

# Digitale Demokratie

Digitale Technologien zur Verbrechensbekämpfung und zur Stärkung der europäischen Souveränität waren Themen beim Internet-Summit Austria 2025.

Der Internet-Summit Austria des Österreichischen Verbands der Internet Service Provider (ISPA) fand 2025 unter dem Titel „Digitale Demokratie. Codes, Kontrolle und Gestaltung“ statt. Die Veranstaltung widmete sich der Frage, wie demokratische Errungenschaften in einer zunehmend digitalisierten Gesellschaft bewahrt werden können. Ein zentraler Punkt war das Spannungsverhältnis zwischen dem Schutz der Grundrechte und staatlichen Überwachungsmaßnahmen

zur Kriminalitätsbekämpfung. Dies sprach Stefan Ebenberger, Generalsekretär der ISPA, an: „Wenn wir Freiheit und Grundrechte wollen, müssen wir sie auch im digitalen Raum schützen.“ Staatliche Eingriffe müssten technisch umsetzbar, überprüfbar und verhältnismäßig sein. Ebenberger wies darauf hin, dass sich durch Überwachung neue Angriffsflächen ergeben können, was wiederum Schutzmaßnahmen erforderlich mache.

Für Wolfgang Ebner, Sektionschef im Bundeskanzleramt, ist „Verantwortung“ ein Schlüsselwort der digitalen Transformation. Er beschrieb die Vision einer Verantwortungsgesellschaft, in der der Staat die bestmöglichen Rahmenbedingungen für eine gute und krisenfeste Infrastruktur bereitstellt. Vor dem Hintergrund der zahlreichen Cyber-Angriffe sei es ein Ziel, dass sich die Menschen sicher im digitalen Raum bewegen können. Als Masterplan dafür dient der *Digital Austria Act*, der einen gemeinsamen strategischen Rahmen über Ressortgrenzen hinweg bildet.

**Bürger einbeziehen.** Julian Nida-Rümelin, Rektor der humanistischen Hochschule Berlin und Staatsminister für Kultur und Medien a. D., brachte seine Erfahrungen über Demokratie im 21. Jahrhundert als Philosoph und ehemaliger Politiker ein. Er sieht eine Gefahr für die Demokratie darin, dass zunehmend mehr Bürger der Ansicht sei-



Internet-Summit: Stefan Ebenberger, Thomas Lohninger, René Mayrhofer, Omar Haijawi-Pirchner, Thomas Korntheuer

en, sie könnten die Politik nicht beeinflussen. Mit Hilfe digitaler Tools lasse sich die Bevölkerung in politische Entscheidungsprozesse einbeziehen. Damit werde eine Verbindung zwischen der Politik und den Lebenswelten der Menschen hergestellt. In einer Podiumsdiskussion wurde die These „Kriminalität ist der Preis der Freiheit“ aus unterschiedlichen Perspektiven beleuchtet:

**Epicenter-Works.** Thomas Lohninger, Geschäftsführer des Vereins epicenter.works, der sich für digitale Bürgerrechte einsetzt, warnte vor den Gefahren von Maßnahmen wie dem „Bundestrojaner“: „Ist der staatliche Zugriff auf das Private einmal gewährt, dann ist man nur eine Wahl davon entfernt, dass Oppositionelle, NGOs und Journalisten ins Visier der Überwachung geraten.“ In manchen Ländern, deren Behörden einen Trojaner nutzen, werde dieser auch gegen Aktivisten und Medienvertreter eingesetzt. Lohninger hält andere Maßnahmen für ausreichend, um Sicherheit zu gewährleisten, ohne die Freiheit zu gefährden – etwa Prävention, Integration, Deradikalisierung, klassische Polizeiarbeit anhand von Spuren sowie ein schärferes Waffenrecht.

**DSN.** Warum die Maßnahmen nicht ausreichen, die der österreichischen Polizei derzeit zur Verfügung stehen, erklärte der Direktor der Direktion Staatsschutz und Nachrichtendienst Omar

Haijawi-Pirchner am Beispiel des vereitelten Terroranschlags gegen ein Taylor-Swift-Konzert in Wien: „Wir sehen bei der Auswertung des Falls, dass umfangreiche Absprachen stattgefunden haben: zu Waffenkäufen, zu Gewalttaten, zu Mord.“ Mit den entsprechenden Mitteln zur Telekommunikationsüberwachung hätte die DSN schon zum Zeitpunkt der Festnahme gewusst, wer die Mittäter waren und welchen Plan die Terrorzelle hatte. Haijawi-Pirchner wies darauf hin, dass entscheidende Informationen zu

den Anschlagplänen auf eines der Taylor-Swift-Konzerte von ausländischen Diensten kamen, die weitreichendere Befugnisse zur Telekommunikationsüberwachung haben. „Ich kenne keinen einzigen europäischen Staat außer Österreich, der Gefährderüberwachung, Trojaner und Co. derzeit nicht nutzt“, sagte der DSN-Direktor. Österreich bekomme täglich Hinweise aus dem Ausland in Zusammenhang mit Rechtsextremismus, islamistischem Terrorismus oder Spionage und sei auf Informationen ausländischer Dienste angewiesen. Das gelte aber auch für andere Länder, denn ein Staat alleine könne die aktuelle Bedrohungslage nicht bewältigen.

**Kepler-Uni.** René Mayrhofer, Professor am Institut für Netzwerke und Sicherheit der Linzer Johannes-Kepler-Universität, äußerte Bedenken über Sicherheitslücken, die zur Überwachung genutzt werden. „Das Design der Smartphone-Betriebssysteme sieht vor, dass Apps nicht auf die Daten anderer Apps zugreifen können. Wenn man durch eine App auf die gespeicherten Chat-Protokolle zugreifen möchte, funktioniert das nur, indem man mehrere Sicherheitsebenen durchbricht“, gab Mayrhofer zu bedenken. Diese Sicherheitslücke könne auch von Kriminellen genutzt werden. Ein weiteres Risiko sah Mayrhofer darin, dass die österreichischen Behörden nicht in der Lage seien, Überwachungslösungen zu

entwickeln, und diese daher zukaufen müssen. Die Anbieter solcher Lösungen hätten Zugriff auf die Daten der Smartphone-Nutzer. Auch ausländische Dienste könnten „mitlesen“.

**Staatsanwaltschaft.** Thomas Korntheuer von der Vereinigung österreichischer Staatsanwältinnen und Staatsanwälte betrachtete das Thema aus rechtlicher Sicht. Er berief sich auf den Europäischen Gerichtshof für Menschenrechte, der bereits 1978 festgehalten habe, dass geheime Überwachung zum Schutz vor Terrorismus notwendig sei. Ein Missbrauch staatlicher Überwachungsbefugnisse müsse verhindert werden. Die österreichische Strafprozessordnung ermögliche es schon jetzt, SMS und Telefonie zu überwachen – allerdings reicht das laut Korntheuer nicht aus: „Die StPO kann in der momentanen Form mit dem technischen Fortschritt nicht Schritt halten. Tätersforschung und vor allem Vermögenssicherung stellen sich oft als unmöglich dar. Daraus resultiert ein enormer volkswirtschaftlicher Schaden.“ Das Strafrecht müsse zeitgemäße Möglichkeiten haben, um die Gesellschaft vor neuen For-

men der Kriminalität zu schützen. Messengerüberwachung wäre ein nötiger Lückenschluss.

**Souveränität.** Die Table-Sessions waren unterschiedlichen Aspekten der digitalen Souveränität Europas gewidmet. Als Gefahr sahen die Leiter der Sessions die Abhängigkeit Europas von externen Technologieanbietern – von der Chip- und Halbleiterproduktion über Cloud-Dienste bis hin zu Softwareplattformen.

Joe Pichlmayr, CEO der *Ikarus Security Software GmbH*, bezeichnete Europa als „digitale Kolonie“. Die USA würden hier eine dominante Rolle spielen. Sie könnten die europäischen Länder wirtschaftlich unter Druck setzen – etwa, wenn die EU planen würde, rechtlich gegen die großen Plattformen vorzugehen. Auch im militärischen Bereich sei Europa von den Vereinigten Staaten abhängig. Als positives Beispiel führte Pichlmayr das österreichische Bundesheer an: „Trotz begrenzter Mittel hat es eigene Clients ohne US-Technologie entwickelt und ist gut in den europäischen Verband eingebunden.“ US-amerikanische oder chinesische IT-Lösun-

gen für kritische Infrastruktur kopieren zu wollen, ist für Georg Hahn, Generalsekretär der *Austria Open Source Software Business Innovation Group (OS-SBIG)*, nicht der richtige Weg für Europa. Der kleinteilige, multikulturelle, inhomogene Kontinent, dessen demokratische Systeme gut funktionieren, sollte vielmehr auf Open Source und innereuropäische Kooperation setzen.

**Digitalpolitik.** Bei einer Podiumsdiskussion nahmen Vertreter der Parlamentsparteien zur Digitalpolitik in der aktuellen Legislaturperiode Stellung. Als Schwerpunkte wurden Vereinfachungen in der Verwaltung, IT-Bildung und die Umsetzung des AI-Acts genannt. Einigkeit herrschte darüber, dass Fortschritte in der Digitalisierung nur im europäischen Verbund möglich sind. Georg Chytil, erster Vizepräsident der ISPA, wies auf die Chance hin, die Online-Partizipation für die Demokratie bietet, und auf die Notwendigkeit, Europas digitale Souveränität zu stärken. Europa – und auch Österreich – könne selbstbewusst sein, so Chytil: „Wir haben die nötigen Kompetenzen, brauchen aber mehr Kooperation.“ *R. P.*