

# KI-REGULIERUNG UND RECHTLICHE AUSWIRKUNGEN IM FOKUS

## THOMAS HOCHSTRASSER

LL. M., Partner im **Team Private Clients** bei Niederer Kraft Frey, Zürich

## ALEXANDER GÖBEL

MBA, Senior Associate im **Team Corporate/M&A und Technology** bei Niederer Kraft Frey, Zürich

Stichworte: KI-Regulierung, EU AI Act, Datenschutz

Die rasante Entwicklung der künstlichen Intelligenz (KI) bietet neue Chancen, stellt aber auch komplexe Herausforderungen dar (insb. für Politik und Wirtschaft). Während die EU mit der Verordnung über künstliche Intelligenz («AI Act») erste verbindliche Regeln geschaffen hat, prüft die Schweiz noch ihren Ansatz, der zwischen Innovationsförderung und rechtlicher Sicherheit abwägen muss. Dieser Artikel beleuchtet den aktuellen Stand der KI-Regulierung, zeigt Zukunftsperspektiven und gibt praxisnahe Empfehlungen für den Umgang mit (rechtlichen und gesellschaftlichen) Fragen in einem dynamischen Umfeld.

## I. Einleitung

Die künstliche Intelligenz (KI) hat sich in den letzten Jahren zu einer der bedeutendsten Technologien unserer Zeit entwickelt und erlaubt es sowohl Privatpersonen als auch Geschäften aller Industriebereiche, neue Möglichkeiten zu erschliessen.<sup>1</sup> Besonders nützlich sind KI-Technologien derzeit in der Industrie bei der Verbesserung von Vorhersagen, der Optimierung von Abläufen, der Ressourcenzuweisung und der Personalisierung von Dienstleistungen.<sup>2</sup>

Gleichzeitig wirft der rasche Fortschritt der KI-Technologie jedoch auch zahlreiche rechtliche, ethische und gesellschaftliche Fragestellungen auf. In der Schweiz, die traditionell eher eine innovationsfreundliche und marktwirtschaftlich orientierte Regulierungspolitik verfolgt,<sup>3</sup> steht der Gesetzgeber vor der Herausforderung, einen geeigneten rechtlichen Rahmen für KI zu schaffen, der einerseits der rasanten Entwicklung der Technologie gerecht wird, andererseits aber auch die Rechte der Bürger wahrt. Die potenziellen Auswirkungen von KI-Systemen auf die verfassungsrechtlich geschützten Grundrechte, die möglichen Sicherheitsrisiken für die Nutzer, wenn KI-Technologien in Produkte und Dienstleistungen eingebettet sind, sowie die Beeinflussung des Wettbewerbs geben somit Anlass «genauer hinzuschauen».<sup>4</sup> Vor allem können KI-Systeme – rein theoretisch – Grundrechte wie das Diskriminierungsverbot, den Schutz der Privatsphäre, die Meinungsfreiheit und die Menschenwürde gefährden.<sup>5</sup> Vor diesem Hintergrund ist die Frage nach einer

allenfalls erforderlichen gesetzlichen Regulierung daher unumgänglich.

Die Frage nach der Notwendigkeit und dem Umfang des gesetzlichen Regelungsbedarfs für KI wurde in den letzten Jahren vermehrt in der Politik thematisiert: Auf internationaler Ebene gibt es bereits verschiedene Ansätze, um den Einsatz von KI zu regulieren, etwa durch die KI-Verordnung der EU, die KI-Konvention des Europarates sowie den «Blueprint for an AI Bill of Rights» und die Durchführungsverordnung über die sichere und vertrauenswürdige Entwicklung und Nutzung von KI in den USA. Auch in der Schweiz hat der Bundesrat begonnen, verschiedene Regulierungsansätze zu prüfen, und er plant, durch das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) eine konkrete

<sup>1</sup> 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 Verordnungen (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) (AI Act), S. 2.

<sup>2</sup> Vgl. AI Act, S. 2.

<sup>3</sup> WIPO, Global Innovation Index 2023, Switzerland, <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023/ch.pdf> (besucht am 13.1.2025).

<sup>4</sup> AI Act, S. 2.

<sup>5</sup> Vgl. AI Act, S. 2.

Vorlage erarbeiten zu lassen, die sich an der internationalen Entwicklung orientiert.<sup>6</sup> Folglich ist das Ziel dieses Artikels, den aktuellen Stand der KI-Regulierung in der Schweiz (und im Ausland) zu beleuchten, Zukunftsperspektiven möglicher Regulierung aufzuzeigen, zentrale Herausforderungen und Trends zu identifizieren und praxisorientierte Empfehlungen zu geben, wie Unternehmen und die Politik auf die dynamischen Entwicklungen im KI-Umfeld reagieren können.

## II. Status quo der KI-Regulierung in der Schweiz

### 1. Rechtlicher Rahmen in der Schweiz

#### A) Keine spezifischen KI-Gesetze

In der Schweiz ist die Regulierung von KI noch in der Entwicklungsphase; derzeit gibt es keine explizit auf KI zugeschnittenen Gesetze oder Regulierungen.<sup>7</sup> Stattdessen greift ein Mosaik aus bestehenden und technologieunabhängigen Regelungen, die sich auf Teilaspekte von KI-Systemen anwenden lassen. Zu den relevantesten rechtlichen Grundlagen gehören:

- *Datenschutzgesetz (DSG)*: Das DSG schützt personenbezogene Daten, die in vielen KI-Anwendungen verarbeitet werden. Seit der Revision (in Kraft seit 1.9.2023) fordert das DSG Transparenz, insbesondere bei der automatisierten Entscheidungsfindung. Es verlangt, dass betroffene Personen über den Einsatz solcher Systeme informiert werden und gegebenenfalls Rechte wie Korrektur oder Löschung geltend machen können.
- *Praxisproblem*: KI-Systeme nutzen oft grosse Datenmengen, deren Herkunft und Verarbeitung für Nutzer (aber teilweise auch den Betreiber) nicht immer komplett nachvollziehbar sind.<sup>8</sup> Es ist meistens auch technisch nicht möglich, einzelne Datensätze, die für das Training eines KI-Systems verwendet wurden, nachträglich zu löschen.
- *Produkthaftungsgesetz (PrHG)*: Das PrHG greift bei Schäden, die durch fehlerhafte Produkte entstehen. KI-Systeme, die physische Geräte (z. B. autonome Fahrzeuge oder medizinische Geräte) steuern, fallen unter dieses Gesetz. Jedoch gibt es keine klaren Regelungen, wie rein digitale KI-Systeme zu bewerten sind.<sup>9</sup>
- *Diskriminierungsverbot (z. B. Gleichstellungsgesetz)*: Algorithmen, die Entscheidungen treffen, können allenfalls (unbeabsichtigt) diskriminierende Merkmale wie Geschlecht, Herkunft oder Alter heranziehen.<sup>10</sup> Die Schweiz schützt durch verschiedene Gesetze vor Diskriminierung, aber es fehlen spezifische Vorschriften, um KI-Entscheidungen systematisch zu überprüfen. Selbst wenn man versucht, KI-Systeme dahingehend zu trainieren, dass diese Faktoren wie Geschlecht, Herkunft oder Alter ignorieren, haben wissenschaftliche Studien bereits gezeigt, dass frei agierende KI-Systeme dann anhand sekundärer Faktoren doch wiederum diskriminierende Faktoren berücksichtigen<sup>11</sup> (Namen werden z. B. gewissen Nationalitäten zugewiesen oder aus einer Adresse wird die Zahlungsfähigkeit einer Person hergeleitet).

#### B) Soft Law und Selbstregulierung

Die Schweiz verfolgt traditionell einen liberalen Ansatz. Dies zeigt sich auch in der KI-Regulierung, die bisher stark auf Selbstverantwortung und Marktmechanismen setzt. Behörden greifen nur ein, wenn bestehende Gesetze verletzt werden. Somit spielt bisher das Soft Law eine besondere Rolle bei der KI-Regulierung. Die nachfolgend erwähnten Organisationen versuchen, etwaige Nachteile der KI-Technologie durch freiwillige Rahmenbedingungen einzuschränken:

- *Bundesrat*: Der Bundesrat hat am 25.11.2020 das Dokument «Leitlinien «Künstliche Intelligenz» für den Bund» verabschiedet, das als Orientierungsrahmen für den Umgang mit KI in der Bundesverwaltung dient.<sup>12</sup> Darüber hinaus können die Leitlinien aber auch Unternehmen als Grundlage für eine eigene KI-Policy dienen (siehe letztes Lemma).
- *Swiss Digital Initiative (SDI)*: Die SDI entwickelt ethische Standards für die digitale Transformation, einschliesslich KI (u. a. weltweit erstes Digital Trust Label). Dabei stehen Themen wie Transparenz, Fairness und Datenschutz im Fokus.
- *Code of Conduct*: Verschiedene Unternehmen/Branchen (z. B. Banken und Versicherungen, aber auch Hyperscaler wie Microsoft oder Amazon) haben freiwillige Verhaltenskodizes für den Einsatz von KI eingeführt, um Vertrauen zu schaffen und regulatorische Lücken zu schliessen.

#### C) Fehlen klarer Regeln für innovative KI-Technologien

Besonders neue Anwendungen wie generative KI (z. B. Chatbots, Text-zu-Bild-Systeme) oder autonome Fahrzeuge sind u. E. trotz dieser Soft-Law-Bemühungen bisher nur wenig reguliert. Diese Technologien werfen vielfache neue Fragen auf, etwa zu:

- *Urheberrecht*: Wer besitzt die Rechte an durch KI generierten Inhalten? Viele Anbieter von generativer KI

<sup>6</sup> Medienmitteilung des Bundesrates vom 22. 11. 2023, Bundesrat prüft Regulierungsansätze für Künstliche Intelligenz, Abs. 1, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98791.html> (besucht am 13. 1. 2025).

<sup>7</sup> Medienmitteilung des Bundesrates vom 22. 11. 2023.

<sup>8</sup> Bundesamt für Sicherheit in der Informatik, Transparenz von KI-Systemen, S. 5.

<sup>9</sup> BRAUN BINDER/BURRI/LOHMANN/SIMMLER/THOUVENIN/VOKINGER, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, S. 18 f.

<sup>10</sup> Algorithmwatch.ch, Künstliche Intelligenz: In der Schweiz diskriminieren Algorithmen ungestraft, <https://algorithmwatch.ch/de/neues-positionspapier-algorithmische-diskriminierung/> (besucht am 13. 1. 2025).

<sup>11</sup> Deutscher Ethikrat, Mensch und Maschine –Herausforderungen durch Künstliche Intelligenz.

<sup>12</sup> Leitlinien «Künstliche Intelligenz» für den Bund vom 25. 11. 2020, S. 2 im Zusammenhang mit der Medienmitteilung des Bundesrates vom 25. 11. 2020, Leitlinien «Künstliche Intelligenz» für die Bundesverwaltung verabschiedet, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81319.html> (besucht am 13. 1. 2025).

weisen sich in den allgemeinen Geschäftsbedingungen umfangreiche Nutzungsrechte an den generierten Inhalten zu.

- *Verbraucherschutz*: Wie können Nutzer vor manipulativen oder irreführenden Inhalten geschützt werden?

## 2. Zuständigkeit

In der Schweiz gibt es keine zentrale Behörde, die explizit für die Überwachung der KI-Technologie zuständig ist. Vielmehr teilen sich verschiedene Stellen die Zuständigkeiten, vor allem:

- *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)*: Verantwortlich für Datenschutzfragen, insbesondere bei automatisierten Datenverarbeitungen.
- *Staatssekretariat für Wirtschaft (SECO)*: Setzt Regeln zur Arbeitswelt um, z. B. im Bereich automatisierter HR-Systeme.
- *Bundesamt für Kommunikation (BAKOM)*: Überwacht Aspekte wie digitale Kommunikation und deren Regulierung, wobei KI-gesteuerte Systeme wie Sprachmodelle zunehmend relevant werden.

## 3. Regulierung auf internationaler Ebene

### A) Europäische Union

Die Verordnung über künstliche Intelligenz («AI Act») wurde von den Gesetzgebern der EU im Juni 2024 unterzeichnet und trat im August 2024 in Kraft.<sup>13</sup> Er ist die erste weltweit verbindliche horizontale Verordnung über KI, die einen Rahmen für die Nutzung und Bereitstellung von KI-Systemen EU-weit schafft.<sup>14</sup> Als Hauptregelungspunkte des AI Act sind die Definition von KI-Systemen, der risikobasierte Ansatz sowie seine Durchsetzung (Aufsichtsbehörden und Bussen) hervorzuheben.

- *Risikobasierte Klassifikation*: Der AI Act verfolgt einen regelbasierten, risikoorientierten Ansatz, der die regulatorischen Anforderungen je nach Einsatzbereich der KI und der Rolle des Unternehmens differenziert. Hierbei werden KI-Systeme in vier Risikokategorien eingeteilt (minimales Risiko, hohes Risiko, inakzeptables Risiko und «Spezifisches»). Abhängig von der Kategorie gelten unterschiedliche Vorschriften, die von Verhaltenskodizes und Transparenzanforderungen bis hin zu Verboten einzelner Anwendungen reichen.<sup>15</sup>
- *Praktische Implikationen*: KI-Systeme mit hohem Risiko, wie biometrische Überwachung oder medizinische Diagnosen, erfordern umfangreiche Compliance-Massnahmen.

Kritiker bemängeln, dass der AI Act einen zu restriktiven Ansatz verfolge, der Innovationen behindert und den Nutzen von KI einschränken könnte. Die tatsächlichen Auswirkungen des Gesetzes werden sich in den kommenden Jahren zeigen, da die in den parlamentarischen Diskussionen erstellten Auswirkungsstudien nur begrenzt die tatsächlichen regulatorischen Effekte widerspiegeln, was Unsicherheit erzeugt.<sup>16</sup>

Die Auswirkungen auf die Schweiz bestimmen sich gemäss dem Anwendungsbereich des AI Act. Nach Art. 2 AI Act ist die Verordnung auf alle Anbieter und Nutzer von

KI-Systemen anwendbar. Als Anbieter gilt jede natürliche oder juristische Person, die ein KI-System entwickelt und dieses in der EU in Verkehr bringt.<sup>17</sup> Als Nutzer fällt eine natürliche oder juristische Person in Betracht, die ausserhalb ihres persönlichen Bereiches ein KI-System unter ihrer Verantwortung in der EU verwendet.<sup>18</sup> Folglich entfaltet der AI Act auch extraterritoriale Wirkung: Auch Schweizer Unternehmen können unter die extraterritoriale Wirkung fallen und sind somit dem AI Act unterworfen: So werden Schweizer Anbieter, die KI-Systeme in der EU in Verkehr bringen und/oder Schweizer Anbieter und Nutzer von KI-Systemen, welche die vom KI-System erzeugten Ergebnisse in der EU verwenden vom Anwendungsbereich des AI Act erfasst.<sup>19</sup> Zudem hat auch der Bundesrat in seiner Medienmitteilung vom 22.11.2023 betont, dass die Prüfung der Regulierungsansätze in der Schweiz für KI mit dem AI Act kompatibel sein wird (ein vergleichbarer Ansatz wurde bereits im Datenschutzbereich gewählt).<sup>20</sup> Somit sind die Hauptregulierungspunkte – d. h. die Definition von KI-Systemen, der risikobasierte Ansatz sowie die Durchsetzung (insb. die Verhängung von Bussen), inkl. der Kritik daran – auch für die Schweiz relevant.

### B) USA

In den USA wird die Diskussion zur KI-Regulierung zunehmend mit derjenigen der EU verglichen. Mehr als ein Viertel der US-Bundesstaaten prüfen Gesetzesinitiativen zur KI-Regulierung im privaten Sektor. Auf Bundesebene wurde mit dem «Blueprint for an AI Bill of Rights» ein unverbindliches Rahmenwerk von der Biden-Regierung vorgestellt. Darüber hinaus haben führende Unternehmen wie Amazon, Google, Microsoft und OpenAI freiwillige Verpflichtungen zum verantwortungsvollen Umgang mit KI unterzeichnet.

Kalifornien, ein wichtiger Standort für IT-Konzerne, verabschiedete den California Consumer Privacy Act (CCPA), verzichtete jedoch auf eine spezifische KI-Regulierung aus Befürchtungen, dass diese die Innovationsfähigkeit von kalifornischen Unternehmen gefährden könnte. Trotz dieser Unterschiede gibt es in den USA und der EU gemeinsame Themen, etwa die Bekämpfung algorithmischer Diskriminierung und die Verantwortung der KI-Entwickler, verzerrte Ergebnisse in Bereichen wie Kon-

<sup>13</sup> AI Act, S. 1.

<sup>14</sup> AI Act, S. 1.

<sup>15</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 20, <https://www.pwc.ch/de/publications/2024/KI-Standort-Schweiz.pdf> (besucht am 13. 1. 2025).

<sup>16</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 20.

<sup>17</sup> Art. 2 Ziff. 1 Bst. a AI Act.

<sup>18</sup> LAPPERT, EU KI-Verordnung: «Brüssel-Effekt» in der Schweiz?, Untertitel 3, <https://kpmg.com/ch/de/themen/recht/kuenstliche-intelligenz-eu-verordnung-bruessel-effekt.html> (besucht am 13. 1. 2025).

<sup>19</sup> LAPPERT, EU KI-Verordnung: «Brüssel-Effekt» in der Schweiz?, Untertitel 4.

<sup>20</sup> Medienmitteilung des Bundesrates vom 22. 11. 2023, Abs. 3.

sumverhalten und Arbeitsmarkt zu verhindern. In neun US-Bundesstaaten wird derzeit über Massnahmen nachgedacht, um Transparenz und Fairness bei KI-Entscheidungen zu gewährleisten.<sup>21</sup>

#### 4. Zusammenfassung des Status quo

Die Schweiz verfolgt derzeit keinen spezifischen Regulierungsansatz für KI, sondern verlässt sich auf bestehende Gesetze und freiwillige Massnahmen. Dies schafft Innovationsfreiheit. In der Medienmitteilung des Bundesrates vom 22.11.2023 hat der Bundesrat angekündigt, dass er die Regulierungsansätze für KI prüfen wird.<sup>22</sup>

Internationale Entwicklungen, insbesondere der AI Act, üben dahingegen bereits heute einen Einfluss auf die Schweiz aus. Die oben erwähnten weiteren internationalen Regularien zeigen auch, dass viele Länder/Institutionen weltweit bestrebt sind, Rahmenwerke zu etablieren, die sowohl Innovation fördern als auch die ethischen, rechtlichen und sozialen Auswirkungen der KI im Blick behalten. Der internationale Dialog und die Schaffung von Standards wird für die Schweiz bei der Festlegung ihrer eigenen KI-Regulierungsstrategie von zunehmender Bedeutung sein.

### III. Zukunftsperspektiven der KI-Regulierung in der Schweiz

#### 1. Allgemein

Die Schweiz steht, wie im vorherigen Abschnitt erläutert, vor der Herausforderung, die Regulierung der KI in den kommenden Jahren an die rasanten Entwicklungen der Technologie anzupassen. Dabei wird die Schweiz sowohl auf nationale Initiativen als auch auf internationale Entwicklungen reagieren müssen, um ihre Position als wettbewerbsfähiger und innovativer KI-Standort zu sichern. Die regulatorische Landschaft wird u.E. in den nächsten Jahren zunehmend von einem risikobasierten Ansatz und einer verstärkten Zusammenarbeit mit internationalen Partnern geprägt sein.

Insbesondere werden sich u.E. die Fragen der Haftung, des Datenschutzes und der Transparenz von KI-Systemen als zentrale Punkte herauskristallisieren. Aufgrund der Notwendigkeit, die rechtlichen Rahmenbedingungen an die spezifischen Anforderungen von KI anzupassen und bestehende Gesetze, wie das DSG und das PrHG, die in Bezug auf KI teils unzureichend sind, weiterzuentwickeln, strebt der Bundesrat daher an, einen konkreten Vorschlag zur KI-Regulierung zu unterbreiten. Dieser soll auf den bestehenden rechtlichen Grundlagen aufbauen, jedoch spezifische Regelungen für KI-Systeme integrieren, die bislang nicht ausreichend berücksichtigt wurden. Dies ist jedoch kein einfaches Unterfangen: Selbst innovative und fortschrittliche Gesetzgeber sind mitunter (im Vergleich zur Technologie) «langsam» und können mit der technologischen Entwicklung nicht mithalten. Es ist somit eine Gratwanderung, bestehende Gesetze an neue Technologien anzupassen, aber gleichzeitig die Gesetze weitestge-

hend technologieunabhängig zu formulieren, um nicht ständig bei neuen Entwicklungen nachbessern zu müssen.

Ein zentraler Anknüpfungspunkt eines zukünftigen Regulierungsvorschlags könnte u.E. ein risikobasierter Ansatz sein, der KI-Systeme nach ihrem potenziellen Risiko für die Gesellschaft und Wirtschaft klassifiziert. Ähnlich dem AI Act könnte ein solcher Ansatz eine Unterscheidung zwischen hochriskanten und weniger risikobehafteten KI-Anwendungen vorsehen. Hochriskante Technologien, wie etwa autonome Fahrzeuge oder medizinische KI-Systeme, könnten strengeren Auflagen und einer intensiveren Überwachung unterzogen werden, um potenzielle Gefahren zu minimieren. Auf der anderen Seite könnten – und u.E. sollten – weniger risikobehaftete Anwendungen, wie einfache Automatisierungslösungen oder KI-gestützte Chatbots, geringeren regulatorischen Anforderungen unterliegen, um die Innovationskraft nicht zu behindern.

Die Schweiz wird dabei nicht nur nationale Aspekte berücksichtigen können, sondern auch internationale Entwicklungen beobachten müssen. Der AI Act, der wie erwähnt eine umfassende Regulierung von KI auf EU-Ebene vorsieht, stellt eine wichtige Orientierung dar. Die Schweiz wird sich in den kommenden Jahren u.E. eng mit den Entwicklungen auf europäischer Ebene auseinandersetzen müssen und versuchen müssen, ihre regulatorischen Massnahmen mit internationalen Standards abzustimmen, um Wettbewerbsnachteile zu vermeiden und den grenzüberschreitenden Handel zu erleichtern. Eine Harmonisierung mit der EU wird es Unternehmen ermöglichen, auch weiterhin auf dem europäischen Markt zu agieren, ohne dass zusätzliche regulatorische Hürden entstehen. Im Datenschutzbereich wurde ein solches Vorgehen u.E. bereits erfolgreich verfolgt.

Für Unternehmen bedeutet dies, dass sie sich bereits jetzt auf die kommenden regulatorischen Veränderungen vorbereiten sollten. Insbesondere wird die Notwendigkeit bestehen, KI-Systeme hinsichtlich ihrer Risiken und ethischen Implikationen zu überprüfen und entsprechende Massnahmen zur Sicherstellung der Compliance zu ergreifen.

Wenn sich die vorliegenden Ausführungen auch mit der Regulierung von KI befassen, so soll nicht verkannt bleiben, dass Regulierung auch immer Fortschritt einschränkt und die Schweiz in vielen Bereichen eine liberale Politik eingeschlagen hat und die gesetzliche Regulierung nur wo wirklich erforderlich einsetzt. Es ist u.E. demzufolge wichtig, dass auch bei der KI-Regulierung mit Bedacht agiert wird – Regulierung von KI ist u.E. erforderlich, aber man darf die Unternehmen dabei auch nicht zu sehr einschränken. In unserer Beratungspraxis sehen wir, dass Gesetzgeber in anderen Ländern hier teilweise nicht sehr vorsichtig vorgegangen sind. Gewisse Investitionsschutzverordnungen (z.B. UK) – sogenannte Foreign-Direct-In-

<sup>21</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 20.

<sup>22</sup> Medienmitteilung des Bundesrates vom 22. 11. 2023, Abs. 1 ff.

vestment-Verordnungen – könnten bereits dadurch einschlägig werden, dass ein zum Verkauf stehendes Unternehmen KI verwendet. In Anbetracht der weitgehenden Verwendung von KI könnte somit fast jede Transaktion unter Investitionsschutzmassnahmen fallen – das ist u. E. weder sinnvoll noch gewollt.

## 2. Mögliche Szenarien der Regulierung

Ein kürzlich (19.11.2024) veröffentlichtes Whitepaper von PwC, Economiesuisse und SWICA fasst die möglichen Herangehensweisen einer KI-Regulierung in der Schweiz wie folgt u. E. gut zusammen:

### A) Szenario 1: Regulatorischer Stillstand

In diesem Szenario bleibt die Schweiz bei der bestehenden Regulierung, ohne grössere Anpassungen vorzunehmen. Dies birgt das Risiko, dass die Schweiz bei der Entwicklung von KI und der Schaffung einer wettbewerbsfähigen Umgebung zurückfällt. In einem sich rasch entwickelnden Markt könnte die Schweiz als Nachzügler das Potenzial zur Wertschöpfung verpassen, und die technologischen Chancen bleiben ungenutzt.<sup>23</sup>

### B) Szenario 2: Evolution des bestehenden Rahmens

Das Szenario der Evolution schlägt vor, den bestehenden Rechtsrahmen schrittweise und gezielt anzupassen, um die Chancen der KI zu nutzen, ohne die Innovationskraft zu gefährden. Diese punktuellen Anpassungen könnten die Schweiz auf einen erfolgreichen und nachhaltigen Kurs führen, indem sie die regulatorischen Anforderungen flexibel und auf die spezifischen Bedürfnisse von KI anpasst. Dieses Szenario bietet die grössten Chancen, da es sowohl die nötige Regulierung als auch genügend Freiraum für Innovationen lässt.<sup>24</sup>

### C) Szenario 3: Rechtliche Zäsur

Dieses Szenario sieht die Einführung eines vollständig neuen Rechtsrahmens für KI (ähnlich zum AI Act) vor, was tiefgreifende und umfassende regulatorische Veränderungen bedeuten würde. Zwar könnte eine solche Neugestaltung der Rechtslage das Vertrauen und die Klarheit für Unternehmen stärken, jedoch besteht die Gefahr, dass dies zu einer Überregulierung führt, die Innovationen hemmt und das Wachstum bremst. Zudem könnten hohe Anpassungskosten und rechtliche Unsicherheiten die Wettbewerbsfähigkeit der Schweiz beeinträchtigen.<sup>25</sup>

### D) Empfehlung der Autoren des Whitepapers

Die Autoren des Whitepapers empfehlen klar den evolutionären Ansatz (Szenario 2) und somit ein Vorgehen, das bestehende Gesetze gezielt anpasst, anstatt neue, starre Regelungen einzuführen. So soll Innovation gefördert werden, während gleichzeitig Klarheit und Rechtssicherheit gewährleistet bleiben. Dieser Ansatz bietet gemäss den Autoren die besten Chancen, ohne die Risiken einer restriktiven oder zu nachlässigen Regulierung einzugehen.<sup>26</sup>

Wir stimmen der Empfehlung der Autoren grundsätzlich zu, jedoch ist u. E. bei dem Vorgehen die Wichtigkeit

des AI Act zu berücksichtigen. Es muss u. E. klar sichergestellt sein, dass Schweizer Vorgaben nicht im Widerspruch zum EU AI Act stehen, da ansonsten unüberwindbare Hindernisse für Schweizer Unternehmen geschaffen werden.

## 3. Herausforderungen

In den folgenden Abschnitten werden Herausforderungen bei der Nutzung von KI aufgezeigt, die bei Regulierungsbemühungen allenfalls berücksichtigt werden könnten bzw. allenfalls sollten.

### A) Transparenz und Nachvollziehbarkeit (Blackbox-Problematik)

Viele KI-Systeme, insbesondere solche, die auf maschinellem Lernen basieren, sind in ihrer Entscheidungsfindung für Menschen schwer bis gar nicht nachvollziehbar.

*Herausforderung:* KI trifft Entscheidungen (z. B. Kreditvergabe, medizinische Diagnosen), deren Logik weder Entwickler noch Endnutzer vollständig verstehen. Dies erschwert die Überprüfung auf Fehler oder Diskriminierung.

### B) Haftungsfragen

Die Haftung bei Fehlern oder Schäden, die durch KI verursacht werden, ist eine der grössten ungelösten rechtlichen Herausforderungen. Wenn ein autonomes Fahrzeug einen Unfall verursacht, wer ist dann haftbar? Ist es der Hersteller, der Softwareentwickler oder der Fahrzeughalter? Wer haftet für Fehlinformationen generativer KI (z. B. ein KI-System, das falsche medizinische Ratschläge gibt)? In der Schweiz regelt das PrHG zwar physische Schäden, lässt aber Fragen offen, wenn es um rein digitale Fehler geht (s. o.).

### C) Diskriminierung und Grundrechte

KI-Systeme, die auf historischen Daten trainiert wurden, können, wie bereits mehrfach erwähnt, bestehende Vorurteile und Diskriminierung verstärken.

*Herausforderung:* Ein KI-basiertes HR-System bevorzugt aufgrund der Datenlage Bewerber bestimmter Geschlechter oder ethnischer Gruppen.

### D) Datenschutz und Datensicherheit

KI benötigt grosse Mengen an Daten, oft personenbezogener Natur. Der Schutz dieser Daten wird durch die Komplexität moderner KI-Systeme erschwert.

*Herausforderung:* Die Schweiz hat mit dem neuen DSG zwar hohe Standards eingeführt, aber praktische Umsetzungsfragen bleiben: Wie kann sichergestellt werden, dass Trainingsdaten korrekt anonymisiert sind? Wie las-

<sup>23</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 25.

<sup>24</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 26 f.

<sup>25</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 27 f..

<sup>26</sup> FEDERER ET AL., KI-Standort Schweiz: Chancen nutzen und die Zukunft gestalten, S. 3, 28 ff.

sen sich Datenschutz und die Notwendigkeit grosser Datenmengen vereinbaren?

*E) Urheberrecht und Verbraucherschutz*

Technologien wie ChatGPT oder DALL-E haben grosse Fortschritte in der KI-Nutzung für die breite Öffentlichkeit gebracht, werfen jedoch neue Fragen auf:

*Urheberrecht:* Wem gehören durch KI generierte Inhalte? In der Schweiz gibt es bislang keine spezifische Regelung dazu.

*Verbraucherschutz:* Wie können Nutzer vor irreführenden oder manipulierten Inhalten geschützt werden?

**IV. Empfehlungen für die Praxis**

**1. Interne Richtlinien und Governance für KI**

Unternehmen sollten u. E. – ab einer gewissen Grösse – eigene Leitlinien und Strukturen für den ethischen und rechtskonformen Einsatz von KI schaffen:

- *Ethische Grundsätze:* Festlegung von Standards für den KI-Einsatz (z. B. Transparenz, Fairness, Datenschutz).
- *Kontinuierliche Überprüfung:* Etablierung von Mechanismen, um KI-Systeme regelmässig auf ihre Einhaltung von rechtlichen und ethischen Vorgaben zu überprüfen.

Natürlich darf es dabei auch nicht zu einer Überregulierung kommen. Es ist wichtig, dass innovative Unternehmen agil bleiben. Einige wenige, pragmatische Regelungen können dabei allenfalls zielführender sein als lange, komplexe Policies. Nach einer ersten, langen KI-Policy beschränkt sich die KI-Policy für Anwälte bei Niederer Kraft Frey z. B. auf die beiden folgenden Kernpunkte: Es dürfen keine Mandanteninformationen in KI-Systeme übertragen werden, und dem Output von KI darf nicht vertraut werden, d. h., alle Angaben sind zu prüfen.

**2. Risikobewertung und Klassifizierung von KI-Systemen**

Unternehmen sollten ihre KI-Anwendungen nach potenziellen Risiken bewerten, ähnlich dem risikobasierten Ansatz des AI Act:

- *Hochrisikosysteme:* Systeme, die sensible Entscheidungen treffen (z. B. Kredite, Personalentscheidungen), erfordern zusätzliche Tests und Audits.
- *Minimale Risiken:* Für Systeme mit geringem Risiko reicht eine grundlegende Compliance-Prüfung.
- Die Verwendung von generativer KI stellt – wenn diese für den eigentlich angedachten Anwendungsbereich eingesetzt wird – regelmässig kein Problem dar.

**3. Datenschutz und Datensicherheit priorisieren**

Da viele KI-Anwendungen grosse Mengen personenbezogener Daten verarbeiten, sollten Unternehmen sicherstellen, dass sie die Anforderungen des DSGVO erfüllen:

- *Datensammlung und Verarbeitung:* Daten möglichst anonymisieren und nur das Nötigste erfassen.
- *Transparenz für Kunden:* Klar kommunizieren, wie KI-Daten verarbeitet werden, und Nutzern Rechte (z. B. Löschanfragen) zugänglich machen.

**V. Fazit**

Die Regulierung von KI in der Schweiz befindet sich an einem entscheidenden Wendepunkt. Der derzeitige Fokus auf bestehende Gesetze und freiwillige Massnahmen hat den Vorteil, Innovation nicht zu behindern, bringt aber erhebliche Herausforderungen mit sich: unklare Haftungsfragen, mögliche Diskriminierung durch KI-Systeme, fehlende Transparenz und eine wachsende Regulierungsunsicherheit.

Die Schweiz kann ihre Position als führender KI-Standort nur sichern, wenn sie proaktiv handelt. Dabei sollte sie sich u. E. in gewisser Weise an internationalen Entwicklungen wie dem AI Act orientieren, ohne jedoch die eigene Flexibilität und technologieoffene Tradition zu verlieren. Innovationsfreundliche Ansätze wie eine enge Zusammenarbeit mit der Wirtschaft und die Förderung von Forschung sowie Bildung bieten hierfür eine tragfähige Grundlage.

Für Unternehmen ist klar: Warten auf gesetzliche Vorgaben ist keine Option. Sie sollten bereits jetzt Massnahmen ergreifen, um den ethischen und EU-rechtskonformen Einsatz von KI sicherzustellen.