FUTURE LAW
WORKING PAPERS 2025 • 1

MATTHIAS C. KETTEMANN • MALTE KRAMME
CLARA RAUCHEGGER • CAROLINE VOITHOFER
EDITORS

universität innsbruck
Institut für Theorie und Zukunft des Rechts

Alles, was Recht ist (2024)

Gesammelte Blogbeiträge des auf „Der Standard.at“ erscheinenden Blogs der Rechtswissenschaftlichen Fakultät der Universität Innsbruck

HERAUSGEGEBEN VON.

MATTHIAS C. KETTEMANN

INNSBRUCK

JÄNNER 2025 • ZUKUNFTSRECHT@UIBK.AC.AT

The Future Law Working Papers was established in 2022 to offer a forum for cutting-edge research on legal topics connected to the challenges of the future. As the German Constitutional Court recently ruled, we have to act today to save the freedoms of tomorrow. Similarly, the Future Law Working Papers series hosts research that tackles difficult questions and provides challenging, and at times uncomfortable, answers, to the question of how to design good normative frameworks to ensure that rights and obligations are spread fairly within societies and between societies, in this generation and the next. The series is open for interdisciplinary papers with a normative twist and the editors encourage creative thinking. If you are interested in contributing, please send an email to the editors at zukunftsrecht@uibk.ac.at. Submissions are welcome in English and German.

The series is edited by the senior members of the Department of Legal Theory and the Future of Law at the University of Innsbruck, Matthias C. Kettemann, Malte Kramme, Clara Rauchegger and Caroline Voithofer.

Founded in 2019 as the tenth department of the law faculty, the Department of Legal Theory and Future of Law at the University of Innsbruck (ITZR) investigates how law can make individuals as well as society, states as well as Europe "fit" for the future and if and how law has to change in order to meet future challenges. This includes the preservation of freedom spaces as well as natural resources in an intergenerational perspective, the safeguarding of societal cohesion in times of technologically fueled value change, the normative framing of sustainable digitization and digitized sustainability, and the breaking through of traditional legal structures of domination and thought with a view to rediscovering the emancipatory element of law against law.

Publisher: Institut für Theorie und Zukunft des Rechts, Universität Innsbruck
Innrain 15, 6020 Innsbruck
Univ.-Prof. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)
Univ.-Prof. Dr. Malte Kramme
Ass. Prof.in MMag.a Dr. Clara Rauchegger, LL.M. (Cambridge)
Univ.-Ass.in MMag.a Dr.in Caroline Voithofer

Alles, was Recht ist (2024)

Gesammelte Blogbeiträge des auf
„Der Standard.at“ erscheinenden Blogs der
Rechtswissenschaftlichen Fakultät
der Universität Innsbruck

herausgegeben von
Matthias C. Kettemann
Innsbruck

Inhaltsverzeichnis

Neue Herausforderungen, alte Rechte: Wie robust sind unsere Menschenrechte?

Können uns die bestehenden Menschenrechte vor den Gefahren der digitalen Welt schützen?

Matthias C. Kettemann, Caroline Böck

Im Gastblog diskutieren Matthias C. Kettemann und Caroline Böck, ob die bestehenden Menschenrechte ausreichen, um die Herausforderungen der digitalen Welt zu bewältigen, oder ob es neue Ansätze braucht, um den Schutz in Zeiten von Fake News, Hatespeech und Cybersicherheitsrisiken sicherzustellen.

Menschenrechte – was bringen sie eigentlich noch? Jeden Tag erfahren wir mehr und mehr zu Kriegen, Hungersnöten und menschenunwürdigen Behandlungen in der realen Welt. Doch nicht nur die reale Welt steht vor großen Herausforderungen. Im 21. Jahrhundert ist noch eine weiteres Phänomen hinzugekommen, das unser sozioökonomisches und politisch-kulturelles Zusammenleben auf globaler Ebene mitbestimmt: die Digitalisierung. Hierdurch verändern sich alltägliche Aufgaben, die Arbeit, unsere Kommunikation und auch unsere Entscheidungsfindung.

Diese Veränderungen haben zahlreiche Vorteile, doch es kristallisieren sich auch viele Herausforderungen heraus. Das jüngste Global Risks Perception Survey des World Economic Forum (2023 bis 2024) zählt drei digitalisierungsbedingte Risiken zu den Top 12 globalen Risiken, wobei "Fehlinformationen und Desinformation" bei den kurzfristigen Risiken an erster Stelle und Cybersicherheit an vierter Stelle stehen. In einem langfristigeren Zeitraum von zehn Jahren stehen Fehlinformationen und Desinformation, negative Folgen von KI-Technologien und Cybersicherheit auf den Plätzen fünf, sechs und acht, nur übertroffen von vier Wetter- und ökosystembezogenen Risiken.

Brauchen wir neue Menschenrechte?

Vor dem Hintergrund des 75-jährigen Jubiläums der Allgemeinen Erklärung der Menschenrechte und 30 Jahre nach der Erklärung von Wien und das dazugehörige Aktionsprogramm, die im Bereich der Menschenrechte aus Ebene der Vereinten Nationen eine herausragende Bedeutung aufweisen, haben wir, Matthias C. Kettemann und Caroline Böck, gefördert durch das Außenministerium versucht, die Frage zu beantworten, ob es neue Menschenrechte braucht, um die digitalen Herausforderungen zu bewältigen.
Das Ergebnis aus unserer Sicht ist klar: Neue Menschenrechte sind nicht notwendig und schwer in kurzer Zeit zu erarbeiten. Die Erarbeitung solcher Erklärungen würde demnach in einem angemessenen Zeitraum nicht die gewünschten Ergebnisse liefern. Es ist an der Zeit, sich auf die Nutzung der bestehenden Menschenrechte zu konzentrieren, da sich zahlreiche Staaten auf globaler Ebene hierauf bereits einigen konnten. Die Anwendung der bestehenden Menschenrechte muss auf die Herausforderungen des digitalen Zeitalters abgestimmt werden. Die Wiener Erklärung und das Aktionsprogramm haben vor 30 Jahren einhellig festgestellt, dass es notwendig ist, sich wieder zu einem ganzheitlichen Verständnis der Menschenrechte

zu bekennen. Genau diese Feststellung sollte in die Erinnerung vieler Staaten gerufen werden und sie sollten angehalten werden, für eine Durchsetzung der Menschenrechte zu kämpfen.

Regierungen auf der ganzen Welt müssen entschlossen handeln, um die Menschenrechte zu schützen. Die digitalen Herausforderungen sind erheblich, aber bewältigbar. Es ist an der Zeit, sicherzustellen, dass entstehende digitalisierte Gesellschaften und digitale Kommunikationsräume zu Orten werden, an denen Menschenrechte und menschliche Sicherheit gewährleistet sind und die menschliche Entwicklung unterstützt wird. Um dies zu belegen haben wir in unserer Studie anhand zahlreicher Beispiele aufgezeigt, wie sich die digitale Transformation auf bestehende Menschenrechte auswirkt und wie diese Menschenrechte im Hinblick auf ihre Rolle und Relevanz für das digitale Zeitalter angewendet und gestärkt werden müssen. Ein Hinterfragen der Menschenrechtskataloge im Ganzen ist demnach nicht erforderlich.

Lethal Autonomous Weapon Systems

Ein besonders einprägsames Beispiel in diesem Zusammenhang stellt die Nutzung von sogenannten Lethal Autonomous Weapon Systems (LAWS, Letale Autonome Waffensysteme) dar. Diese werden durch eine UN Working Group wie folgt definiert: LAWS zeichnen sich durch die Ausführung tödlicher Angriffe ohne vorherige menschliche Entscheidung im konkreten Einzelfall aus. Die Systeme entscheiden selbst, zum Beispiel auf Basis von KI-Systemen, wie und wo ein tödlicher Angriff durchgeführt wird. Ein Mensch schaltet das System nur bei Bedarf ein oder aus.

Diese Definition umfasst angebrachte Landminen, die seit Jahrzehnten im Einsatz sind, aber auch die neuesten Entwicklungen im Bereich der autonomen Raketenabwehrsysteme, sowie "Kamikaze"-Drohnen, die selbstständig den Boden erfassen und ein Ziel für sich bestimmen, sowie bewaffnete autonome Land- und Seefahrzeuge. Gerade diese neuen technischen Entwicklungen der Kriegswaffen sind geeignet großen Schaden für Leib und Leben hervorzurufen, ohne dabei von menschlichen Akteuren gesteuert zu werden, die über eine konkrete Tötung im Einzelfall entscheiden können. Diese Waffen sind aus völkerrechtlicher Sicht umso bedenklicher, wenn sie Zivilisten gefährden oder gar töten.

Kann anhand des bestehenden Menschenrechtskatalogs eine Menschenrechtsverletzung durch LAWS angenommen werden? In Betracht kommt eine Verletzung des Rechts auf Leben aus Artikel eins der Allgemeinen Erklärung der Menschenrechte. Der Schutz des Lebens erfordert im humanitären Völkerrecht in jedem Fall eine ständige Verhältnismäßigkeitsprüfung bei der Entscheidung, ob die Tötung einer Person im Einzelfall gerechtfertigt ist. Diese Prüfung ist dabei ununterbrochen, also bis zum tödlichen Moment durch einen anderen Menschen durchzuführen.

Es ist schwer vorstellbar, dass LAWS – selbst wenn sie durch den Einsatz von künstlicher Intelligenz betrieben werden – als Mensch in diesem Sinne eingestuft werden können. Solche Maschinen können eindeutig nicht wie Menschen "entscheiden", dass/ob von einer Person eine Gefahr ausgeht, die es rechtfertigt, sie zu töten. Vielmehr ist das Argument überzeugend, dass eine solche "Entscheidung" durch ein LAWS aufgrund der Unterschiede zu einer menschlichen,

vernunftbegründeten Entscheidung ohnehin willkürlich ist und daher das Recht auf Leben gefährdet. Eine solche Rechtsverletzung muss nicht erst durch Etablierung neuer Menschenrechte festgestellt werden. Vielmehr muss bereits jetzt gegen den Einsatz solcher Systeme vorgegangen werden, um das besonders wichtige Recht auf Leben zu schützen.

Medizinische Technologien und das Recht auf Leben

Die technologischen Entwicklungen in der Medizin stellen einen weiteren Bereich dar, die geeignet sind, "neue" Bedrohungen des Rechts auf Leben hervorzurufen. So haben neue therapeutische Maßnahmen wie die Präimplantationsdiagnostik bereits jetzt Auswirkungen auf die Menschenrechte, einschließlich des Rechts auf Gesundheit und Würde. Mit der zunehmenden Nutzung von mehr Daten in der Medizin und dem Einsatz leistungsfähigerer (Quanten-)Technologien werden die bereits eingesetzten Therapieansätze es ermöglichen, Erbkrankheiten früher und genauer als heute zu erkennen. Was für die Betroffenen durchaus eine Erleichterung sein kann, ist aus globaler Perspektive problematischer, da insofern Missbrauchspotenzial besteht: Nicht nur Erbkrankheiten werden hierdurch bestimmbar sein, vielmehr können insbesondere ästhetische Vorstellungen der Eltern berücksichtigt werden. Es ist möglich, die Augenfarbe oder die Haarfarbe der Embryos zu bestimmen, aber auch körperliche Eigenschaften wie die Sportlichkeit des Kindes und nach eigenen Vorstellungen zu "gestalten". Doch auch das Geschlecht kann vor dem Inseminieren ausgewählt werden. Die moralische und ethische Verwerflichkeit solcher Auswahlmöglichkeiten ist evident. Mit einer solchen gezielten "Selektion" des ungeborenen Lebens besteht vielmehr die Gefahr einer erfolgreichen Umsetzung sozialdarwinistischer Theorien. Auch wenn die bioethische Debatten den steten medizinischen Fortschritt begleiten, ist aus völkerrechtlicher Perspektive eindeutig, dass solche medizinische Technologien das Recht auf Leben und seine Bedeutung im Zusammenhang mit der Menschenwürde gefährden, wenn hierdurch eine Selektion von menschenwürdigem Leben betrieben wird. Eine solche Rechtsgefährdung ist bereits jetzt evident und muss auf Basis der bestehenden Menschenrechte unterbunden werden.

Diese Beispiele verdeutlichen eindeutig, dass vielen negativen Herausforderungen der digitalen Revolution in Bezug auf Menschenrechtseingriffe durch effektive Durchsetzung der bestehenden Menschenrechtsverpflichtungen gegenüber Staaten begegnet werden kann. Für ein effektives Monitoring und ein präzises Gegensteuern im Einzelfall müssen staatliche Akteure mehr Kapazitäten schaffen, die diese Aufgaben wahrnehmen können.

Die Rolle von Digitalkonzernen im Menschenrechtsschutz

Doch nicht nur die effektive Rechtsdurchsetzung wird von Bedeutung sein. Es ist auch ein Fokus auf die "neuen" Akteure, die die digitale Entwicklung vorantreiben, zu legen. Große Digitalkonzerne, wie Meta und Apple kontrollieren unseren alltäglichen Umgang mit technologischen Innovationen nicht nur im Bereich der Softwarenutzung, zum Beispiel auf sozialen Plattformen, sondern auch in Bezug auf die Hardware. Das verschafft ihnen eine starke Machtposition, die in gewisser Weise mit der Machtposition eines Staates über seine Bürger vergleichbar ist.

Die bisherige Auslegung der Menschenrechte fordert eine staatliche Bindung der Menschenrechte. Das bedeutet, dass nur Staaten verpflichtet sind, die Menschenrechte zu wahren. Menschen und unter gewissen Umständen auch Unternehmen sind hingegen Berechtigte, was bedeutet, dass ihre Menschenrechte zu schützen sind. Diese Auslegung muss vor dem Hintergrund der starken Machtposition dieser digitalen Konzerne neu gedacht werden. Es stellt sich die Frage, ob und wie diese Unternehmen verpflichtet werden (können), die Menschenrechte der einzelnen Nutzer in ihrem Wirkungsbereich, also etwa auf Plattformen, zu schützen. Dies umschreibt die oft vernommene Frage des Horizontalisierungseffekt der Menschenrechte, da nicht nur Staaten gegenüber den Bürgern vertikal (von oben nach unten) zur Wahrung der Menschenrechte verpflichtet werden sollen, sondern auch Private gegenüber Privaten (horizontal).

Die Frage nach der Rechenschaftspflicht dieser Unternehmen muss eindeutig aufgrund der globalen Aktivität der Unternehmen auf internationaler Ebene gestellt werden: Die EU hat in diesem Bereich die Notwendigkeit einer neuen Auslegung von Menschenrechten verstanden und durch die Schaffung des Digital Services Act und des Digital Markets Act sowie des AI Acts eine rechtliche Basis geschaffen, die eine Bindung der Digitalunternehmen an die Einhaltung der Menschenrechte in der EU vorschreibt. Die Verknüpfung von menschenrechtlichen Verpflichtungen mit Transparenz- und Verfahrenspflichten und eine Risikobewertung in Verbindung mit Offenlegungspflichten scheint ein gutes Gleichgewicht zwischen den Rechten eines Unternehmens und den gesellschaftlichen Bedürfnissen herzustellen. Dies Ansatz kann somit weltweit empfohlen werden. Es besteht die Hoffnung, dass der europäische Verpflichtungskatalog, wie bereits in der Vergangenheit im Rahmen des Datenschutzrechts, einen positiven Effekt auf die Rechtsentwicklung in anderen Ländern besitzt. Jedenfalls führt die Entwicklung der Rechte auf europäischer Ebene in Österreich, aber auch in allen anderen Staaten der EU dazu, dass die Rechte des Einzelnen bei Nutzung digitaler Technologien besser geschützt wird. Der Einzelne in Österreich kann sich besser gegen rechtswidrige Inhalte, wie Beleidigungen oder Falschmeldungen wehren. Gerade die Untersuchungsmöglichkeit der Funktionsweise durch die EU von sogenannten Empfehlungssystemen der Plattformen, die für die Schaltung von Werbung und das strategische Auswerten von Nutzerinteressen zuständig sind, sorgt für mehr Transparenz und schränkt die Plattformen mit Blick auf die missbräuchliche Verwendung von Daten zu kommerziellen Zwecken ein. Dies kommt den Menschenrechten eines jeden Einzelnen in der EU und in Österreich zu Gute.

Keine neuen Menschenrechte – aber mehr globale Verantwortung

Abschließend kann daher nur noch einmal festgehalten werden: Es braucht keine neuen Menschenrechte. Wir müssen die Bedrohungen für die bestehenden Menschenrechte vielmehr stärker auf globaler Ebene adressieren und Staaten sowie mächtige private Akteure verpflichten, die Bedrohungen zu unterbinden. Das Bewusstsein und der Wille zur Durchsetzung und Einhaltung von Menschenrechtsstandards muss gefördert werden, um aktuellen und zukünftigen Gefahren in diesem Bereich begegnen zu können.
Die Ergebnisse unserer Studie sind in ausführlicher Form unter diesem Link zu finden.

Was Drohnen dürfen – und was nicht

Es genügt nicht, mit einer Drohne fliegen zu wollen, man muss auch Start und Landung einplanen. Und da setzt das Recht einige Schranken

Samantha Pechtl

Warum über den Wolken die Freiheit doch nicht so grenzenlos ist, analysiert im Gastblog die Juristin Samantha Pechtl.

Beim Fliegen (von Drohnen) sind nicht nur luftrechtliche, sondern auch zivilrechtliche Regelungen betreffend die Nutzung von Grund und Boden beim Starten und Landen zu beachten, die hier aufgrund der stetig steigenden Zahl der im Umlauf befindlichen Drohnen sowie der kürzlich geänderten Rechtslage kurz dargestellt werden.

Was gibt es aus öffentlich-rechtlicher Sicht zu beachten?

Das Fliegen mit Drohnen – sogenannten unbemannten Luftfahrzeugen – wird in der EU seit 2021 einheitlich durch die DrohnenVO (2019/947) geregelt. Dieses Regulativ teilt den Betrieb von Drohnen, abgestuft nach dem jeweiligen Risiko, in drei Kategorien – "open", "specific" und "certified" – ein. Für die private Freizeitnutzung ist dabei grundsätzlich die UAS-Betriebskategorie "offen" (Art 4 EU-DrohnenVO) relevant.

Die "offene Kategorie" betrifft alle Hobbypiloten und Betreiber kommerziell genutzter Kamera-Drohnen. Um in dieser Kategorie zu fliegen, müssen die Kopter technisch bestimmten Klassen zugeordnet werden. Daraus ergibt sich dann die jeweilige Unterkategorie A1, A2 oder A3.

- A1 (Flug nahe am Menschen): Hierunter fallen Drohnen mit einem maximalen Abfluggewicht von weniger als 900 Gramm. Der Überflug von unbeteiligten Personen ist jedoch nur mit einer Drohne unter 250 Gramm gestattet.
- A2 (Flug mit sicherem Abstand zu Menschen): Drohnen bis vier Kilogramm. Beim Betrieb ist ein Mindestabstand von 30 Meter zu unbeteiligten Personen einzuhalten.
- A3 (Flug weit entfernt von Menschen): Drohnen mit einem maximalen Abfluggewicht von höchstens 25 Kilogramm. Es ist ein Mindestabstand von 150 Meter zu Wohn-, Gewerbe-, Industrie- und Erholungsgebieten einzuhalten. Innerhalb des Flugbereiches dürfen sich keine unbeteiligten Personen befinden.

Je nach Kategorie muss der Betreiber entsprechende Auflagen erfüllen. Grundsätzlich sind in der "Open" Kategorie Flüge bis zu 120 Meter über Grund gestattet, sofern der Pilot mindestens 16 Jahre alt ist und stets eine direkte Sichtverbindung zur Drohne besteht.

Ferner dürfen keine Menschenansammlungen überfolgen werden. Eine Menschenansammlungen ist eine Vielzahl von Menschen, die so dicht gedrängt stehen, dass es einer einzelnen Person nahezu unmöglich ist, sich aus dieser Menge zu entfernen; Art 2 Z 3 EU-DrohnenVO, 2019/947. Zu beachten sind auch

Flugverbotszonen. So dürfen Drohnen etwa in der Nähe von Flughäfen oder militärischen Einrichtungen nicht betrieben werden. In der Dronespace-App der Austro Control (und hier) können Flugverbotszonen eingesehen werden.

Drohnenführerschein

Drohnenbesitzer müssen den Betrieb der Drohne vorab registrieren. Mit einer Kamera ausgestattete Drohnen bedürfen stets einer Registrierung. Drohnen, die über keinen Sensor zur Erfassung personenbezogener Daten verfügen (Spielzeugdrohnen), müssen grundsätzlich erst ab einem Gewicht von 250 Gramm registriert werden. Die Registrierungsnummer muss sodann gut sichtbar an der Drohne angebracht werden.

Drohnenbesitzer bedürfen unter Umständen einen eigenen Kompetenznachweis ("Drohnenführerschein") sowie jedenfalls einer Haftpflichtversicherung. Abgestuft nach dem Gewicht des Flugmodells bedürfen Drohnenpiloten unterschiedliche Voraussetzungen für den Betrieb. Ab einem Gewicht von 250 Gramm muss ein Onlinekurs samt Test abgelegt werden. Alle betriebenen Drohnen müssen über einen ausreichenden Versicherungsschutz – mindestens 750.000 Sonderziehungsrechte – verfügen (§§ 164 iVm 151 LFG). Siehe hiezu auch *Koziol*/*Apathy*/*Koch*, Haftpflichtrecht III3 A/9/ Rz 66 ff (Stand 1.9.2014, rdb.at).

Auf nationaler Ebene sieht das Luftfahrtgesetz (§§ 24 ff LFG) Regelungen für unbemannte Luftfahrzeuge vor, die nicht von der oben dargestellten EU-Verordnung erfasst werden und teilt diese dabei in zwei Kategorien ein:

- Kategorie 1: unbemannte Luftfahrzeuge mit direkter Sichtverbindung zum Piloten
- Kategorie 2: unbemannte Luftfahrzeuge ohne Sichtverbindung

Für den Betrieb von unbenannten Luftfahrzeugen die nicht dem Unionsrecht unterliegen bedarf es grundsätzlich einer behördlichen Bewilligung (§ 24f und § 24g LFG, § 18 LVR).

Die Austro Control GmbH hat die Bewilligung zu erteilen, wenn die Drohne den Luft- und Betriebstüchtigkeitsanforderungen entspricht und die Sicherheit der Luftfahrt nicht gefährdet und keine Lärmbelästigung herbeigeführt wird.

Von der Anwendbarkeit des europäischen Regulativs für unbemannte Luftfahrzeuge (uLFZ) ausgenommen sind gemäß Art 2 Abs 3 lit a der Verordnung (EU) 2018/1139 uLFZ, wenn sie für Tätigkeiten oder Dienste für das Militär, den Zoll, die Polizei, Such- und Rettungsdienste, die Brandbekämpfung, die Grenzkontrolle und Küstenwache oder ähnliche Tätigkeiten oder Dienste eingesetzt werden, die unter der Kontrolle und Verantwortung eines Mitgliedstaats im öffentlichen Interesse von einer mit hoheitlichen Befugnissen ausgestatteten Stelle oder in deren Auftrag durchgeführt werden, sowie das an den Tätigkeiten und Diensten dieser Luftfahrzeuge beteiligte Personal und die an diesen Tätigkeiten und Diensten beteiligten Organisationen. Somit fallen uLFZ für Tätigkeiten oder Dienste für das Militär und die Polizei nicht unter das europäische Regulativ für uLFZ und es sind weiterhin die nationalen Regelungen anwendbar.

Was gibt es aus privatrechtlicher Sicht zu beachten?

Grundsätzlich sind Liegenschaftseigentümer zwar gemäß § 297 ABGB auch am Luftraum oberhalb ihres Grund und Bodens verfügungsberechtigt. Das (Eigentums-)Recht am Luftraum endet jedoch mit der Einwirkungsmöglichkeit des Grundeigentümers sowie mit dem Fehlen des Interesses an der Rechtsausübung; dann wird der Luftraum zum öffentlichen Gut (Kleewein, Hängegleiten 206; OGH 27.8.1969, 5 Ob 193/69).

Zudem beschränkt § 2 LFG die rechtliche Herrschaft des Eigentümers über den Luftraum gemäß § 297, § 354 ABGB im öffentlichen Interesse. Demnach muss das Überfliegen von Grundstücken – sofern es nicht in einer störenden Tiefe erfolgt – grundsätzlich geduldet werden. Diese gesetzlich angeordnete Duldungspflicht wirkt wie eine privatrechtliche Servitut (sogenannte Legalservitut) und berechtigt unter anderem auch zur Benützung gewisser (bemannter und unbemannter) Luftfahrzeuge (siehe zu den unterschiedlichen Arten von Flugmodellen bzw Luftfahrzeugen die §§ 11 ff, §§ 22f ff LFG; Kleewein, Hängegleiten 206).

Ein Benutzungsrecht der Liegenschaft selbst besteht jedoch grundsätzlich nicht, sofern es sich bei der betreffenden Landfläche nicht etwa um Wald iSd ForstG 1975 handelt. Hier besteht für Drohnenpiloten ein gesetzliches Betretungsrecht zu Erholungszwecken gem § 33 leg cit.

Ein Go fürs Überfliegen, ein Stop fürs Starten

Es kann festgehalten werden, dass der Hobbybetrieb von Drohnen nach der VO (EU) 2019/947 stattfindet und daher grundsätzlich einer bloßen Registrierung der Drohne und keiner gesonderten Bewilligung bedarf. Ferner stellt das bloße Überfliegen von Grundstücken (sowohl mit Drohnen als auch etwa mit Paragleitern) grundsätzlich keinen rechtswidrigen Eigentumseingriff dar, da dieser durch die Freiheit des Luftraums im Sinne des § 2 LFG gestattet ist. Hingegen kann der Start und die Landung auf fremden Grund durchaus einen unzulässigen Eigentumseingriff darstellen, sofern für das betreffende Grundstück kein entsprechendes Nutzungsrecht etwa aufgrund bestehenden Gemeingebrauchs gegeben ist (Kleewein, Hängegleiten 292 f; Kiendl, ZVR 1993, 353, 355).

Ein Nutzungsrecht besteht jedenfalls bei ungeplanten Sicherheits-/Notlandungen sowie Landungen/Abflügen von Rettungs- oder Katastropheneinstätzen. § 10 Abs 1 macht die Zulässigkeit derartiger Tätigkeiten gerade nicht vom Einverständnis des Verfügungsberechtigten abhängig (vgl Nonnenmacher, Neuerungen bei Außenlandungen und Außenabflügen, Jahrbuch Regulierungsrecht 2017, 55).
Kurz gefasst: Drohnen fliegen nicht im rechtsfreien Raum. Neben dem LFG ist besonders die EU-DrohnenVO (2019/947) einschlägig. Für Hobby- und kommerzielle Nutzer ist meist die "offene Kategorie" relevant; Polizeidrohnen und Rettungsdrohnen fliegen unter österreichischem Recht. Beim Betrieb müssen Drohnenpiloten verschiedene Vorschriften beachten, wie Mindestalter, Sichtverbindung zur Drohne und die Vermeidung von Flügen über Menschenansammlungen.

Darüber hinaus erfordern Drohnen ab einem bestimmten Gewicht eine Registrierung und müssen sichtbar gekennzeichnet sein. Zusätzlich ist eine Haftpflichtversicherung erforderlich, und in bestimmten Fällen müssen Piloten einen Drohnenführerschein erwerben. Über Grundstücke fliegen wird regelmäßig erlaubt sein, beim Nachbarn zu starten und zu landen aber nicht.

Wie die Unesco ethische Standards für die Zukunft der Quantentechnologie setzt

Österreichs Rolle in der globalen Ethikgestaltung für Quantentechnologien

Matthias C. Kettemann

Im Gastblog beleuchtet Matthias C. Kettemann die aktuelle Arbeit der Unesco im Bereich der Quantenethik und die Notwendigkeit, ethische Prinzipien für die verantwortungsvolle Entwicklung und Nutzung von Quantencomputing zu etablieren.

Die KI-Regulierung ist zunächst abgeschlossen, doch die Technologie entwickelt sich weiter: Nach dem Nobelpreis braucht die Quantentechnologie dringend klare ethische Regeln. Österreich befindet sich in einer wirtschaftlich, politisch und wissenschaftlich hervorragenden Position, die Zukunft der Quantentechnologie global zu gestalten. Hierfür ist ein festes und abgestimmtes Wertefundament notwendig. An diesem wird in der kommenden Woche eine Unesco-Ethikkommission arbeiten.

Obwohl die Quantenphysik auf das frühe 20. Jahrhundert zurückgeht, befinden sich Quantentechnologien insgesamt noch in einem frühen Entwicklungsstadium. Anwendungen wie Quantensensorik und Quantenkommunikation sind bereits im Einsatz, doch Quantencomputing steckt noch in einer frühen Implementierungsphase. Während ein Großteil der Grundlagenforschung durch den öffentlichen Sektor und akademische Institutionen finanziert wird, spielen private Unternehmen und kommerziell orientierte Ansätze, vor allem in Bereichen wie Quantencomputing, Quantenkryptografie und Quantensensorik, eine zunehmend wichtige Rolle. In diesem Zusammenhang können ethische Prinzipien dazu beitragen, die Entwicklung nationaler und globaler Standards und Prioritäten zu gestalten, um eine verantwortungsvolle Nutzung dieser Technologie sicherzustellen.

2025: Internationales Quantenjahr

Die UN-Generalversammlung hat das Jahr 2025 zum Internationalen Jahr der Quantenwissenschaft und -technologie erklärt. Bereits jetzt haben internationale Organisationen und Staaten damit begonnen, Prinzipien für die verantwortungsvolle Entwicklung und Nutzung von Quantencomputing zu definieren. Angesichts dessen ist eine Diskussion über die ethischen Grundlagen dieser Technologie von zentraler Bedeutung. Diese wird kommende Woche im Rahmen der Unesco-Kommission für Wissenschafts- und Technikethik stattfinden.

Wie jede neue Technologie hat auch das Quantencomputing positive sowie negative Auswirkungen auf Menschenrechte, menschliche Entwicklung und Sicherheit. Technologie ist weder inhärent gut noch schlecht, doch sie ist auch nicht neutral. Jede technologische Entwicklung geschieht im Kontext bestimmter sozialer und politischer Gegebenheiten und hat dementsprechend Auswirkungen auf diese. Auch das Quantencomputing unterliegt diesen Dynamiken. Im aktuellen Entwicklungsstadium der Quanteninformatik ist die Notwendigkeit eines ethischen Rahmens deutlich geworden. Staaten und internationale Organisationen haben das Potenzial von Quantentechnologien erkannt und massiv investiert. Gleichzeitig haben private

Akteure bereits damit begonnen, diese Technologien zu nutzen. Viele ethische Fragestellungen, die sich in den letzten Jahren mit dem Aufkommen neuer Hochtechnologien ergeben haben, rücken erneut in den Vordergrund.

Neue Technologien – wichtige Werte

Zu den drängendsten Fragen gehören: Wer entscheidet über die Standards für das Quantencomputing? Wer legt fest, in welchen gesellschaftlichen Bereichen diese Technologie eingesetzt wird und in welchen nicht? Wer bestimmt, für welche Zwecke – medizinisch, finanziell oder meteorologisch – Quantenrechenkapazitäten genutzt werden? Wie wird das Quantencomputing in die digitale Agenda der Vereinten Nationen, insbesondere in den Global Digital Compact, integriert? Und wer stellt sicher, dass der Zugang zu Quantencomputing nicht auf eine kleine Gruppe von Forscher:innen beschränkt bleibt?

Technologischer Fortschritt erfolgt nicht automatisch, sondern ist das Ergebnis bewusster Entscheidungen. Diese Entscheidungen sollten von ethischen Überlegungen geleitet werden. Der Einsatz und die Weiterentwicklung des Quantencomputings und seinen Anwendungen müssen durch ethische Grundsätze gelenkt werden. Die Erfahrungen aus der unzureichenden Regulierung sozialer Medien zeigen, welche Risiken entstehen, wenn normative Standards allein der Industrie überlassen werden. Hierbei gerieten individuelle Rechte, gesellschaftliche Werte und globale öffentliche Güter oft ins Hintertreffen, und erst neue Gesetze, wie der Digital Services Act und der Digital Markets Act der EU, schaffen hier Abhilfe.

Diese ethischen Leitplanken müssen auf dem Schutz der individuellen Würde und Autonomie aufbauen, während sie gleichzeitig demokratische Verantwortlichkeit und Transparenz im Standardisierungsprozess garantieren. Darüber hinaus sollte sichergestellt werden, dass Quantencomputing als globales öffentliches Gut angesehen und im Sinne internationaler Solidarität und generationenübergreifender Gerechtigkeit reguliert wird.

Ein solides ethisches Fundament für Quantencomputing

Beim Aufbau ethischer Standards für das Quantencomputing liegt ein besonderer Schwerpunkt auf der Überwindung der sich abzeichnenden digitalen Kluft. Ziel ist es, Zugangsgerechtigkeit und Chancengleichheit in der Nutzung von Quantentechnologien zu gewährleisten. Ethische Leitlinien werden essenziell sein, um globale Gerechtigkeit, internationale Solidarität, den Schutz der Privatsphäre und die Vermeidung einer missbräuchlichen Nutzung der Technologie sicherzustellen.

Im Zentrum steht die Förderung des Zugangs zu Quantencomputing als globalem öffentlichen Gut. Zudem muss sichergestellt werden, dass alle Staaten Zugang zu den nötigen Software- und Hardware-Ressourcen sowie Rechenkapazitäten erhalten, um von Quantencomputing zu profitieren.

Es ist von entscheidender Bedeutung, dass alle relevanten Akteure in die Diskussion über aktuelle und zukünftige Governance-Fragen einbezogen werden – nicht nur von den Unternehmen, die das Quantencomputing kommerziell nutzbar machen. Daher sind Multi-Stakeholder-Foren für die Normenentwicklung von großer Bedeutung.

Das Internet Governance Forum mit seinen nationalen Vertretungen bietet hier ein bewährtes Vorbild.

Die Arbeit an der Empfehlung der Unesco zur Ethik des Quantencomputings soll bis Herbst 2025 abgeschlossen sein.

Cybermobbing: Wie wäre es mit Opfer- statt Täterschutz?

Eine kritische Auseinandersetzung mit der aktuellen Gesetzeslage in Österreich

Sophia Katharina Thoma

Sophia Katharina Thoma, Spezialistin für Recht und Digitalisierung, erklärt im Gastblog anhand eines Beispiels, welche rechtlichen Grundlagen bei Cybermobbing überarbeitet werden sollten.

Unlängst in Vorarlberg: Zwei Gewalttäter misshandeln und demütigen ihre wehrlosen Opfer, während die Komplizen die Szenen mit der Handykamera filmen. Schließlich werden die Videos über den WhatsApp-Kanal ins Internet gestellt und durch Hochladen in die Snapchat-Story der Öffentlichkeit zugänglich gemacht. Dadurch gehen diese dann später viral.

Vorfälle wie diese spielen sich immer häufiger ab. Die körperlichen Schmerzen lassen beim Opfer meist schnell nach, aber die traumatisierenden Folgen bestehen hingegen oft jahrelang und bringen nicht selten psychische Erkrankungen mit sich. Hauptgrund dafür ist meist die anhaltende öffentliche Demütigung, die durch die Verbreitung des kompromittierenden Videos entsteht. Das Internet vergisst bekanntlich nie. Der beschämende Film ist aus dem Netz nicht mehr zu entfernen, das Opfer ist fortan gezwungen, damit zu leben.

Strafrechtliche Konsequenzen für die Urheber der Videos

Strafrechtliche Konsequenzen für die Urheber der Videos in den zitierten Vorarlberger Fällen? Fehlanzeige. Die aktuelle Gesetzeslage schützt den Täter. In der Begründung, mit der das Ermittlungsverfahren schließlich laut § 190 Z 2 StPO eingestellt wurde, heißt es sinngemäß: Der Werkersteller habe das Video zwar nachweislich ins Internet hochgeladen, für eine weitere Verbreitung sei er aber nicht verantwortlich. Vielmehr sei nicht davon auszugehen, dass das jeweilige Video über einen längeren Zeitraum hinweg für eine größere Zahl von Personen sichtbar war. Was unter "größere Zahl" und "längere Zeit" genau zu verstehen ist, wurde vom Gesetzgeber nicht weiter konkretisiert und ist jeweils vom Einzelfall abhängig.

Dem Tatbestand des § 107c StGB entsprechen Handlungen, die für eine größere Zahl von Menschen über längere Zeit hindurch wahrnehmbar gemacht werden, wobei dem Täter diesbezüglich der Vorsatz nachzuweisen ist. In der praktischen Umsetzung offenbart sich freilich die Absurdität dieser Intention: Der Nachweis dieses Vorsatzes ist in der Regel kaum zu erbringen. Hier ist an eine Beweislastumkehr zuungunsten des Werkerstellers zu denken: Dieser sollte nämlich den Nachweis zu erbringen haben, dass er das kompromittierende Material eben nicht zum Zwecke der Verbreitung erstellen wollte. Er hätte zu erklären, welche Maßnahmen er ergriffen hatte, um die Gefahr einer möglichen Verbreitung seines Machwerkes im Internet zu verhindern. Dies wird ihm freilich meist nur dann gelingen, wenn das Werk direkt und ausschließlich zum Zweck der Beweissicherung an die Behörden übermittelt worden ist.

Straffrei bleibt der Täter nach § 107c StGB ebenso, wenn er die Bild- oder Videoaufnahme löscht, bevor "von längerer Zeit" ausgegangen werden kann. Dass sich der Inhalt dennoch schon verbreitet hat, kann dem Täter nicht angelastet werden. So war es im geschilderten Fall möglich, Straffreiheit zu erlangen, obwohl der Täter zum Zeitpunkt des Uploads in seine Snapchat-Story über mehr als 400 Follower verfügte, für die allesamt eine Einsichtnahme und theoretisch eine Weiterverbreitung möglich war. Dass das Video auch tatsächlich von mehreren Personen gesehen und wiederum unkontrolliert verbreitet wurde, konnte dem Beschuldigten nicht angelastet werden.

Vom Gesetzgeber wird in diesem Versuch, gegen Cybermobbing vorzugehen, übersehen, dass zum einen die Kurzlebigkeit von Beiträgen in gewissen Medien systematisch verankert ist, zum anderen schädigt bereits allein die Veröffentlichung von entsprechendem Material im Internet das Opfer nachhaltig, da mit diesem ein Kontrollverlust über die Handhabung der kompromittierenden Inhalte einhergeht.

Opferschutz hilft auch der Generalprävention

Dieser Zustand ist untragbar, und zwar im doppelten Sinne: sowohl im Hinblick auf den Opferschutz als auch im Sinne einer Generalprävention, also der Abschreckung potenzieller Täter. Durch das Ignorieren der typischen Charakteristiken des Internets wie dem "viral gehen" binnen Sekunden und der Persistenz beziehungsweise Unlöschbarkeit von hochgeladenen Dateien etablieren sich Lücken für Täter, die im aktuellen Internet-Zeitalter von großer praktischer Relevanz sind.

Wer Bild- oder Videomaterial herstellt, dessen Inhalt geeignet ist, das Opfer einer Straftat in der Öffentlichkeit bloßzustellen oder der Lächerlichkeit preiszugeben (Mobbing), der trägt in besonderer Weise Verantwortung dafür, dass jenes von ihm erstellte Werk eben gerade nicht einer breiten Öffentlichkeit zugänglich gemacht werden kann. Diesem Umstand wird die aktuelle Gesetzeslage nicht gerecht.

Die besondere Verantwortung des Werk-Erstellers ergibt sich allein schon daraus, dass eine öffentliche Demütigung mit all den zum Teil lebenslangen traumatisierenden Folgen für das Opfer nicht erfolgen könnte, wenn das Werk gar nicht erst erstellt worden wäre. Die Erschaffung des Videos beziehungsweise der Fotos ist ursächlich dafür, dass die weit verbreiteten Mobbing-Delikte überhaupt erst verübt werden können. Dies ist also an sich schon als Straftat oder zumindest als Vorbereitung einer strafbaren Handlung zu betrachten.

Allein schon die Wahrnehmung des Opfers, das es in einer demütigenden Situation gefilmt wird, ist dazu geeignet, bei ihm Angst und Schrecken vor einer Veröffentlichung auszulösen. Dem Opfer muss hier dringend ein Schutzrecht vor Film– und Videoaufnahmen zugestanden werden. Ohnehin geht es dem Ersteller eines Bild– oder Videowerkes, dass die Demütigung eines Opfers dokumentiert, nur darum, sich selbst oder andere an dessen Leid zu ergötzen oder zu belustigen – bereits diesem Verhalten wohnt kriminelle Energie inne.

Es ist dem Ersteller des Werkes daher jede, auch nur einmalige Verbreitung auf digitalem Wege im Internet zu untersagen. Schon durch die einmalige Weiterleitung

des Werkes an eine einzige unbeteiligte Person nimmt der Werkersteller eine unkontrollierte und vielfache Verbreitung, das sogenannte "viral gehen", in der Folge ja billigend in Kauf, was als schuldhaftes Verhalten anzusehen ist.

OGH zur Haftung der Verbreiter

Diese Ansicht wird auch vom Obersten Gerichtshof vertreten, der jüngst im Urteil (6 Ob 210/23k) erläutert, was unter einem Shitstorm zu verstehen ist und wer schließlich für die Verbreitung von entsprechenden Inhalten zur Verantwortung gezogen werden kann. Demnach wird erkannt, dass es nicht Aufgabe des Opfers sein kann, die konkrete Quelle der herabsetzenden Äußerung benennen zu müssen, sondern der Nachweis genügt, Opfer eines Shitstorms gewesen zu sein. Als Konsequenz für die Unaufklärbarkeit des konkreten Verursachers haftet dem Opfer gegenüber also jeder an der Verbreitung Beteiligter, solidarisch für den entstandenen Gesamtschaden. Damit ein Shitstorm überhaupt erst entstehen kann, sei das Zusammenwirken vieler Menschen immanent. Schließlich begeht jeder einzelne Teilnehmende durch das Teilen des Postings mit der Öffentlichkeit oder seinen Mitmenschen für sich eine Datenschutz– und Bildnisschutzverletzung.

Das Erstellen kompromittierenden Bild– oder Videomaterials erfordert nota bene, ein aktives vorsätzliches Handeln, dass sich gegen das Opfer richtet und geeignet ist, dessen Leid zu vermehren. Es ist möglich, Cybermobbing schon bei der Entstehung zu unterbinden. Angesichts einer Strafbarkeit der Produktion von entsprechendem Film– oder Bildmaterial würde sich in der Folge wohl mancher hüten, solche Werke in sozialen Medien oder in anderer Weise zu teilen. Von Strafbarkeit auszunehmen, wäre freilich das Erstellen und Weiterleiten von Bild– oder Videoaufnahmen an eine Ermittlungsbehörde zum Zwecke der Strafverfolgung.

Causa Vamed: Was heißt denn hier Whistleblowing?

Einblicke in die unternehmensinterne Amnestie und die gesetzliche Lage des Hinweisgeber:innenschutzes in Österreich

Marlon Possard

Im Gastblog beleuchtet Marlon Possard die Versprechung des Gesundheitsunternehmens Vamed, Mitarbeitenden Amnestie bei der Offenlegung interner Missstände zu gewähren, und erläutert die gesetzlichen Regelungen und Schutzmechanismen für Whistleblower in Österreich.

Das Vorstandsteam des Gesundheitsunternehmens Vamed verspricht in einem Schreiben, das den Mitarbeiterinnen und Mitarbeitern des Konzerns zugestellt wurde, eine Art Begnadigung, wenn sie Informationen preisgeben, die mit unrechtmäßigem Verhalten im Betrieb in Zusammenhang stehen. DER STANDARD berichtete darüber. Dass ein solches Vorgehen in Bezug auf eine unternehmensinterne rechtliche Amnestierung kein gutes Licht auf Prozesse und Entwicklungen innerhalb von Vamed wirft, ist offensichtlich. Aufgezeigt wird dadurch aber auch, dass Compliance in Unternehmen immer wichtiger wird. Der Fall Vamed kann dazu anregen, sich grundlegend Gedanken darüber zu machen, was unter Whistleblowing und unter dem Schutz von Hinweisgeberinnen und Hinweisgebern zu verstehen ist. Welche gesetzlichen Normen gibt es?

Gesetzliche Bestimmungen

Das Hinweisgeben, umgangssprachlich auch nur Whistleblowing genannt, ist in Österreich in verschiedenen gesetzlichen Bestimmungen und Verordnungen geregelt und berührt verschiedene Rechtsmaterien (zum Beispiel das Datenschutzrecht, das Arbeitsrecht oder das Strafrecht). Grundlage für die gesetzliche Regelung in Österreich bildet die sogenannte EU-Whistleblower-Richtlinie (RL EU 2019/1937), die im Jahr 2019 vom EU-Parlament verabschiedet wurde mit dem Ziel, unionsweit einheitliche Standards für den Schutz von Whistleblowerinnen und Whistleblowern zu schaffen.

Der österreichische Gesetzgeber etablierte in weiterer Folge – wenn auch verspätet – das sogenannte Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (HinweisgeberInnenschutzgesetz, kurz HSchG) mit Inkrafttreten am 25. Februar 2023. Bis 25. August 2023 hatten sodann private Unternehmen mit Sitz in Österreich und mit mehr als 250 Mitarbeiterinnen und Mitarbeitern Zeit, ein geeignetes Hinweisgeber:innenportal als Meldestelle einzurichten. Im Dezember 2023 folgte die Ausweitung der Anwendung der gesetzlichen Bestimmungen auf Unternehmen, die mehr als 50 Beschäftigte (bis 249) aufwiesen. Ebenso wurde der öffentliche Sektor (insbesondere Gemeinden ab 10.000 Einwohnerinnen und Einwohnern) dazu angewiesen, solche Meldekanäle zu etablieren.

Wer oder was wird geschützt?

Ein Hinweisgeber:innenportal schützt primär die Whistleblower:innen selbst vor diversen wirtschaftlichen und tätigkeitsbezogenen Nachteilen (beispielsweise vor unrechtmäßiger Entlassung oder Mobbing) bei Offenlegung von Missständen und/oder strafbarem Verhalten. Wichtig ist, dass eine Verbindung zwischen Hinweisgeberin beziehungsweise Hinweisgeber und dem betroffenen Betrieb existiert. Mit der Einrichtung eines durch das HSchG gesetzlich geforderten Meldekanals, der zudem alle datenschutzrechtlichen Voraussetzungen und Schutzmechanismen erfüllen muss (Stichwort: Schutz der Identität), wird sichergestellt, dass auf Wunsch die Anonymität der unternehmensinternen oder -externen Hinweisgeberinnen und Hinweisgeber gewahrt bleibt, die damit konnektierte Vertraulichkeit gewährleistet wird und die Kommunikation zwischen Hinweisgeberin beziehungsweise Hinweisgeber und dem Unternehmen verschlüsselt stattfinden kann.

Sofern es sich um strafrechtlich relevante Angelegenheiten handelt, die eine externe Person melden möchte, kann auf das Online-Meldeportal des österreichischen Bundesamtes für Korruptionsbekämpfung und -prävention (kurz BAK) zurückgegriffen werden. Um den Schutz des HSchG zu genießen, muss es sich um natürliche Personen handeln (juristische Personen sind demnach ausgenommen), wobei auch ehemalige Mitarbeitende darunter zu subsumieren sind. Das HSchG stellt sicher, dass die meldenden Personen weder eine verwaltungs- oder zivilrechtliche noch eine strafrechtliche Haftung wegen ihrer Meldung trifft. Zudem gilt eine typische Beweislastumkehr, das heißt, die Nachweispflicht trifft die Unternehmen. Gleichzeitig wurden die Unternehmen mit dem HSchG dazu verpflichtet, die Hinweisgebenden, wenn auch auf anonyme und verschlüsselte Art und Weise, über den Status quo beziehungsweise etwaige getroffene Maßnahmen innerhalb von drei Monaten, in Ausnahmefällen innerhalb von sechs Monaten, zu informieren (siehe hierzu § 17 Abs. 6 HSchG).

Welche Konsequenzen können drohen?

Es können gemäß § 24 HSchG sowohl die Unternehmen als auch die Hinweisgebenden mit einer Geldstrafe von bis zu 20.000 Euro bestraft werden (40.000 Euro im Falle einer Wiederholung). Unternehmen trifft eine Geldstrafe dann, wenn sie Maßnahmen ergreifen, die gegen den Schutzbereich des HSchG gerichtet sind (zum Beispiel wird das Meldeportal gar nicht oder mangelhaft eingerichtet oder die meldenden Personen erfahren aufgrund ihres Hinweises Nachteile). Hinweisgeberinnen und Hinweisgeber können wiederum dann bestraft werden, wenn sie eine wissentlich falsche Meldung abgeben und über das jeweilige Meldeportal einreichen. Mit der Umsetzung der EU-Whistleblower-Richtlinie und des HSchG wurde jedenfalls ein umfassender Rechtsrahmen für einen verstärkten Schutz von Whistleblowerinnen und Whistleblowern geschaffen, der mit EU-weit einheitlichen Mindeststandards verbunden ist.

Österreichs neue Verbandsklagen: Kollektiver Rechtsschutz nach Wiener Art

Ein kritischer Blick auf Chancen und Schwächen der österreichischen Umsetzung der Verbandsklagen-Richtlinie

Susanne Augenhofer, Philipp Reicht

Im Gastblog setzen sich Susanne Augenhofer und Philipp Reicht vom Institut für Unternehmensrecht der Universität Innsbruck mit der Umsetzung der Verbandsklagen-Richtlinie in Österreich auseinander und beleuchten deren Vor- und Nachteile für Verbraucher:innen und Unternehmen.

Was lange währt, wird endlich gut. So will es der Volksmund. Lange gewährt hat die Umsetzung der Verbandsklagen-Richtlinie (kurz: Verbandsklagen-RL) in Österreich allemal. Die Verbandsklagen-RL verpflichtet die EU-Mitgliedsstaaten dazu, es eigens benannten Verbraucherorganisationen und öffentliche Institutionen zu ermöglichen, im Namen der Verbraucher:innen gegen rechtswidrige Unternehmenspraktiken zu klagen. Dies soll die Rechte der Verbraucher:innen stärken und, indem nicht jede:r Einzelne individuell vor Gericht ziehen muss, den Zugang zum Recht vereinfachen. Gerade im Zusammenhang mit Vorkommnissen wie dem VW-Dieselskandal, der tausende Verbraucher:innen betrifft, ist dies besonders relevant. Der österreichische Gesetzgeber hatte bis zum 25. 12. 2022 Zeit, die Vorgaben auch in nationales Recht umzusetzen.

Dem langen Warten setzte das Bundesministerium für Justiz erst Anfang Mai 2024 ein Ende, als endlich ein erster Entwurf in die öffentliche Begutachtung ging. Die zahlreichen kritischen Stellungnahmen zu diesem Ministerialentwurf blieben in der Regierungsvorlage weitestgehend unberücksichtigt. Die Zustimmung im Plenum des Nationalrats erfolgte (gegen die Stimmen von SPÖ und Neos) erst kürzlich am 5. 7. 2024, jene im Bundesrat am Donnerstag, den 11. 7. 2024. Dass sich die schwarz-grüne Koalition erst rund 18 Monate nach Beendigung der Umsetzungsfrist zu einer Einigung durchringen konnte, ist eine eindeutige Aussage. Diese Haltung lässt ein klares Bekenntnis zur EU missen und kommt die österreichischen Verbraucher:innen mitunter teuer zu stehen: Würde die Richtlinie weiterhin nicht umgesetzt, werden nicht nur Steuergelder für das von der Europäischen Kommission eingeleitete Vertragsverletzungsverfahren aufgewendet. Auch zahlen sie mit mangelndem Rechtsschutz, liegt doch der Verbandsklagen-RL der Gedanke einer bedeutenden Stärkung des kollektiven Verbraucher:innenrechtsschutzes zugrunde.

Qualifizierte Einrichtungen

Stellvertretend für Verbraucher:innen können künftig sogenannte Qualifizierte Einrichtungen jene Unternehmen, die (verbraucher-)rechtswidrig handeln, klagen. Es kann dabei nicht nur die Feststellung oder Unterlassung rechtswidriger Geschäftspraktiken, sondern auch – sofern dem oder der Verbraucher:in ein finanzieller Nachteil entstanden ist – Abhilfe in Form von Geldleistungen verlangt werden. Um dieses Ergebnis zu erreichen, musste bislang die sogenannte

"Sammelklage österreichischer Prägung" bemüht werden: Verbraucher:innen konnten ihre Forderungen an einen Verband abtreten, der dann gegebenenfalls mit Unterstützung eines gewerblichen Prozesskostenfinanzierers die Ansprüche der Betroffenen im eigenen Namen eingeklagt hat. Diese Vorgehensweise hat zur Recht auch im Ausland Lob erhalten und vor allem der Verein für Konsumenteninformation (VKI) und die Arbeiterkammer haben mit Hilfe dieses Konstruktes für Verbraucher:innen wichtige Erfolge erstritten. Gleichwohl bestanden juristische Hürden dieser Konstruktion und auch psychologische für Verbraucher:innen, die ja ihren Anspruch – unjuristisch gesprochen – aus der Hand geben mussten.

Mit der neuen Verbandsklage wird nun auch in Österreich endgültig ein Mittel des kollektiven Rechtsschutzes für Verbraucher:innen eingeführt. Als zu Verbandsklagen legitimierte Qualifizierte Einrichtungen nennt das Gesetz etwa Arbeiter- und Wirtschaftskammer oder den VKI. Auch andere Verbände, die sich der Durchsetzung von Verbraucher:inneninteressen verschrieben haben, können sich als Qualifizierte Einrichtung eintragen lassen. So hat etwa bereits der Verbraucherschutzverein (vsv) angekündigt, ehestmöglich einen Antrag auf Anerkennung als Qualifizierte Einrichtung stellen zu wollen.

The Good

Ausgangspunkt einer Verbandsklage ist immer der Rechtsbruch eines Unternehmens. Dies gilt es zu betonen, erweckt doch die Diskussion um die sogenannte "Klageindustrie" oft den Eindruck, "arme, rechtsschaffende" Unternehmen könnten in Zukunft ohne jeglichen Verstoß verklagt werden. Die Verbandsklagen-RL selbst enthält hierzu eine abschließende Aufzählung jener Rechtsakte, deren Verletzung eine Verbandsklage begründen kann. Es handelt sich dabei in erster Linie um EU-Recht, wie etwa die Datenschutz-Grundverordnung (DSGVO), die Warenkauf-Richtlinie (die das Gewährleistungsrecht regelt) oder die Verbraucherkredit-Richtlinie. In Österreich hat man sich darauf geeinigt, diesen Anwendungsbereich (auch auf nationales Recht) auszudehnen. Damit kann etwa auch die Verletzung einer Norm des österreichischen Schadenersatzrechts Gegenstand einer Verbandsklage sein.

Zivilprozesse sind kostspielig. Sachverständigengutachten und lange Verfahren können zu einer finanziellen Herausforderung für Kläger:innen werden. Verbände, wie etwa der VKI, sind deshalb nicht selten auf Finanzierung durch Dritte angewiesen. In der Vergangenheit wurde dies insbesondere mit Hilfe gewerblicher Prozesskostenfinanzierung gelöst. Die Verbandsklagen-RL überlässt es den Mitgliedstaaten, ob Drittfinanzierung für Verbandsklagen zulässig ist. Entscheiden sich die Mitgliedstaaten hierzu, so sieht die Verbandsklagen-RL aber gewisse Mindesterfordernisse an die Prozessfinanzierer vor, um zu verhindern, dass diese missbräuchlich das Verfahren beeinflussen. Der österreichische Gesetzgeber wählt hier einen liberalen Zugang: Im Gleichlauf mit der bisherigen Praxis in Österreich ist eine Finanzierung von dritter Seite weiterhin zulässig. Verbraucher:innen sind dabei wie erwähnt durch die umfassenden Schutzvorschriften der Richtlinie geschützt und selbst auch nicht Vertragspartner:innen der Prozesskostenfinanzierer. Das sind vielmehr die Qualifizierten Einrichtungen. Dass Drittfinanzierung für Verbandsklagen ermöglicht wird, ist erfreulich, schließlich hängt der Erfolg von Verbandsklagen gegen (mitunter finanziell übermächtige) Unternehmen nicht zuletzt auch von ausreichender monetärer Ausstattung der Qualifizierten Einrichtungen ab.

Die Klagen sind ausschließlich beim Handelsgericht (HG) Wien einzubringen. Zuständig für die Verbandsklagen ist unbeachtlich des Streitwerts ein Senat aus drei Berufsrichter:innen. Diese Neuregelung überzeugt insofern, als am HG bereits eine entsprechende Expertise mit Sammelklagen besteht. Die Verfahren können so effizienter geführt werden. Dies setzt aber voraus, dass das HG Wien ausreichend finanziell und personell ausgestattet wird – ein Einwand, den das Gericht auch selbst in seiner Stellungnahme angemahnt hat.

The Bad

Bei der Umsetzung der Verbandsklagen-RL wählt man in Österreich den Weg eines "Opt-in-Modells": Verbraucher:innen müssen sich bei der klagenden Qualifizierten Einrichtung aktiv zum Verfahren anmelden, um beteiligt zu sein. Hierzu haben sie drei Monate Zeit, nachdem der Verband die Durchführung eines Verbandsklageverfahrens angekündigt hat. Zu einem gegenläufigen "Opt-out-Modell", wonach alle Betroffenen eo ipso von der Klage repräsentiert werden – wie das etwa in den Niederlanden bereits gelebte Praxis ist – konnte man sich hierzulande nicht durchringen. Dies hätte insbesondere bei sogenannten Bagatell- oder Streuschäden (das sind geringfügige Schäden, die durch rechtswidriges Verhalten eines Unternehmens massenhaft auftreten) durchaus Vorteile: Verbraucher:innen tendieren nachgewiesenermaßen dazu, sich die Mühen des Rechtsweges zu ersparen, wenn der persönliche Schaden unter einer gewissen "Schmerzgrenze" bleibt. Beläuft sich der finanzielle Nachteil des oder der Einzelnen auf etwa unter 50 bis 100 Euro, so werden sich verhältnismäßig wenige Verbraucher:innen bei der Qualifizierten Einrichtung zur Teilnahme am Verfahren melden. Das dann unbelangt bleibende, rechtswidrig handelnde Unternehmen kann aber dennoch durch dieses Verhalten große Gewinne machen.

Zudem steht es den klagebefugten Verbänden offen, von den Verbraucher:innen eine Beitrittsgebühr zu verlangen. Das Gesetz deckelt diese auf 20 Prozent der geltend gemachten Anspruchssumme (des oder der jeweiligen Verbraucher:in) beziehungsweise auf höchstens 250 Euro. Gerade im Hinblick auf Bagatellschäden dürfte es sich dabei um eine weitere Hürde für ein "Opt-in" von Verbraucher:innen handeln. Offen lässt das Gesetz im Übrigen auch, wie eine Verteilung der eingeklagten Summen an die beteiligten Verbraucher:innen bei erfolgreicher Abhilfeklage zu erfolgen hat.

Bedauerlich ist das Versäumnis, die Verbandsklage überschießend auch für kleine und mittelgroße Unternehmen (KMUs) zu öffnen. KMUs sind genauso wie Verbraucher:innen nicht selten Opfer von unfairen Geschäftspraktiken größerer Unternehmen, aber auch sie haben oft nicht die finanziellen Ressourcen, um komplexe und kostspielige Einzelklagen zu führen. Deshalb würden KMUs gerade im Verhältnis zu großen Unternehmen von der neuen Verbandsklage profitieren. Auch würde man vermuten, dass es eigentlich im Interesse der Wirtschaft läge, schwarze Schafe zu eliminieren. Dass KMUs nicht berücksichtigt werden, verwundert nicht zuletzt auch deshalb, weil die Wirtschaftskammer als gesetzlich anerkannte Qualifizierte Einrichtung vorgesehen ist. Diese ist somit explizit zur Erhebung von Verbandsklagen legitimiert, obwohl sie selbst aber keinerlei Verbraucher:inneninteressen vertritt.

And the Ugly

Der Unionsgesetzgeber überlässt es in der Verbandsklagen-RL den Mitgliedstaaten, für die Zulässigkeit einer Verbandsklage auf Abhilfe eine notwendige Mindestanzahl an betroffenen Verbraucher:innen vorauszusetzen. Die österreichische Umsetzung sieht diesbezüglich vor, dass der Verband ein Klagebegehren von mindestens 50 Verbraucher:innen gegen dasselbe Unternehmen vorbringen muss. Orientiert hat sich der österreichische Gesetzgeber dabei wohl am Nachbarn Deutschland, wo die Mindestgrenze ebenso bei 50 liegt, dessen Bevölkerung (wie der VKI richtig festhält) aber auch das Zehnfache an Verbraucher:innen umfasst.

Eine Begründung liefert der österreichische Gesetzgeber für diese Zahl nicht. Das ist nicht unproblematisch: Schließlich kann es durchaus zielführend sein, bereits gerichtlich gegen ein Unternehmen vorzugehen, auch wenn bislang nur bei einzelnen Verbraucher:innen ein Schaden eingetreten ist. Das Unternehmen soll ja durch die neue Verbandsklage auch davon abgehalten werden, weiterhin rechtswidrig zu handeln. Die Qualifizierten Einrichtungen müssen dann zuwarten, bis ausreichend Verbraucher:innen betroffen sind, die dem Verfahren dann auch beitreten können und wollen. Nicht zu vernachlässigen ist letztlich, dass die administrativen Aufwendungen des Verbands vor der Klageerhebung umso höher sind, je mehr Betroffene für eine Verbandsklage benötigt werden.

Der europäische Gedanke, in allen Mitgliedsstaaten ein effektives Instrument zur Durchsetzung von kollektiven Verbraucher:inneninteressen zu etablieren, ist zweifelsohne zu begrüßen. Die Verbandsklage "nach Wiener Art" lässt aber einiges an Potenzial des EU-Rechtsakts ungenützt. Lücken (wie etwa, dass KMUs nicht von der neuen Verbandsklage profitieren) können aber weiterhin durch die "Sammelklage österreichischer Prägung" geschlossen werden. Es bleibt also abzuwarten, wie die neue Klageform von den qualifizierten Einrichtungen und Verbraucher:innen angenommen werden wird und ob sie in Fällen wie Dieselgate künftig tatsächlich für effizienteren Rechtsschutz sorgt.

OSZE-Empfehlungen zur Online-Kommunikation in Krisenzeiten

Menschenrechtsbasierte Strategien für staatliche Regulierung und Plattform-Governance

Julia Haas, Matthias C. Kettemann, Raphael Wibmer

Im Gastblog diskutieren Julia Haas, Matthias C. Kettemann und Raphael Wibmer die Bedeutung und Umsetzung von OSZE-Empfehlungen zur Sicherstellung der Medienfreiheit und freien Meinungsäußerung auf Online-Plattformen während Krisenzeiten.

Da Krisen stets auch Kommunikationskrisen mit sich ziehen, hat die OSZE fünf menschenrechtsorientierte Empfehlungen für die staatliche Politik und deren rechtliche Rahmenbedingungen erarbeitet. Aufbauend auf allgemeingültigen Prinzipien wie Transparenz, menschenrechtlicher Sorgfalt und Rechenschaftspflicht zielen die Empfehlungen darauf ab, die freie Meinungsäußerung und den Medienpluralismus im Zusammenhang mit automatisierter Content-Moderation auf Online-Plattformen auch im Krisenkontext zu gewährleisten.

Sowohl der russische Angriffskrieg auf die Ukraine als auch der Terrorangriff der Hamas gegen Israel und die Reaktion Israels darauf im Gaza-Streifen haben eine digitale Dimension; ebenso wie Naturkatastrophen, Pandemien, Klimanotstände und andere Krisen. In all diesen Situationen sind Internetplattformen wesentlich für den Zugang zu teils lebensnotwendigen Informationen, zur Mobilisierung oder etwa zur Dokumentation von Menschenrechtsverletzungen. Gleichzeitig werden sie allerdings auch für Propaganda, Gewaltanstiftung, gesellschaftliche Spaltung sowie Zensur und Überwachung genutzt.

Desinformation und verlässliche Information

Internetplattformen haben einen wesentlichen Einfluss auf die Gestaltung von unseren Kommunikationsräumen, sei es in Bezug auf Desinformation oder den Zugang zu verlässlichen Informationen. Dabei stellt sich die Frage, welche Verantwortung Staaten in der Regulierung und Kontrolle dieser zentralen Informationsräume zur Wahrung des Rechts auf freie Meinungsäußerung und Medienfreiheit haben. Insbesondere die Skalierbarkeit von Künstlicher Intelligenz (KI) beinhaltet Risken für die Online-Kommunikation sowie deren *Governance* – und macht ihre Regulierung umso wichtiger.

Artikel 19 des Internationalen Pakts über bürgerliche und politische Rechte fordert, dass Eingriffe in die Meinungsäußerungs- und Medienfreiheit gesetzlich vorzugeben, legitim, verhältnismäßig und notwendig sein müssen. Im Zuge der letzten Jahre – und insbesondere in Krisenkontexten – haben autoritäre Staaten digitale Informationsräume zunehmend zu kontrollieren versucht und automatisierte Content-Moderation als Waffe eingesetzt, um gesellschaftliche Freiräume zu schmälern, Lügen und Hass zu verbreiten und Meinungsvielfalt zu limitieren. Die allgegenwärtige Datenerfassung und -analyse, die dem heutigen, von *Big Tech* dominierten Internet

zugrunde liegt, lässt sich besonders zweckdienlich für Überwachung nutzen. Autokratische Kontrolle verschärft die ohnehin bestehenden menschenrechtlichen Herausforderungen im Zusammenhang mit "information disorder" und den oft inadäquaten, inkonsistenten oder anderweitig problematischen Krisenreaktionen der Internetplattformen.

Ein demokratischer, öffentlicher Diskurs zur menschenrechtlichen Regulierung von Internetplattformen kann dazu beitragen, dass auch in Krisensituationen inklusive gesellschaftliche Kommunikationsräume bereitstehen, die einen positiven Beitrag zu Informationszugang und -austausch und somit zur Krisenbewältigung leisten. Bis heute gibt es allerdings kaum Staaten, die spezifische Verfahren oder Strategien für Plattform-Governance in Krisenzeiten ausgearbeitet haben. Ein menschenrechtsbasierter Ansatz erfordert klare Terminologie und Kriterien, um festzulegen, welche Umstände eine Krise darstellen, wie Krisenprotokolle zu erarbeiten und wann sie zu aktivieren sind und welche spezifischen Maßnahmen in welcher Phase und für welche Dauer vorzunehmen sind. Obwohl sich Krisen je nach Art und Kontext unterscheiden, können durch die Identifizierung von Gemeinsamkeiten und Parallelitäten allgemeine Grundsätze entwickelt werden, die verhältnismäßigere, menschenrechtsfokussierten Maßnahmen ermöglichen.

Empfehlungen von der OSZE

Folgende Empfehlungen wurden diesbezüglich von der OSZE erarbeitet:

1. Staaten sollten sich auf Krisen vorbereiten und Internetplattformen verpflichten, konkrete krisenspezifische Maßnahmen zu erarbeiten. Dazu gehören umfassende menschenrechtsbasierte Krisenprotokolle, die sicherstellen, dass Reaktionen nicht ad hoc, sondern kohärent sind, und die eine lokale Kontextualisierung, Zusammenarbeit mit der Zivilgesellschaft und klare Zeitrahmen gewährleisten. Protokolle sollten schon vorab festlegen, was eine Krise definiert und wie der Zugang zu Information im öffentlichen Interesse verbessert werden kann.
2. Staaten sollten Plattformen beauftragen, krisensensibel die menschenrechtlichen Auswirkungen ihrer Aktivitäten und Maßnahmen zu prüfen und umfassende Risikoabschätzungen durchzuführen. Jede Krise erfordert je nach ihrer Art (kurz-, mittel-, langfristig) und Phase (vor, während, nach der Krise) einen maßgeschneiderten Ansatz zur Bewertung der Menschenrechtsverträglichkeit. Dabei müssen die kulturellen, sprachlichen und politischen Dimensionen der jeweiligen Krise berücksichtigt und ein Fokus auf Prävention und Risikominimierung gelegt werden. Maßnahmen sollten vor ihrer Umsetzung auf ihre Vereinbarkeit mit den Menschenrechten geprüft und regelmäßig unabhängig reevaluiert werden. Dieser Prozess muss umso transparenter und inklusiver gestaltet werden, je länger eine Krise andauert.
3. Staaten sollten lokale Expertise einbinden, relevante internationale Partnerorganisationen und die Zivilgesellschaft in Entscheidungsprozesse über Krisenprotokolle und angewendete Maßnahmen einbinden, um Legitimität, Gerechtigkeit und eine Verankerung in lokale Kontexte zu gewährleisten. In diesem Zusammenhang ist auf einen evidenzbasierten, interdisziplinären und inklusiven Ansatz zur Regulierung von KI-basierter Content Moderation zu achten. Darüber hinaus sollen Plattformen mandatiert werden, Zugang zu

Daten über krisenspezifische Regelungen und Praktiken zu gewähren, um unabhängige Forschung, Dokumentation und Kontrolle zu fördern.

4. Besonders in Krisenzeiten ist es wichtig, menschenrechtsorientierte Ansätze gegen die Instrumentalisierung von Informationen zu entwickeln. Staaten haben eine positive Verpflichtung, Menschenrechte zu achten, zu schützen und zu verwirklichen. Diese Verpflichtung sollte transparent und rechtsstaatlich wahrgenommen werden. Staaten sollten weder innerhalb nach außerhalb ihres Hoheitsgebiets Informationen manipulieren oder anderweitig einsetzen, um zu täuschen oder Verwirrung zu stiften. Stattdessen sollten sie breite Informationsvielfalt fördern und gegen Inhalte vorgehen, die Kriegspropaganda, Hass oder Anstiftung zur Gewalt oder Diskriminierung verbreiten. In Krisenzeiten müssen Staaten besonders dafür Sorge tragen, dass Plattformen nicht die Gewinnmaximierung über die Menschenrechte und das öffentliche Interesse stellen.
5. Krisenprotokollen und allen präventiven oder reaktiven Maßnahmen sollten intersektionelle Überlegungen zugrundeliegend, die geschlechtsspezifische Perspektiven berücksichtigen, sowie Risiken und Folgen von struktureller Diskriminierung, historischer Marginalisierung und globalen Machtungleichheiten.

Digital Services Act der EU

Einen ersten Schritt in Richtung eines nachhaltigen Krisenmanagements digitaler Inhalte und Plattformen beinhaltet der Digital Services Act der EU, der seit 17. Februar 2024 für die gesamte Union unmittelbar anwendbar ist. Konkret berechtigt die EU-Verordnung die Europäische Kommission dazu, sehr große Internetplattformen aufzufordern, in Krisenzeiten bestimmte Maßnahmen zu ergreifen, wie zum Beispiel die Anpassung von KI-Tools, um krisenrelevante und verlässliche Informationen prominenter anzuzeigen, oder um freiwillige Krisenprotokolle zu initiieren. Solche Protokolle sollten (1) Parameter zur Bestimmung "außergewöhnlicher Umstände" definieren, sowie (2) die Rolle der Beteiligten und zu ergreifenden Maßnahmen, und (3) ein Verfahren zur Aktivierung, und (4) zur Festlegung der Dauer der Maßnahmen. Weiters sollten die Krisenprotokolle (5) Schutzmaßnahmen zur Vermeidung negativer Auswirkungen auf die Menschenrechte festlegen sowie (6) Verfahren zur öffentlichen Berichterstattung der ergriffenen Maßnahmen, deren Dauer und Auswirkungen.

Das Jahr 2024 ist geprägt von Wahlen. Nicht nur in der EU, den USA und Indien, sondern in mehr als 75 Ländern – das betrifft die Hälfte der Weltbevölkerung – wird zur Wahlurne gerufen. Gleichzeitig ist die Welt von vielzähligen und vielfältigen Krisen erschüttert – bewaffneten Konflikten, Gesundheitskrisen, Klimanotständen. Eine Regulierung von Plattformen auf der Grundlage eines menschenrechtsbasierten Ansatzes ist dringend geboten, um Demokratie, Sicherheit und Menschenrechte nachhaltig zu garantieren.

Wie die Internetfreiheit in Belarus von der Telekom Austria abhängt

Die A1 Telekom Austria Group bleibt in Belarus aktiv und muss sich entscheiden, ob sie Kundenrechte schützen oder dem belarussischen Regime nachgeben will

Raphael Wibmer

Im Gastblog schreibt Raphael Wibmer von der Universität Innsbruck über die Internetfreiheit in Belarus und welche Rolle die A1 Telekom Austria Group dabei spielt.

Dass sich das freie Internet als dezentraler Ort des gegenseitigen Austauschs und der Information schlecht mit den Ideen von autoritären Regimen verbinden lässt, bekam das belarussische Regime im Vorfeld der Wahl des belarussischen Präsidenten 2020 zu spüren. Der unerwartete oppositionelle Gegenwind, der vom Internet bis in die Straßen von Belarus reichte, führte nicht nur zu ausufernder Polizeigewalt gegenüber den zehntausenden Protestierenden, sondern auch zu Internet-Shutdowns, Zensur und Verfolgung im Internet. So wurden beispielsweise am Wahltag zur Wahl des Präsidenten nicht nur physische Blockaden rund um Minsk von Polizei und Armee errichtet, sondern weite Teile des Landes wurden auch durch partielle Internet-Shutdowns vom Internet abgeschnitten.

Rolle des Internets bei den Protesten 2020

Im Mittelpunkt dieser Proteste stand Sergei Tikhanovsky, der 2019 den YouTube-Kanal "Ein Land zum Leben" (Страна для жизни) gegründet hatte. Anfangs veröffentlichte der Kanal hauptsächlich Interviews, in denen die gewöhnlichen Probleme der belarussischen Bürger:innen beleuchtet wurden. Innerhalb eines Jahres kamen auch immer mehr Akteur:innen der Opposition zu Wort und der Kanal wuchs auf über 140.000 Abonnent:innen, bis Sergei Tikhanovsky schließlich am 7. Mai 2020 auf selbigen YouTube-Kanal seine Kandidatur für das Amt des Präsidenten ankündigte. 22 Tage später wurde er verhaftet und schließlich im Dezember 2021 zu 18 Jahren Haft verurteilt. Dies stellte einen Verstoß gegen seine kommunikativen und politischen Freiheit dar – und ist auch ein fatales Signal für die Internetfreiheit in Belarus.

Was ist Internetfreiheit?

Im weitesten Sinne versteht man unter Internetfreiheit die Geltung der universellen Menschenrechte im Internet. Es gilt der Grundsatz: Was offline gilt, gilt auch online. Von besonderer Wichtigkeit sind hierbei die Meinungsäußerungsfreiheit, Informationsfreiheit und Medienfreiheit. Beispielsweise erstrecken sich diese Grundrechte im Bereich des Internets auf den Schutz vor Eingriffen durch Zensur, staatliche Überwachung, verteilte Netzwerkangriffe (DDoS attacks), Internet Shutdowns – und auf den Schutz von YouTubern vor Verhaftung.

Konkret geschützt werden diese Kommunikationsrechte in Europa etwa in Artikel 10 der Europäischen Menschenrechtskonvention (EMRK). In Österreich bietet daneben der Art 13 des Staatsgrundgesetzes einen noch weiterreichenden Schutz im Bereich

der Meinungsäußerungsfreiheit und Medienfreiheit. In Belarus gilt kein österreichisches Recht und – als einziges von 47 europäischen Ländern auch nicht die EMRK. Gebunden ist Belarus an die Kommunikationsgrundrechte trotzdem, da es seit 1973 Partei des Internationalen Pakts über bürgerliche und politische Rechte ist, dessen Art 19 fast mit gleichem Wortlaut wie der der EMRK, die Freiheit der Meinungsäußerung schützt.

Internetfreiheit in Belarus

Ein guter Anhaltspunkt, um Entwicklungen der Internetfreiheit festzustellen, ist der Freedom of Net Index der NGO Freedom House. Der Index quantifiziert Entwicklungen im Bereich der Beschränkung des Zugangs zum Internet, der Beschränkung des Inhalts und der Verletzung von Nutzer:innenrechte auf einer Skala von 1 (am wenigsten Freiheit) bis 100 (am meisten Freiheit). 2016 erreichte Belarus einen Freedom of Net Wert von 38/100, im Lichte der Proteste in Belarus 2020/21 fiel der Wert auf 31/100. Auch laut der neusten Erhebung im Freedom of Net Bericht 2023 verzeichnet der Index die fortlaufende Talfahrt der Internetfreiheit in Belarus mit einem Wert von 25/100.

Die Defizite der Internetfreiheit in Belarus lassen sich insbesondere auf Internet-Shutdowns und der Zensur und Verfolgung von Online-Äußerungen zurückführen. Internet-Shutdowns oder Internetabschaltungen, sind absichtliche Unterbrechungen des Internets oder der elektronischen Kommunikation mit dem Ziel, Kontrolle über den Informationsfluss auszuüben. Während der Proteste rund um die Wahl des Präsidenten 2020 wurden insgesamt sechs Internet-Shutdowns dokumentiert.

Antiextremismusgesetze

Die Unterdrückung der Meinungsfreiheit online basiert vorrangig auf einer Reihe von Antiextremismusgesetzen, wie dem Gesetz zur Bekämpfung des Extremismus, dem Gesetz zur Bekämpfung des Terrorismus, dem Gesetz zur Verhinderung der Rehabilitierung des Nazismus sowie der entsprechenden extremismusbezogenen Artikel in den Straf- und Verwaltungsgesetzen. Mit der Novellierung des Gesetzes zur Bekämpfung des Extremismus 2021, wurde der Begriff noch vager ausgestaltet.

Außerdem wurde mit der Einführung des Begriffs extremistische Strukturen anstatt extremistischer Organisationen die Feststellung des Vorliegens solcher Gebilde von Gerichten hin zum belarussischen Innenministerium verschoben. Auf dieser Grundlage lassen sich nun Eigentümer:innen, Administratoren:innen und Anhänger:innen von unliebsamen Online-Ressourcen strafrechtlich verfolgen. Auch das bloße Teilen solcher Inhalte kann Grundlage für strafrechtliche Verfolgung sein.

Zur Identifikation solcher unliebsamen Online-User:innen greifen Behörden vermehrt auf Online-Überwachung zurück, beispielsweise durch fortlaufende Überwachung öffentlicher Social-Media-Kanäle, Hacken privater Geräte oder umfangreiche Datenerfassung. Zusätzlich verbreitet die belarussische Regierung immer häufiger Propaganda online, speziell seit den Protesten 2020/21 ist die Veröffentlichung von Geständnisvideos, in denen Oppositionelle zu Schuldeingeständnissen gezwungen werden, ein gängiges Mittel.

Die Entwicklungen seit 2020 resultieren darin, dass heute beinahe alle nichtstaatlichen Medien aus dem Exil heraus agieren. Mit Ihnen wanderten etwa 250.000 Belaruss:innen aus. Mindestens 3.300 Personen wurden wegen politischer Verbrechen verurteilt, wobei momentan von 1.496 politischen Inhaftierten ausgegangen wird, von denen einige zu zehn Jahren übersteigenden Haftstrafen verurteilt wurden.

Die Rolle von A1

A1 Belarus, bis 2019 Velcom, ist mit 4,9 Millionen Kund:innen, der zweitgrößte Mobilfunkanbieter in Belarus. Seit 2007 ist das Unternehmen Teil der österreichischen A1 Telekom Austria Group. Das Unternehmen und die dahinterstehende österreichische Unternehmensgruppe sieht sich mit der Kritik konfrontiert, bei den Netzsperren rund um die Proteste in Belarus 2020/21 mit der Regierung kooperiert zu haben. Insbesondere wird A1 Belarus vorgeworfen, an der Sperrung oppositioneller Webseiten und kritischer Medien beteiligt gewesen zu sein.

Die UN-Leitprinzipien für Wirtschaft und Menschenrechte als auch OECD-Leitsätze für multinationale Unternehmen betonen ganz konkret, dass Unternehmen Menschenrechte zu achten, potenziellen Schaden zu verhindern oder möglichst gering zu halten haben und Wiedergutmachung leisten müssen für Schaden, den sie verursachen oder an den sie beteiligt sind. Als zweitgrößter Mobilfunkanbieter hat A1 eine besondere Verantwortung gegenüber der belarussischen Bevölkerung.

Maßnahmen

Um dieser Verantwortung gerecht zu werden und damit zumindest ein gewisses Maß an Internetfreiheit in Belarus erhalten bleibt, schlägt #KeepItOn, ein globales Netzwerk, das sich gegen Internets-Shutdowns einsetzt, folgende Maßnahmen vor:

- Beweissicherung und Kommunikation über Forderungen der belarussischen Regierung den Internetzugang zu unterbrechen
- Transparente Information über Unterbrechung von Internetdiensten, einschließlich Information über ihren Status und wann sie wieder online sein werden
- Koordination mit der Zivilbevölkerung und anderen Akteur:innen im Telekommunikationsbereich, um sich gegen Zensurforderungen der Regierung zu wehren
- Veröffentlichung von Transparenzberichten, um einen sicheren und offenen Internetzugang zu fördern und künftigen Abschaltungen entgegenzuwirken
- Aufrechterhaltung des Dialogs mit den relevanten Stakeholdern und betroffenen Gemeinschaften, um Beschwerde- und Hilfsmechanismen zu entwickeln

Bisher gab es aber kein Zeichen eines Kurswechsels des Unternehmens, das durch die vielen an Belarus gerichteten Sanktionsrunden der Europäischen Union immer mehr unter Druck gerät. Nachdem Belarus 2022 schon aus dem Swift-System ausgeschlossen wurde und es allgemein zur starken Einschränkung der

Finanzflüsse gekommen war, wurden in den neuesten Sanktionsrunden gegen Belarus – auch in Antwort auf Belarus Unterstützung des russländischen Angriffskriegs gegen die Ukraine – nun die Ausfuhr von Gütern mit doppeltem Verwendungszweck, fortschrittliche Güter und Technologien, Güter, die zur militärischen und technologischen Stärkung von Belarus oder zur Weiterentwicklung seines Verteidigungs- und Sicherheitssektors beitragen könnten und Gütern und Technologien, die für die Verwendung in der Luftfahrt oder Raumfahrtindustrie geeignet sind, unter Sanktion gestellt. Dies erschwert A1 Belarus die Geschäfte am Laufen zu halten, nicht zuletzt, weil laufende Investitionen im Bereich der Telekommunikation und besonders der Ausbau neuer Technologien nur mehr unter großem Aufwand möglich sein wird.

Österreichische Unternehmen – österreichische Verantwortung

Dass menschenrechtliche Belange mehr Gewicht haben als Einzelinteressen bestimmter Unternehmen, versteht sich mit Blick auf die österreichischen verfassungsrechtlich gewährleisteten Grundrechte von selbst. Doch in Hinblick auf Österreichs Außenpolitik scheinen die im Inland hochgehaltenen Menschenrechte einen geringeren Stellenwert zu haben.

So priorisierte die österreichische Regierung klar den Schutz der Geschäfte der Raiffeisen Bank International (RBI), als sie dem zwölften Sanktionspaket erst zustimmte, als die Ukraine die RBI von der Schwarzen Liste nahm. Auch in Bezug auf Sanktionen gegen Belarus 2021, nachdem ein Ryanair Flug von Belarus zum Landen gezwungen wurde, war Österreich laut EU-Diplomaten bedacht, Geschäfte österreichischer Unternehmen in Belarus nicht zu beeinträchtigen.

Eine klare Positionierung Österreichs hinsichtlich einer wertegeleiteten Außenwirtschaftspolitik erscheint wünschenswert. Einen Vorstoß in diese Richtung stellt beispielsweise die gescheiterte Schweizer Volksinitiative "Für verantwortungsvolle Unternehmen – zum Schutz von Mensch und Umwelt" dar. Ziel war es, durch eine Änderung der Verfassung die schweizerischen Unternehmen im Ausland an die Menschenrechte und den Schutz der Umwelt zu binden und im Schadensfall dafür haftbar zu machen.

Auch weniger drastische und, wie sich im Fall der Schweiz zeigt, schwer umzusetzende Maßnahmen wären schon zweckdienlich. Eine kohärente Kommunikation der österreichischen Diplomatie, bei Menschenrechten keine Kompromisse einzugehen, ob auf EU-Ebene, in der Wirtschaftsdiplomatie oder gegenüber österreichischen Unternehmen, wäre zielführend. Anzumerken sei auch, dass Österreich bei der Causa A1 Belarus nicht nur in Angelegenheiten der Gesetzgebung und der Exekutive eine Verantwortung trifft. Die österreichische Beteiligungs AG (Öbag) ist mit einem Anteil von 28,4 Prozent direkt an der Telekom Austria beteiligt und könnte sich somit auch unternehmsintern für die Rechte der Bürger:innen in Belarus einsetzen.

Österreichisches GmbH-Gesetz: Was bei Notfällen beachtet werden muss

Mit der Bestellung von Notgeschäftsführern sind häufig komplexe rechtliche Fragestellungen verbunden. Dies hat sich auch in der Covid-19-Pandemie gezeigt

Marlon Possard

Im Gastblog schreibt Marlon Possard, was das Gesetz für Notfälle innerhalb einer Gesellschaft vorsieht.

Das pandemische Geschehen rund um Covid-19 hatte nicht nur Auswirkungen auf ökonomische und gesundheitsrechtliche Bereiche, sondern auch auf handelsrechtliche Aspekte. Unterschiedliche Rechtsformen wurden durch Covid-19 mit neuen Fragestellungen und Problemfeldern konfrontiert. Darunter fanden sich unter anderem Fragen in Bezug auf die Bestellung von Geschäftsführerinnen und Geschäftsführern, welche speziell für eine GmbH von Relevanz waren. Aber wie muss grundsätzlich mit Situationen umgegangen werden, in denen die Geschäftsführerin oder der Geschäftsführer einer GmbH ausfällt?

Das gesellschaftliche Organ "GeschäftsführerIn" wird zunächst in § 15 GmbHG wie folgt geregelt:

(1) Die Gesellschaft muss einen oder mehrere Geschäftsführer haben. Zu Geschäftsführern können nur physische, handlungsfähige Personen bestellt werden. Die Bestellung erfolgt durch Beschluss der Gesellschafter. Werden Gesellschafter zu Geschäftsführern bestellt, so kann dies auch im Gesellschaftsvertrage geschehen, jedoch nur für die Dauer ihres Gesellschaftsverhältnisses.

(2) Wenn im Gesellschaftsvertrage sämtliche Gesellschafter zu Geschäftsführern bestellt sind, so gelten nur die der Gesellschaft bei Festsetzung dieser Bestimmung angehörenden Personen als die bestellten Geschäftsführer.

(3) Im Gesellschaftsvertrag kann die Bestellung von Geschäftsführern durch den Bund, ein Land oder durch eine andere öffentlichrechtliche Körperschaft vorbehalten werden.

Zunehmende Bedeutung

Aufgrund von Krankheit (meist handelte es sich in den vergangenen Jahren um eine Infektion mit Sars-CoV-2) zeigte sich jedoch in den letzten Monaten vermehrt, dass bestellte handelsrechtliche Geschäftsführerinnen und Geschäftsführer plötzlich mit einem persönlichen Ausfall konfrontiert waren und ihrer geschäftsführenden Tätigkeit nicht mehr (in vollem Maße) nachgehen konnten.

In vielen Fällen war die Krankheit sehr stark ausgeprägt, und den Betroffenen war es prinzipiell nicht mehr möglich, ihren geschäftsführenden Pflichten nachzukommen. In manchen Fällen trat der Tod der Geschäftsführerin oder des Geschäftsführers ein. Solche Beispiele stehen somit in unmittelbarem Konnex zu Fragen der (Neu-)Bestellung einer GmbH-Geschäftsführerin beziehungsweise eines GmbH-Geschäftsführers.

Gerichtliche Bestellung oft notwendig
Kommt es zu solchen Anlassfällen, regelt das österreichische GmbHG diesbezüglich die Möglichkeit der Bestellung einer sogenannten Notgeschäftsführerin beziehungsweise eines Notgeschäftsführers. Ziel einer solcher "Notbestellung" ist die Verhinderung einer etwaigen Handlungsunfähigkeit der GmbH.

§ 15a GmbHG normiert eine solche Vorgehensweise wie folgt:
(1) Soweit die zur Vertretung der Gesellschaft erforderlichen Geschäftsführer fehlen, hat sie in dringenden Fällen das Gericht auf Antrag eines Beteiligten für die Zeit bis zur Behebung des Mangels zu bestellen.

(2) Dies gilt auch, wenn kein Geschäftsführer seinen gewöhnlichen Aufenthalt im Inland hat.

(3) Der Beschluss über die Bestellung des Geschäftsführers ist mit dessen Zustimmung sowie, sofern im Beschluss nichts anderes angeordnet ist, mit Zustellung an den Geschäftsführer wirksam.
Somit ist es demnach möglich, dass das jeweilige zuständige Firmenbuchgericht eine Notgeschäftsführerin beziehungsweise einen Notgeschäftsführer ernennt. Dabei ist jedoch zu beachten, dass eine solche Bestellung grundsätzlich nur dann gerichtlich erfolgen kann, wenn die GmbH-Gesellschafterinnen beziehungsweise -gesellschafter selbst noch keine Geschäftsführerin oder keinen Geschäftsführer bestellt haben. Eine noch nicht durchgeführte GeschäftsführerInnen-Bestellung ist somit Voraussetzung für das gerichtliche Agieren.

Tritt ein Krankheits- oder Todesfall der Geschäftsführerin beziehungsweise des Geschäftsführers ein (etwa durch Covid-19) und wurde seitens der Gesellschaft selbst noch keine Geschäftsführerin oder kein Geschäftsführer bestellt, so muss seitens der Gesellschaft, also von mindestens einem Mitglied ebendieser, ein Antrag bei Gericht gestellt werden, damit eine Notgeschäftsführerin oder ein Notgeschäftsführer gerichtlich bestellt werden kann, der in weiterer Folge angemessen zu entlohnen ist. Im Rahmen der Bewertung der Erkrankung beziehungsweise des Ausfalles der Geschäftsführerin beziehungsweise des Geschäftsführers gilt es zu berücksichtigen, dass eine kurze Erkrankung (zum Beispiel Fieber über mehrere Tage) nicht ausreicht, um eine ebensolche gerichtliche Bestellung zu erwirken.

Möglichkeiten der Annullierung der gerichtlichen Bestellung
Im juristischen Kontext ist weiters zu beachten, dass unter einem Mitglied im Rahmen des GmbHG nicht nur die an der Gesellschaft beteiligten Gesellschafterinnen und Gesellschafter verstanden werden, sondern beispielsweise auch Gläubigerinnen beziehungsweise Gläubiger oder Mitarbeiterinnen und Mitarbeiter. Somit können auch diese Personenkreise einen Antrag bei Gericht für die Bestellung von Notgeschäftsführerinnen beziehungsweise -geschäftsführern einbringen und nicht nur die unmittelbaren GmbH-Gesellschafterinnen und -Gesellschafter.

Bei einer etwaigen Genesung der ursprünglichen Geschäftsführerin beziehungsweise des ursprünglichen Geschäftsführers der GmbH mit der Option, die GmbH-Geschäfte wieder ordnungsgemäß durchführen zu können, wird die gerichtliche Bestellung der Notgeschäftsführerin beziehungsweise des Notgeschäftsführers automatisch

aufgehoben, da der Grund für die Bestellung fehlt. Nicht nur eine Genesung infolge einer Erkrankung kann ein Aufhebungsgrund betreffend die gerichtliche Bestellung sein, sondern auch die Bestellung einer neuen Geschäftsführerin beziehungsweise eines neuen Geschäftsführers. Auch letzteres Vorgehen würde zu einer Annullierung der ursprünglichen Notbestellung führen.