gesetzbuch vom 1. Juni 1811, LGBl. 1811 Nr. 1.

[10] Mediengesetz vom 19. Oktober 2005, LGBl. 2005 Nr. 250.

Minderjährige vor Sendungen, nutzergenerierten Videos und audiovisueller kommerzieller Kommunikation zu schützen, die ihre körperliche, geistige oder sittliche Entwicklung beeinträchtigen können.

Erhebliche Bedeutung für die Regulierung von Deepfakes kommt dem Datenschutzrecht zu. Die Datenschutz-Grundverordnung (DSGVO)[11], welche im EWR unmittelbar gilt und das liechtensteinische Datenschutzgesetz (DSG)[12] stellen ein umfassendes Schutzsystem gegen unerlaubte Verarbeitung personenbezogener Daten bereit. Die Erstellung oder Verbreitung von Deepfakes stellt regelmässig eine Verarbeitung personenbezogener Daten dar und kann durch die in der DSGVO verankerten Betroffenenrechte, insbesondere das Recht auf Löschung nach Art. 17 DSGVO, abgewehrt werden. Bei grenzüberschreitenden Sachverhalten ermöglicht Art. 60 DSGVO die Zusammenarbeit der Aufsichtsbehörden.

Auch das Strafrecht bietet verschiedene Anknüpfungspunkte zur Ahndung des missbräuchlichen Einsatzes von Deepfakes. Das Strafgesetzbuch (StGB)[13] enthält mehrere Tatbestände, unter welche Deepfake-Anwendungen – abhängig vom konkreten Einzelfall – subsumiert werden können. In Betracht kommen insbesondere §§ 105 f. StGB (Nötigung, schwere Nötigung), § 107 StGB (gefährliche Drohung), § 107c Abs. 1 StGB (Cybermobbing), § 108 StGB (Täuschung), § 111 StGB (üble Nachrede), § 112 StGB (Verleumdung), § 126a StGB (Datenbeschädigung), §°144 StGB (Erpressung), §§ 146 ff. StGB (schwerer oder gewerbsmässiger Betrug), § 148a StGB (betrügerischer Datenverarbeitungsmissbrauch), § 218a StGB (Pornografie), § 219 StGB (Kinderpornografie)[14], § 225a (Datenfälschung), § 246

---

[11] Datenschutzverordnung vom 11. November 2018, LGBl. 2018 Nr. 415.

[12] Datenschutzgesetz vom 4. Oktober 2018, LGBl. 2018 Nr. 272.

[13] Strafgesetzbuch vom 24. Juni 1987, LGBl. 1988 Nr. 37.

[14] Aktuell ist eine Anpassung von § 219 StGB in Vorbereitung. Das Delikt von § 219 soll statt «Pornographische Darstellungen Minderjähriger» neu «Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellungen minderjähriger Personen» lauten. Mit einem neuen Abs. 1a soll eine

StGB (Verbreitung falscher Nachrichten bei Wahlen) sowie § 293 StGB (Beweismittelfälschung). Ebenfalls relevant sind Bestimmungen zu unerlaubten Tonbandaufnahmen oder zur Manipulation von Bild- und Videoaufzeichnungen. Ein eigenständiger Straftatbestand «Deepfake» besteht, wie bereits ausgeführt, nicht, doch können Deepfakes als Tathandlung im Rahmen bestehender Delikte erfasst werden. Die strafrechtliche Durchsetzung ist jedoch teilweise erschwert, insbesondere wenn Urheberinnen oder Urheber technisch schwer identifizierbar sind oder es sich um Ermächtigungs- oder Privatanklagedelikte[15] handelt.

Im Bereich des Urheber- und Privatrechts bestehen ebenfalls einschlägige Schutzmechanismen. Das Urheberrechtsgesetz (URG)[16] schützt in Art. 37a die Persönlichkeitsrechte ausübender Künstlerinnen und Künstler, während das Personen- und Gesellschaftsrecht (PGR)[17] in Art. 38 ff. allgemeine Persönlichkeitsrechte im Privatrechtsverkehr garantiert. Das ABGB schützt in § 16 die angeborenen Rechte des Menschen und bildet damit die zentrale Grundlage für Unterlassungs- und Beseitigungsansprüche bei Persönlichkeitsrechtsverletzungen; bei schwerwiegenden Verletzungen der Persönlichkeitsrechte bestehen Ansprüche auf Schadenersatz. Ergänzend kommen insbesondere § 17 ABGB (Schutz persönlicher Eigenschaften) sowie § 1328a ABGB (Bestimmung hinsichtlich Schadenersatz) als Anspruchsgrundlagen in Betracht. § 879 ABGB kann in Fällen sittenwidriger Einwilligungen oder Handlungen zusätzliche Relevanz entfalten. Diese zivilrechtlichen

---

besondere, qualifizierte Strafdrohung vorgesehen werden, wenn bestimmte Tathandlungen in Bezug auf eine «Vielzahl von Abbildungen oder Darstellungen» des Kindesmissbrauchsmaterials begangen werden. Hier dient § 207a öStGB als Vorbild, welcher bereits die Erstellung von bildlichem sexualbezogenem Kindesmissbrauchsmaterial und bildlichen sexualbezogenen Darstellungen minderjähriger Personen unter Strafe stellt.

[15] Die strafrechtliche Verfolgung von Deepfakes kann erschwert oder blockiert sein, weil das Strafrecht verschiedene Deliktskategorien kennt, die unterschiedliche Voraussetzungen für die Einleitung eines Strafverfahrens vorsehen. Sobald der Täter nicht ermittelt werden kann (was bei Deepfakes häufig ist), bringen insbesondere Privatanklage- und Ermächtigungsdelikte erhebliche praktische Vollzugsprobleme mit sich.

[16] Gesetz vom 19. Mai 1999 über das Urheberrecht und verwandte Schutzrechte, LGBl. 1999 Nr. 160.

[17] Personen und Gesellschaftsrecht vom 20. Januar 1926, LGBL. 1926 Nr. 4.

Normen bilden die Grundlage, um gegen unberechtigte Nutzungen, Verfälschungen oder Zuschreibungen von Bild- und Tonmaterial vorzugehen.

Über den bestehenden nationalen Rechtsrahmen hinaus wird die künftige Übernahme europäischer Digitalisierungsrechtsakte zusätzliche Möglichkeiten zur Bekämpfung der missbräuchlichen Verbreitung von Deepfakes schaffen. Besonders relevant in diesem Zusammenhang sind dabei die Verordnung (EU) 2022/2065 (Digital Services Act; DSA)[18] sowie die Verordnung (EU) 2024/1689 (KI-Verordnung; AI-Act)[19]. Diese Regelwerke enthalten spezifische Vorgaben für Plattformbetreiber, KI-Anbieter und Hersteller, etwa in Form von Melde- und Löschpflichten, Transparenzanforderungen oder Risikomanagementpflichten.

In der Gesamtschau zeigt sich somit, dass das geltende liechtensteinische Recht bereits heute verschiedene wirksame Mechanismen zur Bekämpfung von Deepfakes bereitstellt. Die bestehenden Regelungen adressieren sowohl staatliche als auch private Eingriffe und ermöglichen Betroffenen, wirksame Abwehr- und Durchsetzungsansprüche geltend zu machen. Die Hauptprobleme liegen weniger in der Rechtslage als vielmehr in der Identifikation der Urheberschaft und in der praktischen Durchsetzung, insbesondere bei anonymen oder im Ausland ansässigen Tätern. Ob eine spezifische gesetzliche Definition von Deepfakes oder die Einführung eines eigenen Straftatbestands künftig zweckmässig wäre, stellt eine rechtspolitische Frage dar, die auch im Kontext der europäischen Entwicklungen zu beurteilen ist. Gegenwärtig besteht allerdings nach Einschätzung

---

[18] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. 277 vom 27.10.2022, S.1).

[19] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnung (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU/, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024).

der Regierung keine Notwendigkeit für eine entsprechende Legaldefinition oder die Schaffung eines neuen Straftatbestands.

3.2.2 Europäische Digitalisierungsrechtsakte

Auf EU-Ebene werden Deepfakes sowohl indirekt als auch ausdrücklich durch zwei zentrale Rechtsakte adressiert: die Verordnung (EU) 2024/1689 (KI-Verordnung; AI-Act) und die Verordnung (EU) 2022/2065 (Digital Services Act; DSA). Nach ihrer Übernahme in das EWR-Abkommen werden beide Rechtsakte unmittelbar in Liechtenstein Geltung entfalten und damit einen harmonisierten Rechtsrahmen im europäischen Binnenmarkt gewährleisten. Aufgrund der zentralen Aufsichtskompetenz der EU-Kommission werfen sowohl die KI-Verordnung als auch der DSA grundlegende Fragen der Zwei-Pfeiler-Struktur des EWR auf, weshalb sich die EWR-Übernahme verzögert. Mit einer Übernahme ist realistischerweise nicht vor Ende 2026 zu rechnen. Ergänzend zu diesen EU-Regelungen ist auch die «KI-Konvention des Europarates (Framework Convention on Artificial Intelligence)»[20] zu berücksichtigen, welche ebenfalls Anforderungen an Transparenz-, Aufsichts- und Risikomanagementmechanismen im Umgang mit KI-generierten Inhalten – einschliesslich Deepfakes – stellt.

3.2.2.1 KI-Verordnung

Die KI-Verordnung enthält erstmals konkrete Regeln für den Umgang mit Deepfakes. Insbesondere führt die KI-Verordnung eine Definition von Deepfakes ein, die für die weitere rechtliche Behandlung von grosser Bedeutung ist. Nach der EWR-Übernahme wird diese Definition im Rahmen des Anwendungsbereichs der KI-Verordnung auch in Liechtenstein Geltung erlangen. Damit wird im gesamten

[20] Rahmenübereinkommen des Europarates über künstliche Intelligenz, Menschenrechte, Demokratie und Rechtsstaatlichkeit (SEV Nr. 225) vom 17. Mai 2024.

EWR ein einheitliches Verständnis für Deepfakes erzeugt, was die grenzüberschreitende Kooperation und Verfolgung von rechtswidrigen Deepfakes erleichtern soll. Als Deepfake im Sinne der KI-Verordnung ist zu verstehen: *«[…] einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäss erscheinen würde.»*[21]

Die KI-Verordnung beinhaltet Transparenzpflichten[22], wonach zwischen Anbietern, die KI-Systeme bereitstellen, und Betreibern, die solche Systeme eigenverantwortlich einsetzen, zu unterscheiden ist. Anbieter im Sinne der Verordnung sind alle Personen, Unternehmen oder öffentlichen Stellen, die ein KI-System entwickeln oder unter ihrem eigenen Namen in Verkehr bringen. Sie tragen insbesondere Verantwortung für KI-Systeme, die künstliche Inhalte erzeugen – also Texte, Bilder, Audio- oder Videodateien. Nach Art. 50 Abs. 2 AI-Act müssen solche Anbieter sicherstellen, dass diese Inhalte klar als künstlich erzeugt oder verändert erkennbar sind. Vorgesehen ist eine technische Kennzeichnung, die maschinenlesbar ist und insbesondere Plattformen ermöglicht, solche Inhalte automatisch zu erkennen und auszulesen. Wer ein System bereitstellt, das Deepfakes erzeugen kann, hat demnach die Pflicht, sicherzustellen, dass alle damit erstellten Inhalte eindeutig als KI-generiert gekennzeichnet sind.

Zudem verpflichtet die KI-Verordnung (Art. 13 und 26 AI-Act) auch die Betreiber, die KI-Systeme selbst einsetzen, zu besonderen Transparenzpflichten. Betreiber sind Unternehmen und Behörden, die solche Systeme in ihrem eigenen Aufgabenbereich verwenden. Werden Inhalte mit Hilfe eines KI-Systems erzeugt oder manipuliert, müssen Betreiber offenlegen, dass es sich nicht um reale, sondern um

---

[21] Verordnung (EU) 2024/1689, Art. 3 Ziff. 60.

[22] Verordnung (EU) 2024/1689, Art. 13, 26, 50, 52.

künstliche Inhalte handelt. Dies betrifft insbesondere Deepfakes sowie andere synthetische Darstellungen, die für Nutzerinnen und Nutzer ohne Hinweis nicht als künstlich erkennbar wären. Art. 50 Abs. 4 AI-Act verpflichtet Betreiber dazu, die künstliche Erzeugung oder Veränderung solcher Inhalte deutlich offenzulegen, sodass eine Verwechslung mit echten Aufnahmen ausgeschlossen ist.

Ergänzend dazu verlangt die Verordnung gemäss Art. 50 Abs. 1, dass Anbieter von interaktiven KI-Systemen – etwa Chatbots – sicherstellen, dass Personen erkennen können, dass sie mit einem KI-System kommunizieren. Für besonders eingriffsintensive Systeme wie Emotionserkennung oder biometrische Kategorisierung gilt darüber hinaus, dass betroffene Personen über deren Einsatz informiert werden müssen und die Verarbeitung personenbezogener Daten im Einklang mit den einschlägigen Datenschutzvorgaben zu erfolgen hat (Art. 50 Abs. 3 AI-Act).

Hinsichtlich möglicher Manipulationen mit politischem Inhalt reagiert die KI-Verordnung durch klare rechtliche Vorgaben: Deepfakes müssen nach Art. 50 Abs. 4 AI-Act stets eindeutig als künstlich erzeugt oder manipuliert kenntlich gemacht werden, damit sie nicht mit echten politischen Aussagen oder Ereignissen verwechselt werden können. Ergänzend verbietet Art. 5 AI-Act manipulative KI-Techniken, die darauf abzielen, Menschen in ihrer Entscheidungsfindung zu beeinflussen. Zusammengenommen führen diese Verpflichtungen dazu, dass KI-Systeme, die potenziell zur Wahlbeeinflussung eingesetzt werden könnten, besonders streng reguliert werden.

Die KI-Verordnung ist im Kern ein Instrument der staatlichen Aufsicht und Produktsicherheit. Sie setzt verbindliche Regeln für Entwicklung und Einsatz von KI und sieht bei Verstössen empfindliche Bussgelder vor. Ergänzend dazu eröffnet die Verordnung einen begrenzten individuellen Rechtsschutz. Personen können sich

bei der zuständigen Aufsichtsbehörde[23] beschweren, wenn sie den Eindruck haben, dass gegen die Vorgaben der KI-Verordnung verstossen wurde. Gerade im Zusammenhang mit Deepfakes ist diese Durchsetzungsmöglichkeit von Bedeutung. Zugleich ist zu berücksichtigen, dass die KI-Verordnung nicht jeden denkbaren Anwendungsfall erfasst. Private Nutzungen durch Einzelpersonen, die ausschliesslich im persönlichen und nicht beruflichen Kontext erfolgen, fallen grundsätzlich nicht unter die Verordnung. So können etwa manipulierte private Grussbotschaften oder private Deepfakes – einschliesslich solcher aus dem intimen Bereich[24] – ausserhalb des Anwendungsbereichs liegen. Werden solche Inhalte jedoch öffentlich verbreitet oder einer grösseren Personengruppe zugänglich gemacht, handelt es sich in der Regel nicht mehr um eine rein private Tätigkeit. In diesen Fällen greift die KI-Verordnung.

3.2.2.2 Digital Services Act

Der Digital Services Act schafft einen unionsweiten Rahmen für Online-Plattformen, die als zentrale Verbreitungskanäle von Deepfakes gelten. Er enthält keine eigene Deepfake-Definition und keine Spezialnorm, adressiert Deepfakes aber mittelbar über horizontale Sorgfalts-, Transparenz- und Risikomanagementpflichten[25]. Massgeblich ist die Einordnung des konkreten Inhalts: rechtswidriger Inhalt

---

[23] Die Behördenstruktur für die Durchführung der KI-Verordnung wird derzeit noch erarbeitet und steht noch nicht abschliessend fest. Aller Voraussicht nach wird es mehrere zuständige Behörden geben (Marktüberwachungsbehörde, zentrale Anlaufstelle, Datenschutzstelle, etc.).

[24] Zukünftig soll dies jedoch dahingehend eingeschränkt werden, in dem die KI-Verordnung dahingehend abgeändert bzw. ergänzt wird, dass KI-Systeme verboten werden, welche sexuelle Darstellungen realer Personen künstlich erzeugen, es sei denn, die betroffene Person hat vorgängig ausdrücklich zugestimmt. An dieser Stelle wird auf die Ausführungen unter Punkt 3.6 zu den jüngsten Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung verwiesen.

[25] Mit «horizontalen Sorgfalts-, Transparenz- und Risikomanagementpflichten» sind im Rahmen des DSA jene allgemeingültigen, inhaltsunabhängigen Verpflichtungen gemeint, die für sämtliche Plattformen und für alle Arten von Inhalten gelten. «Horizontal» bedeutet, dass diese Pflichten nicht auf bestimmte Inhalte – wie etwa Deepfakes – zugeschnitten sind, sondern plattformweit greifen und ein systematisches Vorgehen gegen rechtswidrige oder risikobehaftete Inhalte insgesamt sicherstellen sollen.

(z.B. Persönlichkeitsrechtsverletzung, Betrug, Urheberrechtsverstoss) oder schädlicher, aber nicht per se illegaler Inhalt, der als systemisches Risiko gilt (z.B. Desinformation, Beeinträchtigung demokratischer Prozesse).

Für rechtswidrige Inhalte verpflichtet der DSA Hosting-Dienste[26] und Online-Plattformen zu leicht zugänglichen Melde- und Abhilfeverfahren (Notice-and-Action; Art. 16 DSA) und zur Begründung ihrer Entscheidungen gegenüber Meldenden (Art. 17 DSA). Erlangen die Plattformen Hinweise auf Straftaten mit Gefährdung für Leben oder Sicherheit, müssen sie die zuständigen Strafverfolgungsbehörden informieren (Art. 18 DSA). Liegt eine Bestätigung der Rechtswidrigkeit vor, haben die Plattformen den betreffenden Inhalt zu sperren oder zu entfernen. Diese Mechanismen greifen auch bei Deepfakes, soweit sie gegen EU- oder nationales Recht verstossen.

Als systemisches Risiko behandelt der DSA insbesondere die Verbreitung rechtswidriger Inhalte, Beeinträchtigungen von Grundrechten, Risiken für Wahlprozesse und die öffentliche Sicherheit sowie Desinformation – Bereiche, zu denen massenhaft verbreitete Deepfakes typischerweise beitragen. Sehr grosse Online-Plattformen und -Suchmaschinen mit 45 Mio. und mehr monatlich aktiven Nutzern müssen daher regelmässig systemische Risiken bewerten (Art. 34 DSA) und wirksame Risikominderungsmassnahmen ergreifen (Art. 35 DSA), etwa Anpassungen der Empfehlungslogik, Dämpfung viraler Verbreitung, verstärkte Moderation, Kooperation mit vertrauenswürdigen Hinweisgebern[27] und Fact-Checking-Stellen[28]. Art. 35 Abs. 1 Bst. k DSA nennt ausdrücklich die Kennzeichnung von Deepfakes als

[26] Hosting Dienste sind Dienste, die nutzergenerierte Inhalte Speichern: Bspw. Facebook, Instagram, TikTok, YouTube etc.

[27] Vertrauenswürdige Hinweisgeber sind staatlich anerkannte Expertenorganisationen, deren Meldungen Plattformen prioritär bearbeiten müssen.

[28] Fact-Checking-Stellen sind unabhängige Prüfinstanzen, die Plattformen bei der Erkennung von Falschinformationen – darunter Deepfakes – unterstützen.

geeignete Massnahme, wenn Nutzer solche Inhalte sonst für echt halten könnten. Der DSA adressiert damit primär die Pflichten der Plattformen und nicht einzelner Nutzer. Nutzerpflichten ergeben sich mittelbar aus den Allgemeinen Geschäftsbedingungen (AGB) der entsprechenden Plattformen.

Die Beaufsichtigung bzw. Durchsetzung erfolgt für sehr grosse Online-Plattformen und -Suchmaschinen zentral durch die EU-Kommission, für andere kleinere Dienste durch nationale Koordinatoren, sogenannte «Koordinatoren digitaler Dienste»[29]. Bei Verstössen drohen hohe Bussgelder.

Der DSA ist in der EU bereits vollumfänglich wirksam. Die Verordnung befindet sich derzeit noch im EWR-Übernahmeprozess. Nach der Übernahme wird auch in Liechtenstein ein «Koordinator digitaler Dienste» eingerichtet. Dieser soll bei der Stabsstelle für Digitale Innovation (SDI) angesiedelt werden. Aufgrund der zentralen und ausschliesslichen Aufsichtskompetenz der EU-Kommission über sehr grosse Online-Plattformen und -Suchmaschinen wirft der Rechtsakt grundsätzliche Fragen der Aufgabenverteilung und Aufsichtskompetenzen im Zwei-Pfeiler-System des EWR auf. Diese Fragen sind derzeit Gegenstand der Diskussionen rund um die EWR-Übernahme mit der EU-Kommission.

3.2.2.3 Bedeutung der KI-Verordnung und des Digital Services Acts für Liechtenstein

Liechtenstein ist aufgrund seiner kleinen Marktgrösse sowie der engen wirtschaftlichen und regulatorischen Verflechtung mit dem EWR darauf angewiesen und verpflichtet, sich an den europäischen Regulierungsrahmen zu halten. Dies gilt insbesondere im digitalen Raum, in dem nationale Alleingänge angesichts global

[29] Zentrale nationale Aufsichts- und Koordinationsbehörde nach Art. 49 DSA für die Durchsetzung des DSA.

operierender Plattformen nicht zielführend sind. Die EU hat diese Problematik erkannt und mit dem DSA und dem AI-Act umfassende Vorgaben für Transparenz, Risikomanagement und Aufsicht bei der Verbreitung synthetischer Inhalte geschaffen. Da diese Instrumente extraterritorial wirken und auch ausserhalb der EU ansässige Anbieter verpflichten, ist für Liechtenstein eine aktive Mitwirkung an den europäischen und internationalen Kooperationsmechanismen zwingend, um eine durchsetzbare Handhabe gegenüber weltweit tätigen Plattformen sicherzustellen.

Der DSA und der AI-Act schaffen dabei die zentralen Rahmenbedingungen. Das «Marktortprinzip»[30] des DSA stellt auf die Ausrichtung eines Dienstes auf den Binnenmarkt ab und führt dazu, dass auch globale Plattformanbieter wie Meta, TikTok oder X den Pflichten des DSA unterliegen. Hierzu gehören insbesondere risikobasierte Vorgaben zur Identifikation, Eindämmung und Kennzeichnung manipulierter oder KI-generierter Inhalte. Für die grenzüberschreitende Aufsicht der sehr grossen Online-Plattformen und -Suchmaschinen ist die EU-Kommission zuständig. Unterstützt wird diese durch das «European Board for Digital Services (EBDS)» [31], in dem die nationalen Koordinatoren digitaler Dienste und die EU-Kommission Einsitz nehmen.

Der AI-Act ergänzt diese Vorgaben um spezifische Transparenzpflichten für generative KI. Ein erster Entwurf des «Verhaltenskodex zur Transparenz von KI-generierten Inhalten»[32] legt technische und organisatorische Mindeststandards für die Kennzeichnung synthetischer Inhalte – etwa über maschinenlesbare

---

[30] Vgl. Verordnung (EU) 2022/2065 (Digital Services Act), Erwägungsgrund 7 und 8.

[31] Art. 61 DSA (Verordnung (EU) 2022/2065; Europäische Kommission, European Board for Digital Services.

[32] Der Entwurf kann über diese Webseite bezogen werden https://digital-strategy.ec.europa.eu/de/library/first-draft-code-practice-transparency-ai-generated-content, zuletzt geprüft am 09.03.2026. Der Zeitplan für die Finalisierung kann hier abgerufen werden https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content, zuletzt geprüft am 09.03.2026.

Wasserzeichen oder Metadaten – fest und soll Anbieter und Betreiber bei der Erfüllung ihrer Pflichten unterstützen. Mit der finalen Version des Kodex wird im Juni 2026 gerechnet. Zusätzlich veröffentlicht die EU-Kommission Leitlinien, die zentrale Begriffe, den Anwendungsbereich sowie Ausnahmen präzisieren und damit eine kohärente Anwendung in allen Mitgliedstaaten fördern.[33] Diese international abgestimmten Mechanismen unterstützen die effiziente Erkennung und Einordnung von Deepfakes über Plattformgrenzen hinweg und erhöhen die Rechtssicherheit für Anbieter ebenso wie für Aufsichtsbehörden.

3.2.2.4 Integration des AI-Act und DSA in die nationale Gesetzgebung

Nach ihrer Übernahme in das EWR-Recht gelten sowohl der AI-Act als auch der DSA unmittelbar in Liechtenstein und werden damit Bestandteil des nationalen Rechts; die materiellen Verpflichtungen sind direkt anwendbar. Ergänzend ist für beide Verordnungen die Schaffung nationaler Durchführungsgesetze erforderlich. Diese sind bei der Übernahme von EU-Rechtsakten in den EWR der übliche Standard und regeln insbesondere jene Aspekte, die sich nicht unmittelbar aus der Verordnung ergeben – namentlich die Zuständigkeiten der nationalen Behörden, die Sanktionsbestimmungen, den Ablauf der nationalen und internationalen Zusammenarbeit, sowie verfahrensrechtliche Einzelheiten. Die Ausarbeitung dieser Durchführungsgesetze erfolgt parallel zu den laufenden EWR-Übernahmeverfahren und ist inhaltlich an diese gekoppelt.

---

[33] Beispiele hierfür sind die Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäss der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act, zuletzt geprüft am 09.03.2026, oder die Leitlinien der Kommission zur Definition eines Systems der künstlichen Intelligenz gemäss der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application, zuletzt geprüft am 09.03.2026.

Die Frage der Aufsicht ist derzeit Gegenstand grundlegender Gespräche. Beide Verordnungen sehen teilweise eine unmittelbare Aufsicht der EU-Kommission vor. Diese kollidiert jedoch mit der Zwei-Pfeiler-Struktur des EWR, weshalb die EWR-EFTA-Staaten in einer gemeinsamen Task-Force Lösungsvorschläge erarbeitet haben, die gegenwärtig mit der EU-Kommission abgestimmt werden. Die Zeitpläne für die Übernahme des AI-Act und des DSA in das EWR-Abkommen hängen wesentlich von diesen Verhandlungen ab; aus heutiger Sicht ist nicht mit einer Übernahme vor Ende 2026 zu rechnen.

3.2.3 KI-Konvention des Europarats

Die KI-Konvention des Europarates (CAI-HR) ergänzt den europäischen Rechtsrahmen, indem sie einen völkerrechtlich bindenden, technologieneutralen Rahmen vorgibt, der den gesamten Lebenszyklus von KI-Systemen an Menschenrechten, Demokratie und Rechtsstaatlichkeit ausrichtet. Sie enthält, anders als die EU-Regelwerke, keine spezifischen Bestimmungen zu Deepfakes, verpflichtet die Vertragsstaaten aber dazu, angemessene Transparenz- und Aufsichtsmechanismen für KI-generierte Inhalte vorzusehen (Art. 8 CAI-HR). Besonders geschützt werden sollen demokratische Prozesse (Art. 5 CAI-HR) und die Menschenwürde (Art. 7 CAI-HR), womit die Konvention denselben sensiblen Bereich adressiert wie der AI-Act und der DSA. Zudem verlangt sie ein Risikomanagementsystem, das Risiken identifiziert und mindert – ein Ansatz, der dem risikobasierten Regulierungsmodell des AI-Act und den systemischen Risikopflichten des DSA entspricht. Liechtenstein hat die KI-Konvention am 27. Februar 2025 unterzeichnet, wobei die Ratifikation noch geprüft wird.

3.2.4 Einordnung der EU-Digitalisierungsrechtsakte und KI-Konvention des Europarates im Zusammenhang mit nationalen Bestimmungen

Der AI-Act, der DSA und die KI-Konvention bilden zusammen einen abgestuften europäischen Regulierungsrahmen für den Umgang mit künstlich erzeugten oder manipulierten Inhalten. Der DSA adressiert insbesondere Plattformen und deren Sorgfaltspflichten, der AI-Act regelt Entwicklung und Einsatz von KI-Systemen und verpflichtet Anbieter wie Betreiber zu Transparenz und Kennzeichnung, während die KI-Konvention eine übergeordnete menschenrechtliche Leitnorm[34] setzt. Diese Instrumente ergänzen einander, sind jedoch bewusst nicht als vollständige Regelung aller denkbaren Missbrauchsformen ausgestaltet, sondern als Rahmen, der durch die nationalen Rechtsordnungen konkretisiert und ergänzt wird.

Für die Frage eines wirksamen Schutzes vor missbräuchlichen Deepfakes ist daher nicht entscheidend, dass die europäischen Instrumente für sich allein keinen lückenlosen Schutz gewährleisten, sondern ob das nationale Recht die in der Praxis relevanten Fallkonstellationen bereits abdeckt. Die Regierung hat dies geprüft und kommt zum Ergebnis, dass die bestehenden liechtensteinischen Bestimmungen, insbesondere im Straf-, Datenschutz-, Medien- und Persönlichkeitsrecht, gegenwärtig ausreichend sind, um rechtswidrige Deepfake-Konstellationen zu erfassen und Betroffenen wirksame Abwehr- und Durchsetzungsmechanismen zur Verfügung zu stellen.[35] Auf dieser Grundlage sieht die Regierung derzeit keinen Bedarf, nationale Regelungen anzupassen oder zu erweitern.

---

[34] Die KI-Konvention setzt – anders als DSA und AI-Act – übergeordnete menschenrechtliche, demokratische und rechtsstaatliche Grundpflichten. Sie wirkt damit wie eine Leitnorm, weil sie die Grundprinzipien definiert, an denen sich technische und regulatorische Detailnormen orientieren müssen.

[35] An dieser Stelle wird auf die Ausführungen unter Punkt 3.6 zu den jüngsten Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung verwiesen.

Wollte man ungeachtet dieser Einschätzung der Regierung dennoch eine Anpassung oder Erweiterung bestehender Rechtsnormen vornehmen, würde sich anschliessend die weitergehende Frage stellen, wie solche rechtspolitischen Überlegungen konkret auszugestalten wären und welche Handlungsoptionen sich daraus ergeben würden. Dies beträfe insbesondere die Bestimmung des Regelungsziels, die Abgrenzung zu bereits bestehenden Normen, die Vereinbarkeit mit den unionsrechtlichen Vorgaben sowie die praktische Durchsetzbarkeit. Diese Fragen sollen im nachfolgenden Punkt 3.2.5 exemplarisch beleuchtet werden.

3.2.5 Nationale Regelungen von Deepfakes über die unionsrechtlichen Vorgaben hinaus

Ob über die unionsrechtlichen Vorgaben hinaus weitergehende nationale Regelungen geschaffen werden sollen, ist eine rechtspolitische Frage. Sie liegt im politischen Ermessen des nationalen Gesetzgebers und muss dementsprechend auf nationaler Ebene adressiert werden. Eine solche Entscheidung würde auf politischen Zielsetzungen beruhen, etwa einen erweiterten Schutzrahmen einzuführen oder bestimmte Risiken stärker zu gewichten. In anderen europäischen Staaten werden vergleichbare rechtspolitische Fragen bereits aufgegriffen, indem neue Straftatbestände geschaffen, bestehende Strafnormen gezielt erweitert oder Urheber- und Persönlichkeitsrechte fortentwickelt werden. Die unterschiedlichen nationalen Ansätze verdeutlichen allerdings, dass bislang keine einheitliche Herangehensweise besteht.

Nachfolgend wird beispielhaft aufgezeigt, welche unterschiedlichen Ansätze europäische Staaten im Umgang mit missbräuchlichen Deepfake-Konstellationen verfolgen: Während einzelne Staaten Anpassungen vorgenommen und neue Normen geschaffen haben, werden entsprechende Vorstösse in anderen Staaten aktuell noch diskutiert; weitere Staaten haben zwar Vorstösse lanciert, letztlich jedoch von einer Abänderung ihres nationalen Rechts abgesehen.

3.2.5.1 Fortentwicklung der Urheber- und Persönlichkeitsrechte

Hinsichtlich der Fortentwicklung der nationalen Urheber- und Persönlichkeitsrechte kann der derzeit diskutierte dänische Vorstoss zu einem weitreichenden Deepfake- bzw. KI-Identitäts-Schutzgesetz als Beispiel dienen. Hierzu ist zunächst festzuhalten, dass bislang weder eine geprüfte noch eine autorisierte deutschsprachige Fassung des dänischen Entwurfs vorliegt; ein präziser Rechtsvergleich wurde daher nicht vorgenommen. Die nachfolgenden Ausführungen sind folglich rein orientierend zu verstehen.

Nach dem derzeit bekannten Regelungsansatz soll das dänische Urheber- und Persönlichkeitsrecht dahingehend fortentwickelt werden, dass der nicht einwilligungsbasierte Einsatz von Aussehen, Stimme und weiteren identitätsprägenden Merkmalen natürlicher Personen in öffentlich verbreiteten KI-generierten Inhalten untersagt wird. Vorgesehen sind ein materielles Verwertungs- und Veröffentlichungsverbot für realistische Deepfake-Imitationen sowie ein zusätzlicher Schutz digital nachgebildeter künstlerischer Darbietungen.[36] Die Durchsetzung soll über subjektive Rechte, Unterlassungs- und Beseitigungsansprüche sowie gegebenenfalls Schadenersatz erfolgen. Dieser Ansatz geht damit über die Systematik der KI-Verordnung hinaus, die primär auf Transparenz- und Kennzeichnungspflichten abstellt und kein generelles Verbot der Nutzung persönlicher Identitätsmerkmale ohne Zustimmung enthält.[37]

Während die KI-Verordnung typischerweise am KI-System und dessen Anbieter oder Betreiber anknüpft, fokussiert sich der dänische Entwurf auf das hergestellte Produkt (die konkrete digitale Imitation) und adressiert damit einen Bereich, der

---

[36] https://www.heise.de/news/Daenemark-will-Persoenlichkeitsrechte-gegen-Deepfakes-staerken-10463430.html, zuletzt geprüft am 09.03 2026.

[37] https://www.swr.de/kultur/gesellschaft/daenemark-ki-gesetz-kampf-gegen-deepfakes-100.html, zuletzt geprüft am 09.03 2026.

vom europäischen Rahmen nicht geregelt ist.[38] Den betroffenen Personen wird faktisch eine urheberrechtsähnliche Rechtsposition am eigenen Bild, an der eigenen Stimme und an typprägenden Merkmalen eingeräumt. Ein solcher Ansatz könnte – sofern tragfähig umgesetzt – als Referenzmodell für künftige nationale oder europäische Regelungen zur Sicherung digitaler Identitätsrechte dienen.

Gleichwohl hat dieser Ansatz auch seine Grenzen. Insbesondere die grenzüberschreitende Durchsetzbarkeit wäre bei einer rein nationalen Regelung angesichts globaler Plattformstrukturen und multipler Veröffentlichungswege deutlich eingeschränkt, weshalb eine solche Regelung nur dann eine tiefergehende Wirkung entfalten würde, wenn sie auf europäischer Ebene beschlossen werden würde.[39] Zudem ist bis anhin fraglich, ob derartige nationale Vorstösse der vollharmonisierenden Wirkung der KI-Verordnung nicht zuwiderlaufen und entsprechend unzulässig sind.

3.2.5.2 Erweiterung bestehender Strafnormen bzw. Schaffung neuer Strafnormen

In Deutschland und Italien stellte sich die Frage, ob der nationale Gesetzgeber über die unionsrechtlichen Vorgaben des AI-Act und des DSA hinaus strafrechtliche Regelungen für besonders sensible, intime Deepfakes schaffen solle – zumal die KI-Verordnung keinen eigenständigen Straftatbestand für derartige Konstellationen vorsieht. Dazu kann zunächst folgendes festgehalten werden:

---

[38] https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id/, zuletzt geprüft am 09.03 2026.

[39] https://www.swr.de/kultur/gesellschaft/daenemark-ki-gesetz-kampf-gegen-deepfakes-100.html, zuletzt geprüft am 09.03 2026.

Die KI-Verordnung enthält bzw. begründet grundsätzlich keine strafrechtlichen Tatbestände. Sie führt also keinen eigenen Straftatbestand[40] ein und regelt nicht, dass jemand wegen «Deepfake» strafrechtlich verfolgt werden kann. Stattdessen ist sie vor allem ein Regelwerk für Aufsicht- und Produktregulierung: Sie legt Pflichten fest (Kennzeichnungs- und Informationspflichten) und sieht bei Verstössen vor allem verwaltungsrechtliche Konsequenzen vor, etwa Aufsichtsmassnahmen und Geldbussen. Die KI-Verordnung unterscheidet damit nicht, ob ein Deepfake «harmlos» ist oder ob er besonders intime Bereiche betrifft. Das bedeutet, dass auch Deepfakes, die stark in die Privat- oder Intimsphäre eingreifen, grundsätzlich unter dieselben Regeln fallen – etwa unter die Pflicht, Deepfakes als künstlich zu kennzeichnen bzw. offenzulegen, sofern die Voraussetzungen erfüllt sind. Im Einzelfall müsste jedoch geprüft werden, wer den Deepfake erstellt und wofür: Wenn eine natürliche Person Deepfakes ausschliesslich privat im persönlichen Bereich erstellt oder nutzt, kann dies zur Folge haben, dass die KI-Verordnung nicht zur Anwendung gelangt. Allfällige Schutzlücken wären dann über anderweitige nationale Rechtsinstrumente (insbesondere Straf-, Zivil- oder Datenschutzrecht) zu beurteilen.

Deutschland

Der deutsche Bundesrat entschied im Juli 2024, auf Initiative des Freistaates Bayern, einen Gesetzesentwurf zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes in den Deutschen Bundestag einzubringen. Der Entwurf sah die Einführung eines neuen § 201b dStGB («Verletzung von Persönlichkeitsrechten

[40] Es wird davon ausgegangen, dass dies für Liechtenstein ohnehin irrelevant wäre, da das EWR-Abkommen keinen eigenständigen Kompetenzbereich im Strafrecht enthält und damit die Ausgestaltung der Durchsetzungsinstrumente grundsätzlich im nationalen Recht verbleibt.

durch digitale Fälschung») vor. Nach § 201b Abs. 1 S. 1 dStGB-E[41] wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer das Persönlichkeitsrecht einer anderen Person verletzt, indem er einen mit computertechnischen Mitteln hergestellten oder veränderten Medieninhalt, der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äusseren Erscheinungsbildes, des Verhaltens oder mündlicher Äusserungen dieser Person erweckt, einer dritten Person zugänglich macht.[42] Nach § 201b Abs. 1 S. 2 StGB-E gilt Gleiches, wenn sich die Tat auf eine verstorbene Person bezieht und deren Persönlichkeitsrecht dadurch schwerwiegend verletzt wird. § 201b Abs. 2 StGB-E enthält einen Qualifikationstatbestand für Fälle, in denen in den Fällen des Abs. 1 S. 1 der Medieninhalt der Öffentlichkeit zugänglich gemacht wird oder der Medieninhalt einen Vorgang des höchstpersönlichen Lebensbereichs[43] zum Gegenstand hat.[44]

Die Bundesregierung führte in ihrer Stellungnahme zu diesem Gesetzentwurf aus, dass die Verbreitung missbräuchlicher Deepfakes bereits von diversen Straftatbeständen, insbesondere der Verleumdung (§ 187 dStGB), der Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a Abs. 2 dStGB) und den Pornographie-Tatbeständen (§§ 184, 184b, 184c dStGB) sowie § 33 dStGB i. V. m. §§ 22 f. KunstUrhG erfasst sei.[45] Nach Ansicht der damaligen Bundesregierung ergab sich daraus ein ausreichendes Netz an Sanktionsmöglichkeiten, ohne dass es eines neuen Straftatbestands bedürfe.

---

[41] E steht hier für Entwurf.

[42] Deutscher Bundestag, Gesetzentwurf des Bundesrates, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes,, Drucksache 20/12605, 21.08.2024.

[43] Bspw. manipulierte bzw. künstlich hergestellte Nacktaufnahmen.

[44] Vgl. BR-Drs. 222/24, 14.05.2024 § 201b, Abs.1 S.1-2 und Abs. 2.

[45] https://www.bundestag.de/resource/blob/1014026/1fb7ea9cad5313fa77849ba92ef04fd5/WD-7-038-24-pdf.pdf oder zu Einwänden der Bundesregierung: https://kripoz.de/2025/12/01/strafrechtlicher-persoenlichkeitsschutz-vor-deepfakes/, Teichmann, Strafrechtlicher Persönlichkeitsschutz vor Deepfakes https://kripoz.de/2025/12/01/strafrechtlicher-persoenlichkeitsschutz-vor-deepfakes/, zuletzt geprüft am 09.03.2026.

Nachdem dieser Entwurf infolge der parlamentarischen Diskontinuität nicht mehr verabschiedet wurde, brachte der Bundesrat den Entwurf zu Beginn der neuen Legislaturperiode 2025 erneut ein, wobei der Vorschlag nach wie vor umstritten bleibt.[46] Zum Zeitpunkt der Ausarbeitung der vorliegenden Postulatsbeantwortung war das parlamentarische Verfahren noch nicht abgeschlossen; eine Verabschiedung des Gesetzes ist bis dato nicht erfolgt.[47]

Italien

In Italien erlangte die Diskussion um einen spezifischen strafrechtlichen Umgang mit Deepfakes besondere Dringlichkeit, nachdem pornografisches, mittels künstlicher Intelligenz manipuliertes Material veröffentlicht wurde, das angeblich Ministerpräsidentin Giorgia Meloni zeigte. Dieser Vorfall führte zu einer breiten gesellschaftlichen und politischen Debatte über die Gefahren missbräuchlicher synthetischer Medieninhalte und trug dazu bei, dass Italien einen eigenständigen strafrechtlichen Tatbestand gegen die unrechtmässige Verbreitung KI-generierter oder KI-manipulierter Inhalte einführte.[48]

Mit dieser Gesetzesreform hat Italien als erstes EU-Mitglied eine spezifische gesetzliche Regelung zum Umgang mit KI-generierten bzw. KI-manipulierten Inhalten geschaffen. Die Regelung steht ausdrücklich im Kontext des europäischen AI-Act und ergänzt die nationale Rechtsordnung punktuell, insbesondere durch die

---

[46] https://www.brak.de/newsroom/newsletter/nachrichten-aus-berlin/2025/ausgabe-20-2025-v-1102025/bundesrat-bringt-erneut-gesetzentwurf-gegen-deepfakes-ein-brak-skeptisch/, zuletzt geprüft am 09.03.2026.

[47] Vgl. weiterführend Deutscher Bundestag, Gesetzentwurf des Bundesrates, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, Drucksache 20/12605, 21.08.2024.

[48] https://www.wolterskluwer.com/de-de/expert-insights/deepfakes-rechtlicher-schutz, zuletzt geprüft am 09.03.2026.

Einführung eines strafrechtlichen Tatbestands gegen die unrechtmässige Verbreitung entsprechender Inhalte.[49]

Schweiz

Unabhängig von den EU-Digitalisierungsrechtsakten wurden auch in der Schweiz die rechtspolitischen Herausforderungen im Zusammenhang mit Deepfakes bereits parlamentarisch thematisiert. Es kam zu mehreren Vorstössen, die eine spezifische strafrechtliche oder regulatorische Antwort auf missbräuchliche KI-generierte Inhalte forderten.[50] Nach derzeitiger Einschätzung des Bundesrates besteht jedoch kein unmittelbarer Bedarf, neue strafrechtliche Normen zu schaffen oder bestehende Bestimmungen anzupassen. Dieser verweist darauf, dass die gegenwärtige schweizerische Rechtsordnung – insbesondere in den Bereichen Persönlichkeitsrecht, Strafrecht und Datenschutzrecht – bereits heute ein ausreichend dichtes Netz an Schutzmechanismen bereithalte, um missbräuchlichen Deepfake-Konstellationen in der Regel angemessen begegnen zu können.[51]

3.2.5.3 Schlussfolgerung

Diese Beispiele veranschaulichen, dass sich der «europäische Umgang» mit missbräuchlichen Deepfakes derzeit als heterogen darstellt. Zwar setzen AI-Act und DSA einen gemeinsamen unionsrechtlichen Mindestrahmen im EWR, einzelne Staaten verfolgen darüber hinaus jedoch entsprechend unterschiedliche nationale Ansätze. Damit unterscheiden sich nicht nur die gewählten Instrumente, sondern

---

[49] Siehe LEGGE 23 settembre 2025, n. 132., https://www.gazzettaufficiale.it/eli/gu/2025/09/25/223/sg/pdf, zuletzt geprüft am 09.03.2026.

[50] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233563, zuletzt geprüft am 09.03.2026.

[51] https://www.srf.ch/news/schweiz/identitaetsdiebstahl-mit-ki-du-ploetzlich-im-porno-muss-der-bund-mehr-tun-gegen-deepfakes, zuletzt geprüft am 09.03.2026.

auch die rechtspolitischen Schlussfolgerungen: Gewisse Staaten sehen eine Schutzlücke, die gezielt zu schliessen ist, andere erachten das bestehende Normengefüge – ergänzt durch die unionsrechtlichen Transparenz- und Plattformpflichten – als ausreichend. Darüber hinaus bleibt festzuhalten, dass die im Ausland beobachtbaren Gesetzgebungsaktivitäten bislang überwiegend punktuell sind. Aus den vorliegenden Beispielen folgt nicht, dass sich derzeit europaweit ein allgemeiner Trend zu nationalen Sonderregelungen etabliert. Vielmehr spricht der Umstand, dass nur einzelne Staaten vertiefte Anpassungen vornehmen, dafür, dass die überwiegende Zahl europäischer Staaten derzeit keine zusätzliche Notwendigkeit erkennt, die nationale Gesetzgebung über die EU-Digitalisierungsrechtsakte hinaus anzupassen.[52]

3.2.5.4 Notwendigkeit einer eigenständigen nationalen Legaldefinition von «Deepfake»

Vor dem Hintergrund der bisherigen Ausführungen und in Anbetracht der im Postulat aufgeworfenen juristischen Fragen sowie unter Berücksichtigung der nationalen Rechtslage, kann für Liechtenstein grundsätzlich folgendes festgehalten werden:

Wie bereits ausgeführt, existiert in der liechtensteinischen Rechtsordnung derzeit keine ausdrückliche gesetzliche Definition des Begriffs «Deepfake». Zunächst ist festzuhalten, dass eine klare Legaldefinition grundsätzlich sinnvoll sein kann, um Rechtsklarheit zu schaffen. Denn ohne präzise Begriffsbestimmung bleibt unklar bzw. der Rechtsprechung überlassen zu definieren, welche Inhalte überhaupt als Deepfake gelten, was die Anwendung bestehender Rechtsnormen – etwa im Strafrecht, Urheberrecht oder Persönlichkeitsrecht – erschwert. Eine Definition kann

[52] An dieser Stelle wird auf die Ausführungen unter Punkt 3.6 zu den jüngsten Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung verwiesen.

zudem dabei helfen, zwischen «harmlosen» Anwendungen wie Satire oder künstlerischen Bearbeitungen und schädlichen Formen wie Desinformation oder gezielter Rufschädigung abzugrenzen. Darüber hinaus könnte eine klare Begriffsbestimmung den Schutz betroffener Personen stärken, indem sie es erleichtert, sich gegenüber täuschend echten Fälschungen auf klare Rechtsnormen zu berufen.

Gleichzeitig birgt eine zu enge oder zu weit gefasste Definition entsprechende Risiken. Die technologischen Entwicklungen im Bereich der künstlichen Intelligenz verlaufen äusserst dynamisch, sodass eine starre Legaldefinition rasch veralten könnte. Eine zu weit gefasste Definition wiederum könnte Bereiche wie Kunst, Parodie und Satire oder technisch legitime Anwendungen – etwa in Filmproduktion oder Bildung – unnötig einschränken und Innovation hemmen. In den deutschsprachigen nationalen Rechtsordnungen existiert bislang weder in Deutschland noch in Österreich oder der Schweiz eine einheitliche gesetzliche Definition des Begriffs «Deepfake»; vielmehr stützt man sich auf bestehende Normen, insbesondere im Straf-, Persönlichkeits- und Urheberrecht.

Vor diesem Hintergrund und insbesondere unter Verweis auf die bereits in der Verordnung (EU) 2024/1689 (AI-Act) enthaltene Begriffsbestimmung zu «Deepfake» erscheint eine eigenständige nationale Legaldefinition nicht angezeigt. Eine zusätzliche nationale Definition wäre wohl weder erforderlich noch zweckmässig, da sie die unions- bzw. EWR-weit angestrebte Harmonisierung unterlaufen und die Rechtssicherheit durch divergierende Begriffsverwendungen beeinträchtigen könnte. Es wäre daher sachgerecht, an die in der KI-Verordnung verankerte Terminologie anzuknüpfen und diese im Rahmen der EWR-Übernahme konsistent anzuwenden.

3.2.5.5 Notwendigkeit zur Anpassung nationaler Rechtsnormen

Grundsätzlich könnte der Schutzbereich in Bezug auf Deepfakes durch ein nationales Gesetz erweitert werden. Allerdings zeitigt ein nationaler Alleingang, vor allem, was seine grenzüberschreitende Durchsetzbarkeit angeht, nur einen sehr eingeschränkten Wirkungsbereich (Beispiel Dänemark). Eine Prüfung der Zweckmässigkeit muss daher vor dem Hintergrund einer umfassenden Analyse der bereits bestehenden rechtlichen Möglichkeiten vorgenommen werden (siehe dazu die Ausführungen unter Punkt 3.2.1). Unabhängig davon erscheint es ratsam, solche Massnahmen auf europäischer Ebene zu prüfen und voranzutreiben.

Vordergründig ergeben sich folglich insbesondere die nachfolgenden Optionen:

Option 1: Nationaler Regelungsansatz

Ein nationales Regelungsmodell könnte es Liechtenstein ermöglichen, einen eigenständigen Schutzrahmen gegen unautorisierte Deepfakes zu etablieren und damit ein klares Signal für den Schutz digitaler Persönlichkeitsrechte zu setzen. Die unmittelbare regulatorische Wirkung wäre jedoch aufgrund fehlender relevanter inländischer Plattformanbieter sowie mangelhafter Durchsetzbarkeit begrenzt. Ein nationaler Ansatz hätte daher vor allem deklaratorischen Charakter, könnte aber zur Sensibilisierung der Bevölkerung beitragen. Dem stehen ein geringer praktischer Wirkungsgrad sowie potenzielle Fragmentierungseffekte gegenüber.

Option 2: Europäische Harmonisierung priorisieren

Die Fokussierung auf europäische Regelungsprozesse würde einen kohärenten und grenzüberschreitend durchsetzbaren Schutzrahmen ermöglichen. Angesichts der globalen Strukturen im Bereich generativer KI ist ein wirksamer Schutz digitaler Persönlichkeitsrechte ohne europäische Harmonisierung kaum realisierbar.

3.2.6 Aktuelle Rechtslage in Liechtenstein

Die folgenden Ausführungen adressieren die im Postulat und im Landtag aufgeworfenen Fragen hinsichtlich der Vorgehensweise gegen nicht autorisierten Deepfakes und KI-generierten Inhalten in Liechtenstein. Zur Beantwortung der Fragen soll dabei die entsprechende Rechtslage erläutert und gleichzeitig Bezug genommen werden auf die im EWR-Übernahmeprozess befindlichen Rechtsakte (AI-Act, DSA).

3.2.6.1 Recht auf Löschung von Deepfake-Inhalten

Durchsetzbare Rechte bzw. Ansprüche auf Löschung rechtswidriger Deepfake-Inhalte ergeben sich aus den bereits erwähnten einschlägigen datenschutzrechtlichen und zivilrechtlichen Bestimmungen. Das Datenschutzrecht stellt mit Art. 17 der Datenschutz-Grundverordnung (DSGVO) ein unmittelbar wirkendes «Recht auf Löschung» zur Verfügung, das gegenüber Verantwortlichen – einschliesslich Plattformbetreibern – geltend gemacht werden kann. Bei grenzüberschreitenden Sachverhalten ermöglicht Art. 60 DSGVO die Zusammenarbeit der Aufsichtsbehörden. Die Datenschutzstelle kann als nationale Aufsichtsbehörde angerufen werden, wenn die Verarbeitung rechtswidrig erfolgt oder der Verantwortliche nicht ermittelt werden kann; in solchen Fällen ist auch der Rückgriff auf Plattformbetreiber als datenschutzrechtlich Verantwortliche möglich.

Ergänzend gewähren die zivilrechtlichen Persönlichkeitsrechtsschutzbestimmungen, insbesondere § 16 und § 1328a ABGB sowie Art. 38 ff. PGR, Ansprüche auf Unterlassung, Beseitigung und Schadenersatz bei Eingriffen in Persönlichkeitsrechte.

In diesem Zusammenhang ist ergänzend festzuhalten, dass der DSA Pflichten für Online-Plattformen zur Behandlung gemeldeter rechtswidriger Inhalte enthält. Ein

subjektives, unmittelbar einklagbares «Recht auf Löschung» konkreter Deepfakes enthält er jedoch nicht.

3.2.6.2 Juristische Verfolgung bei der Verbreitung von Deepfakes, insbesondere bei politischer Manipulation oder Rufschädigung

Sobald eine Online-Plattform ihre Dienstleistungen in der EU (nach der EWR-Übernahme im EWR) anbietet, unterliegt diese den Pflichten des DSA. Der DSA sieht Meldemechanismen für rechtswidrige Inhalte vor, die die Plattformen einrichten müssen. Die Plattformen müssen diese Meldungen prüfen und bei bestätigter Rechtswidrigkeit den Inhalt sperren oder entfernen. Bei sehr grossen Online-Plattformen (mehr als 45 Mio. Nutzer in der EU) bestehen zusätzliche Pflichten. Diese müssen systemische Risiken analysieren und Massnahmen gegen die Verbreitung manipulierter Inhalte einführen.

Sehr grosse Online-Plattformen werden von der EU-Kommission direkt beaufsichtigt, kleinere Plattformen von nationalen Koordinatoren digitaler Dienste. Nach der EWR-Übernahme wird auch in Liechtenstein eine Behörde als Koordinator digitaler Dienste benannt (voraussichtlich bei der SDI). Die EU-Kommission und die Koordinatoren digitaler Dienste bilden gemeinsam das «European Board for Digital Services (EBDS)». Der EBDS setzt sich aus den nationalen Behörden unter dem Vorsitz der EU-Kommission zusammen, die bei der Durchsetzung des DSA eng zusammenarbeiten. Verstösse gegen den DSA können zu hohen Bussgeldern führen.

Der DSA wie auch die KI-Verordnung sehen jedoch ausschliesslich verwaltungsrechtliche Sanktionen vor. Während der DSA die Pflichten der Plattformen im Umgang mit rechtswidrigen Inhalten festlegt, bestimmt das jeweils einschlägige materielle Recht – insbesondere das nationale Zivil- und Strafrecht sowie unmittelbar anwendbares Unionsrecht wie etwa die DSGVO – ob ein Inhalt rechtswidrig ist und welche Ansprüche (etwa auf Löschung, Unterlassung oder Schadenersatz)

bestehen. Die materielle Feststellung der Rechtswidrigkeit erfolgt dabei stets im konkreten Einzelfall und richtet sich nach der jeweils einschlägigen Rechtsordnung: Handelt es sich etwa um strafrechtlich relevante Deepfakes – etwa betrügerische oder ehrverletzende Inhalte – obliegt die Beurteilung und allfällige Verfolgung den Strafverfolgungsbehörden. Verstösse gegen den DSA selbst hingegen fallen in die Zuständigkeit des nationalen Koordinators für digitale Dienste bzw. – bei sehr grossen Plattformen – der EU-Kommission.

Meldungen an die Plattformen dienen primär dazu, dass diese die beanstandeten Inhalte unverzüglich entfernen oder sperren können. Stellt eine Plattform keine angemessenen Möglichkeiten zur Verfügung, um rechtswidrige Inhalte zu melden, liegt darin selbst ein Verstoss gegen den DSA vor. In diesen Fällen ist der nationale Koordinator für digitale Dienste die zuständige Anlaufstelle. Dieser kann entsprechende Hinweise über das europäische Netzwerk der Koordinatoren an den jeweils zuständigen nationalen Koordinator oder – falls erforderlich – an die EU-Kommission weiterleiten, um die Einhaltung der DSA-Pflichten sicherzustellen.

Für die zivilrechtliche Durchsetzung wird an dieser Stelle auf die Ausführungen zu den einschlägigen nationalen Rechtsgrundlagen zu Punkt 3.2.1 verwiesen. Wie dort dargelegt, stehen betroffenen Personen bei Persönlichkeitsrechtsverletzungen insbesondere Ansprüche auf Unterlassung und Beseitigung sowie bei schwerwiegenden Eingriffen auch auf eine Geldentschädigung zu.

Bei den Straftatbeständen sind je nach Tatbestand entsprechende Bestrafungen vorgesehen. Im Falle von «politischer Manipulation», beispielsweise die Veröffentlichung eines Deepfake-Videos, um eine Wahl oder Abstimmung gezielt zu beeinflussen wäre § 263 StGB (Täuschung bei einer Wahl oder Abstimmung) oder § 264 StGB (Verbreitung falscher Nachrichten bei einer Wahl oder Abstimmung) einschlägig. Hinsichtlich Rufschädigung wäre auf die bereits genannten Paragrafen

betreffend Üble Nachrede (§ 111 StGB) oder Verleumdung (§ 112 StGB) zu verweisen.

3.2.6.3 Bekämpfung von Identitätsdiebstahl durch Deepfakes

Identitätsdiebstahl mittels Deepfakes kann derzeit gestützt auf bestehende nationale Rechtsgrundlagen – insbesondere das Persönlichkeitsrecht, das Datenschutzrecht sowie das Strafrecht – verfolgt werden. Ergänzend bietet auch die KI-Verordnung Hand: Sie verpflichtet Anbieter von Deepfake-Technologien zur eindeutigen Kennzeichnung solcher Inhalte, sodass künstlich erzeugtes Material als solches erkennbar sein muss.

3.2.6.4 Schutz der Meinungsfreiheit, Kunstfreiheit und Satire, ohne Missbrauch

Bei der Regulierung von Deepfake-Videos/Bildern -Audios sind die relevanten Grund- und Persönlichkeitsrechte zu berücksichtigen und es ist insbesondere auf den besonderen Schutz der Meinungsäusserungsfreiheit und der Kunstfreiheit zu achten. Auch hier wird, wie beim zivilrechtlichen Persönlichkeitsschutz im Allgemeinen, eine Interessenabwägung bzw. eine Prüfung auf der Rechtfertigungsebene vorzunehmen sein.

Mögliche Rechtfertigungsgründe wären etwa die Einwilligung des Betroffenen, die Meinungsäusserungsfreit (Art. 40 LV) sowie andere Grundrechte oder Persönlichkeitsrechte. Im Rahmen der Interessenabwägung wäre insbesondere die Kunstfreiheit (Art. 40 LV) zu berücksichtigen, die auch satirische Darstellungen schützt.

Dabei ist zu beachten, dass Politikern sowie Personen des öffentlichen Lebens (auch «public figures» genannt) von Rechtsprechung und Literatur im Allgemeinen nur ein eingeschränkter Persönlichkeitsschutz zugestanden wird, je nachdem ob die Veröffentlichung zu einer Debatte von allgemeinem gesellschaftlichem

Interesse beiträgt oder bloss zur Befriedigung der Neugier eines bestimmten Publikums dient.[53] Grenzen finden sich beim Wertungsexzess, bei Vorwürfen ohne Tatsachensubstrat und bei Berührung des höchstpersönlichen Lebensbereichs.[54]

Kennzeichnung von Deepfakes im Bereich der Kunst- und Meinungsäusserungsfreiheit sollten ermöglichen, dass es zu keinerlei Einschränkung dieser Kunstform bzw. der Grundfreiheit kommt. Es geht der Satire grundsätzlich nicht darum zu täuschen, im Gegensatz zur Desinformation.[55]

3.2.6.5 Haftungsregelung bei Deepfakes mit unbekannter Urheberschaft

Auf nationaler Ebene erfolgt die rechtliche Behandlung von Deepfakes grundsätzlich über das Straf- und Zivilrecht. Je nach Ausgestaltung kann ein Deepfake unter verschiedene Tatbestände des Strafgesetzbuches fallen. Solange die verantwortliche Person jedoch nicht identifiziert ist, kann weder eine strafrechtliche Verantwortlichkeit begründet noch ein zivilrechtlicher Anspruch gegen den Täter durchgesetzt werden. Zivilrechtlich bestehen Unterlassungs-, Beseitigungs- und Schadenersatzansprüche nach den allgemeinen Regeln des ABGB; sie setzen jedoch einen identifizierten Anspruchsgegner voraus.

Für die Haftung von Plattformen, über welche Deepfakes verbreitet werden, stützt sich die Beurteilung auf die bestehenden nationalen Regelungen betreffend digitaler Dienste, insbesondere das Gesetz über den elektronischen Geschäftsverkehr (E-Commerce-Gesetz; ECG)[56], und – soweit einschlägig – auf die Bestimmungen des Mediengesetzes (MedienG). Ergänzend kommen je nach Einzelfall auch Anspruchsgrundlagen nach ABGB, PGR, URG und DSG bzw. DSGVO in Betracht. Das

---

[53] Vgl. https://www.urheberrecht.org/news/4064/, zuletzt geprüft am 09.03.2026.

[54] Vgl. Meissel in Klang³ § 16 ABGB Rz 102.

[55] Siehe Bundeskanzleramt, Aktionsplan Deepfake, Wien 2022, S. 9.

[56] Gesetz vom 16. April 2003 über den elektronischen Geschäftsverkehr, LGBl. 2003 Nr. 133.

MedienG scheidet in der Regel eine direkte Entschädigungspflicht von Video-Sharing-Plattform-Diensten (bspw. YouTube) aus, da diese mangels redaktioneller Verantwortung nicht als Medieninhaber gelten (Art. 2 Abs. 1 Ziff. 10 MedienG); für ihre Verantwortlichkeit ist primär das E-Commerce-Gesetz massgeblich.

Das E-Commerce Gesetz, ebenso wie der DSA auf europäischer Ebene, enthält ein Haftungsprivileg für Vermittlungsdienste. Plattformen haften grundsätzlich nicht für von Dritten eingestellte Inhalte und sind nicht verpflichtet, diese aktiv auf Rechtswidrigkeit zu überprüfen. Sie verlieren dieses Privileg jedoch, wenn sie tatsächliche Kenntnis von einem rechtswidrigen Inhalt erlangen und nicht unverzüglich tätig werden. Erfolgt nach der Meldung eines rechtswidrigen Deepfake keine Löschung oder Sperrung, haftet die Plattform gegenüber den betroffenen Personen oder Unternehmen. Das Haftungsprivileg dient dabei auch der Wahrung der Meinungsfreiheit, da Plattformen ansonsten zu präventiven Eingriffen und übermässigem Löschen veranlasst wären.

Davon zu unterscheiden ist die öffentlich-rechtliche Verantwortlichkeit nach dem DSA. Plattformen müssen nutzerfreundliche Verfahren zur Meldung illegaler Inhalte vorsehen und weitere Sorgfaltspflichten einhalten. Kommen sie diesen Pflichten nicht nach, können der nationale Koordinator für digitale Dienste oder – bei sehr grossen Plattformen – die EU-Kommission aufsichtsrechtliche Massnahmen ergreifen, etwa Verbesserungsanordnungen oder Bussen. Eine allgemeine Pflicht zur aktiven, flächendeckenden Überwachung von Inhalten oder zur eigenständigen Ermittlung der Urheber rechtswidriger Inhalte besteht jedoch nicht. Die Verantwortung der Plattformbetreiber beschränkt sich damit auf reaktive Sorgfaltspflichten im Umgang mit konkreten Hinweisen auf illegale Inhalte.

3.2.6.6 Wirksame Belangung von Plattformen im Ausland

Hinsichtlich der im Postulat und im Landtag aufgeworfenen Frage, wie Liechtenstein gegenüber im Ausland ansässigen Plattformen wirksam vorgehen kann bzw. ob hierfür EU/EWR-weite Regelungen erforderlich sind, ist vorweg festzuhalten, dass generell die Belangung internationaler Plattformen oder im Ausland befindlicher Täter bzw. Urheber grundsätzlich nur über justizielle Rechtshilfeverfahren an den Staat des jeweiligen Unternehmens bzw. Wohnsitzes erfolgt. Diese Verfahren sind erfahrungsgemäss zeitaufwendig und erschweren eine rasche Sicherung oder Herausgabe relevanter elektronischer Beweismittel erheblich.

In Bezug auf unions- bzw. EWR-weite Mechanismen zur Behandlung rechtswidriger Inhalte und zur Zusammenarbeit mit Plattformen ist auf die Ausführungen zum Digital Services Act (DSA) in Punkt 3.2.2.2 zu verweisen. Plattformen haben Melde- und Abhilfeverfahren für rechtswidrige Inhalte bereitzustellen, insbesondere nach Art. 16 DSA, der elektronische, nutzerfreundliche und hinreichend substantiierte Hinweise mit zeitnaher Entscheidung und Benachrichtigung vorsieht. Die Aufsicht erfolgt durch nationale Koordinatoren digitaler Dienste sowie – bei sehr grossen Online-Plattformen und Suchmaschinen – durch die Europäische Kommission.

Vor dem Hintergrund der Frage, ob EU/EWR-weite Regelungen erforderlich sind, um Verzögerungen bei der internationalen Beweissicherung zu verhindern, kann als unionsrechtliches Referenzinstrument die Verordnung (EU) 2023/1543 über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (E-Evidence-Verordnung, EEVO)[57] herangezogen werden.

[57] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. 191 vom 28.07.2023, S.118).

Diese ermöglicht den Strafverfolgungsbehörden der EU-Mitgliedstaaten eine unmittelbare Anordnung gegenüber Diensteanbietern, die elektronische Kommunikationsdienste im Gebiet der EU erbringen, unabhängig vom physischen Speicherort der Daten. Rechtsgrundlage bildet Art. 82 Abs. 1 AEUV[58], der die justizielle Zusammenarbeit und die gegenseitige Anerkennung strafprozessualer Entscheidungen regelt.

Die inhaltlichen Unterschiede zwischen dem DSA bzw. dem AI-Act einerseits und der EEVO andererseits sind eindeutig abzugrenzen: DSA und AI-Act sind auf die Regulierung des digitalen Binnenmarkts ausgerichtet und adressieren primär Plattform- und Anbieterpflichten, insbesondere Transparenz-, Risikomanagement-, Kennzeichnungs- sowie Aufsichts- und Koordinationsmechanismen. Die EEVO verfolgt demgegenüber einen eigenständigen Regelungszweck. Sie schafft ein strafprozessuales Instrumentarium für die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel. Während DSA und AI-Act somit vor allem präventiv auf die Governance und Durchsetzung von Pflichten gegenüber Plattformen und KI-Anbietern ausgerichtet sind, betrifft die EEVO die repressive Ebene der Strafverfolgung, indem sie unmittelbare Herausgabe- bzw. Sicherungsanordnungen gegenüber Diensteanbietern ermöglicht.

Da der EWR die Binnenmarkt-Rechtsakte abdeckt und Instrumente der strafrechtlichen Zusammenarbeit, gestützt auf Art. 82 AEUV, grundsätzlich nicht in den EWR übernommen werden, ist eine unmittelbare EWR-Übernahme der E-Evidence-Verordnung rechtlich nicht vorgesehen.

---

[58] Vertrag über die Arbeitsweise der Europäischen Union, ABl. C326 vom 26.10.2012, S. 47-390.

3.3 Technische Fragen

Nachdem die juristischen Fragen erörtert wurden, werden nun die technischen Fragen nach möglichen und sinnvollen Schutzmechanismen, effektiven Löschmechanismen, technischen Erkennungsmethoden sowie der Beweissicherung bei Deepfake-Vorfällen thematisiert. Dazu werden die in der KI-Verordnung genannten technischen Umsetzungsmassnahmen, und weitere Verfahren (Einsatz von Hash-Datenbanken, etc.), sowie verschiedene Erkennungsmethoden beschrieben und bewertet.

3.3.1 Technische Schutzmassnahmen

Gemäss KI-Verordnung (Art. 50 Abs. 2) sind Anbieter von KI-Systemen, die synthetisches Bild-, Audio- oder Videomaterial erzeugen, verpflichtet, diese maschinenlesbar zu kennzeichnen. Die Erwägungsgründe der KI-Verordnung nennen als mögliche technische Mittel u.a. Wasserzeichen, Metadatenidentifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden und Fingerabdrücke.[59]

Bei der Kennzeichnung haben die Anbieter insbesondere den allgemein anerkannten Stand der Technik in Form der einschlägigen technischen Normen zu berücksichtigen. Das «European Committee for Standardization (CEN)»[60] und das «European Committee for Electrotechnical Standardization (CENELEC)»[61] wurden diesbezüglich von der EU-Kommission mit der Erarbeitung relevanter Standards für die KI-Transparenz beauftragt.[62] Ein möglicher Standard zur Umsetzung eines

[59] Vgl. Verordnung (EU) 2024/1689 (KI-Verordnung), Erwägungsgrund 133.

[60] Committee for Standardization (CEN), https://www.cencenelec.eu.

[61] European Committee for Electrotechnical Standardization (EENELEC), https://www.cencenelec.eu.

[62] https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence, zuletzt geprüft am 09.03.2026.

digitalen Gütesiegels für Echtheit ist der «Coalition for Content Provenance and Authenticity (C2PA)»[63] Standard, welcher ebenfalls als möglicher ISO-Standard[64] für die Echtheit von Informationen vorgesehen ist, wobei sich dieser noch im Entwurfsstadium befindet.

Das Einbetten von Wasserzeichen oder Meta-Markierungen in durch KI generierte Inhalte stellt eine wichtige Schutzmassnahme dar, um sie als solche erkennbar zu machen. Dabei können zwei Gruppen von Wasserzeichen unterschieden werden: Sichtbare und unsichtbare Wasserzeichen.[65]

Sichtbare Wasserzeichen oder Labels (bspw. Sora von OpenAI) sind ein technisches Mittel, um die Herkunft und Authentizität digitaler Inhalte kenntlich zu machen. Sie werden direkt in das Bild- oder Videomaterial integriert und sind für den Betrachter erkennbar (sichtbare Wasserzeichen sind gleichzeitig auch maschinenlesbar). Ziel ist es, Transparenz über die Verwendung von KI-generierten Inhalten zu schaffen und Missbrauch zu erschweren.

Unsichtbare, maschinenlesbare Wasserzeichen sind digitale Markierungen wie Google SynthID[66] oder die C2PA-Wasserzeichen, die in Bild-, Audio- oder Videodateien eingebettet werden, ohne für den Betrachter erkennbar zu sein. Sie dienen der Authentifizierung und Nachverfolgbarkeit von Inhalten. Solche Markierungen können von Plattformen oder Prüf-Software ausgelesen werden, um Deepfakes zu kennzeichnen. C2PA ist ein internationaler defacto-Standard für Herkunftsnachweise, getragen unter anderem von Adobe, Google, Microsoft, und TikTok. Die

---

[63] Coalition for Content Provenance and Authenticity (C2PA), Standard-Entwurf und technische Dokumentation: https://c2pa.org.

[64] https://www.iso.org/standard/90726.html.

[65] Vgl European Parliament, BRIEFING zu Generative AI and watermarking, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI%282023%29757583_EN.pdf, zuletzt geprüft am 09.03.2026.

[66] SynthID - https://deepmind.google/models/synthid/.

Europäische Union verlangt ab August 2026 eine Kennzeichnungspflicht für synthetische Medien[67], was bedeutet, dass KI-generierte Inhalte maschinenlesbar als künstlich ausgewiesen werden müssen (etwa durch Wasserzeichen oder Hinweise).

Jedoch muss darauf hingewiesen werden, dass die Anforderungen der KI-Verordnung zur Kennzeichnung durch Wasserzeichen bislang nur teilweise umgesetzt wurden,[68] da sich die heute bekannten Marker, ob sichtbar oder unsichtbar, durch Zuschneiden, Neucodierung oder durch erneutes KI-Rendering[69] ganz oder teilweise entfernen lassen. Keine Methode ist derzeitig robust genug, um gegen einen entschlossenen Angreifer zu bestehen.[70] Dementsprechend bieten Wasserzeichen eine sinnvolle Prävention, insbesondere für Akteure mit guten Absichten, aber keinen zuverlässigen Schutz gegen gezielten Missbrauch. So ist beispielsweise Googles SynthID auch nur auf KI-Produkte von Google wie Gemini anwendbar. Dieses Problem der modellspezifischen Erkennung ist nicht neu: Bereits OpenAI musste feststellen, dass deren Detektor vorwiegend Inhalte der eigenen Modelle identifizieren konnte (siehe auch unter Punkt 3.3.3) andere, modellfremde jedoch nur unzureichend oder gar nicht.[71]

Eine andere Schutzmassnahme stellen sogenannte kryptografische Methoden zum Nachweis der Herkunft und Authentizität digitaler Inhalte – insbesondere

---

67 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689; https://www.imatag.com/blog/eu-ai-act-update-new-watermarking-requirements-for-ai-generated-content, zuletzt geprüft am 09.03.2026.

68 https://arxiv.org/html/2503.18156v3, zuletzt geprüft am 09.03.2026.

69 KI-Rendering bezeichnet den Vorgang, bei dem ein KI-System aus Eingabedaten (z.B. Text, Bildern, Audio oder Video) neue Medieninhalte erzeugt oder bestehende Inhalte neu berechnet.

70 Watermarking Without Standards Is Not AI Governance: https://arxiv.org/abs/2505.23814; Vgl. weiters https://datainnovation.org/2024/07/the-ai-acts-ai-watermarking-requirement-is-a-misstep-in-the-quest-for-transparency, zuletzt geprüft am 09.03.2026.

71 Vgl. https://openai.com/index/new-ai-classifier-for-indicating-ai-written-text/, geprüft am 09.03.2026.

digitale Signaturen und darauf aufbauende Provenance-Systeme[72] – dar. Diese gelten als ein zentraler technischer Baustein im Kampf gegen manipulierte oder vollständig synthetisch erzeugte Medieninhalte.

Im Kern bieten kryptografische Verfahren die Möglichkeit, ein digitales Medium eindeutig einer bestimmten Quelle zuzuordnen und nachzuweisen, dass es seit dem Zeitpunkt der Signatur nicht mehr verändert wurde. Wird ein Medienobjekt beispielsweise mittels eines Hash-Werts (etwa SHA-256[73]) erfasst und dieser Hash anschliessend mit einer digitalen Signatur einer vertrauenswürdigen Stelle versehen, entsteht ein robuster Integritäts- und Authentizitätsnachweis. Solange der Hash unverändert bleibt und die Signatur gültig ist, kann jede Person oder Plattform zweifelsfrei überprüfen, dass das Material tatsächlich von der angegebenen Quelle stammt. Dadurch wird ein hohes Mass an Transparenz und Verantwortlichkeit erreicht: Die Quelle ist kryptografisch eindeutig identifizierbar, und spätere Manipulationen werden sofort erkennbar.

Diese Verfahren verhindern jedoch nicht, dass die Quelle selbst – also derjenige, der signiert – ein Material vor der Signatur manipuliert oder synthetisch erzeugt. Der Vertrauensschutz reicht nur so weit, wie die Quelle selbst vertrauenswürdig ist.[74] Mit aktuellen technischen Entwicklungen wird daher versucht, den Zeitpunkt der Signatur vorzuverlagern, indem eine digitale Signatur bereits während des Aufnahmeprozesses (z.B. direkt in der Kamera) erzeugt wird. Ein solcher ergänzender Ansatz ist das Konzept «Authentic-by-Design». Dabei steht nicht die nachträgliche

---

[72] Provenance-Systeme sind technische Verfahren, die die Entstehungs- und Veränderungshistorie digitaler Inhalte manipulationssicher dokumentieren (z.B. mittels digitaler Signaturen und unveränderbarer Metadaten), sodass Herkunft, Integrität und Authentizität eines Mediums nachprüfbar bleiben.

[73] SHA-256 ist eine kryptografische Hashfunktion, die aus beliebigen Daten einen eindeutigen 256-Bit-Prüfwert erzeugt; bereits kleinste Änderungen am Original führen zu einem völlig anderen Hash und ermöglichen so einen Integritätsnachweis.

[74] Vgl. https://spec.c2pa.org/specifications/specifications/1.3/explainer/Explainer.html, zuletzt geprüft am 09.03.2026.

Erkennung von Manipulationen im Vordergrund, sondern die nachweisbare Echtheit von Inhalten bereits im Moment ihrer Entstehung. Digitale Aufnahmen werden unmittelbar beim Erstellen mit kryptografisch gebundenen Metadaten, Hashwerten und Signaturen versehen; das Aufnahmegerät bildet damit eine geschlossene Vertrauenskette vom Rohmaterial bis zur allfälligen Weiterverarbeitung. Jede spätere Veränderung – auch geringfügige – führt dazu, dass die Verifikation bricht oder ausgewiesen werden muss. Im Unterschied zu rein nachgelagerten kryptografischen Verfahren (digitale Signaturen, Hash-/Provenance-Datenbanken), die typischerweise erst eine bereits vorliegende Datei schützen und ab diesem Zeitpunkt Integrität belegen, schliesst «Authentic-by-Design» die Entstehungsphase selbst ein: Schlüsselmaterial ist gerätegebunden (Secure Hardware), Rohdaten werden beim Erfassen gehasht und signiert, Bearbeitungsschritte werden protokolliert und – sofern erlaubt – ihrerseits verifizierbar gemacht. So entsteht eine lückenlose Evidenzkette «ab Werk»; nachträgliche Signaturen oder Hash-Einträge ohne Bindung an den Aufnahmeprozess können demgegenüber nicht verlässlich abbilden, was vor der Signatur mit dem Inhalt geschehen ist. Das Problem bleibt jedoch bestehen, dass moderne KI-Systeme Inhalte heute vollständig synthetisch erzeugen können, ohne dass überhaupt eine ursprüngliche Aufnahme existiert, deren Integrität gesichert werden könnte.[75]

Auch automatisierte Erkennungsmethoden – etwa Deepfake-Detektoren – können eine ergänzende Rolle spielen. Diese beruhen in der Regel selbst auf KI-Modellen und analysieren Muster, Artefakte oder Anomalien in Bild-, Audio- oder Videodaten. Doch ihre Zuverlässigkeit ist begrenzt: Sie sind nicht universell

[75] Eine Übersicht über den noch verhältnismässig neuen Ansatz bietet ua. https://contentauthenticity.org/how-it-works, zuletzt geprüft am 09.03.2025 oder auch https://contentauthenticity.org/blog/leica-launches-worlds-first-camera-with-content-credentials, zuletzt geprüft am 09.03.2026. Zum Standard selbst https://spec.c2pa.org/specifications/specifications/1.3/explainer/Explainer.html, zuletzt geprüft am 09.03.2026.

anwendbar, ihr Erfolg hängt stark vom Training ab, und sie sind angreifbar, da Deepfake-Modelle oft schneller weiterentwickelt werden als die Detektionssysteme. Dadurch können Erkennungsmethoden im Wettlauf mit immer leistungsfähigeren Generierungsmodellen rasch an Wirksamkeit verlieren.[76]

Insgesamt zeigt sich, dass kryptografische Verfahren zwar ein wichtiges und effektives Mittel darstellen, um die Herkunft und Unverändertheit von Aufnahmen zu garantieren, sie jedoch keine umfassende Lösung gegen synthetisch erzeugte oder bewusst manipulierte Inhalte bieten. Die Grenzen liegen besonders dort, wo gar kein authentischer Ursprung existiert oder technische Angriffe darauf abzielen, Erkennungsmechanismen zu umgehen.[77]

3.3.2 Löschmechanismen für Deepfake-Inhalte

Ein zentrales Instrument für schnelles Entfernen von Deepfakes ist ein effizientes «Notice-and-Action-Verfahren»[78]. Online-Plattformen müssen leicht zugängliche Meldewege bieten, damit Betroffene oder Behörden manipulierte Inhalte umgehend melden können. Da manuelle Meldungen oft zu langsam und reaktiv sind, setzen viele grosse Dienste auf KI-gestützte Inhaltsfilter, um Deepfakes proaktiv zu identifizieren. Deepfake-Detektoren können theoretisch Medienobjekte scannen und verdächtige Inhalte, bevor diese publiziert werden, entfernen oder zur manuellen Überprüfung markieren. So verfügt beispielsweise YouTube über Richtlinien gegen irreführende Deepfakes[79] und entwickelt Systeme, um manipulierte Videos (insbesondere im politischen Kontext) automatisch zu erkennen und zu

---

[76] Richings, Performance Decay in Deepfake Detection: The Limitations of Training on Outdated Data, https://arxiv.org/abs/2511.07009, zuletzt geprüft am 09.03.2026.

[77] Vgl. insb. European Parliament, BRIEFING zu Generative AI and watermarking, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI%282023%29757583_EN.pdf, zuletzt geprüft am 09.03.2026.

[78] Vgl. Verordnung (EU) 2022/2065 (DSA), Art. 16.

[79] Disclosing use of altered or synthetic content - https://support.google.com/youtube/answer/14328491.

entfernen. Solche Filtersysteme sind allerdings nur so zuverlässig wie die zugrundeliegenden Erkennungsalgorithmen und KI-Modelle selbst (siehe dazu auch Punkt 3.3.3).

Eine andere technische Lösung für schnelles Entfernen ist der Einsatz von Hash-Datenbanken für bekannte Deepfake-Inhalte. Hierbei wird von identifizierten gefälschten Medien ein digitaler Fingerabdruck in Form eines Hashs erzeugt und mit anderen Unternehmen geteilt. Der Service StopNCII.org[80] ist ein Beispiel für einen Dienst, der bereits eingesetzt wird, um die unerwünschte Verbreitung intimer Bilder zu verhindern. Betroffene können dort Hashes ihrer (auch KI-verfälschten) Fotos hinterlegen, und grosse Techfirmen nutzen diese, um Übereinstimmungen automatisch zu finden und zu löschen. Microsoft hat sich 2024 diesem Netzwerk angeschlossen und verhindert, dass bei deren Suchmaschine Bing per Hash erkannte Deepfake-Nacktbilder, überhaupt noch in den Suchergebnissen angezeigt werden. Innerhalb kurzer Zeit konnten dadurch ca. 260'000 Bilder entfernt werden.[81] Eine Ausweitung solcher gemeinsamen Hash-Pools auf weitere Deepfake-Kategorien (bspw. Deepfakes von Politikern) könnte die Löschung erheblich beschleunigen. Daher erscheint eine Anbindung an bestehende internationale Kooperations- und Meldestrukturen als grundsätzlich prüfenswert, um die grenzüberschreitende Entfernung rechtswidriger Deepfake-Inhalte zu erleichtern. Die konkrete Umsetzbarkeit wäre jedoch vertieft zu prüfen.

Es sei jedoch erneut nachdrücklich erwähnt, dass auch diese Vorgehensweise keine ganzheitliche Behandlung des Problems bietet. So können nach wie vor Deepfakes leicht abgeändert werden, was zu einem völlig neuen Hash führt,

[80] Stop Non-Consensual Intimate Image Abuse - https://stopncii.org/.

[81] Siehe https://blogs.microsoft.com/on-the-issues/2024/09/05/an-update-on-our-approach-to-tackling-intimate-image-abuse/, zuletzt geprüft am 09.03.2026.

welcher dementsprechend nicht in der Datenbank hinterlegt ist und für den keine automatisierte Löschung in die Wege geleitet werden kann.

3.3.3 Deepfakes-Erkennungsmethoden

Mittlerweile gibt es zahlreiche spezialisierte Erkennungsalgorithmen, welche mit grossen Datensätzen von echten und gefälschten Medien trainiert wurden, um Manipulationen automatisch zu erkennen. Solche sogenannten «Deepfake-Detector-Modelle» nutzen hauptsächlich Methoden der Video- und Bild-Forensik und Maschinelles Lernen (Machine Learning), um verdächtige Merkmale in Gesichtern, Stimmen oder Bewegungen zu finden. Sensity AI[82] ist ein Beispiel eines solchen kommerziellen Detektionsdienstes. Unter Punkt 3.3.1 wurde bereits SynthID von Google erwähnt, welches jedoch ausschliesslich auf die Produktpalette von Google anwendbar ist. Diese Systeme geben oft einen Wahrscheinlichkeitswert aus, welcher signalisiert, wie wahrscheinlich es ist, dass das Medium mit Hilfe von KI generiert wurde. Die Zuverlässigkeit dieser Erkennungsmethoden und Modellen ist jedoch im Allgemeinen umstritten und sie liefern keine absolute Gewissheit.

Die Problematik der mangelnden Zuverlässigkeit zeigt sich auch daran, dass selbst führende Technologieunternehmen mit Spezialisierung auf KI ihre Erkennungstools wieder eingestellt haben. OpenAI beispielsweise hat im Juli 2023 seinen KI-Text-Klassifikator zurückgezogen, mit der Begründung, dass dieser eine zu niedrige Genauigkeitsrate aufwies. Das Tool konnte lediglich 26% der KI-generierten Texte korrekt identifizieren und klassifizierte zudem 9% menschlich verfasster Texte fälschlicherweise als KI-generiert.[83] Dieser Schritt verdeutlicht ein grundsätzliches Dilemma: Während KI-Generatoren kontinuierlich verbessert werden und immer

[82] All-In-One Deepfake Detection - https://sensity.ai/.

[83] New AI classifier for indicating AI-written text (OpenAI): https://arxiv.org/abs/2511.07009, zuletzt geprüft am 11.03.2026.

realistischere Outputs produzieren, hinken die Erkennungssysteme dieser Entwicklung hinterher.[84] Diese Entwicklung lässt sich auch dadurch begründen, dass die Technologie zur Erstellung synthetischer Inhalte stärker gefördert wird als deren Erkennung. Daher können solche Detektionswerkzeuge zwar eingesetzt werden, um verdächtige Inhalte vorzusortieren und zu prüfen. Dennoch bleibt für die finale Entscheidung eine manuelle Verifikation durch einen menschlichen Gutachter erforderlich. Dies gilt insbesondere dann, wenn die Ergebnisse für juristische Beweisführungen herangezogen werden sollen, da hier hohe Sicherheitsstandards und menschliche Urteilsfähigkeit unerlässlich sind (siehe dazu auch unter Punkt 3.3.4).

Ein derzeit noch aussagekräftiger Indikator für KI-generiertes Videomaterial ist die Videolänge, da aktuelle generative Modelle typischerweise nur Clips von wenigen Sekunden (Google Veo, Luma AI Dream Machine) bis maximal einigen Minuten (OpenAI Sora, Kuaishou KlingAI) produzieren können. Zudem weisen KI-generierte Videos häufig Fehler bei physikalischen Nuancen auf, etwa inkonsistente Schattenwürfe, unrealistische Lichtreflexionen, fehlerhafte Bewegungsabläufe oder Verstösse gegen physikalische Gesetze wie Gravitation und Objektpermanenz.

KI-generierte Bilder lassen sich ähnlich wie bei Videos häufig durch typische Artefakte identifizieren, darunter anatomische Ungereimtheiten wie zusätzliche oder fehlende Finger, asymmetrische Gesichtszüge, unrealistische Zahnstrukturen oder verzerrte Körperproportionen. Weitere Hinweise sind inkonsistente Beleuchtung, fehlerhafte Spiegelungen, unscharfe oder verschwommene Übergänge zwischen Objekten, unnatürliche Texturen sowie unleserliche oder verformte Schriftzüge im Hintergrund. Auffällig ist zudem oft eine übermässige Makellosigkeit,

[84] Evading Deepfake-Image Detectors with White- and Black-Box Attacks - https://arxiv.org/abs/2004.00622.

insbesondere bei Gesichtern mit unnatürlich glatter Haut, die kaum Poren, Unreinheiten oder natürliche Hautstrukturen aufweist.[85]

Bei KI-generiertem Audiomaterial können charakteristische Merkmale wie eine unnatürliche Sprachmelodie, monotone Betonung ohne emotionale Varianz, roboterhaft wirkende Stimmführung oder plötzliche Verzerrungen und Artefakte in der Tonqualität auf synthetische Erzeugung hindeuten. Besonders auffällig sind oft fehlende Atemgeräusche, unnatürliche Pausen sowie Inkonsistenzen in der Aussprache komplexer Wörter oder Namen.[86]

3.3.4 Gewährleistung der Beweissicherung bei Deepfake-Vorfällen

Die Beweissicherung bei Deepfake-Vorfällen erfordert ein systematisches und rasches Vorgehen, um die Verwertbarkeit digitaler Beweise im Strafverfahren zu gewährleisten. Im Zentrum steht die sofortige und umfassende Sicherung des Originalmaterials sowie des gesamten Kontextes. Sobald eine betroffene Person auf manipulierte Inhalte stösst, wird empfohlen, das gefälschte Material durch Screenshots, vollständige Kopien und Web-Archivierung (inklusive HTTP-Header, Plattform-ID, User-ID) zu sichern. Dabei sollten der exakte Zeitpunkt der Entdeckung, die Fundstelle (Plattform, URL) sowie sämtliche Begleitumstände präzise dokumentiert und mit Zeitstempeln versehen werden. Diese Momentaufnahme schafft die Grundlage für spätere Beweisführung, insbesondere wenn Täter das Material nachträglich entfernen.

Von entscheidender Bedeutung sind die forensische Analyse und Integritätssicherung der gesicherten Daten. IT-Forensik-Experten[87] können mittels spezialisierter

---

[85] Vgl. https://arxiv.org/abs/2406.14130, zuletzt geprüft am 09.03.2026.

[86] Vgl. https://arxiv.org/abs/2308.14970, zuletzt geprüft am 09.03.2026.

[87] Das Kommissariat Digitale Kriminalität bei der Landespolizei verfügt über entsprechend ausgebildetes Personal im Bereich digitale Forensik.

Tools (siehe dazu auch unter Punkt 3.3.3) die Authentizität des Materials untersuchen, Manipulationsartefakte aufdecken und die Deepfake-Natur versuchen nachzuweisen. Dabei ist die Unveränderbarkeit der Beweise essenziell. Jede Datei sollte in ihrem Originalzustand verbleiben, was durch die Berechnung kryptographischer Hashes sichergestellt wird.

Die Zusammenarbeit zwischen Plattformen und Behörden bildet eine weitere Säule zur effektiven Beweissicherungsstrategie.[88] Online-Plattformen verfügen über Meta-Daten, Log-Informationen und IP-Adressen, die zur Täteridentifikation beitragen können. Diese Informationen sollten zeitnah angefordert werden, bevor automatische Löschfristen greifen. Daher ist die frühzeitige Benachrichtigung der Behörden empfohlen. Selbstständige Ermittlungen sind zu vermeiden, da sie die Beweiskette gefährden können.

3.4 Präventive und gesellschaftliche Fragen

Nachdem die juristischen und technischen Rahmenbedingungen im Zusammenhang mit der Regulierung, Kennzeichnung, Erkennung sowie Löschung von Deepfakes dargelegt wurden, ist im Weiteren zu beleuchten, welche präventiven und gesellschaftlichen Massnahmen erforderlich sind, um einem Missbrauch solcher Technologien wirksam zu begegnen. Prävention kommt in diesem Bereich eine besonders hohe Bedeutung zu, da Deepfakes nicht nur rechtliche und technische Herausforderungen mit sich bringen, sondern auch das Vertrauen der Bevölkerung, die Integrität öffentlicher Institutionen sowie die digitale Sicherheit von Unternehmen und Privaten unmittelbar berühren.

Die zunehmende Verfügbarkeit leistungsfähiger KI-Werkzeuge macht es unabdingbar, dass die Bevölkerung aller Altersstufen, aber auch Unternehmen, Schulen

[88] Eine Zusammenarbeit setzt regelmässig ein vorangegangenes Rechtshilfeersuchen voraus.

und andere staatliche Institutionen über entsprechende Kenntnisse, Sensibilisierung und Schutzmechanismen verfügen. Präventive Massnahmen dienen nicht nur dem individuellen Schutz einzelner Betroffener, sondern leisten auch einen wesentlichen Beitrag zur Stärkung der gesellschaftlichen Resilienz gegenüber digitaler Manipulation, Desinformation und Identitätsmissbrauch.

Vor diesem Hintergrund gilt es, bestehende Initiativen auf nationaler Ebene zu beleuchten, bereits eingeführte oder geplante Programme sowie potenzielle weitere Massnahmen zu prüfen und daraufhin zu beurteilen, wie Liechtenstein in diesem sich rasch entwickelnden Bereich eine angemessene, wirksame und vorausschauende Schutzarchitektur gewährleisten kann. Erst durch ein Zusammenspiel aus rechtlicher Regulierung, technischer Expertise, pädagogischer und institutioneller Aufklärung kann ein umfassender Schutz[89] vor den Risiken künstlich erzeugter Manipulationen erreicht werden.

3.4.1 Fachgruppe Medienkompetenz (FGMK)

Der Fachgruppe Medienkompetenz (FGMK) kommt im Zuge der Aufklärung und Sensibilisierung zu digitalen Risiken, sowie der Förderung und Vermittlung von Bildungs- und Medienkompetenz eine entscheidende koordinierende Rolle zu.

Die Fachgruppe wurde im Frühjahr 2014 durch die Regierung als zentrale staatliche Koordinationsstelle für Fragen der Medienkompetenz eingerichtet.[90] Ihr Auftrag besteht darin, die im Land vorhandenen fachlichen Ressourcen zu bündeln und den gesamtgesellschaftlichen Zugang zu einem verantwortungsvollen Umgang mit digitalen Medien zu stärken. Sie versteht sich als Anlaufstelle für die

---

[89] An dieser Stelle ist klarzustellen, dass ein umfassender Schutz im Sinne einer vollständigen oder hundertprozentigen Sicherheit nicht realisierbar ist; erreichbar ist lediglich ein bestmöglicher, risikoorientierter Schutz, der fortlaufend den entsprechenden Entwicklungen angepasst werden muss.

[90] Entscheidung der Regierung vom 13. Mai 2014, LNR 2014-582 BNR 2014/638.

Bevölkerung und verfolgt einen klar präventiven Ansatz, der insbesondere Kinder, Jugendliche, Eltern und Fachpersonen unterstützt. Zu ihren Kernaufgaben gehören die Sensibilisierung für digitale Risiken, die Förderung eines sicheren und bewussten Medienumgangs, die Koordination bestehender Angebote sowie die Entwicklung und Bereitstellung niederschwelliger Informationsmaterialien. Die FGMK ist interdisziplinär zusammengesetzt und umfasst Vertreterinnen und Vertreter des Amts für Soziale Dienste, der Datenschutzstelle, des Schulamts, der Schulsozialarbeit, des Amts für Kommunikation und der Stabsstelle Cyber-Sicherheit; bei Bedarf wirken Staatsanwaltschaft und Landespolizei[91] mit. Sie betreibt zudem die Website «www.medienkompetenz.li», die seit 2021 als zentrale Plattform umfassende medienpräventive Inhalte bereitstellt und über aktuelle Kampagnen, Handlungsempfehlungen und Unterstützungsangebote informiert. Durch vielfältige Projekte – etwa Kampagnen zu Online-Betrug oder die medienpräventive Performance «angek(l)ickt»[92] in Kooperation mit dem Schulamt – trägt die Fachgruppe wesentlich dazu bei, Medienkompetenz in Liechtenstein nachhaltig zu fördern und auf neue gesellschaftliche Herausforderungen im digitalen Raum zu reagieren.

Aufgrund veränderter Bedingungen in der Medienlandschaft und nach über zehn Jahren Bestehen sollten die bisherigen Tätigkeiten evaluiert und mögliche Anpassungen – unter Einbezug externer Expertise – erörtert werden. Im Jahr 2025 wurden hierzu in zwei Workshops bestehende Akteure, Angebote und Zielgruppen im Bereich Medienkompetenz in Liechtenstein systematisch erfasst und analysiert. Gleichzeitig wurde eine neue Organisationsstruktur beschlossen, deren Umsetzung einen Regierungsantrag erfordert; die Einreichung dieses Regierungsantrags ist für das zweite Quartal 2026 vorgesehen.

---

[91] Kommissariat Digitale Kriminalität.

[92] https://www.llv.li/de/landesverwaltung/schulamt/bildungsbereiche/themen-und-projekte/angek-l-ickt---medien-praeventions-performance.

3.4.2 Aufklärung und Sensibilisierung der Bevölkerung

Die Aufklärung und Sensibilisierung der Bevölkerung zu Deepfakes erfolgt im Wesentlichen über die bestehenden Aktivitäten und Strukturen der FGMK. Sie nutzt etablierte Austauschplattformen wie die LIHGA[93], an der sie seit vielen Jahren mit einem eigenen Stand präsent ist und jeweils ein entsprechendes Schwerpunktthema setzt. Für 2026 könnte das Thema «Deepfakes» im Fokus stehen, wodurch eine breite und niederschwellige Sensibilisierung zu dieser Thematik ermöglicht werden soll.[94] Ergänzend organisiert die FGMK jährlich eine Herbstveranstaltung, bestehend aus Vorträgen und Podiumsdiskussionen, um die Bevölkerung vertieft über aktuelle digitale Risiken zu informieren und unterschiedliche Zielgruppen anzusprechen. Darüber hinaus stellt die Fachgruppe über ihre Website laufend Informationen, Hinweise und praktische Tipps bereit; insbesondere die Rubrik «Gut zu wissen»[95] bietet niedrigschwellige Orientierung, während externe Quellen wie die EU-kofinanzierte Plattform «klicksafe»[96] weiterführende Erklärungen und Beispiele zu Deepfakes vermitteln. Hinzu kommen Sensibilisierungskampagnen im Rahmen des «Safer Internet Day»[97], bei denen die FGMK in Kooperation mit der Landespolizei jeweils aktuelle Risiken thematisiert – ein Format, das künftig auch gezielt zur Aufklärung über Deepfakes genutzt werden soll. Schliesslich besteht jederzeit die Möglichkeit, Anliegen oder Fragen direkt an die FGMK zu richten[98], was eine unmittelbare Unterstützung und individuelle Sensibilisierung der

---

[93] Liechtensteinische Industrie-, Handels- und Gewerbeausstellung.

[94] Zum Zeitpunkt der Erstellung der Postulatsbeantwortung, hat die FGMK noch keine finale Entscheidung getroffen, ob sie an der LIHGA 2026 vertreten sein wird. Ausschlaggebend hierfür ist insbesondere die geplante organisatorische Neuausrichtung der FGMK im Jahr 2026. Mit Ausnahme der Teilnahme an der LIHGA 2026 sollen aber sämtliche geplanten Aktivitäten wie vorgesehen organisiert und durchgeführt werden.

[95] https://www.medienkompetenz.li/.

[96] https://www.klicksafe.de/.

[97] https://www.medienkompetenz.li/news/safer-internet-day-2025 und https://better-internet-for-kids.europa.eu/en/saferinternetday/liechtenstein.

[98] office@medienkompetenz.li.

Bevölkerung ermöglicht. Insgesamt verfügt Liechtenstein damit über ein breites, wirksames Instrumentarium, das ohne strukturelle Änderungen auf das Thema Deepfakes ausgerichtet werden kann.

Im Zuge der Behandlung des Postulats im Landtag wurde die Frage aufgeworfen inwiefern, neben der FGMK, auch die SCS ansprechende und zielgruppenorientierte Informations- und Aufklärungskampagnen zum Thema Deepfakes durchführen könne.

Dazu kann festgehalten werden, dass die Aufgaben der Stabsstelle gesetzlich in Art. 15 Cyber-Sicherheitsgesetz (CSG)[99] geregelt sind. Danach nimmt die SCS zentrale Funktionen als Drehscheibe, Vermittlungs- und Verbindungsstelle gegenüber Bevölkerung, Wirtschaft, kritischen Infrastrukturen und Staatsorganen wahr. Zudem ist die SCS die national zuständige Behörde für Cybersicherheit nach Art. 8 Abs. 1 der Richtlinie (EU) 2022/2555[100] (NIS-2) und übt die Aufsicht und den Vollzug des CSG aus.

Aus dieser gesetzlichen Zuordnung ergibt sich ein klarer Fokus auf wesentliche und wichtige Einrichtungen (kritische Infrastrukturen) als primäre Anspruchsgruppe. Der Schwerpunkt der Tätigkeit der SCS liegt damit auf der Sicherstellung der Cybersicherheit in den kritischen Sektoren im weiteren Sinn. Die Gestaltung zielgruppenspezifischer Informations- und Aufklärungskampagnen im Hinblick auf Deepfakes gehört nicht zu den originären Aufgaben der SCS und ist vom Gesetzgeber auch nicht vorgesehen. Wie bereits ausgeführt, fällt diese Aufgabe vielmehr in den Zuständigkeitsbereich der Fachgruppe Medienkompetenz.

---

[99] Cyber-Sicherheitsgesetz vom 5. Dezember 2024, LGBl. 2025 Nr. 111.

[100] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. 333 vom 27.12.2022, S. 80).

3.4.3 Bildungs- und Medienkompetenzmassnahmen für Kinder und Jugendliche

Die rasche Entwicklung der Informations- und Kommunikationstechnologien prägt die Lebenswelt von Kindern und Jugendlichen immer stärker und beeinflusst, wie sie kommunizieren, lernen, Beziehungen gestalten und Informationen verarbeiten. Digitale Medien sowie KI-generierte Inhalte – einschliesslich Deepfakes – verändern die Art und Weise, wie Wirklichkeit wahrgenommen wird und wie Informationen beurteilt werden müssen. Für Kinder und Jugendliche bedeutet dies, dass sie früh Kompetenzen aufbauen müssen, um sich in einer vielfältigen und teils schwer durchschaubaren digitalen Umgebung sicher orientieren zu können. Die Schule übernimmt hierbei eine zentrale Rolle.

Die Bedeutung digitaler Medien wirkt sich in vier Bereichen auf Schule und Unterricht aus. Aus der Lebensweltperspektive begegnen Kinder und Jugendliche bereits vor Schuleintritt einer Vielzahl digitaler Angebote; die Schule muss diesen Umgang aufgreifen und reflektieren. Aus der Berufsperspektive sind Medien-, Informatik- und IKT-Kompetenzen in nahezu allen beruflichen Laufbahnen erforderlich und müssen daher bereits während der obligatorischen Schulzeit aufgebaut werden. Aus der Bildungsperspektive erfordert die stetig zunehmende Informationsmenge Orientierungsfähigkeit, Problemlösungskompetenz und kooperatives Arbeiten. Und aus der Lehr-Lernperspektive müssen Schulen digitale Werkzeuge sinnvoll und stufengerecht in Unterricht und Lernprozesse integrieren, um die Potenziale neuer Medien für Lernen und Zusammenarbeit zu nutzen.[101]

Um diesen Veränderungen wirksam zu begegnen, ist eine verbindliche, fächerübergreifende Medien- und Informatikbildung erforderlich. Digitale

[101] https://fl.lehrplan.ch/index.php?code=e|10|2.

Grundkompetenzen müssen systematisch aufgebaut werden, damit Schülerinnen und Schüler digitale Inhalte verstehen, kritisch prüfen und verantwortungsvoll nutzen können. Dies geschieht an Liechtensteins Schulen basierend auf dem Lehrplan zu Medien und Informatik: In den Klassen 1. - 3. erfolgt der Aufbau digitaler Grundkompetenzen fächerintegrativ; in den Klassen 4. - 9. ist hierfür je eine Wochenlektion in den dafür vorgesehenen Stunden vorgesehen.[102] Wesentliche Elemente sind der Kompetenzaufbau bezüglich technischer Grundlagen digitaler Medien und der Funktionsweise manipulierter Inhalte, die Förderung kritischen Denkens sowie die Stärkung von Analyse- und Handlungskompetenzen. Dazu gehört auch, dass Lernende Quellen einordnen, Absichten hinter Inhalten erkennen und mögliche Manipulationsmerkmale beurteilen können. Praktische Übungen sowie die Reflexion rechtlicher und ethischer Aspekte – insbesondere des Persönlichkeitsschutzes – sind dabei zentral. Die wirksame Umsetzung setzt eine kontinuierliche Weiterbildung der Lehrpersonen voraus; diese wird in Liechtenstein bereits systematisch sichergestellt und fortlaufend angeboten (Weiterbildungsprogramme), damit Lehrpersonen fachlich sicher und pädagogisch wirksam mit KI-basierten Tools und digitalen Entwicklungen arbeiten können.[103]

Der Unterricht soll Schülerinnen und Schüler befähigen, zwischen echten und manipulierten Inhalten zu unterscheiden, Quellen kritisch zu hinterfragen und die Plausibilität digitaler Informationen einzuschätzen. Dazu gehören technische Grundlagen über digitale Bilder, Videos und Audiodateien, ein Verständnis für die Funktionsweise von KI-basierten Manipulationen sowie die Fähigkeit, Indikatoren für mögliche Bearbeitungen zu erkennen. Ergänzend sind praktische Analyseübungen mit altersgerechten Beispielen sinnvoll, wobei stets betont wird, dass solche

---

[102] https://regionalkonferenzen.ch/sites/default/files/2022-09/Stundentafeln_2022_Stand_2022-08-25_mit_FL.pdf.

[103] https://fl.lehrplan.ch/index.php?code=a|10|0|1|0|2.

Indikatoren keine absolute Sicherheit bieten. Die Förderung der Reflexionsfähigkeit und die Thematisierung rechtlicher und ethischer Fragen – etwa zum Umgang mit Persönlichkeitsrechten und zum Weiterverbreiten manipulierter Inhalte – sind weitere zentrale Elemente. Handlungskompetenz bedeutet dabei auch, dass Schülerinnen und Schüler wissen, wie sie im Verdachtsfall vorgehen und welche Ansprechstellen sie beiziehen können.

An Liechtensteins Schulen werden im Bereich Medien und Informatik Lehrmittel aus anerkannten Schweizer Schulbuchverlagen[104] (bspw. inform@21[105], Connected[106], Apropo Medien[107]) verwendet. Zu den unterschiedlichen Themen können Lehrpersonen ergänzend auf Materialien von «klicksafe.de», «jugendundmedien.ch» oder «saferintert.at» zurückgreifen. Diese bieten sowohl Unterrichts- als auch Informationsmaterialien zur Aufklärung der verschiedenen Zielgruppen (Schülerinnen und Schüler, Lehrpersonen, Eltern); verbindliche Lehrmittelvorgaben bestehen jedoch nicht. Die pädagogische Verantwortung für Planung, Auswahl und didaktisch zweckmässige Verwendung für den Kompetenzaufbau obliegt den jeweiligen Lehrpersonen im Rahmen der geltenden Vorgaben des Lehrplans.

Auf der Primarstufe liegt der Schwerpunkt darauf, ein grundlegendes Verständnis für die Manipulierbarkeit digitaler Inhalte zu entwickeln. Kinder sollen erkennen, dass nicht alles, was sie online sehen oder hören, echt sein muss. Sie lernen einfache Fragen zu Quelle und Zweck eines Inhalts zu stellen. Auch ein altersangemessenes Bewusstsein für respektvollen Umgang und Verantwortung in digitalen Räumen wird aufgebaut.[108]

---

[104] https://www.lehrmittelverlag.ch/suche?search=inform%4021.
[105] https://inform21.ch/de/.
[106] https://www.lmvz.ch/lehrmittel/connected.
[107] https://www.lehrmittelverlag.ch/suche?search=apropo.
[108] https://fl.lehrplan.ch/index.php?code=a|10|0|1|0|1.

In der Sekundarstufe werden diese Grundlagen vertieft: Jugendliche analysieren konkrete Beispiele digitaler Fälschungen, setzen sich mit Motiven und Auswirkungen von Manipulationen auseinander und lernen technische, kontextuelle und ethische Kriterien zur Beurteilung digitaler Inhalte kennen.[109] Ergänzend erfolgen praktische Übungen mit einfachen KI-Tools sowie die Auseinandersetzung mit rechtlichen und moralischen Aspekten, insbesondere zu Datenschutz, Persönlichkeitsrechten und den Folgen des Erstellens oder Verbreitens manipulierter Inhalte.[110]

Diese Unterrichtsinhalte werden im Rahmen einer Pilotphase durch sogenannte «Social-Media-Sprechstunden» nach dem Konzept der deutschen Medienexpertin Silke Müller[111] ergänzt. Über die Schulsozialarbeit und die Pädagogischen Medienkoordinatoren wird das Angebot zunächst an ausgewählten Schulen umgesetzt. Für die Schülerinnen und Schüler stehen hierzu regelmässige Sprechstunden zu festen Zeiten zur Verfügung. Auf Grundlage der Erfahrungen aus dieser Pilotphase wird im Verlaufe des kommenden Schuljahres geprüft, ob eine flächendeckende Einführung sinnvoll und machbar ist.

Die Fachgruppe Medienkompetenz ergänzt die schulischen Aktivitäten durch präventive, sensibilisierende und praxisnahe Angebote. Sie versteht sich als Akteurin, die konkrete Massnahmen bereitstellt und Schulen operative Unterstützung bietet, ohne selbst in die Lehrplanverantwortung einzugreifen. Ihre Mitglieder – darunter Mitarbeitende des Schulamts und der Schulsozialarbeit – verfügen über die notwendige Expertise, um altersgerechte Inhalte zu entwickeln und diese wirksam in den Schulkontext einzubringen. Ein zentraler Schwerpunkt der FGMK sind

---

[109] https://fl.lehrplan.ch/index.php?code=a|10|0|1|0|2.

[110] https://fl.lehrplan.ch/index.php?code=a|10|0|1|0|3 und https://fl.lehrplan.ch/index.php?code=a|10|0|1|0|4.

[111] https://www.socialmediasprechstunde.de/.

Workshops, die Kinder und Jugendliche unmittelbar erreichen. Bestehende Formate, wie Workshops zu Cyber-Mobbing, zeigen die Wirksamkeit solch niedrigschwelliger Angebote. Ergänzend sollen zusätzliche Workshops zu Deepfakes als realistische Weiterentwicklung angeboten werden. Darüber hinaus ist auf externe Programme zu verweisen, insbesondere die kostenlosen «aha»-Workshops für die 5. bis 9. Klassen, die gezielt auf den Aufbau von Medien- und Informationskompetenz ausgerichtet sind.[112] Ein weiterer Baustein ist die multimediale Präventions-Performance «angek(l)ickt»[113], die häufig von Schulklassen genutzt wird und deren Aktualisierung notwendig ist, um das Thema Deepfakes stärker zu integrieren. Auf diese Weise soll die FGMK bestehende Lücken schliessen, die Präventionsarbeit verstärken und dazu beitragen, dass Kinder und Jugendliche über den Unterricht hinaus sensibilisiert und handlungsfähig gemacht werden.

Der systematische, stufengerechte Aufbau von Medien- und Informationskompetenz ist eine zentrale Voraussetzung, um Kinder und Jugendliche in einer digital geprägten Welt zu einem sicheren, verantwortungsvollen und reflektierten Umgang mit Medien zu befähigen. Ergänzende Präventionsangebote der FGMK verstärken die schulischen Massnahmen und leisten einen wichtigen Beitrag, indem sie Sensibilisierung, Handlungssicherheit und konkrete Unterstützung im Schulalltag fördern.

3.4.4 Unterstützung von Eltern, Schulen und (weiteren) Institutionen

Schulen, Eltern und weitere Institutionen können beim Umgang mit Deepfakes wirksam unterstützt werden, indem sie einen niederschwelligen Zugang zu Fachwissen und klaren Handlungsschritten erhalten, um sich in der Thematik gezielt zu orientieren. Entscheidend sind dabei klare Leitlinien, praktische Unterstützung

[112] https://www.aha.li/medienworkshops_ab_14.
[113] https://www.angeklickt.li/.

und eindeutig benannte Ansprechstellen, damit Unsicherheiten reduziert und Vorfälle rasch und koordiniert bearbeitet werden können.

Für Eltern steht im Vordergrund, dass sie als erste Ansprechpersonen im Alltag gezielt entlastet und befähigt werden. Sinnvoll sind leicht verständliche Orientierungshilfen in alltagsnaher Sprache. Dazu zählen insbesondere bestehende Online-Angebote wie bspw. medien-kindersicher.li, klicksafe.de, saferinternet.at, jugendundmedien.ch, die erläutern, wie digitale Manipulation thematisiert werden kann und wie Gespräche mit Kindern und Jugendlichen gelingen. Flankierend sollen Informationsabende sowie ergänzende Leitfäden dazu beitragen, bestehende Unsicherheiten abzubauen.

Für Schulen und weitere Institutionen sind insbesondere praxisnahe Unterrichtsmaterialien, gezielte Weiterbildungsangebote und klare Eskalations- und Unterstützungswege unerlässlich. Lehrpersonen benötigen ein solides Grundverständnis sowie pädagogische Sicherheit, um Deepfakes einordnen, thematisieren und bei Vorfällen angemessen reagieren zu können. Hierzu tragen schulinterne Weiterbildungen, regionale Netzwerke sowie die Arbeit pädagogischer Medienkoordinatorinnen und -koordinatoren bei. Eine koordinierte Zusammenarbeit aller Beteiligten ist zentral, damit bei problematischen Konstellationen – etwa wenn Deepfakes in Mobbing-Situationen eingesetzt werden – rasch, abgestimmt und mit klarer Rollenverteilung gehandelt werden kann.

Strukturell wird diese Unterstützung im Schulbereich durch bereits vorhandene Funktionen abgesichert: An jeder Schule sind technische und pädagogische Medienkoordinatoren im Einsatz, die durch den Schul-IT-Koordinator (SIK)[114] und den

[114] SIK: https://www.llv.li/de/landesverwaltung/schulamt/organisation-schulamt/lebensraum-schule-zentrum-fuer-schulmedien#collapse-accordion-698f436f14ea8974976532-3.

pädagogischen Medienmentor (PMM)[115] des Schulamts strategisch begleitet werden. Dadurch stehen vor Ort planerische Kompetenzen und inhaltliche Unterstützung für Lehrpersonen zu Medien und Informatik zur Verfügung. Ergänzend stellt das Schulamt Weiterbildungen für Lehr- und Schulpersonal[116] bereit und informiert regelmässig über aktuelle Themen über den Newsletter «Schule heute» sowie über das Schulintranet Liechtenstein (SIL). Ebenso ist die Zusammenarbeit mit externen Fachstellen ein tragendes Element, um Fachwissen zu bündeln und Fälle zielgerichtet zu begleiten; dabei kommt auch der Schulsozialarbeit eine zentrale Rolle zu, insbesondere bei herausfordernden Situationen, in denen neben den Schülerinnen und Schülern auch Eltern Unterstützung benötigen.

Unterstützung wird dabei auf mehreren Ebenen angeboten, wobei im schulischen Umfeld die Schulsozialarbeit als besonders wichtiges, kostenloses und niederschwelliges Angebot des Schulamts hervorzuheben ist. Deren Kernleistungen umfassen Beratung, Intervention, Prävention und Projektarbeit für Schülerinnen und Schüler, Eltern sowie das Schul- und Lehrpersonal[117]. Zusätzlich leisten externe Akteure wie der Verein «aha» oder die FGMK Beiträge in Form kostenloser Dienstleistungen für Schulen und Erziehungsberechtigte. Konkret kann hierzu ausgeführt werden, dass die FGMK in der Vergangenheit Elternabende inhaltlich gestaltet oder zusammen mit Dritten organisiert hat; als Beispiel dient ein Impulsvortrag «Digitale Medien» in Kooperation mit der Landespolizei an weiterführenden Schulen, ergänzt durch eine Podiumsdiskussion unter Einbezug weiterer relevanter Stellen. Solche Formate stärken die Orientierung, fördern gemeinsame

---

115 PMM: https://www.llv.li/de/landesverwaltung/schulamt/organisation-schulamt/lebensraum-schule-zentrum-fuer-schulmedien#collapse-accordion-698f436f14ea8974976532-5.

116 Akademie BildungsPlus https://abp.studytube.com/discover.

117 https://www.llv.li/de/landesverwaltung/schulamt/bildungsbereiche/schulische-foerdermassnahmen/schulsozialarbeit.

Handlungssicherheit und verbessern die Abstimmung zwischen Schule, Elternhaus und unterstützenden Institutionen und sollen auch in Zukunft fortgeführt werden.

3.4.5 Zielgruppengerechte Gestaltung der Informationsarbeit auf Social-Media

Die FGMK bewirtschaftet keine eigenen Social-Media-Kanäle. Im Rahmen einzelner Projekte – etwa zum «Safer Internet Day» – werden jedoch Online-Werbung, Google-Anzeigen und Meta-Ads eingesetzt, um definierte Zielgruppen situativ zu erreichen. Für die professionelle Umsetzung solcher Kampagnen hat die FGMK den Auftrag für Konzept und Durchführung an eine externe Agentur vergeben.

In diesem Rahmen wurde die FGMK über zentrale Anforderungen einer zielgruppengerechten Kommunikation im Social-Media-Kontext informiert. Wesentlich sind eine klare strategische Ausrichtung und der gezielte Einsatz geeigneter Formate. Social-Media sind keine Kanäle für spontane oder konzeptlose Kommunikation; Inhalte müssen auf präzise definierten Zielgruppen, Botschaften und Formaten beruhen.

Die zielgruppenspezifische Gestaltung beginnt mit einer sauberen Segmentierung. Alter, Mediennutzung, Informationsverhalten und Interessen bestimmen, welche Plattformen beziehungsweise Formate geeignet sind. Inhalte müssen alltagsnah, visuell klar und in kurzen, leicht konsumierbaren Formaten vermittelt werden, insbesondere über kurze Videos oder Infografiken. Die Tonalität ist an die Zielgruppe anzupassen; Transparenz und Vertrauenswürdigkeit sind Grundvoraussetzungen.

Zielgruppengerechte Informationsarbeit gelingt, wenn Inhalte konsequent an den tatsächlichen Informationsbedürfnissen der Nutzerinnen und Nutzer ausgerichtet sind. Verständliche Sprache, klare Struktur und eine authentische, unaufdringliche Ansprache erhöhen die Akzeptanz. So wird Social-Media-Kommunikation nicht als

einseitige Mitteilung wahrgenommen, sondern als zugängliche, dialogorientierte Form öffentlicher Kommunikation.

Sollte sich die FGMK künftig dazu entscheiden, eigene Social-Media-Kanäle zu bewirtschaften, kann sie auf diese Informationen und Empfehlungen zurückgreifen und die Kommunikation entsprechend den dargelegten Anforderungen zielgruppengerecht ausgestalten.

3.5 Strategische Überlegungen

3.5.1 Alternative Lösungen, wenn gesetzliche Massnahmen gegen Plattformen nicht greifen

Wenn gesetzliche Massnahmen gegen Plattformbetreiber nicht greifen oder nicht wirksam durchgesetzt werden können, kommen alternative Ansätze in Betracht, die technische, organisatorische und präventive Elemente miteinander verbinden.

Aus praktischer Sicht sind temporäre Sperrungen einzelner Dienste eine mögliche Massnahme, wenn Betreiber rechtlichen Vorgaben oder Sanktionen nicht nachkommen. Beispiele aus anderen europäischen Staaten – etwa die zeitweise Sperrung eines Dienstes in Italien aufgrund datenschutzrechtlicher Verstösse[118] – zeigen jedoch, dass solche Eingriffe selten zu nachhaltiger Verhaltensänderung führen. Zudem können sie technische Umgehungsmöglichkeiten fördern und potenziell negative Auswirkungen auf Gesellschaft, Unternehmen und digitale Infrastrukturen haben.[119] Auch geopolitische Aspekte spielen eine Rolle, da viele relevante Plattformen von ausserhalb Europas betrieben werden.

---

[118] https://www.handelsblatt.com/technik/ki/kuenstliche-intelligenz-italien-wirft-chatgpt-verstoesse-gegen-datenschutzregeln-vor/100011242.html, zuletzt geprüft am 11.03.2026.

[119] https://www.security-insider.de/wirtschaftliche-auswirkungen-netzsperren-studie-a-8f422dbca2629c756e36c1923bd32bf8/.

Als Alternative zu etablierten, mehrheitlich US-amerikanischen oder chinesischen Plattformen existieren zwar dezentrale oder europäische Angebote, diese besitzen jedoch bislang überwiegend Nischencharakter. Das Beispiel des Mikroblogging-Dienstes «Mastodon»[120] mit wenigen Millionen aktiven Nutzern verdeutlicht die Diskrepanz im Vergleich zu globalen Plattformen wie X, die mehrere hundert Millionen monatliche Nutzer verzeichnen.[121] Ein Umstieg oder eine Verlagerung der öffentlichen Kommunikation ist daher nur in begrenztem Umfang realistisch und abhängig von politischen, gesellschaftlichen und geopolitischen Entwicklungen. Dennoch könnte die Diskussion um digitale Souveränität dazu führen, dass alternative Plattformen mittel- bis langfristig stärker genutzt werden.

Ein zentraler Baustein ist die Stärkung von Prävention und Bildung – insbesondere durch Medienkompetenz und breite Aufklärungskampagnen. Parallel dazu werden fortlaufend technische Ansätze entwickelt, die es erleichtern sollen, KI-generierte Inhalte zu erkennen oder zu kennzeichnen. Dazu gehören, wie bereits unter Punkt 3.3.1 ausgeführt, digitale Wasserzeichen wie SynthID sowie kryptografische Verfahren zur Authentifizierung von Medieninhalten. Für staatliche Kommunikation könnte künftig die systematische Kennzeichnung offizieller Inhalte über Signaturzertifikate eine zusätzliche Sicherheit schaffen. Detailliertere Ausführungen dazu finden sich unter Punkt 3.5.2.

Ergänzend könnte der Aufbau eines Frühwarnsystems geprüft werden, das KI-generierte Inhalte systematisch beobachtet und potenziell problematische Entwicklungen frühzeitig identifiziert. Eine Kooperation mit europäischen Partnern, Medienunternehmen oder bestehenden internationalen Initiativen kann die Wirksamkeit solcher Systeme erhöhen. Vor einer konkreten Umsetzung eines solchen

[120] https://joinmastodon.org/de.

[121] https://digiexe.com/blog/x-twitter-statistics.

Frühwarnsystems wäre zu klären, bei welcher inländischen Behörde dieses System organisatorisch zu verorten wäre. Die Aufgaben eines solchen Systems würden die kontinuierliche Beobachtung KI-generierter Inhalte, die Bewertung identifizierter Risiken sowie die koordinierte Information von Regierung, Verwaltung und gegebenenfalls der Öffentlichkeit umfassen. Ebenso wären die finanziellen und personellen Ressourcen zu bestimmen, da der Betrieb eines solchen Systems kontinuierliche technische Expertise sowie eine operative Auswertungs- und Reaktionsfähigkeit voraussetzt. Erst auf dieser Basis liesse sich beurteilen, ob ein nationales Frühwarnsystem eigenständig betrieben werden kann oder ob eine engere Anbindung an bestehende ausländische oder internationale Strukturen effizienter wäre.

Insgesamt zeigt sich, dass nachhaltige Alternativen zu regulatorischen Eingriffen nur dort entstehen, wo rechtliche Vorgaben, technische Schutzmechanismen und präventive Massnahmen ineinandergreifen. Ein koordiniertes Vorgehen auf nationaler und internationaler Ebene sowie die Einbindung von Forschung, Technologieanbietern und zivilgesellschaftlichen Akteuren könnten dabei die Grundlage für eine robuste und zukunftsfähige Strategie gegen Deepfakes bilden.

3.5.2 Stärkung des Vertrauens in Institutionen und Demokratie

Das Vertrauen in Institutionen und Demokratie könnte trotz der wachsenden Deepfake-Bedrohung gestärkt werden, wenn staatliche Stellen mehrere ineinandergreifende Massnahmen konsequent umsetzen.

Ausgangspunkt ist eine konsequente Sensibilisierung aller relevanten Zielgruppen: Behörden, Politik, Wirtschaft und Bevölkerung müssen verstehen, wie Deepfakes funktionieren, welche typischen Manipulationsmuster auftreten und weshalb Informationen stets über offizielle, verifizierte Kanäle abgeglichen werden sollten. Aufklärungskampagnen schaffen diese Grundhaltung und verhindern, dass einzelne Deepfake-Vorfälle das Vertrauen in den gesamten staatlichen

Informationsraum erschüttern. An dieser Stelle sei auf die vorangegangenen Ausführungen in Punkt 3.4 verwiesen.

Gleichzeitig braucht es einen belastbaren rechtlichen Rahmen. Die prioritäre Umsetzung der relevanten EU-Digitalisierungsrechtsakte – insbesondere DSA und KI-Verordnung – schafft klare Verantwortlichkeiten und stärkt die Aufsicht (siehe dazu die Ausführungen unter Punkt 3.2.2.1 und 3.2.2.2). Wie bereits unter Punkt 3.2.4 ausgeführt, sieht die Regierung gegenwärtig keinen Bedarf, darüber hinaus die bestehenden nationalen Rechtsnormen anzupassen oder zu ergänzen.

Wesentlich ist zudem, dass staatliche Informationskanäle (bspw. die offizielle Regierungswebseite, Webseiten einzelner Amtsstellen, verifizierte Social-Media-Accounts staatlicher Stellen) absolut verlässlich und eindeutig erkennbar sind. Eine konsistente visuelle und sprachliche Identität über alle Kanäle hinweg, die eindeutige Kennzeichnung verifizierter Konten und der konsequente Einsatz offizieller Kommunikationskanäle schaffen Orientierung und reduzieren die Wirksamkeit manipulierter Inhalte. Ergänzend müssen Institutionen transparent und proaktiv kommunizieren: Bei Desinformation oder Deepfake-Vorfällen erhöht eine schnelle, klare und konsistente Kommunikation die Glaubwürdigkeit. Wenn nachvollziehbar offengelegt wird, wie Informationen geprüft und Falschinformationen korrigiert werden, entsteht Vertrauen in die institutionelle Kompetenz.

Technische Schutzmechanismen stellen ein zusätzliches Vertrauenselement dar. Medienobjekte könnten bei ihrer Erstellung gehasht werden und die resultierende Prüfsumme (Hash-Wert) mit einem staatlichen Zertifikat kryptografisch gekennzeichnet werden. Dieses Signaturzertifikat würde als kryptografische Signatur im Hintergrund zur technischen Sicherstellung von Herkunft und Integrität digitaler Medieninhalte verwendet werden. Manipulationen am signierten Original wären damit eindeutig erkennbar. In einem staatlich geführten Register könnte ein für jedes offiziell publizierte Medienobjekt der Hashwert sowie die zugehörige

staatliche Signatur abgelegt werden. Die Einträge müssten zeitgestempelt und nur durch autorisierte Stellen schreibbar und für Dritte jederzeit les- und verifizierbar sein. Ein solches Register würde es erlauben, einen verlässlichen Abgleich zwischen Original und verbreiteten (gefälschten) Kopien vorzunehmen und sicherzustellen, dass die Integrität staatlicher Inhalte durch eine einfache zentrale Infrastruktur zuverlässig nachgewiesen werden kann (ergänzende Ausführungen dazu finden sich unter Punkt 3.3.1.).

Für die staatliche Kommunikation wäre eine solche kryptografische Kennzeichnung mittels Signaturzertifikat bereits heute technisch umsetzbar. Eine Implementierung würde jedoch ein entsprechendes Projekt erfordern, das in einer noch zu bestimmenden Behörde oder Amtsstelle angesiedelt werden müsste. Neben der technischen Umsetzung (Registerbetrieb, Schlüsselinfrastruktur, Schnittstellen für Publikationssysteme) wären umfassende juristische Abklärungen notwendig, insbesondere zu Zuständigkeiten, Datenhaltung, Haftung, Archivierungspflichten, öffentlicher Zugänglichkeit und zur gesetzlichen Grundlage für die Verwendung solcher kryptografischer Herkunfts- und Integritätsnachweise im Kontext multimedialer Inhalte. Zudem wäre zu definieren, welche Stelle die eingestellten Inhalte prüft, welche Qualitätsanforderungen daran gestellt werden und wie Support, Betrieb sowie allfällige Missbrauchsfälle gehandhabt werden. In diesem Zusammenhang wäre zu prüfen, ob eine zentrale staatliche Plattform als infrastruktureller Basisdienst aufgebaut werden kann, die es allen Behörden ermöglicht, ihre Medieninhalte technisch verifizierbar zu veröffentlichen.

In der Summe kann die Kombination dieser Elemente das Vertrauen stärken: Sensibilisierung erhöht die Aufmerksamkeit, klare Rechtsgrundlagen schaffen Orientierung, verlässliche staatliche Kommunikationskanäle geben Sicherheit, und technische Integritätsnachweise stellen sicher, dass offizielle Informationen überprüfbar bleiben.

3.5.3 Einrichtung einer zentralen Beschwerdestelle oder Anlaufstruktur

Im Verlauf der Landtagsdebatte wurde die Frage aufgeworfen, ob es möglich wäre, klare Melde- und Löschwege, eine technische Erkennung und Beweissicherung einzurichten sowie eine Zuständigkeit zu institutionalisieren (zentrale Beschwerdestelle oder Anlaufstruktur), die koordiniert und sanktioniert.

Dazu kann zunächst festgehalten werden: Wie bereits unter Punkt 3.2.6.1 ausgeführt, hat jede Person ein Recht auf Löschung ihrer widerrechtlich verarbeiteten Daten. Dieses Recht ergibt sich aus Art. 17 Abs. 1 Bst. d DSGVO und umfasst auch die Löschung von Deepfakes, sofern diese ohne Rechtsgrundlage verarbeitet werden. Die grossen Medienplattformen stellen hierfür üblicherweise direkte Meldewege bei einzelnen Beiträgen oder Videos bereit, über welche Verstösse der Datenverarbeitung angezeigt und Löschungsanträge gestellt werden können. Wird einem solchen Antrag nicht entsprochen, kann die betroffene Person Beschwerde bei der zuständigen Aufsichtsbehörde einreichen; in Liechtenstein ist dies die Datenschutzstelle. Eine Beschwerde kann gemäss Art. 77 DSGVO bei der Aufsichtsbehörde des Wohnsitzstaates eingebracht werden, selbst wenn der Verantwortliche seinen Sitz in einem anderen EU- oder EWR-Staat hat. Die Aufsichtsbehörde kann gestützt auf Art. 58 Abs. 2 Bst. g DSGVO die Löschung anordnen und durchsetzen oder die Beschwerde an die Behörde des Sitzstaates weiterleiten (Art. 56, 60 ff. DSGVO).

Wird eine Person aufgrund einer Veröffentlichung von Deepfakes Opfer einer Straftat (sog. Medieninhaltsdelikt nach Art. 2 Abs. 1 Ziff. 27 Mediengesetz), ist in strafrechtlicher Hinsicht zunächst zu unterscheiden, ob ein Privatanklagedelikt oder ein Offizialdelikt vorliegt. Bei Ehrverletzungsdelikten nach §§ 111 ff. StGB handelt es sich um Privatanklagedelikte im Sinne von § 2 Abs. 2 in Verbindung mit

§ 31 Abs. 1 StPO[122]. Dies betrifft etwa Fälle, in denen ein verfälschtes, jedoch inhaltlich nicht verbotenes pornographisches Bild oder Video veröffentlicht wird, welches je nach Sachverhalt den Tatbestand der üblen Nachrede oder der Verleumdung erfüllt. In diesen Fällen hat die betroffene Person binnen sechs Wochen ab Kenntnis von Tat und Tatverdächtigen direkt beim Landgericht Anzeige zu erstatten; Landespolizei und Staatsanwaltschaft sind nicht zuständig.

Alle Deepfake-Sachverhalte, die nicht als Privatanklagedelikte zu qualifizieren sind, stellen Offizialdelikte dar und werden gemäss § 2 Abs. 3 StPO von der Landespolizei und der Staatsanwaltschaft von Amtes wegen verfolgt. Dies ist beispielsweise der Fall, wenn ein Deepfake kinderpornographisches Material im Sinne von § 219 StGB enthält oder ein verfälschter Telefonanruf zur Begehung eines Betruges nach § 146 StGB eingesetzt wird. In diesen Fällen kann die betroffene Person Anzeige bei der Landespolizei oder der Staatsanwaltschaft erstatten (§ 55 StPO).

Nach Erstattung einer Anzeige sind die Behörden verpflichtet, die erforderlichen Beweise möglichst rasch zu sichern. Dies erfolgt durch die Landespolizei, bei Privatanklagedelikten jedoch erst nach einem entsprechenden Auftrag des Landgerichts. Die Beweissicherung umfasst insbesondere Screenshots, Audiofiles, Chatverläufe und URLs; detailliertere Ausführungen zu technischen Erkennungsmethoden und Beweissicherung finden sich unter Punkt 3.3.3 und 3.3.4.

Bei Offizialdelikten nimmt die Landespolizei die Vorerhebungen eigenständig vor oder handelt im Auftrag der Staatsanwaltschaft, sofern diese bereits involviert ist. Die Staatsanwaltschaft prüft zudem, ob eine Beschlagnahme oder Löschung der betreffenden Deepfake-Aufnahme angezeigt ist, insbesondere bei verbotenem

[122] Strafprozessordnung vom 18. Oktober 1988, LGBl. 1988 Nr. 62.

Inhalt (§ 96 StPO). Liegt ein Medieninhaltsdelikt vor, stehen zusätzlich die Mittel des Mediengesetzes zur Verfügung, insbesondere die Beschlagnahme nach Art. 50 und das Recht auf Gegendarstellung gemäss Art. 25, wobei diese je nach Deliktsart entweder von der betroffenen Person oder von der Staatsanwaltschaft zu beantragen sind. Unabhängig vom Strafverfahren können zivilrechtliche Ansprüche gegen Plattformbetreiber vor dem Landgericht geltend gemacht werden, etwa gestützt auf Art. 32 MedienG oder Art. 40 PGR.

Die Frage, ob die Einrichtung einer zentralen Beschwerdestelle oder Anlaufstruktur, welche die Aufgaben der Koordination und Sanktionierung wahrnimmt, sinnvoll ist, ist eine rechtspolitische Frage, die im Ermessen des Gesetzgebers liegt. Eine solche Stelle könnte für betroffene Personen den Vorteil eines einzigen Ansprechpartners bieten. Gleichzeitig wären die damit verbundenen Einschränkungen oder Nachteile zu berücksichtigen. Insbesondere bei Delikten im Internet ist eine rasche Sicherung der Beweise entscheidend; eine zwischengeschaltete Stelle birgt das Risiko zeitlicher Verzögerungen. Zu beachten ist zudem, dass bei Privatanklagedelikten sehr kurze Fristen gelten, deren Versäumnis zu einer Verfristung der Strafverfolgung führen und Haftungsfragen aufwerfen kann. Weiter ist mit Abgrenzungsfragen hinsichtlich der Zuständigkeiten zu rechnen. Schliesslich ist offen, ob eine solche Stelle in der Praxis überhaupt ausreichend ausgelastet wäre; sollte dies der Fall sein, müsste sie personell so ausgestattet werden, dass die fristgebundene Beweissicherung jederzeit gewährleistet werden kann.

Abschliessend besteht, wie bereits unter 3.2.7.1 ausgeführt, in der Praxis das Problem der Beweissicherung bzw. der Herausgabe relevanter elektronischer Beweismittel, wenn sich die entsprechenden Daten im Ausland befinden.

3.6 Jüngste Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung

Zum Zeitpunkt der Finalisierung der gegenständlichen Postulatsbeantwortung wurden in kurzer zeitlicher Abfolge mehrere Entwicklungen bekannt, auf die im Sinne der Vollständigkeit noch hinzuweisen ist. Diese Entwicklungen konnten im Hauptteil der Ausführungen nicht mehr systematisch berücksichtigt werden, sind jedoch für die rechtspolitische Einordnung von Bedeutung.

Zum einen geht es um die nicht einvernehmliche pornografische Darstellung durch Deepfakes und die damit verbundene Verbreitung in sozialen Medien. Innert kürzester Zeit wurde auf bundesdeutscher Ebene reagiert und angekündigt, einen Gesetzesentwurf vorzulegen, der die Herstellung und Verbreitung pornographischer-Deepfakes ausdrücklich unter Strafe stellen soll.[123]

Nahezu zeitgleich wurde auf europäischer Ebene berichtet, dass das Europäische Parlament eine weitere Verschärfung der Regulierung im Bereich Künstliche Intelligenz unterstützt. Im Zentrum steht ein Verbot bestimmter KI-Anwendungen, die es ermöglichen, nicht einvernehmliche pornographische Deepfakes zu erzeugen. Konkret soll die KI-Verordnung dahingehend abgeändert bzw. ergänzt werden, dass Systeme untersagt werden, die sexuelle Darstellungen realer Personen künstlich erzeugen oder bestehendes Material entsprechend verändern, sofern keine Einwilligung der betroffenen Person vorliegt. Die endgültige Ausgestaltung dieser Regelungen ist Gegenstand der laufenden Verhandlungen zwischen Europäischem Parlament und Rat der Europäischen Union. Gemäss Medienberichten soll das

123 https://www.dw.com/de/fall-fernandes-regierung-k%C3%BCndigt-kampf-gegen-deepfakes-an/a-76453422, zuletzt geprüft am 26.03.2026.

Verbot in einigen Monaten greifen, sobald die Änderung endgültig beschlossen ist.[124]

Die Regierung nimmt die dargestellten Entwicklungen zur Kenntnis und verfolgt diese mit besonderer Aufmerksamkeit. Dies betrifft sowohl den konkreten Fall in Deutschland als auch die aktuellen regulatorischen Initiativen auf europäischer Ebene im Bereich nicht einvernehmlicher pornographischer Deepfakes.

In diesem Zusammenhang ist zu berücksichtigen, dass sich, wie bereits ausgeführt, eine Weiterentwicklung des bestehenden europäischen Rechtsrahmens abzeichnet. Im Rahmen der KI-Verordnung sollen zusätzliche materielle Vorgaben oder Verbote im Zusammenhang mit bestimmten Deepfake-Anwendungen eingeführt werden. Da die KI-Verordnung nach ihrer Übernahme in das EWR-Abkommen auch für Liechtenstein unmittelbar Geltung entfaltet, erscheint es sachgerecht, diese Entwicklungen abzuwarten. Ein nationaler Vorgriff auf laufende europäische Gesetzgebungsprozesse wäre mit Blick auf die angestrebte Harmonisierung sowie die grenzüberschreitende Natur der betroffenen Sachverhalte nicht zweckmässig.

3.7 Zusammenfassung

Zusammenfassend kann festgehalten werden, dass das geltende liechtensteinische Recht bereits heute verschiedene wirksame Mechanismen zur Bekämpfung von Deepfakes bereitstellt. Es wird deshalb gegenwärtig nicht als erforderlich erachtet, über die EU-Digitalisierungsrechtsakte, namentlich die KI-Verordnung und den Digital Services Act, hinaus Ergänzungen im nationalen Recht vorzunehmen. Ein Blick ins europäische Ausland zeigt, dass entsprechende Gesetzgebungsaktivitäten bislang überwiegend punktuell sind. Ein europaweiter Trend zu nationalen

---

124 https://www.derstandard.at/story/3000000314251/eu-parlament-stimmte-f252r-verbot-von-ki-systemen-f252r-porno-deepfakes zuletzt geprüft am 26.03.2026.

Sonderregelungen ist derzeit nicht erkennbar. Die Regierung nimmt zudem jüngste Entwicklungen zum Zeitpunkt der Finalisierung der Postulatsbeantwortung im Zusammenhang mit nicht einvernehmlichen Deepfake-Anwendungen sowie entsprechende rechtspolitische Diskussionen zur Kenntnis und beobachtet diese fortlaufend; ein nationaler Vorgriff auf laufende europäische Gesetzgebungsprozesse erscheint gegenwärtig nicht angezeigt. Sobald sich gesetzliche Lösungswege in umliegenden Ländern abzeichnen, erwägt die Regierung eine zeitnahe Umsetzung von griffigen Strafbarkeitsnormen, um Betroffene in Liechtenstein schützen zu können.

Darüber hinaus ist festzustellen, dass die nationale Rechtsdurchsetzung insbesondere dort an ihre Grenzen stösst, wo Urheber unbekannt oder im Ausland tätig sind und Plattformen ihren Sitz ausserhalb Liechtensteins haben. In diesen Fällen sind straf- und zivilrechtliche Schritte zwar grundsätzlich möglich, ihre praktische Durchsetzung erfolgt jedoch in der Regel über langwierige internationale Rechtshilfeverfahren. Weder die Übernahme der KI-Verordnung noch des DSA vermögen diese strukturellen Vollzugsgrenzen vollständig zu beseitigen; sie können jedoch in bestimmten Konstellationen – insbesondere im Verhältnis zu den in der EU tätigen Plattformen – die praktische Durchsetzung erleichtern.

Aus den technischen Ausführungen kann der Schluss gezogen werden, dass obwohl verschiedene technische Schutz-, Lösch- und Erkennungsmethoden existieren, diese bis dato keinen zuverlässigen Schutz gegen entschlossenen Missbrauch bieten.

Hinsichtlich Prävention, Sensibilisierung und Medienkompetenz verfügt Liechtenstein über gut ausgebaute und wirksame Strukturen, die ohne strukturelle Änderungen gezielt auf das Thema Deepfakes ausgerichtet werden können. Die bestehenden Angebote ermöglichen es, Medienkompetenz zu stärken, Aufklärung zu

leisten und Bevölkerung, Schulen und Eltern im Umgang mit Deepfakes wirksam zu unterstützen.

Die strategischen Überlegungen zeigen, dass neben rechtlichen, technischen und präventiven Instrumenten auch weiterführende organisatorische Massnahmen geprüft werden können, um den Umgang mit Deepfakes längerfristig abzusichern. Eine Option ist die Prüfung eines Frühwarnsystems, das künstlich erzeugte Inhalte frühzeitig identifizieren soll. Ein solches System wäre jedoch ressourcenintensiv und würde zusätzlichen finanziellen, personellen und administrativen Aufwand verursachen. Weiter kann die Kennzeichnung staatlicher Kommunikation mittels Signaturzertifikat erwogen werden. Dies würde die Nachvollziehbarkeit amtlicher Inhalte erhöhen, erfordert aber umfassende rechtliche Abklärungen zu Zuständigkeiten, Datenhaltung und Haftung sowie einen dauerhaften administrativen Betrieb. Auch ein staatlich geführtes Register für authentische staatliche Medienobjekte wäre denkbar. Für eine Umsetzung bräuchte es klare gesetzliche Grundlagen, technische Infrastruktur und zusätzliche Ressourcen. Ergänzend könnte die Einrichtung einer zentralen Beschwerde- oder Anlaufstelle geprüft werden. Eine solche Stelle könnte den Zugang für Betroffene vereinfachen, würde aber ebenfalls zusätzlichen organisatorischen und administrativen Aufwand auslösen und müsste sorgfältig mit bestehenden Zuständigkeiten (Datenschutzstelle, Landespolizei, Staatsanwaltschaft, Gerichte) abgestimmt werden.

II. ANTRAG DER REGIERUNG

Aufgrund der vorstehenden Ausführungen unterbreitet die Regierung dem Landtag den

A n t r a g ,

der Hohe Landtag wolle diese Postulatsbeantwortung zur Kenntnis nehmen und das Postulat vom 26. August 2025 abschreiben.

Genehmigen Sie, sehr geehrter Herr Landtagspräsident, sehr geehrte Frauen und Herren Abgeordnete, den Ausdruck der vorzüglichen Hochachtung.

REGIERUNG DES
FÜRSTENTUMS LIECHTENSTEIN

gez. Brigitte Haas