RISIKO

POLIZEI & MILITÄR

Radikalisierung im Bereich des islamistischen Extremismus: Allgemeine Beobachtungen und ausgewählte Modelle
[Thomas Noll / David Hans / Michael Weber]

UMWELT & GESUNDHEIT

Chlorothalonil-Rückstände im Trinkwasser – eine Bestandesaufnahme und rechtliche Einordnung
[Tobias Tschumi / Marc Häusler]

TECHNIK & INFRASTRUKTUR

Digital Sovereignty in Switzerland: the laboratory of federalism
[Yaniv Benhamou / Frédéric Bernard / Cédric Durand]

RISIKO & RECHT AUSGABE 01 / 2023

RECHT

Risiko & Recht macht es sich zur Aufgabe, Rechtsfragen der modernen Risikogesellschaft zu analysieren. Berücksichtigung finden Entwicklungen in verschiedensten Gebieten, von denen Sicherheitsrisiken für Private, die öffentliche Ordnung, staatliche Einrichtungen und kritische Infrastrukturen ausgehen. Zu neuartigen Risiken führt zuvorderst der digitale Transformationsprozess und der damit verbundene Einsatz künstlicher Intelligenz; des Weiteren hat die Covid-Pandemie Risikopotentiale im Gesundheitssektor verdeutlicht und auch der Klimawandel zwingt zu umfassenderen Risikoüberlegungen; schliesslich geben gesellschaftliche Entwicklungen, u.a. Subkulturenbildung mit Gewaltpotential, Anlass zu rechtlichen Überlegungen. Risiko und Recht greift das breite und stets im Wandel befindliche Spektrum neuartiger Risikosituationen auf und beleuchtet mit Expertenbeiträgen die rechtlichen Herausforderungen unserer Zeit.

RISIKO & RECHT AUSGABE 01 / 2023

Editorial 1

POLIZEI & MILITÄR

Radikalisierung im Bereich des islamistischen Extremismus: Allgemeine Beobachtungen und ausgewählte Modelle
[Thomas Noll / David Hans / Michael Weber] 3

UMWELT & GESUNDHEIT

Chlorothalonil-Rückstände im Trinkwasser – eine Bestandesaufnahme und rechtliche Einordnung
[Tobias Tschumi / Marc Häusler] 38

TECHNIK & INFRASTRUKTUR

Digital Sovereignty in Switzerland: the laboratory of federalism
[Yaniv Benhamou / Frédéric Bernard / Cédric Durand] 65

TAGUNGS-BERICHT

6. Fachtagung Bedrohungsmanagement: Umsetzung Istanbul-Konvention
[Luca Lehmann / Vivian Stein] 102

Sehr geehrte Leserinnen und Leser

Die Herausgeberschaft von „Sicherheit & Recht“ hat sich Ende 2022 entschieden, das Konzept der Zeitschrift sowohl inhaltlich als auch formal zu überdenken. Inhaltlich ergab sich das Bedürfnis, auf neue Sicherheitsszenarien zu reagieren, formal sollten vor allem neue, digitale Vertriebsmöglichkeiten aufgegriffen werden. Das Resultat unserer Überlegungen ist die Nachfolgerin „Risiko & Recht“, eine thematisch breiter angelegte Fachzeitschrift, die als Open Access eJournal sowie gedruckt im Wege des Print on demand vertrieben wird.

Inhaltlich macht es sich Risiko & Recht zur Aufgabe, Rechtsfragen der modernen Risikogesellschaft zu analysieren. Berücksichtigung finden Entwicklungen in verschiedensten Gebieten, von denen Sicherheitsrisiken für Private, die öffentliche Ordnung, staatliche Einrichtungen und kritische Infrastrukturen ausgehen. Zu neuartigen Risiken führen zuvorderst der digitale Transformationsprozess und der damit verbundene Einsatz künstlicher Intelligenz; des Weiteren hat die Covid-Pandemie Risikopotenziale im Gesundheitssektor verdeutlicht und auch der Klimawandel zwingt zu umfassenderen Risikoüberlegungen; schliesslich geben gesellschaftliche Entwicklungen, u.a. Subkulturenbildung mit Gewaltpotenzial, Anlass zu rechtlichen sowie interdisziplinären Überlegungen. Risiko & Recht greift das breite und stets im Wandel befindliche Spektrum neuartiger Risikosituationen auf und beleuchtet mit Expertenbeiträgen die rechtlichen Herausforderungen unserer Zeit. Neben wissenschaftlichen Beiträgen wird Risiko & Recht auch Rechtsprechungsanalysen, Tagungsbeiträge und Literaturbesprechungen umfassen.

Formal setzt Risiko & Recht auf neue digitale Vertriebs- und Marketingmöglichkeiten, um eine breitere, internationale Leserschaft zu erreichen und aktuelle Beiträge schneller und unkompliziert verfügbar zu machen. Die digitale Vertriebsform umfasst zum einen die Lese- und Download-Option der Zeitschrift auf der Verlagswebseite (www.eizpublishing.ch) und weiteren Internet-Plattformen sowie den Versand der Zeitschrift in Gestalt von E-Mails für jede einzelne Ausgabe. Printexemplare können direkt beim Verlag oder auch im Buchhandel bestellt werden. Geplant sind drei Ausgaben pro Jahr. Da die Finanzierung von Publikationsprojekten im Open Access-Zeitalter nicht mehr durch den Verkauf von Printexemplaren erfolgt, freuen wir uns über jegliche Unterstützung unseres Projekts für die Wissenschafts-Community und interessierte Kreise. Eine hilfreiche Unterstützungsform bilden Print-Abonne-

ments (CHF 200.00 pro Jahr) sowie Gönner-Abonnements (CHF 400.00 einschliesslich Einladung zu einem jährlichen Event mit Vortrag und Networking-Möglichkeiten).

Wir freuen uns über Ihre Kommentare, Inputs sowie Anregungen und hoffen, Sie künftig zu unserer Stammleserschaft zählen zu dürfen.

In diesem Sinn wünschen wir Ihnen eine anregende Lektüre der ersten Nummer von Risiko & Recht!

Tilmann Altwicker
Goran Seferovic
Franziska Sprecher
Stefan Vogel
Sven Zimmerlin

Radikalisierung im Bereich des islamistischen Extremismus: Allgemeine Beobachtungen und ausgewählte Modelle

Thomas Noll / David Hans / Michael Weber*

Islamistische Attentate sind seltene, aber für Betroffene und Gesellschaft sehr einschneidende Ereignisse. Im Interesse von Forschung und Praxis steht insbesondere die „radikalisierte" Täterschaft. Im vorliegenden Beitrag werden einige der wichtigsten Radikalisierungsmodelle vorgestellt. Begriffe wie Radikalisierung, Extremismus und Jihadismus werden erläutert und verschiedene Annahmen wie diejenige, dass bei islamistischen Anschlägen religiöse Ideologien handlungsleitend seien, kritisch diskutiert.

Inhalt

I. Einleitung 4

II. Allgemeine Beobachtungen 5
1. Inzidenz islamistischer Anschläge 5
2. Terminologie 8
3. Radikalisierung als Zusammenspiel von Individuum, Ideologie und Umwelt 11

* PD Dr. iur. Dr. med. Thomas Noll ist Arzt und Strafrechtler. Er hat als Allgemein- und Gefängnispsychiater gearbeitet, war Chef Vollzug der JVA Pöschwies und Direktor des Schweizerischen Ausbildungszentrums für das Strafvollzugspersonal. Heute ist er Forscher im JuWe (Justizvollzug und Wiedereingliederung des Kantons Zürich). BSc David Hans ist wissenschaftlicher Mitarbeiter in der Abteilung Forschung und Entwicklung (F&E) im JuWe, wo er zu Themen wie Extremismus und Sicherheit forscht. Vor seiner Tätigkeit bei F&E arbeitete er rund 10 Jahre als Fachberufsoffizier im Kommando Spezialkräfte der Schweizer Armee. MSc Michael Weber ist Psychologe mit Vertiefungen im Bereich Klinische Psychologie und Neurowissenschaften sowie Forensische Psychologie. Er arbeitet als wissenschaftlicher Mitarbeiter in der Abteilung F&E im JuWe und an der Klinik für Forensik der Universitären Psychiatrischen Kliniken Basel.

III. Spezifische Radikalisierungsmodelle 15
1. Social Identity Perspective 16
2. Attitudes-Behavioral Corrective Model 20
3. Two Pyramids Model 22
4. Four Stage Model 23
5. Staircase Model 24
6. Significance Quest Model 25

IV. Präzisierungen 27
1. Radikalisierungsmodelle und Rational Choice Theory: Ein Widerspruch? 27
2. Einordnung bestehender Radikalisierungsmodelle 30

V. Zusammenfassung 31

Literatur 32

I. Einleitung

In seinem jüngsten Lagebericht beurteilt der Nachrichtendienst des Bundes (NDB) die Terrorbedrohung für die Schweiz als erhöht. Die Bedrohung wird primär vom islamistischen Extremismus geprägt, insbesondere durch Personen, die von jihadistischer Propaganda inspiriert werden.[1] Das Problem der Radikalisierung ist also real. Es darf andererseits aber auch nicht überschätzt werden, da eine solche Haltung rasch zu überschiessenden Reaktionen seitens des Staats und zu unverhältnismässigen Freiheitsbeschränkungen für bestimmte Teile der Bevölkerung führen kann.[2] Wichtig für die staatlichen Stellen, die sich mit jihadistischer Radikalisierung beschäftigen, ist eine umfassende Kenntnis des aktuellen Forschungsstandes. Terminologische Präzision bei den Begriffen Radikalisierung, Extremismus und Terrorismus ist von zentraler Bedeutung. Gewissen Experten zufolge ist Radikalisierung „what goes on before the bomb goes off".[3] Dass dies zu kurz greift, wird im folgenden Text dargelegt. Es werden zunächst zentrale Erkenntnisse zu jihadistischen Anschlägen in Europa und zur Radikalisierung im Allgemeinen präsentiert. Dabei

---

1 NDB, Sicherheit Schweiz 2022, Lagebericht des Nachrichtendienstes des Bundes, 39, abrufbar unter: <https://www.vbs.admin.ch/de/sicherheit/nachrichtenbeschaffung/gewaltextremismus.detail.document.html/vbs-internet/de/documents/nachrichtendienst/lageberichte/Lagebericht-NDB-2022-d.pdf.html>.

2 Silber/Bhatt, 1 ff.

3 Neumann, 4.

wird auf typischerweise benutzte Begrifflichkeiten wie Terrorismus, gewalttätigen Extremismus oder politisch motivierte Gewalt eingegangen. Es werden einige der verbreitetsten theoretischen Modelle zur Radikalisierung im Kontext des islamistischen Extremismus vorgestellt und kritisch diskutiert. In einer allgemeinen Kritik an bestehenden Radikalisierungsmodellen wird erläutert, dass die Modelle prototypische Entwicklungen zu erklären vermögen, sich aber aufgrund der geringen Spezifität ihrer Merkmale wenig für Risikoeinschätzung bzgl. gewalttätigem Extremismus eignen.

II. Allgemeine Beobachtungen

1. Inzidenz islamistischer Anschläge

In Europa haben im vergangenen Jahrzehnt bereits in verschiedenen Grossstädten – Madrid, London, Berlin, Brüssel, Paris, Nizza, Wien – islamistisch motivierte Anschläge mit zahlreichen Todesopfern stattgefunden. Während z.B. die Bombenanschläge auf Madrider Vorort-Züge am 11. März 2004 das Ergebnis einer konzertierten Aktion der Terrororganisation al Qaida waren, ist die überwiegende Mehrheit der aktuelleren Gewaltdelikte im öffentlichen Raum, die in Europa durch Personen mit islamistischem Hintergrund begangenen worden sind, mit einfachsten Mitteln wie z.B. dem Einsatz von Messern erfolgt. Derartige Attacken werden als „jihadistisch inspiriert" bezeichnet, da häufig keine formale Anbindung der Täter an eine extremistische Organisation bestand[4] und zugleich das eigentliche Ziel des gewalttätigen Jihadismus (dem sog. „kleinen" Jihad), das islamische Herrschaftsgebiet mit Gewalt auszudehnen und zu verteidigen, nicht immer im Fokus der handelnden Personen gestanden hat.[5] Nach der Definition von Europol sind aber auch derartige Delikte, darunter ein tödlicher Messerangriff auf eine Verwaltungsbeamtin in einer französischen Polizeistation am 23. April 2021 oder eine Messerattacke auf Reisende in einem deutschen Fernverkehrszug am 6. November 2021 mit fünf Verletzten, als jihadistische Terroranschläge zu werten.[6]

---

4 NDB, 2022, 39 f.

5 NDB, 2022, 43.

6 Europol, European Union Terrorism Situation and Trend Report 2022, 21 ff., abrufbar unter: <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat>.

Unabhängig von der dahinterliegenden Ideologie ist in Europa die Wahrscheinlichkeit für eine Einzelperson, einem terroristischen Attentat zum Opfer zu fallen, sehr gering. So hat etwa in England im vergangenen Jahrzehnt das Risiko, bei einem terroristischen Anschlag getötet zu werden, 1:11,4 Millionen pro Jahr betragen.[7] Zum Vergleich: Die jährliche Wahrscheinlichkeit, bei einem Strassenunfall zu sterben, hat in England in der Periode 2020-2021 1:48'000 betragen,[8] war also ca. 240-mal höher. Das Risiko, in Europa einem *islamistischen* Anschlag zum Opfer zu fallen, ist nochmals deutlich reduziert: Lediglich 15% der zwischen 2015 und 2021 in der Europäischen Union begangenen terroristischen Anschläge hatten einen islamistischen Hintergrund – durchschnittlich 19 Attentate pro Jahr in diesem Zeitraum.[9] Im jüngsten Berichtszeitraum 2021 sind dadurch zwei Personen ums Leben gekommen (2020: 12 Todesopfer).[10] In der Schweiz hat es in der jüngeren Vergangenheit genau ein islamistisch motiviertes Gewaltdelikt gegeben, infolgedessen ein Todesopfer zu beklagen war, nämlich am 12. September 2020 in Morges.[11] Insofern ist die Wahrscheinlichkeit, in der Schweiz einem islamistischen Terroranschlag zum Opfer zu fallen, sehr gering.

Dass die Gefahr terroristischer Handlungen, und hierbei insbesondere die Furcht vor islamistischem Terrorismus, in der Wahrnehmung der Bevölkerung dennoch so präsent ist,[12] hat unter anderem mit der sog. Verfügbarkeitsheu-

---

7 NOWRASTEH.

8 Gov.Uk, National statistics. Reported road casualties in Great Britain, provisional estimates: year ending June 2021, abrufbar unter: <https://www.gov.uk/government/statistics/reported-road-casualties-in-great-britain-provisional-estimates-year-ending-june-2021/reported-road-casualties-in-great-britain-provisional-estimates-year-ending-june-2021>.

9 Europol, European Union Terrorism Situation and Trend Report 2019, 13; abrufbar unter: <https://www.europol.europa.eu/publications-events/main-reports/terrorism-situation-and-trend-report-2019-te-sat>; Europol, European Union Terrorism Situation and Trend Report 2021, 12 f., <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-te-sat>.

10 Europol, 2022, 22.

11 NDB, Sicherheit Schweiz 2020, Lagebericht des Nachrichtendienstes des Bundes, 38 <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80848.html> (zit. NDB, 2020); FUMAGALLI, NZZ, 12 f.

12 In einer Umfrage des PEW Research Center aus dem Jahr 2017 bezeichneten 62% der Personen aus einer Stichprobe aus 38 Ländern den Islamischen Staat (IS) als die grösste aktuelle Gefahr. Dass in Frankreich und im Vereinigten Königreich 2017 sogar 88% bzw. 70% der Befragten den IS als grösste Gefahr identifizierten, zeigt, dass gerade in gewissen europäischen Ländern die Auswirkungen der Terroranschläge deutlich stärker zu sein schienen und Themen wie Klimawandel und Weltwirtschaft verdrängt wurden (POUSTHER/MANEVICH, 2 ff.).

ristik zu tun. Dabei handelt es sich um die Tendenz von Menschen, bei Entscheidungen Informationen zu verwenden, die schnell und einfach verfügbar sind.[13] In der Presse ist das Thema Terrorismus unverhältnismässig häufig repräsentiert, da die Medien um aufmerksamkeitsstarke Schlagzeilen konkurrieren.[14] In der Folge erscheint das Risiko, Opfer eines terroristischen Anschlags zu werden, unverhältnismässig hoch. Das Thema gewinnt an politischer Bedeutung, weil es in aller Munde ist. Die Reaktion des politischen Systems richtet sich nach der Intensität der öffentlichen Stimmung. Zusammengenommen können diese Tendenzen in der Bevölkerung eine irrationale Sensibilität auslösen, die bis hin zu Forderungen nach Abschaffung oder Einschränkungen von bestimmten Grundrechten verdächtiger Bevölkerungsgruppen führen kann. Die Verfügbarkeitsheuristik hat damit die Prioritäten neu gesetzt.[15] In der heutigen Welt sind Terroristen „die bedeutendsten Praktiker in der Kunst der Verfügbarkeitsheuristik".[16]

Diese Überlegungen ändern aber wohlverstanden nichts daran, dass terroristische Anschläge vorkommen, immenses Leid verursachen und bestmöglich verhindert werden müssen.

---

13 Die Verfügbarkeitsheuristik ist eine kognitive Verzerrung, bei der man eine Entscheidung auf der Grundlage eines Beispiels, einer Information oder einer kürzlich gemachten Erfahrung trifft, die einem unmittelbar zur Verfügung steht, auch wenn es vielleicht nicht das beste Beispiel für die Entscheidung ist (Tversky/Kahneman, 207 ff.).

14 Ein weiterer Grund für die prominente Darstellung des Themas in der Presse besteht in der Vermischung unterschiedlicher Phänomene: Personen, die terroristische Organisationen ideologisch unterstützen, werden mit Personen, die im Ausland kämpfen wollen, aber niemals eine terroristische Operation im Inland durchführen würden, sowie mit den wenigen Personen, die tatsächlich auch bereit wären, ein terroristisches Attentat durchzuführen, in einen Topf geworfen. Damit erscheint die Zahl der „Terroristen" erhöht, was die Presse entsprechend präsentiert (Sageman, Misunderstanding, 21).

15 Kahneman, 142.

16 Kahneman, 144; Marc Sageman hat festgehalten: „Engagierte Journalisten haben sich bei mir darüber beschwert, dass ihre Berichte (von der Redaktion) so bearbeitet wurden, dass sie ein negatives Bild der Verdächtigen zeichnen, um dem gängigen Stereotyp zu entsprechen. Solche Verzerrungen stellen die Zuverlässigkeit von fehlerhaften Zeitungsberichten als Quellen für die Terrorismusforschung in Frage." (Sageman, Political Violence, xii).

2. Terminologie

Als Konsequenz diverser Anschlagsgeschehen sind Schlagwörter wie Radikalisierung, Extremismus und Terrorismus zu prägenden Begriffen des medialen, politischen und gesellschaftlichen Diskurses geworden. Eine allgemeingültige oder uneingeschränkt akzeptierte Definition dieser Begriffe existiert jedoch nicht.[17]

Als kleinster gemeinsamer Nenner der zahlreichen verschiedenen Definitionen[18] kann Radikalisierung als ein Prozess definiert werden, bei dem sich jemand zunehmend zu einer revolutionären, militanten oder extremistischen Person wandelt.[19] Meist ist eine bestimmte Ideologie in der Definition enthalten. Radikalisierung im Kontext des Islamismus wäre demnach die Hinwendung zu (möglicherweise gewalttätigem) Extremismus in (zumindest vordergründiger) Verbindung mit einer islamistischen bzw. jihadistischen Interpretation des Islam.[20] Jihadismus kann hierbei als Unter-Variante von islamistischem Extremismus verstanden werden, deren primäres Ziel in der kriegerischen/ gewaltsamen Ausweitung und Verteidigung des islamischen Herrschaftsgebiets besteht (der sog. „kleine" Jihad, in Abgrenzung zum sog. „grossen" Jihad, welcher das übergeordnete geistig-religiöse Bemühen der Gläubigen mit dem Ziel eines gottgefälligen, moralisch einwandfreien Lebens meint).[21] In der jüngeren Vergangenheit wird Jihadismus oft in Verbindung gebracht mit Jihad-Reisenden in syrische oder irakische Krisengebiete, die sich dort dem bewaffneten Kampf gegen die örtlichen Regierungen anschliessen. Die Rolle derartiger auch geopolitisch geprägter Bestrebungen ist häufig jedoch unklar bei den oben genannten niederschwellig durchgeführten Attentaten durch Einzeltäter, die sich in der Regel durch eine komplexe Motivlage auszeichnen.[22]

Das Ergebnis des Radikalisierungsprozesses besteht somit zunächst in einer mehr oder weniger feststehenden extremistischen Überzeugung. Diese ist normativ definiert als Abweichung von einer innerhalb einer bestimmten Zeit und innerhalb einer bestimmten Population als „normal" geltenden Geisteshaltung; im Fall des Islamismus umfasst eine solche abweichende Haltung z.B. das Höhersetzen religiöser über staatliche Gesetze, die Ablehnung „westli-

17 Weber/Rossegger/Endrass, 833; Bötticher, 73; Schmid, 158.
18 Für eine Liste verschiedener Definitionen: s. Borum, I, 12 f.
19 McGilloway/Ghosh/Bhui, 39.
20 Demichelis/Mezzetti, 266.
21 Pfahl-Traughber, 68.
22 NDB, 2022, 43.

cher“ Werte wie Liberalismus, das Etablieren von Feindbildern wie Feministinnen und Feministen, Juden und Jüdinnen, Christinnen und Christen und rivalisierende islamische Glaubensrichtungen sowie die Ablehnung der universellen Menschenrechte. Je nach Definition beinhaltet eine extremistische Überzeugung auch das Befürworten von Gewaltanwendung oder das willentliche Ausleben normabweichenden Verhaltens.[23]

Von Terrorismus hingegen wird nach gängiger wissenschaftlicher Definition erst dann gesprochen, wenn im Rahmen einer fest strukturierten und arbeitsteilig organisierten Struktur Gewaltdelikte im öffentlichen Raum durchgeführt werden, die einen Botschaftscharakter haben und in der Regel stellvertretend gegen Zivilpersonen gerichtet sind, um auf diese Weise Verunsicherung und Panik in der Bevölkerung auszulösen.[24] Dass diese enge Definition nicht auf sämtliche als islamistische Terroranschläge bezeichneten Angriffe der jüngsten Zeit zutrifft, dürfte bereits beim Lesen des vorigen Abschnitts aufgefallen sein.

Mangels klarer Definitionen erscheint es umso wichtiger, möglichst exakt zu beschreiben, mit welchen Prozessen und mit welchen Personen man sich befasst. So führt nicht zuletzt das Vermischen von Personen, die die Handlungen einer extremistischen Organisation gutheissen, mit Personen, die im Ausland kämpfen wollen, aber niemals eine terroristische Operation im Inland durchführen würden (Ausreisende in Kriegs- und Krisengebieten) sowie mit den wenigen Personen, die tatsächlich Gewalt anwenden, zu vollkommen anderen Zahlen bezüglich dieser unterschiedlichen Gruppen an „radikalisierten“ bzw. „extremistischen“ Personen.[25]

Um das Risiko einer Fehldeutung von gewalttätigem Verhalten als zwangsläufiges Ergebnis von radikaler, Gewalt rechtfertigender Ideologie zu verringern, wird statt von „Radikalisierung“ zum Teil auch von der „Hinwendung zu

---

23 Khalil/Horgan/Zeuthen, ABC, 1 ff.; Crettiez/Duclos, 52 f.

24 Schmid, 158 f.

25 Giustozzi, 33 ff.; Merari et al., 89; Sageman, Political Violence, 21; In einer Umfrage in 35 mehrheitlich islamischen Ländern mit 50'000 befragten Moslems, die statistisch repräsentativ waren für die 1,3 Milliarden Moslems weltweit, gaben 37% an, die terroristischen Attacken vom 11. September 2001 teilweise, weitgehend oder vollkommen gutzuheissen. Dies impliziert Hunderte von Millionen Moslems, die diese Angriffe zumindest teilweise billigten. Dem gegenüber stehen einige Tausend, die tatsächlich willens sind, terroristische Gewalt auszuüben. Dasselbe Phänomen ist in Europa zu beobachten, wo aus einer Population von ca. 20 Millionen Moslems weniger als 3'000 Personen aufgrund islamistischer Aktivitäten inhaftiert sind (Atran, Enemy, 57 f.; Esposito/Mogahed, 1 ff.).

politischer Gewalt“ gesprochen.[26] Die Hinwendung zu politischer Gewalt ist das, was man gemeinhin unter dem Begriff „Terrorist werden“ versteht,[27] und demnach die Bereitschaft umfasst, ideologisch motivierte Gewalt auszuüben. Gleichwohl berührt eine solche Auffassung zeitgeschichtlich geprägte Interpretationen dessen, was gerechtfertigte und nicht gerechtfertigte politische Gewalt darstellt.[28]

Im vorliegenden Phänomenbereich z.B. wird in der Öffentlichkeit streng islamisches Gedankengut (z.B. Salafismus) oft automatisch mit gewalttätigem islamistischem Handeln (Jihadismus) gleichgesetzt.[29] Aus einer forensischen, präventiven Sichtweise ist genau diese Unterscheidung zentral: Ein Hauptziel des Handelns von Sicherheitsbehörden besteht letztlich im Verhindern von Gewalt, sodass Risikomerkmalen ein besonderes Gewicht zukommt, die unmittelbar der Einschätzung der Wahrscheinlichkeit des Überschreitens der Handlungsschwelle dienen. Für den vorliegenden Text wird für die spezifische Art der Gewalt (Zieldelikt) der Begriff des gewalttätigen Extremismus (sofern ideologie-übergreifend) bzw. des gewalttätigen Islamismus (spezifisch für das Thema der vorliegenden Arbeit) verwendet. Auch in der englischsprachigen Fachliteratur ist der Begriff des „violent extremism“ gebräuchlich und wird zum Teil synonym zu den Begriffen „Terrorismus“ oder „politisch motivierte Gewalt“ verwendet. Entsprechend ist im Verständnis des vorliegenden Texts die Ausübung von Gewalt vor dem Hintergrund einer islamistischen Ideologie der seltene, aber mögliche Endpunkt einer Radikalisierung, den zu erreichen es zu verhindern gilt.

Bevor spezifische Radikalisierungsmodelle vorgestellt und deren Inhalte eingeordnet werden, soll an dieser Stelle eine kritische Auseinandersetzung mit dem Begriff der „Radikalisierung“ als solcher erfolgen. Dieser kann eine Art *Indoktrination, Manipulation und Gehirnwäsche* durch Dritte insinuieren. Eine

---

26 Crettiez/Duclos, 1 ff.

27 Sageman, Political Violence, 9 f.

28 Das aus den 1970er Jahren stammende und dem US-amerikanischen Terrorismusforscher Brian Jenkins zugeschriebene Bonmot „Der Terrorist des einen ist der Freiheitskämpfer des anderen“ veranschaulicht dies (Berger/Weber, 2008, 14). So hat die westliche Welt beispielsweise einen afghanischen Mudschahed in den 1980er Jahren einen Freiheitskämpfer genannt, als er auf ihrer Seite war, ihn aber 20 Jahre später als Terroristen verurteilt, obwohl er immer noch genau das Gleiche tat: sein Land mit Gewalt gegen ausländische Invasoren zu verteidigen (Sageman, Political Violence, 10).

29 Amghar, 95 ff.

solche kommt in der Realität allerdings nur höchst selten vor.[30] Insbesondere im Radikalisierungsmodell der Social Identity Perspective (SIP, siehe unten III.1.) wird betont: „There is no brainwashing or mysterious process of radicalization. These group members just carry out their social identity, like soldiers carrying out violence because that is who they are and what they do, and not because of their need for approval, fear of sanction, or group pressure to conform".[31] Eine eigentliche Rekrutierung islamistischer Terroristen mit gezielter Sensibilisierung und Indoktrination komme in Wirklichkeit nicht vor. Tatsächlich ist die Vorstellung realitätsfremd, dass Personen durch Gehirnwäsche dazu gebracht würden, sich in extremistischen Kleingruppen mit definierten „Infrastrukturen" zu organisieren.[32] Dass es sich bei extremistischen Gewalttätern gar um reduziert urteilsfähige oder sogar willenslose Tatinstrumente handelt, wird in der Literatur dezidiert abgelehnt.[33]

3. Radikalisierung als Zusammenspiel von Individuum, Ideologie und Umwelt

Der folgende Abschnitt soll einen kursorischen Überblick liefern, welche Eigenschaften und Entwicklungsprozesse bei Personen berichtet werden, die in Europa ein islamistisch motiviertes Gewaltdelikt begangen haben. Wie im vorhergehenden Abschnitt im Hinblick auf die öffentliche Darstellung beschrieben, besteht auch in der Fachliteratur zu Merkmalen von Gewalttätern mit einer bestimmten Ideologie eine Herausforderung darin, dass häufig Gewalttäter mit unterschiedlichen extremistischen Ideologien[34] oder gewalttätige und nicht gewalttätige Personen mit islamistischer Einstellung gemeinsam betrachtet werden.[35] Dies führt dazu, dass vermeintliche Indikatoren für gewalttätigen Islamismus tatsächlich lediglich Indikatoren der im Allgemeinen gewaltfreien islamistischen Protestgesellschaft sind.[36]

---

30 Dass ein Effekt durch Hirnwäsche intuitiv rasch einleuchtet, hängt möglicherweise mit ihrer übermässigen Repräsentation in Büchern und Filmen zusammen: Siehe beispielsweise den empfehlenswerten Politthriller „The Manchurian Candidate" von John Frankenheimer oder die aktuelle französische Miniserie „Le Syndrome E".

31 Sageman, Political Violence, 22.

32 Atran, Enemy, 50.

33 Introvigne, 1 ff.; Nuraniyah, 890; Bloom, 1 ff.; Gambetta, 1 ff.; Hafez, 1 ff.; Merari, 1 ff.; Pape, 1 ff.; Pedahzur, 1 ff.

34 Z.B. Thijssen et al., Background Characteristics.

35 Doering/Garth/Corrado, 1 ff.; Thijssen et al., Motivational Classes.

36 Sageman, Misunderstanding, 167 f.; Bartlett/Miller, 16.

Beim Versuch, die individuelle Motivlage eines extremistisch eingestellten Menschen zu eruieren, ist es von zentraler Bedeutung, auf die Person selbst und nicht ausschliesslich auf die Ideologie ihrer Gruppe zu fokussieren. In der öffentlichen Wahrnehmung und auch unter Fachpersonen ist eine Neigung zu beobachten, die ursächliche Rolle der – vermeintlich – einem Gewaltakt zugrundeliegenden islamistischen Ideologie zu stark zu gewichten – auf Kosten politischer, wirtschaftlicher, sozialer oder in der Persönlichkeit liegender Ursachen.[37] Umgekehrt wird von Fällen islamistisch anmutender Gewalt berichtet, in denen z.B. materiellen Motiven, einem Gefühl der Zugehörigkeit, dem Abenteuer, dem Status etc. eine zentrale Rolle auf dem Weg zur Gewalt zugekommen ist.[38] Kurzum: Einstellungen und Verhalten müssen sich keineswegs entsprechen, sondern müssen als zwei unterschiedliche Dimensionen des Extremismus verstanden werden.

Die Absichten von Extremisten lassen sich eher aus Worten und Taten ableiten als aus einer (religiösen) Ideologie per se.[39] Als Handlungserklärung ist die Ideologie zu allgemein und zu unbestimmt.[40] Hinzu kommt ein grosser Anteil an Gewalttätern im öffentlichen Raum, deren Ideologie als „composite violent extremism" bezeichnet wird, da sie durch eine individuell ausgestaltete Verschmelzung unterschiedlicher Überzeugungen oder Anliegen gekennzeichnet ist.[41]

Bezogen auf den gewalttätigen Islamismus wird berichtet, dass die überwiegende Mehrheit von aus Europa sowie den USA stammenden Islamisten im Tatvorfeld weder eine Einrichtung (z.B. Trainingslager), die eine gewalttätige Ideologie lehrt, noch Moscheen oder Gebetsräume besucht hatten. Vielmehr wiesen sie keinerlei Anzeichen von Religiosität auf.[42] In einer longitudinalen, prospektiven Studie konnte die Entwicklung von 150 Personen über ein Jahr beobachtet werden, die in einem staatlichen französischen Präventionsprogramm betreut wurden, weil sie wegen islamistischer Aktivitäten (grossmehrheitlich wegen des Versuchs, sich dem IS anzuschliessen) bei den Sicherheitsbehörden auffällig geworden waren.[43] Am Ende der Beobachtungsperiode hatten sich – trotz Intervention – 10% der Personen dem IS angeschlossen und 13% galten als weiterhin radikalisiert. Es konnte gezeigt werden, dass fol-

---

37 Sageman, Misunderstanding, 80; Sageman, Political Violence, 44; Demichelis/Mezzetti, 227.

38 Khalil/Horgan/Zeuthen, ABC, 2; Khalil, 198.

39 Rapport, 1 ff.

40 McCauley/Moskalenko, Them and us, 280.

41 Gartenstein-Ross et al., 1.

42 Demichelis/Mezzetti, 227; Sageman, Misunderstanding, 80.

43 Campelo et al., 1 ff.

gende Eigenschaften prädiktiv für einen in diesem Sinn ungünstigen Radikalisierungsverlauf waren: männliches Geschlecht, verheiratet, verheiratete Eltern, von Geburt an Muslim zu sein (im Gegensatz zu Konvertiten), Tod eines Verwandten vor der Radikalisierung, eigene Radikalisierungsversuche bei Verwandten sowie die Inhaftierung eines Freundes oder Verwandten vor der Radikalisierung.[44] Ebenfalls aus Frankreich stammt eine Untersuchung zu 88 zwischen 2015 und 2018 von Islamisten begangenen Gewaltdelikten.[45] An den Delikten waren 163 Personen beteiligt, davon 14% Frauen. Die Autoren arbeiten als hauptsächlichen Antreiber für die Beteiligung an Gewalt in dieser Stichprobe die Wichtigkeit eines radikalen Netzwerks heraus, sowohl in Form einer extremistischen Gruppierung als auch über eine islamistische Sozialisation im Internet sowie, bei einem geringeren Teil der Islamisten, über Freunde, Bekannte und radikale Moscheen.[46]

In einer Studie zu Personen (davon ein Fünftel Frauen), die zwischen 2012 und 2015 aus Belgien und den Niederlanden in den Irak oder nach Syrien ausgereist sind, wurde die zentrale Bedeutung der direkten Bekanntschaft, Freundschaft oder Verwandtschaft mit Gleichgesinnten als Motivator für die Ausreise aufgezeigt.[47] Ähnliches wird für die Gesamtheit der 784 aus Deutschland nach Syrien oder den Irak ausgereisten Personen berichtet (davon ebenfalls ein Fünftel Frauen), die sich dort dem bewaffneten Kampf des IS angeschlossen haben:[48] Die Hälfte der Personen, zu denen entsprechende Angaben vorlagen, hatte vor ihrer Ausreise Moscheen besucht, die eine extremistische Interpretation des Islam vertraten. Hauptsächlicher Treiber der Ausreise waren neben Kontakten im Internet vor allem die persönlichen Kontakte zu Gleichgesinnten.[49]

Zusammengenommen entspricht das einem Muster, dass Menschen eher für ihre Gruppe oder für ihre Mitstreiter kämpfen als für eine bestimmte Ideologie,[50] was im Übrigen auch für US-amerikanische Soldaten im zweiten Weltkrieg festgestellt werden konnte.[51]

---

44 Campelo et al., 5.
45 Crettiez/Barros, 1 ff.
46 Crettiez/Barros, 16 ff.
47 Bakker/De Bont, 844 ff.
48 BKA, BfV, & HKE, 1 ff.
49 BKA, BfV, & HKE, 20.
50 Crenshaw, Explaining Terrorism, 73; Atran, Enemy, 328.
51 Stouffer et al., The American soldier II, 105 ff.

Der Faktor Ideologie muss also mit weiteren Faktoren kombiniert werden, die die Wahrscheinlichkeit für gewalttätiges Handeln erhöhen, um die Eskalation einer Entwicklung hin zum Ausüben von extremistischer Gewalt erklärbar zu machen. Eine sehr wichtige Rolle kommt dabei der Beeinflussung im sozialen Umfeld zu.[52] Ideologien sind beispielsweise geeignet, andere aus der entsprechenden sozialen Gruppe zu ermutigen, den Tätern von Gewalt lobenswerte Eigenschaften wie Pflichtgefühl, Härte, Mut usw. zuzusprechen.[53] Diese Zuschreibungen qualifizieren als Anreize.[54]

Typologien als idealtypische Beschreibungen haben sich in der forensischen Psychologie und Psychiatrie als hilfreich erwiesen, um verschiedene Fallkonstellationen abzubilden, die zugleich Ansatzpunkte für Interventionen bieten. Unterschiedliche Typologien, die den Kern der jeweils zugrundeliegenden Deliktdynamik beschreiben, wurden auch für unterschiedliche Fallkonstellationen bei Tätern extremistischer Gewaltdelikte entwickelt.[55] Beispielsweise haben Endrass et al. drei Prototypen von Tätern extremistischer Gewalt vorgeschlagen:[56] Beim ersten Typ ist die Gewaltbereitschaft primär durch eine Realitätsverkennung aufgrund einer schweren unbehandelten psychiatrischen Erkrankung z.B. aus dem schizophrenen Formenkreis getrieben. Beim zweiten Typ liegen die primären Treiber für die Gewaltbereitschaft in einer impulsiven, aggressiven und normablehnenden Persönlichkeit; diese Gewaltbereitschaft manifestiert sich in verschiedenen Lebensbereichen und kann sich *auch* im Rahmen einer extremistischen Ideologie zum Überschreiten der Handlungsschwelle entwickeln. Beim dritten Typ hingegen ist die Gewaltbereitschaft stark kontextabhängig: Dieser beschreibt einen zunächst sozial angepassten Menschen, der erst durch einen Prozess der zunehmenden Legitimierung von Gewaltanwendung die Bereitschaft entwickelt, Normen zu verletzen und letztlich selbst Gewalt anzuwenden. Endrass und weitere Autoren illustrieren diesen Prozess am Beispiel der Entwicklung vom Muslim zum Islamisten.[57] Die Legitimierungsarbeit kann parallel zu einem Sozialisationsprozess hin zu einer

---

52 Sageman, Misunderstanding, 96 f.

53 Leader Maynard, 832.

54 Khalil/Horgan/Zeuthen, Clarifications, 6.

55 Atran, Enemy, 106; Sageman, Political Violence, 38; Endrass et al., 330 ; Endrass/Rossegger, Herausforderungen, 38.

56 Endrass et al., 328 ff.

57 Endrass et al., 333.

bestimmten (gewaltorientierten) Ideologie stattfinden oder durch diesen Prozess vorangetrieben werden, ist aber als grundsätzlich eigenständiger kognitiver Prozess konzipiert.[58]

Zusammengefasst ist der Prozess hin zum gewalttätigen Extremismus am ehesten als ein Zusammenspiel von persönlichen und umweltbedingten Faktoren zu verstehen, die sich ständig ändern. Es gibt Persönlichkeitsausprägungen, die erfahrungsgemäss gehäuft bei Tätern extremistischer Gewalt beobachtet worden sind, z.B. Feindseligkeit, mangelnde Empathie[59] oder psychiatrische Symptome wie ein Verfolgungswahn.[60] Andererseits können auch situative Umstände wie ökonomische Prekarität,[61] politische Frustration,[62] soziale Marginalisation oder schlicht eine akut krisenhaften Lebenssituation einen starken Druck auf Menschen ausüben, sich in einer bestimmten Weise zu verhalten. Kausal erklärbar ist die Anwendung von Gewalt vor dem Hintergrund einer islamistischen Ideologie also weder durch die Ideologie an sich noch durch andere, in der Person oder in ihrem Umfeld zu verortende einzelne Faktoren.[63]

III. Spezifische Radikalisierungsmodelle

Die Wissenschaft hat eine Vielzahl von Modellen entwickelt, um die Entwicklung von Menschen in den gewalttätigen Extremismus zu interpretieren. Der Zweck dieses Abschnitts besteht darin, einige der bekanntesten Beispiele, die auch im Bereich des Islamismus Beachtung gefunden haben, kurz zu präsentieren und kritisch zu reflektieren. Einschränkend voranzustellen ist der Hinweis, dass es sich bei allen vorgestellten Modellen um Theorien handelt, die idealtypisch zu erklären versuchen, wie sich anfangs „normale", unauffällige und gut integrierte Individuen dahingehend entwickeln können, dass sie zu Gewalt greifen, um extremistische Überzeugungen zu vertreten.[64]

---

58 Endrass et al., 331 f.

59 Pressman, 1 ff.

60 Endrass/Rossegger

61 Piazza, 350; Goodwin, 2035.

62 Humphreys/Weinstein, 440.

63 Cretiez/Duclos, 50; Khalil/Horgan/Zeuthen, Clarifications, 4; Sageman, Misunderstanding, 105.

64 McGilloway/Ghosh/Kamaldeep, 39.

1. Social Identity Perspective

Das soziologische Modell der Social Identity Perspective (SIP) besagt in seiner Quintessenz, dass sich die meisten Menschen nicht aus persönlichen Motiven an gewalttätigem Extremismus beteiligen, sondern aus Gruppenmotiven. Von zentraler Bedeutung sind dabei die sozialen Netzwerke und Bezugsgruppen, mit denen die Person verbunden ist. Nach diesem Modell ist Radikalisierung ohne Identifizierungsprozess mit einer Gruppe nicht möglich.[65] Bekanntester Exponent der SIP im Zusammenhang mit Radikalisierung ist der Terrorismusexperte, Psychiater und ehemalige CIA-Mitarbeiter Marc Sageman.

Die SIP geht auf Henri Tajfel zurück, einen polnischen Juden, der nach Frankreich ausgewandert war und sich der französischen Armee angeschlossen hatte um gegen die Nationalsozialisten zu kämpfen. Er wurde gefangen genommen und überlebte eine Reihe von Kriegsgefangenenlagern in Deutschland. Nach seiner Befreiung hat er sein Leben der Erforschung der Ursachen des Holocausts gewidmet.[66]

Tajfels Minimalgruppenexperimente zeigen, dass Menschen sich selbst verschiedenen Gruppen zuteilen. Dieser einfache Prozess der Kategorisierung fördert Vorurteile und Voreingenommenheit gegenüber anderen Gruppen. Menschen neigen dazu, bei der Wahl ihrer Freunde, Geschäftspartner und anderer Personen, mit denen sie interagieren und sich austauschen, Mitglieder ihrer eigenen Gruppe gegenüber Aussenstehenden zu bevorzugen. Diese Kategorisierung und Identifikation mit anschliessender Differenzierung zwischen „In-Group-" und „Out-Group-Personen" sind gemäss SIP der Schlüssel zum Verständnis von kollektivem Verhalten, einschliesslich sozialer Bewegungen und Terrorismus.[67] Kategorisierung ist ein schneller, natürlicher, assoziativer, emotionaler, müheloser und automatischer Prozess der Vereinfachung unserer Umwelt, um ihr einen Sinn zu geben. Kategorien werden auf der Grundlage gemeinsamer wahrgenommener Merkmale gebildet.[68] Es handelt sich dabei um einen Teil dessen, was vom Psychologen Daniel Kahneman „System 1" genannt wird.[69]

---

65 Van Stekelenburg, 1 ff.

66 Sageman, Political Violence, 6.

67 Atran, Enemy, 295; Haslam/Reicher/Reynolds, 201 ff.; Hornsey, 204 ff.; van Stekelenburg, 1 ff.; Sageman, Political Violence, 6.

68 Sageman, Misunderstanding, 113.

69 Kahneman, 19 ff.

Eine offensichtliche und häufige Kategorisierung erfolgt via Religion und „sacred values" („heilige Werte").[70] Religion ist eine – aber bei weitem nicht die einzige – Form von „sacred values". Diese sind eine abstrakte Konzeptualisierung dessen, „wer ich bin" resp. „wer wir sind".[71] Menschen mit der gleichen Religionszugehörigkeit neigen dazu, ihre Gruppe zu bevorzugen und gegenüber den Angehörigen anderer Religionen voreingenommen zu sein.[72]

Konkret führt der Weg zur Radikalisierung gemäss SIP über zwei Schritte: Der erste Schritt in diesem Prozess besteht in der Aktivierung einer „politisierten sozialen Identität", durch die man Teil einer politischen Protestgemeinschaft wird. Angesichts eines eskalierenden Konflikts mit einer kontrastierenden Aussengruppe (häufig der Staat), der Desillusionierung über die vermeintliche Erfolglosigkeit von friedlichem Protest und der moralischen Empörung über die Aggression der Aussengruppe (i.d.R. der Staat) sehen sich einige Aktivisten in einem zweiten Schritt als Kämpfer, die ihre politische Gemeinschaft schützen. Diese zweite Selbstkategorisierung von der „politisierten sozialen Identität" in eine „martialische soziale Identität" veranlasst einige wenige, sich der Gewalt zuzuwenden, denn die martialische soziale Identität legitimiert die Anwendung von Gewalt zur Verteidigung der eigenen Gruppe.[73] Kumulative Voraussetzung für den Übergang von der ersten zur zweiten Selbstkategorisierung sind die Eskalation eines Konflikts, Desillusionierung und moralische Empörung.[74] Zum heutigen Zeitpunkt gibt es keine empirische Evidenz darüber, wie man die Individuen erkennen könnte, die die Grenze zur martialischen sozialen Identität passiert haben. Mögliche begünstigende Faktoren sind ein ausgeprägtes Ehrgefühl[75] und eine gesteigerte Empfindlichkeit gegenüber Geringschätzung durch andere für die eigene soziale Identität.[76]

---

70 Ysseldyk/Matheson/Anisman, 60 ff.; Atran, Enemy, 1 ff.; Graham/Haidt, 140.

71 Atran, Devoted Actor, 193.

72 Jackson/Hunsberger, 509 ff.; Irons, 1 ff.; Die Ergebnisse eines verhaltensökonomischen Experiments suggerieren, dass bei Muslimen dieser Effekt stärker ausgeprägt ist als bei chinesischen Buddhisten und Christen. Darüber hinaus haben die Forscher festgestellt, dass, je höher der Grad der Religiosität eines Gläubigen ist, desto höher auch das Ausmass ist, in dem er ein Mitglied der eigenen Gruppe in spieltheoretischen Versuchen favorisiert (Xia et al.).

73 Sageman, Misunderstanding, 117; Sageman, Political Violence, 17; Von Geheimdiensten wird der erste Schritt häufig als „Radikalisierung", der zweite als „Mobilisierung" bezeichnet (Sageman, Turn, 108).

74 Sageman, Political Violence, 29.

75 Nisbett/Cohen, 1 ff.

76 Sageman, Political Violence, 38.

Im weiteren Verlauf nach dem Übergang zur martialischen sozialen Identität isolieren sich die wenigen „auserwählten Kämpfer" wegen ihrer Gewaltbereitschaft allmählich von ihrer bisherigen Gruppe mit politisierter sozialer Identität, die nicht in einen Konflikt mit den Behörden geraten wollen und deshalb beginnen, die gewaltbereiten Aktivisten zu meiden. Die „Kämpfer" ihrerseits betrachten ihre ehemaligen Mitstreiter zunehmend als Feiglinge, verlieren das Vertrauen in sie und halten sich von ihnen fern. Die selbsternannten Kämpfer fangen an, sich als etwas Besonderes zu fühlen. Sie glauben, dass sie sich vom Rest ihrer Gruppe unterscheiden und auf ihrem neuen Weg Geschichte schreiben. Sie entwickeln einen starken „Esprit de Corps". Je grösser die persönliche Aufopferung, desto grösser ist ihr Selbstwertgefühl und desto enger fühlen sie sich miteinander verbunden. Sie verbringen schliesslich ihre gesamte Zeit miteinander. Ihr Feindbild erweitert sich allmählich vom Staat auf ehemalige Mitstreiter, die Gewalt ablehnen, und umfasst schliesslich die gesamte Bevölkerung wegen ihrer Unterstützung des Staates. Um einer Verhaftung zu entgehen, gehen diese selbsternannten Soldaten in den Untergrund. Durch ihre soziale Isolation sind sie viel weniger unterschiedlichen Ereignissen, Ideen, Gefühlen, Perspektiven und Interpretationen der Welt, die sie nur noch in ihrer klandestinen Kleingruppe teilen, ausgesetzt.[77] Ohne den Kontakt mit einer breiteren Palette von Ideen erleben sie eine Verengung ihres kognitiven Horizonts.[78] In ihrer Isolation werden sie zunehmend selbstreferenziell und entwickeln teilweise eine Privatsprache, die für Aussenstehende, auch ehemalige Mitstreiter, bald unverständlich wird. Die gewaltbereiten „Kämpfer" beginnen sich einzureden, dass Gewalt Reformen bewirken könne und häufiger sei, als sie tatsächlich ist. Dies führt dazu, dass sie glauben, kurz vor dem Erreichen der Ziele zu stehen. Ihr Verhalten wird obsessiv, denn mehrfache Fehlschläge, Verhaftungen und zum Teil auch Todesfälle halten sie nicht mehr davon ab, bis zum bitteren Ende weiterzumachen. Es ist, als ob das gewalttätige Ziel die Kontrolle über das Leben, die Gedanken, die Bemühungen und die Emotionen dieser Personen übernimmt. Der Begriff der Besessenheit resp. Obsession steht im Einklang mit Erkenntnissen der Sozialpsychologie. Ein bestimmtes Ziel vor Augen zu haben, lenkt die Aufmerksamkeit selektiv auf relevante Hinweise auf dieses Ziel und filtert irrelevante heraus. Dieses Phänomen wird „Aufmerksamkeitsblindheit" („attentional blindness") genannt.[79]

---

77 Sageman, Political Violence, 41 f.

78 Della Porta, 252 ff.

79 Bargh/Gollwitzer/Oettingen, 288 f.; Sageman, Misunderstanding, 159 f.

Gemäss SIP ist der Übergang zur politischen Gewaltbereitschaft kein vernunftgesteuerter Prozess und kann daher nicht mit der rational choice theory (RCT)[80] erklärt werden.[81] Die Gewaltbereitschaft von Extremisten sei meist durch die moralische Verpflichtung gegenüber kollektiven Interessen bedingt. Ziel sei die physische Verteidigung der „sacred values" einer Sache – in der SIP-Logik letztendlich einer Gruppe – allen Widrigkeiten zum Trotz. Diese Werte übertrumpfen oft marktwirtschaftliches Denken und realpolitische Erwägungen. Bei einer rationalen Entscheidung geht es darum, die besten Mittel zu ergreifen, um bestimmte Ziele in der Zukunft zu erreichen. Je weiter in der Zukunft ein Ziel liegt, desto geringer ist sein tatsächlicher Wert im Hier und Jetzt und desto weniger engagiert ist eine Person, die Mittel zur Verwirklichung dieses Ziels einzusetzen. Bei „sacred values" gelten diese Zusammenhänge jedoch nicht: Gestützt auf „sacred values" werden sich gewisse Personen im Hier und Jetzt auf eine Weise verhalten, die einem fernen, möglicherweise postumen Ziel dienen. Diese Handlungen stehen gemäss SIP in keinem rational begründbaren Verhältnis zur kurzfristigen individuellen Gratifikation, die möglicherweise daraus erwächst.[82] Die Extremposition dieser Logik stellten Selbstmordattentäter dar. Sie opferten ihr wertvollstes Gut für die Gruppe, was nicht als nüchtern-rationaler Vorgang gewertet werden könne und daher gegen die RCT spreche.

Die Grenze von der politisierten zur martialischen sozialen Identität ist fluid und durchlässig, sie kann je nach Kontext mehrmals in beide Richtungen passiert werden. Nach Ansicht von Vertretern der SIP folgt als Implikation aus der Theorie, dass der Staat insbesondere darauf achten sollte, dass er nicht Indikatoren für den Übergang von normaler sozialer Identität zu politisierter sozialer Identität (erste Selbstkategorisierung) mit dem Schritt von politisierter sozialer Identität zur martialischen sozialen Identität (zweite Selbstkategorisierung) verwechselt und überreagiert. Denn in einem Prozess der sich selbst erfüllenden Prophezeiung können übertrieben repressive Massnahmen durch den Staat erst dazu führen, dass Personen ihre soziale Identität letztlich durch gewalttätiges Handeln ausleben. Sympathisierende innerhalb der

---

80 Für einen Überblick der Entwicklung der RCT s. GREEN, 2002, 1 ff.; siehe unten, IV.1.

81 SAGEMAN, Political Violence, 384.

82 ATRAN, Enemy, 344 f.; Gemäss Darwin bringen „sacred values" zugunsten einer Gruppe selektive Vorteile: „(...) obwohl ein hoher moralischer Anspruch jedem einzelnen Mann und seinen Kindern nur einen geringen oder gar keinen Vorteil gegenüber den anderen Männern desselben Stammes verschafft, wird eine Zunahme der Zahl entschlossener Männer und eine Verbesserung der Moral sicherlich einen immensen Vorteil für einen Stamm gegenüber einem anderen bringen" (DARWIN, 166).

Peer-Gruppe können sich zudem durch derartiges Handeln von vermeintlichen „Märtyrern“ in ihrer sozialen bzw. politischen Identität bestärkt sehen.[83] Die Empfehlung der SIP-Experten lautet, in Verdachtsfällen die Betroffenen zurückhaltend zu beobachten und keinesfalls zum Agent Provocateur zu werden.

2. Attitudes-Behavioral Corrective Model

Auch das Attitudes-Behavioral Corrective (ABC)-Modell basiert auf der klaren Trennung von Sympathie einer Person für terroristische Handlungen und Bereitschaft, tatsächlich an solchen teilzunehmen. Diese Trennung von Sympathisierenden und Handelnden teilt das ABC-Modell mit der SIP und dem Zweipyramiden-Modell[84]. Prominentester Vertreter des ABC-Modells ist James Khalil.

Das ABC-Modell besagt, dass viele der Personen, die im Kontext einer Ideologie Gewalt anwenden, tatsächlich gleichgültig gegenüber der entsprechenden Ideologie und ihren angeblichen Zielen seien. Stattdessen handelten sie hauptsächlich zum Beispiel aus materiellen Interessen, einem Zugehörigkeitsgefühl, Abenteuerlust oder Statusgründen.[85] Das ABC-Modell ist explizit dynamisch und nimmt an, dass Individuen ihre Einstellungen und Verhaltensweisen im Laufe der Zeit ändern. So kann eine Person im zeitlichen Verlauf beispielsweise in Bezug auf ihre Haltung zunehmend Abstand nehmen von gewaltbefürwortender Einstellung („Deradikalisierung“), aber dennoch in Bezug auf ihr Verhalten gewaltbereiter werden („Engagement“). Eine solche Entwicklung ist beispielsweise gegeben, wenn eine zunächst von der radikalen Ideologie begeisterte Person aufgrund beobachteten unmoralischen Handelns von Gruppenführern zunehmend desillusioniert ist, gleichzeitig aber das Zugehörigkeitsgefühl oder der Gruppendruck innerhalb der extremistischen Kleingruppe zunimmt.[86]

Das ABC-Modell berücksichtigt auch, dass der Prozess der Beteiligung an gewaltbereitem Extremismus sowohl „bottom-up“ als auch „top-down“ sein kann. Mit anderen Worten, es wird anerkannt, dass Interessierte oft aktiv

---

83 Sageman, Political Violence, 39.

84 McCauley/Moskalenko, Them and us, 205 ff.; siehe unten, III.3.

85 Khalil, 198 ff.

86 Khalil/Horgan/Zeuthen, ABC, 6.

nach Möglichkeiten suchen, sich gewaltbereiten extremistischen Organisationen anzuschliessen, dass diese Organisationen aber auch selbst häufig proaktiv bei der Identifizierung und Anwerbung neuer Mitglieder tätig werden.[87]

Auf dem Weg zum einstellungs- und/oder verhaltensbezogenen Extremismus existieren gemäss ABC-Modell verschiedene Motivatoren:[88]

- *Strukturelle Motivatoren*, die lokal relevant sein können, sind beispielsweise staatliche Repression, politische Ausgrenzung, Korruption, Armut, Ungleichheit und Diskriminierung. Sie können den Weg zum Extremismus bestenfalls indirekt erklären. Basierend auf der Rational-Choice-Theorie (RCT) entscheiden sich in den allermeisten Fällen selbst diejenigen, die mit dieser Gewalt sympathisieren, dafür, nur „Trittbrettfahrer" zu sein. Denn sie sind sich bewusst, dass ihre Beteiligung höchstens marginal zu den angeblichen Zielen der Gewalt beitragen würde, gleichzeitig aber hohe individuelle Risiken wie Inhaftierung, Verletzung und sogar Tod in sich birgt.[89] Strukturelle Motivatoren beeinflussen vor allem die Haltungen (attitudes).
- *Individuelle Anreize* bestehen beispielsweise in materiellen Anreizen (Gehälter usw.), Schutz, Status, Abenteuerlust, Zugehörigkeit, Rache, erwarteten Belohnungen im Jenseits und ein Sinngefühl, das durch Handeln in Übereinstimmung mit wahrgenommenen ideologischen Grundsätzen gewonnen wird. Individuelle Anreize beeinflussen v.a. das Verhalten (behavior).
- *Ermöglichende resp. fördernde Faktoren* verhelfen Bewegungen zu grösserer Radikalität, erleichtern oder kanalisieren sie, anstatt sie per se zu motivieren. Dazu gehören zum Beispiel „radikale" Mentoren, Anwerber, breitere soziale Netzwerke und Online-Communities, andere Formen traditioneller und moderner Medien oder der Zugang zu Waffen und anderen Technologien.

Ein Vorteil des ABC-Modells besteht darin, dass damit die häufig dynamischen Zustände der Individuen in Bezug auf ihre Einstellungen (attitudes: Radikalisierung oder Deradikalisierung) und Verhaltensweisen (behavior: Engagement

---

87 Khalil/Horgan/Zeuthen, ABC, 7.

88 Khalil/Horgan/Zeuthen, ABC, 9; Dabei gilt das Prinzip der sog. „Equifinalität", wonach ein bestimmter Endzustand (in diesem Fall sowohl die Sympathie für „gerechtfertigte Gewalt" als auch ihre Beteiligung daran) von verschiedenen Faktoren oder Kombinationen von Faktoren bestimmt werden kann (Reidy, 1 ff.).

89 Levi 19 ff.; Moore 417 ff.

oder Disengagement) im zeitlichen Verlauf grafisch nachgezeichnet werden können.[90] Aus Forschungsperspektive bietet dies eine Möglichkeit, um die Lebensgeschichten bestimmter Personen besser zu verstehen.[91]

Kritisiert wird, dass nicht klar sei, wie die Einstellungs- und Verhaltensdimensionen im ABC-Modell gemessen und die exakte Position darin benannt werden sollen oder wie die drei Arten von Motivatoren (strukturelle Motivatoren, individuelle Anreize, fördernde Faktoren) Personen erfassen können, die das Wohl ihrer Gruppe über ihr eigenes Wohl stellen.[92]

3. Two Pyramids Model

Ebenso wie die SIP (siehe oben, III.1.) basiert das Zweipyramiden-Modell auf soziologischen Faktoren mit besonderem Fokus auf Gruppenvariablen. So sind gemäss diesem Modell Bezahlung, Beförderung, Medaillen, Anerkennung etc. als Motivatoren viel weniger wichtig als „meine Kumpels nicht im Stich zu lassen".[93]

Entwickelt worden ist das Zweipyramiden-Modell von Clark McCauley und Sophia Moskalenko.[94] McCauley und Moskalenko definieren Radikalisierung als Veränderungen in Überzeugungen, Gefühlen und Handlungen in Richtung einer verstärkten Unterstützung für eine Seite eines politischen Konflikts.[95] Wie die SIP und das ABC-Modell unterscheidet auch das Zweipyramiden-Modell Radikalisierung der Meinungen (Überzeugungen und Gefühle) von Radikalisierung des Verhaltens, indem es eine „Opinion Radicalization Pyramid" (ORP) und eine „Action Radicalization Pyramid" (ARP) vorschlägt. Die Stufen der ORP von unten nach oben lauten „Neutral", „Sympathizers", „Justifyers" und „Personal Moral Obligation", diejenigen der ARP „Inert", „Activists", „Radicals" und „Terrorists". In der ARP werden auf dem Weg zur Spitze der Pyramide, also zum gewalttätigen Extremismus, zwölf Mechanismen der Radikalisierung unterschieden (z.B. Rache für eine erlebte Ungerechtigkeit oder

---

90 Allerdings ist es im ABC-Modell, das mit Grafiken arbeitet, schwierig, den aktuellen Zustand klar in Worten zu definieren, so wie dies beim Zweipyramiden-Modell mit der Bezeichnung der jeweiligen Schicht innerhalb einer Pyramide möglich ist.

91 Khalil/Horgan/Zeuthen, ABC, 17.

92 McCauley, 457.

93 McCauley/Moskalenko, Profile, 73; Stouffer et al., The American soldier I, 1ff.

94 McCauley/Moskalenko, How radicalization happens, 1 ff.; McCauley/Moskalenko, Profile, 69 ff.; McCauley/Moskalenko, Two-Pyramids, 205 ff.; Leuprecht et al., 42 ff.

95 McCauley/Moskalenko, How radicalization happens, 1 ff.; McCauley/Moskalenko, Profile, 70.

„sensation seeking", dem Bedürfnis nach neuen und abwechslungsreichen Erlebnissen unter Inkaufnahme von Risiken).[96] Mindestens drei dieser zwölf Mechanismen setzen keine Radikalisierung der Einstellung (also keinen Anstieg innerhalb der ORP) voraus. Auch dürfen die Pyramiden nicht als Stufenmodell verstanden werden, wonach ein Individuum linear jede Ebene durchschreiten muss, um – im Fall der ARP – in der letzten Stufe ein Terrorist zu werden.[97]

Für den ursächlichen Übergang von radikaler Meinung zu radikalem Handeln spielt gemäss Zweipyramiden-Modell die konkrete Ideologie nur eine untergeordnete Rolle.[98] Viel entscheidender seien praktische, situative Ereignisse. Als Hochrisiko-Konstellation wird das Zusammentreffen von radikaler Einstellung und entsprechender situativer Gelegenheit erachtet.[99]

Beim Zweipyramiden-Modell wird kritisiert, dass es im Gegensatz zum ABC-Modell den zeitlichen Verlauf der (De)Radikalisierungstendenzen einzelner Individuen nicht aufzuzeigen vermag und den Einfluss der Ideologie zu stark negiert.[100]

4. Four Stage Model

Das vierstufige Konzeptmodell für die Entstehung einer „terroristischen Denkweise" wurde unter Federführung des FBI im Nachgang zu den Anschlägen vom 11. September 2001 entwickelt. Grundlage bildeten anekdotische und unsystematische Analysen mehrerer gewaltbereiter extremistischer Gruppen mit einer Spanne unterschiedlicher Ideologien, um herauszufinden, ob es unter ihnen einige gemeinsame Faktoren in Radikalisierungsprozessen geben könnte. Das konzeptionelle Modell versucht zu erklären, wie sich Missstände und Vulnerabilitäten in Hass auf eine Zielgruppe verwandeln und wie sich Hass – für einige – in eine Rechtfertigung oder einen Anstoss für Gewalt verwandelt. Grundsätzlich beginnt der vierstufige Prozess damit, ein unbefriedigendes Ereignis, einen Zustand oder eine Beschwerde („It's not right") als ungerecht („It's not fair") einzustufen. Die Ungerechtigkeit wird einer Zielpolitik, -person oder -nation angelastet („It's your fault"). Die verantwortliche Partei wird dann diffamiert – oft dämonisiert – („You're evil"), was die Rechtfertigung oder den

96 Crettiez/Duclos, 70; McCauley/Moskalenko, Profile, 70; McCauley/Moskalenko, How radicalization happens, 1 ff.

97 McCauley/Moskalenko, Profile, 73.

98 Crettiez/Duclos, 70; McCauley, 453.

99 McCauley/Moskalenko, Profile, 83.

100 Khalil/Horgan/Zeuthen, Clarifications, 1 ff.

Anstoss für Aggression erleichtert. Das Modell wurde ursprünglich von Randy Borum als Trainingsheuristik für die Strafverfolgung entwickelt, nicht als formale sozialwissenschaftliche Theorie.[101]

Am Vierstufen-Modell wird kritisiert, dass es die Rolle der Ideologie vernachlässigt. Zweitens macht das Modell nicht hinreichend deutlich, dass der Verlauf zur Gewalt nicht linear verläuft und umgekehrt werden kann. Drittens berücksichtigt es nicht deutlich die Unterscheidung zwischen Einstellungen und Verhaltensweisen, die ein zentrales Element der SIP, des ABC-Modells und des Zweipyramiden-Modells ist. Daher bleiben Schlüsselfragen bezüglich des entscheidenden Schritts von der Rechtfertigung von oder dem Sympathisieren mit Gewalt bis zur tatsächlichen Beteiligung an solchen Taten unbeantwortet, was unbefriedigend ist angesichts der weit höheren Anzahl an Sympathisierenden einer extremistischen Idee im Vergleich zu Personen, die Gewalt anwenden.[102]

5. Staircase Model

Im Treppenmodell wird der extremistisch motivierte Gewaltakt als letzter Schritt auf einer sich nach oben verengenden Treppe konzipiert. Entwickelt wurde das Treppenmodell von Fathali Moghaddam.[103]

Im „Erdgeschoss" dominieren Gerechtigkeitswahrnehmungen und Gefühle relativer Entbehrung. Obwohl die überwiegende Mehrheit der Menschen, selbst wenn sie sich benachteiligt und ungerecht behandelt fühlen, im „Erdgeschoss" bleiben, klettern einige Personen nach oben: Im „ersten Stock" suchen sie nach Wegen, ihre Situation zu verbessern und mehr Gerechtigkeit zu erreichen. Gelingt dies nicht, steigen sie in den „zweiten Stock", wo das Erleben von Wut und Frustration im Vordergrund stehen. Insbesondere durch Führungspersonen extremistischer Organisationen können sie dazu gebracht werden, ihre Frustration aggressiv auf eine „Out-Group" zu verlagern. Im „dritten Stock" führt gemäss Treppenmodell die Indoktrination zu einer Wahrnehmung der extremistischen Organisation als legitim. Im „vierten Stock" wird die eigentliche Rekrutierung für extremistische Gewaltakte im Sinn der Organisation verortet, einhergehend mit einem starken „wir-gegen-sie"-Denken. Im „fünften Stock" schliesslich werden die Gewaltakte umgesetzt.[104]

---

101 Borum, Extremism II, 38 ff.; Borum, Understanding, 7 ff.

102 Khalil/Horgan/Zeuthen, ABC, 3 f.

103 Moghaddam, 161 ff.

104 Moghaddam, 162.

In der entsprechenden Metapher führt die Treppe zu immer höheren Etagen, und ob jemand auf einer bestimmten Etage bleibt, hängt von den Türen und Räumen ab, die sich diese Person auf dieser Etage für sich als offen vorstellt. Das grundlegend wichtige Merkmal der Situation ist nicht nur die tatsächliche Anzahl der Stockwerke, Treppen, Räume, sondern die entsprechende Wahrnehmung durch die Betroffenen. Wenn Individuen die Treppe hinaufsteigen, sehen sie immer weniger Handlungsalternativen, bis das einzig mögliche Ergebnis ein destruktiver Akt bleibt.[105]

Realistisch erscheint beim Treppenmodell die Vorstellung der Selbstkategorisierung und Trennung von „In-Group-" und „Out-Group-Personen". Dieselbe Kritik wie beim Vierstufen-Modell, insbesondere bezüglich des Postulats der Linearität und einer ungenügenden Trennung von Haltungen und Handlungen, gilt jedoch auch für das Treppenmodell von MOGHADDAM. Eine weitere Kritik betrifft die Vorstellung des Treppenmodells, dass auf dem Weg zum Terrorismus umfassende Indoktrinationsprozesse und eine eigentliche Gehirnwäsche stattfänden. Wie im vorigen Abschnitt erwähnt, geht man in der herrschenden Lehre davon aus, dass es sich bei Personen, die ein extremistisches Gewaltdelikt begehen, keinesfalls um reduziert urteilsfähige oder sogar willenslose Tatinstrumente handelt – so wie dies eine Indoktrination impliziert.[106] Kritisiert wird schliesslich beim Treppenmodell, analog zum Vierstufen-Modell, das Ignorieren der regelhaft beobachteten Gleichgültigkeit oder sogar Ablehnung der Ideologie durch Personen, die im Kontext ebendieser Ideologie Gewaltdelikte begehen. Die Modelle blenden also Personen aus, die hauptsächlich durch wirtschaftliche Anreize, Status, Zugehörigkeit, Abenteuer, Angst usw. zu gewalttätigem Handeln motiviert sind.[107]

6. Significance Quest Model

Gemäss dem Significance Quest Model sind das Streben nach Anerkennung und die Konstruktion von Sinn im eigenen Leben die Hauptmotivationen für radikales Engagement. Wenn bestimmte Menschen unter einem subjektiven Bedeutungsverlust leiden, klammern sie sich an Überzeugungen, die diesen Verlust erklären und Lösungswege aufzeigen. Das Festhalten an einem be-

105 MOGHADDAM, 161.

106 INTROVIGNE, 1 ff.; NURANIYAH, 890; BLOOM, 1 ff.; GAMBETTA, 1 ff.; HAFEZ, 1 ff.; MERARI, 1 ff.; PAPE, 1 ff.; PEDAHZUR, 1 ff.

107 KHALIL/HORGAN/ZEUTHEN, ABC, 4.

stimmten Kreis von Gleichaltrigen soll den Übergang zu gewalttätigen Aktionen fördern.[108] Das Significance Quest Model wurde von Arie Kruglanski et al. entwickelt.[109]

Radikalisierung wird in diesem Modell definiert als Unterstützung von oder Teilnahme an Aktivitäten, die (von anderen) als Verletzung wichtiger sozialer Normen angesehen werden (z.B. die Tötung von Zivilistinnen und Zivilisten). In dieser Hinsicht ist Radikalisierung eine Frage des Grades, wobei die blosse Unterstützung der Haltung gegenüber Gewalt einen geringeren Grad der Radikalisierung widerspiegelt als die tatsächliche Ausübung von Gewalt. Das Significance-Quest-Model enthält drei entscheidende Komponenten: (1) die motivationale Komponente (das Streben nach persönlicher Bedeutung), die ein Ziel definiert, für das man sich engagiert, (2) die ideologische Komponente, die zusätzlich die Mittel der Gewalt als angemessen bezeichnet für die Verfolgung dieses Ziels, und (3) der soziale Prozess der Vernetzung und Gruppendynamik, durch den das Individuum an der gewaltbegründenden Ideologie teilnimmt und sie als Mittel des Bedeutungsgewinns durchsetzt.[110]

Dieses Modell anerkennt korrekterweise das Gewicht der Selbstkategorisierung und Gruppenzugehörigkeit sowie der „sacred values". Die Demütigung der eigenen Gruppe und das „Niedertrampeln" ihrer „sacred values"[111] kann zu einem erheblichen subjektiven Bedeutungsverlust führen, der von allen Mitgliedern der Gruppe (z.B. Musliminnen und Muslimen) als solcher empfunden wird.[112] Die Selbstkategorisierung und die identitäre Verschmelzung mit der Gruppe[113] erhöht die Bereitschaft des einzelnen Mitglieds, im Namen der Gruppe und zur Verteidigung ihrer „sacred values" Selbstaufopferungen auf sich zu nehmen.[114]

Eine Schwäche des Modells ist, dass es nicht klar zwischen Haltungen und Handlungen unterscheidet resp. ein extremistisch motivierter Gewaltakt als lediglich stärkere Ausprägung auf einem linearen Kontinuum definiert. Dabei wird missachtet, dass die Beteiligung an gewalttätigem Extremismus auch bei Personen möglich ist, die die entsprechende Haltung oder Ideologie nicht teilen.

---

108 Crettiez/Duclos, 70.

109 Kruglanski/Bélanger/Gunaratna, 93 ff.; Kruglanski et al., 69 ff.

110 Kruglanski et al., 69.

111 Atran, Enemy, 1 ff.

112 Kruglanski et al., 75.

113 Swann et al., Identity Fusion, 995 ff.

114 Kruglanski/Bélanger/Gunaratna, 93; Atran/Sheikh/Gomez, 17702 f.

IV. Präzisierungen

1. Radikalisierungsmodelle und Rational Choice Theory: Ein Widerspruch?

Die letztlich mit dem Endpunkt der Radikalisierung verbundene Selbstaufopferung für eine bestimmte Ideologie wie z.B. Islamismus erscheint zunächst nicht mit einem vernunftbezogenen Handeln in Einklang zu bringen, wie dies von der Rational Choice Theory (RCT) postuliert wird. Die RCT erklärt soziale Phänomene als Ergebnisse individueller Entscheidungen, die grundsätzlich als rational ausgelegt werden können. Während die RCT den theoretischen Kern der Wirtschaftswissenschaften darstellt, stösst sie in den Sozial- und Verhaltenswissenschaften auf erhebliche Kritik.[115] Zu den kritischen Stimmen gehören auch die Vertreterinnen und Vertreter der SIP und des Zweipyramiden-Modells (siehe oben, III.1 und 3.). So ist der franco-amerikanische Anthropologe Scott Atran der Meinung, dass extremistisch motivierte Gewalt häufig von „ergebenen Akteuren" („devoted actors") ausgeübt wird, die sich an „sacred values" (siehe III.1 und III.6) orientieren und Taten begehen, die sich von rational zu erwartendem Verhalten unterscheiden.[116] Diese „sacred values" widerstehen materiellen Versuchungen.[117] Das Prinzip des „devoted actors" lautet: „Die Menschen sind bereit, moralisch wichtige Werte oder ‚sacred values' durch kostspielige Opfer und extreme Aktionen zu schützen und sogar zu töten und zu sterben, insbesondere wenn solche Werte in die Gruppenidentität eingebettet (...) sind".[118] Wenn also „sacred values" und ein bestimmter Grad von Identitätsfusion („identity fusion")[119] zusammenwirken, entsteht beim betreffenden Individuum die Bereitschaft, der reinen Rationalität widersprechende, kostspielige Opfer, bisweilen das eigene Leben, für eine primäre Bezugsgruppe zu bringen.[120]

---

115 Wittek, 1; Herfeld, 329; Fumagalli, 63.

116 Atran, Devoted Actor, 192.

117 Tetlock, 320 ff.; Dehghani et al., 540 ff. ; Ginges et al., 507 ff.

118 Atran, Devoted Actor, 192.

119 Identitätsfusion – die der Selbstkategorisierung in der SIP (siehe oben, III.1.) stark ähnelt, aber nicht exakt entspricht (Atran, Devoted Actor, 197) – tritt auf, wenn persönliche und Gruppenidentitäten zu einer einzigen Identität zusammenfallen, um ein kollektives Gefühl der Unbesiegbarkeit und besonderen Bestimmung zu erzeugen (Swann et al., Group Membership, 141 ff.).

120 Sheikh/Gomez/Atran, 204 ff.

„Sacred values“ in Kombination mit Identitätsfusion sind beispielsweise in den palästinensischen Gebieten Westjordanland und Gaza beschrieben worden. Dort haben Scott Atran und Jeremy Ginges eine Befragung von über 700 Personen durchgeführt, die die Irrationalität bei Entscheidungen aufzeigt, sobald „sacred values“ mit starker Gruppenzugehörigkeit (Identitätsfusion) zusammenfallen.[121] Die zwei Fragen haben gelautet:

- „Was wäre, wenn jemand einen Bombenanschlag (Selbstmordattentat) gegen die Feinde Palästinas verüben wollte, aber sein Vater krank wird und seine Familie den auserwählten Märtyrer anfleht, sich um seinen Vater zu kümmern – wäre es akzeptabel, den Angriff auf unbestimmte Zeit zu verzögern?“ und
- „Was wäre, wenn eine Person einen Bombenanschlag (Selbstmordanschlag) gegen die Feinde Palästinas verüben wollte, aber seine Familie ihn bittet, das Martyrium auf unbestimmte Zeit hinauszuzögern, weil die Wahrscheinlichkeit, dass die Familie des auserwählten Märtyrers als Vergeltung getötet würde, sehr hoch wäre? Wäre es akzeptabel, den Angriff auf unbestimmte Zeit zu verzögern?“

Die Mehrheit der befragten Palästinenser haben entgegen der RCT irrational geantwortet, indem sie eine Verzögerung eines Selbstmordattentats zur Rettung einer ganzen Familie häufiger missbilligten als eine Verzögerung eines Attentats, um sich um einen kranken Vater zu kümmern.

Emotionen und rationales Denken sind keineswegs als Dichotomie aufzufassen.[122] Die Forschung zu den neurokognitiven Grundlagen des moralischen Denkens deutet auf eine enge Integration zwischen Kognition und Emotion hin, insbesondere wenn es um Handlungen geht. Gehirnregionen von Gefühlen und Gedanken sind eng miteinander verbunden und bei moralischen Entscheidungen zu stark verflochten, um sauber getrennt zu werden,[123] und der Begriff der „Rationalität“ ist elastisch genug, um auch psychosoziale resp. emotionale Anreize zu umfassen.[124]

Prosoziales Verhalten ist tief in unserem genetischen und kulturellen Erbe verwurzelt.[125] Die Identifikation mit einer Gruppe ist eine wichtige Quelle des individuellen Wohlbefindens. In einer wegweisenden Arbeit haben Akerlof

121 Ginges/Atran, 115 ff.
122 Stanley, 48.
123 Sageman, Misunderstanding, 145 f.
124 Khalil/Horgan/Zeuthen, ABC, 12;
125 Hetzer, 3.

und Kranton die Nutzenfunktion gemäss RCT erweitert und aufgezeigt, dass individuelle Entscheidungen nicht nur von idiosynkratischen Präferenzen, sondern auch von internalisierten sozialen Normen bestimmt werden. Internalisierung und Identifikation gemäss SIP sind der Prozess, durch den Menschen eine Reihe von Vorschriften lernen, denen sie ihr Verhalten anpassen können.[126] In diesem Sinn wird individueller Nutzen gewonnen, wenn Handlungen sozialen Normen entsprechen, und verloren, wenn dies nicht der Fall ist. So ist der mit Identität verbundene Nutzen die Freude, die ein Individuum gewinnt, wenn es etwas tut, das zum prototypischen Verhalten der Gruppe passt, der es angehört.[127] Selbst ein Selbstmordattentat kann als mit der RCT in Einklang stehend interpretiert werden: Die Attentäterin oder der Attentäter misst in diesem Fall den besonderen individuellen Anreizen (Sinnhaftigkeit, Rache, Status – häufig vor dem Ereignis, aber auch im Tod –, erwartete Belohnungen im Jenseits und so weiter) mehr Wert bei als dem eigenen Leben.[128] Obwohl die SIP eine Unvereinbarkeit von SIP und RCT proklamiert, hat selbst der bekannte Vertreter der SIP Marc Sageman erklärt: „The willingness to sacrifice oneself for a cause means that the cause is worth personal risks and *gives meaning to one's life*"[129], und auch Scott Atran – ebenfalls ein Vertreter der SIP – hat eingeräumt, dass die Tatsache, dass bestimmte Eliteeinheiten des US-Militärs wie auch die israelische Armee in Ausübung ihrer „heiligen Pflicht" das Leben vieler Soldaten riskiert haben, nur um einen einzelnen ihrer Soldaten zu retten, einen rationalen Sinn hat: Aufrichtige Bereitschaft zur Vergeltung um jeden Preis kann sich langfristig auszahlen, da so aggressive Aktionen stärkerer, aber weniger engagierter Feinde verhindert werden können. Ebenso kann die Bereitschaft, sich für Gleichgesinnte zu opfern, dazu beitragen, einen besseren „Esprit de Corps" zu schaffen, der seinerseits zu einer grösseren Kampfkraft führen kann.[130]

Damit erscheint, dass ein weitaus grösserer Nutzen daraus gezogen werden kann, die Perspektiven der SIP und der RCT nicht als konkurrenzierend zu betrachten, sondern vielmehr als komplementär.[131]

---

126 Akerlof/Kranton, 715 ff.

127 Kalin/Sambanis, 242.

128 Khalil/Horgan/Zeuthen, Clarifications, 3; Crenshaw, Suicide Terrorism, 153.

129 Sageman, Political Violence, 40 f.

130 Atran, Enemy, 245 f.

131 Khalil/Horgan/Zeuthen, Clarifications, 4.

2. Einordnung bestehender Radikalisierungsmodelle

Obwohl die verschiedenen Modelle eine gewisse Inhaltsvalidität aufweisen, um retrospektiv den Radikalisierungsprozess modellhaft darzustellen, mangelt es ihnen an spezifischen Merkmalen, die die Radikalisierung im Einzelfall erklären. So ist zwar bekannt, dass sich viele extremistisch motivierte Attentäter zum Zeitpunkt der Deliktbegehung in einer „Adoleszentenkrise" befunden haben. Dieses Merkmal liegt allerdings bei einer Vielzahl von Menschen in einem bestimmten Altersspektrum vor, ohne dass sie deshalb eine Gewalttat oder gar einen terroristischen Akt begehen. Verwendet man derartige Eigenschaften fälschlicherweise als Risikomerkmal zur Identifikation von potenziell gewalttätigen Personen, führt dies entsprechend zu einer hohen Anzahl an falsch positiven Beurteilungsergebnissen: Insbesondere für das Zieldelikt einer extremistisch motivierten Gewalttat ist die Basisrate verschwindend gering, während bei einer Vielzahl an Personen das vermeintliche Risikomerkmal vorliegt. Dies wird exemplarisch am Vorgehen der New Yorker Polizei (NYPD) deutlich: Diese haben ein vierstufiges Radikalisierungsmodell veröffentlicht,[132] das als Risikofaktoren für die „Prä-Radikalisierung" männliches Geschlecht, muslimische Religionszugehörigkeit, Migrationshintergrund, allenfalls geringe kriminelle Vorgeschichte, einen höheren Bildungsabschluss und jüngeres Alter als 35 Jahre nennt. Das Ergebnis der Verwendung dieser unspezifischen Merkmale war eine Massenüberwachung der muslimischen Bevölkerung New Yorks mit den entsprechenden negativen Konsequenzen für die Betroffenen wie die Angst, aufgrund von bestimmten politischen Äusserungen in Verdacht zu geraten, die Einschränkung der Religionsausübung (weil auch dies verdächtigem Verhalten entsprach) oder der Vertrauensverlust in die Polizei und andere lokale Behörden.[133]

Zusammengefasst handelt es sich bei Modellen zu Radikalisierungsprozessen um theoretische Konstrukte, die sich weder zu einer Diagnostik im Einzelfall eignen noch als Ausgangspunkt einer Risikobeurteilung dienen können – was allerdings auch nicht ihr Anspruch ist.

---

132 Silber/Bhatt, 1 ff.

133 Sadowski et al., 336; Shamas/Arastu, 1 ff.

V. Zusammenfassung

Obwohl ein islamistisches Attentat ein sehr seltenes Ereignis ist und die Wahrscheinlichkeit, Opfer eines solchen Anschlags zu werden, verschwindend klein ist, müssen solche Vorfälle bestmöglich verhindert werden. Zu diesem Zweck interessiert sich die Forschung für die Ursachen der Radikalisierung und der Hinwendung zu gewalttätigem Extremismus. Auch wenn einzelne Besonderheiten hinsichtlich der zugrundeliegenden Ideologie von Personen, die vor dem Hintergrund dieser Ideologie Gewalt angewandt haben, berichtet worden sind, gibt es weder allgemeingültige individuelle Ursachen für gewalttätigen Islamismus noch das typische Profil eines Islamisten. Meist handelt es sich bei der Radikalisierung, unabhängig von ihrem phänomenologischen Inhalt, um ein Zusammenspiel von persönlichen und umweltbedingten Faktoren, die sich im zeitlichen Verlauf ständig ändern.

Der Begriff der Radikalisierung wird in der Literatur aus verschiedenen Gründen kritisiert: Der Begriff ist unpräzis und impliziert, dass radikale Gedanken mit radikaler Handlungsbereitschaft gleichzusetzen seien. Tatsächlich schreitet nur ein verschwindend kleiner Teil der Personen mit radikalen Gedanken zu einer extremistischen Gewalttat, und umgekehrt lässt sich nicht bei allen Personen, die die Handlungsschwelle überschritten haben, die Gewaltbereitschaft auf eine radikale Ideologie zurückführen. Weiter wird kritisiert, dass der Begriff der Radikalisierung eine Art Gehirnwäsche insinuiert, für die es empirisch keinen Nachweis gibt.

Von Wissenschaftlerinnen und Wissenschaftlern wurde eine Vielzahl von Radikalisierungsmodellen entwickelt, um extremistisch motivierte Gewalthandlungen retrospektiv erklärbar zu machen. Im vorliegenden Beitrag sind einige der wichtigsten Modelle, die in der Forschung zu gewalttätigem Extremismus und Islamismus diskutiert werden, präsentiert worden. Dazu zählen die Social Identity Perspective (SIP), die von Marc Sageman auf den Phänomenbereich des gewalttätigen Extremismus übertragen worden ist, das Attitudes-Behavioral Corrective (ABC) Modell von James Khalil, das Zweipyramiden-Modell von Clark McCauley und Sophia Moskalenko, das Vierstufen-Modell von Randy Borum, das Treppenmodell von Fathali Moghaddam und das Significance-Quest-Modell von Arie Kruglanski et al. Alle Modelle haben ihre Stärken und Schwächen. Aus der Sicht der Autoren dieses Beitrags verdienen insbesondere die SIP und das ABC-Modell besondere Würdigung. Die SIP zeichnet sich v.a. durch die Berücksichtigung gruppendynamischer Prozesse aus, die nicht nur in der Theorie sehr plausibel erscheinen, sondern auch durch verschiedene Elemente, die in Feldstudien beobachtet worden sind. Wie die SIP geht auch das ABC-Modell davon aus, dass radikale Gedanken klar von tatsächlicher Ge-

waltanwendung separiert werden müssen. Überzeugend ist beim ABC-Modell weiter, dass zwischen strukturellen Motivatoren, individuellen Anreizen und fördernden Faktoren unterschieden werden muss, die sich im zeitlichen Verlauf ändern können.

In einer allgemeinen Kritik an bestehenden Radikalisierungsmodellen ist darauf hingewiesen worden, dass sie sich aufgrund der geringen Spezifität ihrer Merkmale wenig für Risikoeinschätzung bzgl. gewalttätigem Extremismus eignen. Weiter ist aufgezeigt worden, dass die Rational Choice Theory (RCT) – entgegen zahlreichen anderslautenden Ausführungen – dem theoretischen Konstrukt von „heiligen Werten" und „devoted actors", die insb. in der SIP postuliert werden, nicht widersprechen, da individueller Nutzen gewonnen wird, wenn Handlungen sozialen Normen spezifischer Gruppen entsprechen. Schliesslich ist der Fokus auf die Rolle der Ideologie von extremistischen Attentätern gerichtet worden. Zahlreiche Fachpersonen gehen wie automatisch davon aus, dass eine entsprechende Ideologie dem Motiv eines Attentäters entspricht. Die Forschung weist allerdings vielmehr darauf hin, dass der kausale Anteil der Ideologie am Prozess der Radikalisierung hin zum Überschreiten der Handlungsschwelle oft überbewertet ist.

Literatur

Akerlof George A./Kranton Rachel E., Economics and identity, Quarterly Journal of Economics 2000, 715 ff.

Amghar Samir, Le salafisme en France: de la revolution islamique à la revolution conservatrice, Critique Internationale 2008, 95 ff.

Atran Scott, Talking to the enemy, New York 2010 (zit. Atran, Enemy)

Atran Scott, The devoted actor: Unconditional commitment and intractable conflict across cultures, Current Anthropology 2016, Supp. 13, 192 ff. (zit. Atran, Devoted Actor).

Atran Scott/Sheikh Hammad/Gomez Angel, Devoted actors sacrifice for close comrades and sacred cause, Proceedings of the National Academy of Sciences 2014, 17702 f.

Bakker Edwin/De Bont Roel, Belgian and Dutch jihadist foreign fighters (2012–2015): Characteristics, motivations, and roles in the War in Syria and Iraq, Small Wars & Insurgencies 2016, 837 ff.

Bargh John A./Gollwitzer Peter M./Oettingen Gabriele, Motivation, in: Fiske Susan, Gilbert Daniel, Gardner Lindzey (Hrsg.), Handbook of Social Psychology, Hoboken, NJ 2010, 268 ff.

Bartlett Jamie/Miller Carl, The edge of violence: Towards telling the difference between violent and non-violent radicalization, Terrorism and Political Violence 2012, 1 ff.

Berger, Lars/Weber, Florian., Terrorismus (2. A.). Landeszentrale für politische Bildung Thüringen 2008.

Bloom Mia, Dying to kill: the allure of suicide terror, New York 2005.

Borum Randy, Radicalization into Violent Extremism I: A Review of Social Science Theories, Journal of Strategic Security 2011, 7 ff. (zit. Borum, Extremism I)

Borum Randy, Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research, Journal of Strategic Security 2011, 37 ff. (zit. Borum, Extremism II).

Borum Randy, Understanding the Terrorist Mindset, FBI Law Enforcement Bulletin 2003, 7 ff. (zit. Borum, Understanding).

Böttticher Astrid, Towards academic consensus definitions of radicalism and extremism, Perspectives on Terrorism 2017, 73 ff.

Campelo Nicolas, Joining the Islamic State from France between 2014 and 2016: an observational follow-up study, Palgrave Communications 2018, 1 ff.

Crenshaw Martha, Explaining Suicide Terrorism: A Review Essay, Security Studies 2007, 133 ff. (zit. Crenshaw, Suicide Terrorism)

Crenshaw Martha, Explaining Terrorism: Causes, Processes and Consequences, Oxon 2011 (zit. Crenshaw, Explaining Terrorism)

Crettiez Xavier/Barros Yvan, La Réalité de la menace djihadiste en France 2015-2018, 2019, <https://radical.hypotheses.org/files/2019/11/Chaire-Citoyenneté-Realite-djihadistes.pdf.>

Crettiez Xavier/Duclos Nathalie, Violences Politiques : Théories, Formes, Dynamiques, Paris 2021.

Darwin Charles, The descent of man, and selection in relation to sex, London 1871.

Della Porta Donatella, Clandestine political violence, New York 2013.

Dehghani Morteza et al., Sacred values and conflict over Iran's nuclear program, Judgment and Decision Making 2010, 540 ff.

Demichelis Marco/Mezzetti Giulia, The dynamics of Islamic radicalization in Europe and their prevention: a humanistic approach, in: Mostfa Ali/Younès Michel (Hrsg.), L'Islam au pluriel, Foi, pensée et société, Paris 2018, 225 ff.

Doering Sara/Davies Garth/Corrado Raymond, Reconceptualizing ideology and extremism: Toward an empirically-based typology, Studies in Conflict & Terrorism 2020, 1 ff.

Endrass Jérôme/Rossegger Astrid, Herausforderungen im Bedrohungsmanagement und das Octagon als neuer Ansatz, format magazine 2017, 36 ff. (zit. Endrass/Rossegger, Herausforderungen).

Endrass Jérôme/Rossegger Astrid, OCTAGON-Intervention: Bedrohungsmanagement nach dem Prinzip des „good judgements", Version 3, 2019, abrufbar unter: <www.octagon-intervention.ch>, (zit. Endrass/Rossegger, OCTAGON).

Endrass Jérôme et al., Der Weg zum (terroristischen) Attentäter: Gewalt legitimieren, um Gewalt auszuüben, Kriminalistik 2015, 328 ff.

Esposito John L./Mogahed Dalia, Who speaks for Islam? What a billion muslims really think, New York 2008.

Fumagalli Antonio, Der Jihadist von Morges plante weitere Messerattacken, NZZ vom 12. November 2022, <https://www.nzz.ch/schweiz/jihad-mord-von-morges-der-taeter-plante-weitere-messer-attacken-ld.1716610?reduced=true> (zit. Fumagalli, Der Jihadist).

Fumagalli Roberto, How thin rational choice theory explains choices, Studies in History and Philosophy of Science Part A 2020, 63 ff.

Gambetta Diego, Making sense of suicide missions, Oxford 2005.

Gartenstein-Ross Daveed et al., Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism, Studies in Conflict & Terrorism 2023, 1 ff.

Ginges Jeremy/Atran Scott, Why do people participate in violent collective action: Selective incentives or parochial altruism? Annals of the New York Academy of Sciences 2009, 115 ff.

Ginges Jeremy et al., Psychology out of the laboratory: The challenge of violent extremism, American Psychologist 2011, 507 ff.

Giustozzi Antonio, Koran, Kalashnikov, and Laptop: The Neo-Taliban insurgency in Afghanistan, New York 2008.

Goodwin Jeff, A theory of categorical terrorism, Social Forces 2006, 2027 ff.

Graham Jesse/Haidt Jonathan, Beyond beliefs: Religions bind individuals into moral communities, Personality and Social Psychology Review 2010, 140 ff.

Green, Steven L., Rational Choice Theory: An Overview. Paper prepared for the Baylor University Faculty Development Seminar on Rational Choice Theory, Waco, Texas 2002.

Hafez Mohammed, Suicide bombers in Iraq: the strategy and ideology of martyrdom, Washington D.C. 2007.

Haslam S. Alexander/Reicher Stephen D./Reynolds Katherine J., Identity influence and change: Rediscovering John Turner's vision for social psychology, British Journal of Social Psychology 2012, 201 ff.

Herfeld Catherine, The diversity of Rational Choice Theory: A review note, Topoi 2020, 329 ff.

Hetzer Moritz, The evolution of fairness preferences, altruistic punishment, and cooperation (Doctoral dissertation), ETH Zurich 2011.

Hornsey Matthew J., Social Identity Theory and Self-Categorization Theory: A historical review, Social and Personality Compass 2008, 204 ff.

Humphreys Macartan/Weinstein Jeremy M., Who Fights? The Determinants of Participation in Civil War, American Journal of Political Science 2008, 436 ff.

Introvigne Massimo, Brainwashing: Reality or myth? Cambridge 2022.

Irons William, Religion as a hard-to-fake sign of commitment, in: Nesse Randolph M. (Hrsg.), Evolution and the capacity for commitment, New York 2001 290 ff.

Jackson Lynne M./Hunsberger Bruce, An intergroup perspective on religion and prejudice, Journal for the Scientific Study of Religion 1999, 509 ff.

Kahneman Daniel, Thinking, fast and slow, London 2011.

Kalin Michael/Sambanis Nicholas, How to think about social identity, Annual Review of Political Science 2018, 239 ff.

Khalil James, Radical beliefs and violent actions are not synonymous: How to place the key disjuncture between attitudes and behaviors at the heart of our research into political violence, Studies in Conflict and Terrorism 2014, 198 ff.

Khalil James/Horgan John/Zeuthen Martine, The Attitudes-Behaviors Corrective (ABC) Model of Violent Extremism, Terrorism and Political Violence 2019, 1 ff. (zit. Khalil/Horgan/Zeuthen, ABC).

Khalil James/Horgan John/Zeuthen Martine, The ABC Model: Clarifications and Elaborations, Terrorism and Political Violence 2020, 1 ff. (zit. Khalil/Horgan/Zeuthen, Clarifications).

Kruglanski Arie W. et al., The psychology of radicalization and deradicalization: How significance quest impacts violent extremism, Advances in Political Psychology 2014, 69 ff.

Kruglanski Arie W./Bélanger Jocelyn J./Gunaratna Rohan, Empirical evidence for Significance Quest Theory, in: The three pillars of radicalization: needs, narratives and networks, Kruglanski Arie/Bélanger Jocelyn/Gunaratna Rohan (Hrsg.), Oxford 2019, 93 ff.

Leader Maynard Jonathan, Rethinking the Role of Ideology in Mass Atrocities, Terrorism and Political Violence 2014, 821 ff.

Leuprecht Christian et al., Containing the narrative: Strategy and tactics in countering the storyline of global Jihad, Journal of Policing, Intelligence, and Counter Terrorism 2010, 42 ff.

Levi Margaret, A Model, a method, and a map: Rational choice in comparative and historical analysis, in Lichbach Mark Irving/Zuckerman Alan S. (Hrsg.), Comparative politics: Rationality, culture and structure, Cambridge 1997, 19 ff.

McCauley Clark, The ABC Model: Commentary from the perspective of the Two Pyramids Model of Radicalization, Terrorism and Political Violence 2020, 451 ff.

McCauley Clark/Moskalenko Sophia, Friction: How Radicalization Happens to Them and Us, New York 2011 (zit. McCauley/Moskalenko, How radicalization happens).

McCauley Clark/Moskalenko Sophia, Toward a profile of lone wolf terrorists: What moves an individual from radical opinion to radical action, Terrorism and Political Violence 2014, 69 ff. (zit. McCauley/Moskalenko, Profile).

McCauley Clark/Moskalenko Sophia, Friction: How Conflict Radicalizes Them and Us, New York 2017 (zit. McCauley/Moskalenko, Them and us).

McCauley Clark/Moskalenko Sophia, Understanding Political Radicalization: The Two-Pyramids Model, American Psychologist 2017, 205 ff. (zit. McCauley/Moskalenko, Two-Pyramids).

McGilloway Angela/Ghosh Prijo/Bhui Kamaldeep, A systematic review of pathways to and processes associated with radicalization and extremism amongst Muslims in Western societies, International Review of Psychiatry 2015, 39 ff.

Merari Ariel, Driven to death: psychological and social aspect of suicide terrorism, New York 2010.

Merari Ariel et al., Personality Characteristics of 'Self Martyrs'/'Suicide Bombers' and Organizers of Suicide Attacks, Terrorism and Political Violence 2010, 87 ff.

Moghaddam Fathali, The staircase to terrorism. A psychological exploration, American Psychologist 2005, 161 ff.

Moore Will H., Rational rebels: Overcoming the free-rider problem, Political Research Quarterly 1995, 417 ff.

Neumann, Peter R., Perspectives on Radicalisation and Political Violence: Papers from the First International Conference on Radicalisation and Political Violence. International Centre for the Study of Radicalisation and Political Violence, London 2008.

Nisbett Richard E./Cohen Dov, Culture of honor: The psychology of violence in the south, Boulder, CO 1996.

Nowrasteh, Alex, The Chance of Being Murdered or Injured in a Terrorist Attack in the United Kingdom, Blog vom 15. August 2018 <https://www.cato.org/blog/chance-being-murdered-or-injured-terrorist-attack-united-kingdom>.

Nuraniyah Nava, Not just brainwashed: Understanding the radicalization of Indonesian female supporters of the Islamic State, Terrorism and Political Violence 2018, 890 ff.

Pape Robert, Dying to win: the strategic logic of suicide terrorism, New York 2005.

Pedahzur Ami, Suicide terrorism, Cambridge 2005.

Pfahl-Traughber Armin, Die Islamismuskompatibilität des Islam. Anknüpfungspunkte in Basis und Geschichte der Religion, Aufklärung und Kritik 2007, 62 ff.

Piazza James A., Poverty, minority economic discrimination, and domestic terrorism, Journal of Peace Research 2011, 339 ff.

Pousther Jacob/Manevich Dorothy, Globally, People Point to ISIS and Climate Change as Leading Security Threats, Pew Research Center, 1. August 2017 <https://www.pewresearch.org/global/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/>.

Pressman D. Elaine et al., VERA-2R Violence Extremism Risk Assessment Version 2 Revised: A structured professional judgment approach, Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP), Utrecht 2016.

Rapport Mike, 1848: Year of revolution, New York 2010.

Reidy Ken, Benevolent radicalization: An antidote to terrorism, Perspectives on Terrorism 2019, 1 ff.

Sadowski Friederike et al., Das Violent Extremism Risk Assessment Version 2 Revised (VERA-2R), Kriminalistik 2017, 335 ff.

Sageman Marc, Misunderstanding Terrorism, Philadelphia 2017 (zit. Sageman, Misunderstanding).

Sageman Marc, Turning to political violence, Philadelphia 2017 (zit. Sageman, Political Violence).

Sageman Marc, The Turn to Political Violence in the West, in: Coolsaet Rik (Hrsg.), Jihadi Terrorism and the Radicalization Challenge: European and American Experiences, Farnham 2011 (zit. Sageman, Turn).

Schmid Alex P., The revised academic consensus definition of terrorism, Perspectives on Terrorism 2012, 158 ff.

Shamas Diala/Arastu Nermeen, Mapping Muslims: NYPD spying and its impact on American Muslims, Long Island City 2013.

Sheikh Hammad/Gomez Angel/Atran Scott, Empirical evidence for the devoted actor model, Current Anthropology 2016, Supp. 13, 204 ff.

Silber Mitchell D./Bhatt Arvin, Radicalization in the west: The homegrown threat, New York, 2007.

Stanley Jason, How propaganda works, Princeton 2015.

Van Stekelenburg Jacquelien, Going all the way: Politicizing, polarizing, and radicalizing identity offline and online, Sociology Compass 2014, 1 ff.

Stouffer Samuel Andrew et al., The American soldier: Combat and its aftermath, Vol. II, New York 1965 (zit. Stouffer et al., The American soldier II)

Stouffer Samuel et al., Studies in Social Psychology in World War II: The American Soldier, Vol. I, Princeton 1949 (zit. Stouffer et al., The American soldier I)

Swann William B. et al., Identity fusion: the interplay of personal and social identities in extreme group behavior, Journal of Personality and Social Psychology 2009, 995 ff. (zit. Swann et al., Identity Fusion).

Swann William B. et al., When group membership gets personal: A theory of identity fusion, Psychological Review 2012, 441 ff. (zit. Swann et al., Group Membership).

Tetlock Philip E., Thinking the unthinkable: Sacred values and taboo cognitions, Trends in Cognitive Science 2003, 320 ff.

Thijssen Gaby et al., Understanding violent extremism: Socio-demographic, criminal and psychopathological background characteristics of detainees residing in Dutch terrorism wings, Criminology & Criminal Justice 2021, 17488958211049019 (zit. Thijssen et al., Background Characteristics).

Thijssen Gaby et al., Understanding violent extremism: identifying motivational classes in male jihadist detainees, International Journal of Offender Therapy and Comparative Criminology 2023, 0306624X221144295 (zit. Thijssen et al., Motivational Classes).

Tversky Amos/Kahneman Daniel, Availability: A heuristic for judging frequency and probability, Cognitive Psychology, 1973, 207 ff.

Weber Michael/Rossegger Astrid/Endrass Jérôme, Begutachtung im Bereich Extremismus, in: Venzlaff Ulrich/Foerster Klaus/Dressing Harald/Habermeyer Elmar (Hrsg.), Psychiatrische Begutachtung: Ein praktisches Handbuch für Ärzte und Juristen, München 2020, 831 ff.

Wittek Rafael, Rational Choice, Oxford 2013.

Ysseldyk Renate/Matheson Kimberly/Anisman Hymie, Religiosity as identity: Toward an understanding of religion from a social identity perspective, Personality and Social Psychology Review 2010, 60 ff.

Xia Weiwei et al., Religious identity, between-group effects and prosocial behavior: Evidence from a field experiment in China, Journal of Behavioral and Experimental Economics 2021, <https://doi.org/10.1016/j.socec.2021.101665>.

Chlorothalonil-Rückstände im Trinkwasser – eine Bestandesaufnahme und rechtliche Einordnung

Tobias Tschumi / Marc Häusler*

Chlorothalonil-haltige Pflanzenschutzmittel sind in der Schweiz seit mehr als drei Jahren verboten. Als Folge dieses Verbots führte der Bund einen rechtlich umstrittenen strengen Grenzwert für sämtliche Abbauprodukte dieser Pflanzenschutzmittel im Trinkwasser ein und setzte damit die Kantone und Trinkwasserversorgungen unter erheblichen Handlungsdruck, da der Grenzwert breitflächig überschritten wird und rund 1 Mio. Trinkwasserkonsumentinnen und -konsumenten betroffen sind. Die technischen Möglichkeiten zur Beseitigung dieser Rückstände aus dem Trinkwasser sind beschränkt und mit hohen Investitionen verbunden, was die Problematik zusätzlich verschärft. Der Bund hat bisher weitgehend offengelassen, welches Gesundheitsrisiko im Fall einer Grenzwertüberschreitung besteht und welche rechtliche Bedeutung dem neuen Grenzwert genau zukommt. Indem er bisher auf präzisere Handlungsanweisungen verzichtet hat, belässt er die Kantone und Wasserversorgungen nicht nur in einer problematischen Rechtsunsicherheit, sondern überlässt ihnen auch weitgehend die (politische) Verantwortung für den konkreten Umgang mit dem Chlorothalonil-Problem – dies gilt es zu ändern.

* Tobias Tschumi, Dr. phil.-nat., Rechtsanwalt hat an der ETH Lausanne und der Universität St. Gallen studiert, im Kanton St. Gallen das Anwaltspatent erworben und ist gegenwärtig als Gerichtsschreiber an der verwaltungsrechtlichen Abteilung des Verwaltungsgerichts des Kantons Bern tätig. Marc Häusler, lic. iur., Rechtsanwalt und Notar hat an den Universitäten Bern und Paris studiert und im Kanton Bern das Anwalts- und Notariatspatent erworben. Er ist Richter an der verwaltungsrechtlichen Abteilung des Verwaltungsgerichts des Kantons Bern. Die Autoren geben ausschliesslich ihre persönliche Meinung wieder.

Inhalt

I. Einleitung 40

II. Grundzüge des Trinkwasserversorgungsrechts in der Schweiz 42
1. Begriff des Trinkwassers 42
2. Allgemeiner Rechtsrahmen 43
a) Bundesrecht 43
b) Kantonales Recht 44
3. Vorgaben zur Trinkwasserqualität 44

III. Neubewertung von Chlorothalonil durch die Bundesbehörden und Weisungen des BLV zum Vorgehen bei Grenzwertüberschreitungen 46
1. Allgemeines zur Zulassung und Überprüfung von Pflanzenschutzmitteln 46
2. Überprüfung des Wirkstoffs Chlorothalonil und Widerruf der Zulassung 47
3. Weisungen des BLV zum Vorgehen bei Grenzwertüberschreitungen 49

IV. Seitenblick: Rechtslage in der EU und Grenzwerte im benachbarten Ausland 50
1. EU 50
2. Unterschiedliche Relevanzbeurteilung in Deutschland/Österreich und Frankreich 51
a) Deutschland und Österreich 51
b) Frankreich 52

V. Beschwerdeverfahren vor dem Bundesverwaltungsgericht 52
1. Argumentation von Syngenta 52
2. Zwischenverfügung vom 24. August 2020 53
3. Zwischenverfügung vom 15. Februar 2021 53
4. Unsicherheit in Bezug auf die aktuelle Rechtslage 54

VI. Beschränkte Handlungsoptionen für die Wasserversorgungen 54
1. Aktuelle Belastungssituation 54
2. Sofortmassnahmen 55
3. Weitergehende Massnahmen 55
4. Haltung des Fachverbands 56

VII. Chlorothalonil-Problematik als Anwendungsfall des Vorsorgeprinzips 57
1. Tragweite des Vorsorgeprinzips 57
2. Vorsorgeprinzip im Lebensmittelrecht 58
3. Umsetzung des Vorsorgeprinzips als Zusammenspiel verschiedener Akteure in Bund und Kantonen 58

VIII. Auswirkungen für die Kantone und die Gerichte 60
1. Kantone 60
2. Gerichte 61

IX. Fazit 62

Literaturverzeichnis 63

I. Einleitung

Für viele war es 2019 eine Hiobsbotschaft: Das Bundesamt für Landwirtschaft (BLW) hatte wie zuvor bereits die EU-Kommission den Fungizidwirkstoff Chlorothalonil verboten, der in der Schweiz seit den 1970er eingesetzt wurde. Zur Begründung führte es aus, dass eine Überprüfung durch das Bundesamt für Veterinärwesen und Lebensmittelsicherheit (BLV) ergeben habe, dass der Wirkstoff neu als wahrscheinlich krebserregend eingestuft werden müsse. Aus diesem Grund seien neu auch sämtliche seiner Abbauprodukte (sog. Metaboliten) als trinkwasserrelevant zu betrachten. Da zu erwarten sei, dass die Konzentrationen dieser Abbauprodukte vielerorts über den gesetzlichen Höchstwerten für das Trinkwasser liegen, sei es notwendig, schnell zu handeln, um ihr Vorkommen im Grundwasser zu reduzieren.[1] Diesem Entscheid gingen verschiedene Untersuchungen voraus: Im Jahr 2017 wurden im Rahmen einer Pilotstudie der Nationalen Grundwasserbeobachtung (NAQUA) erstmals Rückstände von Chlorothalonil im Grundwasser festgestellt.[2] Eine Messkampagne des Verbands der Kantonschemiker wies in der Folge im Jahr 2019 nach, dass dies nicht nur punktuell der Fall ist, sondern dass Chlorothalonil-Metaboliten im Grundwasser weit verbreitet sind.[3]

Laut den Angaben des Bundesamts für Umwelt (BAFU) stammt das Trinkwasser in der Schweiz zu etwa 80% aus Grundwasservorkommen. Dabei wird rund 70% des aus dem Grundwasser gewonnen Rohwassers ohne oder nach einer einfachen Aufbereitung direkt als Trinkwasser genutzt.[4] Es überrascht daher nicht, dass auch im Trinkwasser Chlorothalonil-Metaboliten-Konzentrationen vorgefunden wurden, die mit denjenigen im Grundwasser vergleichbar sind. Weil das BLV gleichzeitig mit dem Chlorothalonil-Verbot neue strengere

1 Medienmitteilung des BLW vom 12. Dezember 2019 „Zulassung für Chlorothalonil wird mit sofortiger Wirkung entzogen", abrufbar unter <www.blw.admin.ch/blw/de/home/services/medienmitteilungen.msg-id-77491.html>.

2 Vgl. für eine Übersicht über die Studienergebnisse KIEFER ET AL., 14 ff.

3 Kampagnenbericht „Pflanzenschutzmittel in Trinkwasser" vom 6. September 2019 des Verbandes der Kantonschemiker der Schweiz, abrufbar unter <www.kantonschemiker.ch/medienmitteilungen.html>.

4 BAFU, „Gutes Trinkwasser ist nicht mehr selbstverständlich", in: die umwelt, 3/2020, 45, abrufbar unter <www.bafu.admin.ch/bafu/de/home/dokumentation/magazin.html>.

Höchstgehalte für Chlorothalonil-Rückstände im Trinkwasser eingeführt hat, sahen und sehen sich nunmehr plötzlich zahlreiche Wasserversorgungen sowie ihre Kundinnen und Kunden mit entsprechenden Grenzwertüberschreitungen konfrontiert. Schätzungen zufolge sind in der Schweiz rund eine Millionen Menschen betroffen.[5] Dies löste in der Bevölkerung (vorübergehend) eine starke Verunsicherung aus. Behörden und Fachleute versicherten zwar, dass keine Gesundheitsgefährdung bestehe.[6] Viele Trinkwasserkonsumentinnen und -konsumenten fragten sich aber dennoch, ob sie das Wasser aus ihren Hähnen noch bedenkenlos trinken können.

Obschon die Chlorothalonil-haltigen Pflanzenschutzmittel nunmehr seit mehr als drei Jahren verboten sind, liegen die Konzentrationen seiner Rückstände im Trinkwasser auch heute noch an vielen Orten zum Teil deutlich über den neu eingeführten Grenzwerten. Dennoch hat sich die öffentliche Diskussion um die Chlorothalonil-Problematik unterdessen etwas abgekühlt und scheint nicht mehr so präsent wie noch vor wenigen Jahren. Dies bedeutet allerdings nicht, dass sich die Angelegenheit damit erledigt hätte. Vielmehr sind die zuständigen kantonalen Behörden und die Wasserversorgungsunternehmen nach wie vor intensiv mit der Suche nach möglichen Lösungen beschäftigt.

Der vorliegende Beitrag versucht die Chlorothalonil-Problematik im Rahmen des Verfassungs- und Verwaltungsrechts zu verorten und die nur schwer überschaubaren Zuständigkeiten und Rollen der verschiedenen staatlichen Akteure auf Bundes- und Kantonsebene näher zu beleuchten. Dazu werden zunächst die Grundzüge des Trinkwasserversorgungrechts in der Schweiz vorgestellt (II.) und anschliessend die rechtlichen Hintergründe aufgezeigt, die zum Erlass des Chlorothalonil-Verbots und der Einführung der neuen Grenzwerte geführt haben (III.). Nach einem kurzen Seitenblick auf die Rechtslage in der EU bzw. im benachbarten Ausland (IV.) geht der Beitrag auf das gegen die Einführung der neuen Grenzwerte eingereichte, derzeit noch hängige Beschwerdeverfahren vor Bundesverwaltungsgericht (V.) sowie die aktuelle Belastungssituation und Handlungsoptionen der Wasserversorgungen ein (VI.). Sodann wird die Chlorothalonil-Problematik im Licht des Vorsorgeprinzips

---

5 BAFU (Fn. 4), 44.

6 Vgl. etwa Stellungnahme des Bundesrats vom 19. Februar 2020 zur Interpellation 19.4532 von Nationalrätin Moser vom 19. Dezember 2019; Interview vom 30. März 2020 mit dem Toxikologen Lothar Aicher vom Schweizerischen Zentrum für Angewandte Humantoxikologie (SCAHT), abrufbar unter<www.aquaetgas.ch/aktuell/interview/20200330-interview-lothar-aicher>.

untersucht (VII.) und die Herausforderungen für die Kantone und Gerichte dargelegt (VIII.). Am Ende des Beitrags findet sich schliesslich ein Fazit, in dem die Rolle des Bundes kritisch betrachtet wird (IX.).

II. Grundzüge des Trinkwasserversorgungsrechts in der Schweiz

1. Begriff des Trinkwassers

Da das Trinkwasser dazu bestimmt ist, von Menschen konsumiert bzw. aufgenommen zu werden, gilt es als Lebensmittel im Sinn des LMG[7]. Nach der TBDV[8] handelt es sich bei ihm um dasjenige Wasser, das im Naturzustand oder nach der Aufbereitung zum Trinken, zum Kochen, zur Zubereitung von Lebensmitteln oder zur Reinigung von Gegenständen, die mit Lebensmittel in Berührung kommen, vorgesehen ist oder für diese Zwecke verwendet wird. Dieser Trinkwasserbegriff wurde aus dem EU-Recht, genauer aus der Richtlinie 98/83/EG[9] übernommen.[10] Die TBDV grenzt das Trinkwasser vom Dusch- und Badewasser ab, welches zwar ebenfalls für den Kontakt mit dem menschlichen Körper bestimmt ist, aber kein Lebensmittel darstellt und deshalb anderen rechtlichen Anforderungen unterliegt.

---

7 Bundesgesetz vom 20. Juni 2014 über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz, LMG; SR 817.0).

8 Verordnung des Eidgenössischen Departements des Innern (EDI) über Trinkwasser sowie Wasser in öffentlich zugänglichen Bädern und Duschanlagen vom 16. Dezember 2016 (SR 817.022.11).

9 Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch, ABl L 330 vom 5. Dezember 1998, 32 ff. Diese Richtlinie ist unterdessen nicht mehr in Kraft und wurde ersetzt durch die Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (sog. EU-Trinkwasserrichtlinie), ABl L 435 vom 23. Dezember 2020, 1 ff.

10 Erläuterungen des BLV zur TBDV vom 20. Februar 2017, 2.

2. Allgemeiner Rechtsrahmen

a) Bundesrecht

Das Trinkwasser und die Trinkwasserversorgung werden in der Bundesverfassung[11] nicht explizit erwähnt.[12] Die Volksinitiative vom 18. Januar 2018 „Für sauberes Trinkwasser und gesunde Nahrung – Keine Subventionen für den Pestizid- und den prophylaktischen Antibiotika-Einsatz", welche die ausdrückliche Verankerung des Trinkwasserschutzes in der BV vorgeschlagen hatte, wurde in der Volksabstimmung vom 13. Juni 2021 abgelehnt.[13] Zum Thema Trinkwasser äussern sich allerdings mehrere Verfassungsbestimmungen indirekt.

Gemäss Art. 118 BV trifft der Bund im Rahmen seiner Zuständigkeiten Massnahmen zum Schutz der Gesundheit (Abs. 1) und erlässt Vorschriften über den Umgang mit Lebensmitteln (Abs. 2 Bst. a). Im Rahmen dieses Auftrags hat der Bund das LMG erlassen, dessen Zweck insbesondere darin besteht, die Gesundheit der Konsumentinnen und Konsumenten vor unsicheren Lebensmitteln zu schützen.[14] Gestützt auf dieses Gesetz hat das Eidgenössische Departement des Innern (EDI) den Schutz vor gesundheitsgefährdendem Trinkwasser in der erwähnten TBDV weiter konkretisiert. Das Trinkwasser ist daher – wie bereits angetönt – Gegenstand des eidgenössischen Lebensmittelrechts.

Weiter sieht Art. 76 BV vor, dass der Bund im Rahmen seiner Zuständigkeiten für die haushälterische Nutzung und den Schutz der Wasservorkommen sorgt (Abs. 1), Grundsätze über die Erhaltung und die Erschliessung der Wasservorkommen festlegt (Abs. 2) und Vorschriften über den Gewässerschutz erlässt (Abs. 3). Das gestützt auf diese Verfassungsbestimmungen erlassene GSchG[15] dient insbesondere der Sicherstellung und haushälterischen Nutzung des Trinkwassers.[16] Die Trinkwasserversorgung bildet damit ebenfalls ein wichtiges Motiv für den bundesrechtlichen Gewässerschutz.[17]

---

11 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101).

12 Anders noch Art. 24bis Abs. 2 Bst. a der alten Bundesverfassung vom 29. Mai 1874.

13 Vgl. Bundesratsbeschluss vom 17. September 2021 über das Abstimmungsergebnis, BBl 2021 2135.

14 Art. 1 Bst. a LMG.

15 Bundesgesetz vom 24. Januar 1991 über den Schutz der Gewässer (Gewässerschutzgesetz, GSchG; SR 814.20).

16 Art. 1 Bst. b GSchG.

17 SGK BV-Marti/Hettich, Art. 76 Rz. 13.

Ferner hat der Bund gemäss Art. 74 Abs. 1 BV Vorschriften über den Schutz des Menschen und seiner natürlichen Umwelt vor schädlichen oder lästigen Einwirkungen zu erlassen. Gemäss dem auf dieser Grundlage erlassenen USG[18] verfolgt der Umweltschutz namentlich das Ziel, die natürlichen Lebensgrundlagen dauerhaft zu schützen. Da die Trinkwasserressourcen zu diesen gehören, wird ihr Schutz auch vom Bundesumweltrecht mitumfasst.

b) Kantonales Recht

Gemäss Art. 76 Abs. 4 BV steht die Hoheit über die Nutzung der Wasservorkommen in erster Linie den Kantonen zu. Der Bund hat deshalb keine Kompetenz, Vorschriften über die Organisation der Trinkwasserversorgung zu erlassen.[19] Die kantonalen Verfassungen sehen vor, dass der Kanton – zum Teil zusammen mit den Gemeinden – die Versorgung der Bevölkerung mit Trinkwasser zu gewährleisten oder zu sichern hat.[20] Im Rahmen dieses Verfassungsauftrags haben die Kantone[21] oder Gemeinden[22] entsprechende Wasserversorgungsgesetze erlassen. Die Wasserversorgungen sind zumeist kommunal als öffentlich-rechtliche Anstalten oder Korporationen organisiert.[23] Ihnen obliegt die Pflicht, in ihrem Versorgungsgebiet dauernd Trinkwasser in ausreichender Menge und einwandfreier Qualität abzugeben.[24]

3. Vorgaben zur Trinkwasserqualität

Die rechtlichen Qualitätsvorgaben für das Trinkwasser dienen dem Gesundheitsschutz und sind daher in der Lebensmittelgesetzgebung des Bundes festgelegt. Art. 3 der TBDV sieht vor, dass das Trinkwasser hinsichtlich Geruch, Geschmack und Aussehen unauffällig sein muss und hinsichtlich Art und Konzentration der darin enthaltenen Mikroorganismen, Parasiten sowie Konta-

---

18 Bundesgesetz vom 7. Oktober 1983 über den Umweltschutz (Umweltschutzgesetz, USG; SR 814.01).

19 Komm. GSchG/WBG-Hettich/Jansen/Norer, Einleitung Rz. 11.

20 Z.B. Art. 105 Abs. 2 der Verfassung des Kantons Zürich vom 27. Februar 2005 (KV ZH, LS 101), Art. 35 Abs. 1 der Verfassung des Kantons Bern vom 6. Juni 1993 (KV BE, BSG 101.1) oder Art. 82 Abs. 1 Verfassung des Kantons Graubünden vom 14. September 2003 (KV GR, BR 110.100).

21 Z.B. Wasserwirtschaftsgesetz des Kantons Zürich vom 2. Juni 1991 (WWG ZH, LS 724.11), Wasserversorgungsgesetz des Kantons Bern vom 11. November 1996 (WVG BE, BSG 752.32).

22 Z.B. Wasserversorgungsgesetz der Landschaft Davos vom 28. November 2004, Gesetz über die Wasserversorgung der Gemeinde Zernez vom 18. Oktober 2015.

23 Komm. GSchG/WBG-Hettich/Jansen/Norer, Einleitung Rz. 11.

24 Vgl. etwa § 25 und 27 Abs. 1 WWG ZH oder Art. 8 Abs. 1 und 14 Abs. 1 WVG BE.

minanten keine Gesundheitsgefährdung darstellen darf (Abs. 1). Das bedeutet insbesondere, dass es die in den Anhängen 1–3 der TBDV festgelegten Höchstwerte einzuhalten hat (Abs. 2). In Bezug auf die zulässigen Fremdstoffe wird dort unter anderem festgehalten, dass die in den Pflanzenschutzmitteln enthaltenen Wirkstoffe sowie deren trinkwasserrelevanten Abbauprodukte einen Höchstgehalt von je 0,1 µg/l nicht überschreiten dürfen, während die Gesamtkonzentration dieser Fremdstoffe gesamthaft nicht mehr als 0.5 µg/l betragen darf.[25] Das BLV führt eine Liste, in der die trinkwasserrelevanten Abbauprodukte der Wirkstoffe aufgeführt werden.[26]

Die Gewährleistung der Trinkwasserqualität basiert nach dem Konzept des im Jahr 2017 in Kraft getretenen neuen Lebensmittelrechts grundsätzlich auf dem Prinzip der Selbstkontrolle.[27] Danach liegt es in erster Linie an den Wasserversorgungen, dafür zu sorgen, dass vom Trinkwasser keine Gefahr für die Gesundheit der Konsumentinnen und Konsumenten ausgeht.[28] Stellt eine Wasserversorgung fest, dass das von ihr abgegebene Trinkwasser eine Gesundheitsgefährdung darstellt, ist sie verpflichtet, unverzüglich die zuständige kantonale Vollzugsbehörde zu informieren und in Zusammenarbeit mit dieser die zur Abwendung der Gefahr erforderlichen Massnahmen zu treffen.[29] Um Verunreinigung des Trinkwasser möglichst vorsorglich zu verhindern, müssen die Wasserversorgungen ausserdem im Rahmen der gesamtbetrieblichen Gefahrenanalyse periodisch eine Analyse der Gefahren für die Wasserressourcen durchführen.[30]

Die Lebensmittelgesetzgebung verlangt zwar, dass die Vorgaben über die Qualität von Lebensmittelqualität einzuhalten sind; welche Massnahmen im Fall einer Beanstandung konkret zu treffen sind, lässt sie dagegen weitgehend offen. Art. 34 Abs. 2 LMG sieht lediglich vor, dass die kantonalen Vollzugsbehörden anordnen können, dass ein beanstandetes Produkt weiterhin „mit oder ohne Auflagen“ verwertet werden darf (Bst. a) oder auf Kosten des zuständigen Unternehmens eingezogen und/oder beseitigt oder unschädlich gemacht

---

25 Anhang 2 TBDV.

26 BLV, „Relevanz von Pflanzenschutzmittel-Metaboliten im Grund- und Trinkwasser“, aktuelle Liste vom März 2022 abrufbar unter <www.blv.admin.ch/blv/de/home/zulassung-pflanzenschutzmittel/anwendung-und-vollzug/weisungen-und-merkblaetter.html>.

27 Art. 26 LMG.

28 Vgl. Art. 27 Abs. 1 LMG.

29 Art. 84 Abs. 4 der Lebensmittel- und Gebrauchsgegenständeverordnung vom 16. Dezember 2016 (LGV; SR 817.02).

30 Art. 3 Abs. 3 TBDV.

werden muss (Bst. b und c).[31] Allerdings kann das BLV gestützt auf seine Kompetenz zur Regelung des einheitlichen Vollzugs des eidgenössischen Lebensmittelrechts „zum Zweck der Koordination" den Kantonen bestimmte Massnahmen vorschreiben und sie bei ausserordentlichen Verhältnissen anweisen, bestimmte konkrete Massnahmen zu treffen.[32]

III. Neubewertung von Chlorothalonil durch die Bundesbehörden und Weisungen des BLV zum Vorgehen bei Grenzwertüberschreitungen

1. Allgemeines zur Zulassung und Überprüfung von Pflanzenschutzmitteln

Pflanzenschutzmittel dürfen in der Schweiz nur in Verkehr gebracht und verwendet werden, wenn sie vorgängig behördlich zugelassen worden sind. Das Zulassungsverfahren ist in der PSMV[33] geregelt und wurde zu wesentlichen Teilen aus dem EU-Recht übernommen.[34] Die Zulassung eines Pflanzenschutzmittels setzt unter anderem voraus, dass die in ihm enthaltenen Wirkstoffe genehmigt worden sind.[35] Zudem dürfen bei einem Gebrauch des Pflanzenschutzmittels gemäss der „guten Pflanzenschutzpraxis"[36] und unter realistischen Verwendungsbedingungen weder direkt noch über das Trinkwasser oder anderweitig indirekt schädliche Auswirkungen auf die Gesundheit von Mensch und Tier oder das Grundwasser entstehen, wobei auch sog. Kumulations- und Synergieeffekte zu berücksichtigen sind.[37] Bei der Zulassung eines Pflanzenschutzmittels kann die Zulassungsstelle allgemeine Verwendungsvorschriften wie etwa Regeln zur Anwendungsmenge, Abstandsvorschriften oder die Benutzung bestimmter Geräte erlassen.[38] Die Zuständigkeit

31 Vgl. auch Klemm/Uebe, 141, Lagger, 63.

32 Art. 42 Abs. 3 Bst. b und c LMG.

33 Verordnung über das Inverkehrbringen von Pflanzenschutzmitteln vom 12. Mai 2010 (Pflanzenschutzmittelverordnung, PSMV, SR 916.161).

34 Für einen Überblick über das Zulassungsverfahren vgl. Klauser, 711 ff.

35 Art. 17 Abs. 1 Bst. a PSMV; die Liste der genehmigten Wirkstoffe findet sich in Anhang 1 PSMV.

36 Vgl. Art. 3 Abs. 1 Bst. q PSMV.

37 Art. 17 Abs. 1 Bst. e i.V.m. Art. 4 Abs. 5 Bst. b PSMV.

38 Vgl. Art. 66 PSMV.

für die Aufnahme in die Liste der genehmigten Wirkstoffe liegt beim EDI.[39] Die Zulassungsstelle für Pflanzenschutzmittel ist dem BLV zugewiesen,[40] welches diese Aufgabe per 1. Januar 2022 vom BLW übernommen hat.[41]

Die Genehmigung der Wirkstoffe und die Zulassung der Pflanzenschutzmittel bzw. die dabei erlassenen Verwendungsvorschriften beruhen grundsätzlich auf dem Wissen zum Zeitpunkt des entsprechenden Genehmigungs- bzw. Zulassungsentscheids, die zum Teil relativ weit zurückliegen können. Da sich der Kenntnisstand in Bezug auf unerwünschte Nebenwirkungen fortlaufend verbessert und die Zulassungsanforderungen zunehmend verschärft werden, hat das BLV im Jahr 2010 das Programm der sog. „Gezielten Überprüfung" eingeleitet. Dieses orientiert sich am entsprechenden Reevaluationsprogramm der EU und bezwecket, ausgewählte Pflanzenschutzmittel-Wirkstoffe unter Berücksichtigung von neuen Erkenntnissen einer aktualisierten wissenschaftlichen Risikoeinschätzung zu unterziehen und gegebenenfalls die geltenden Verwendungsvorschriften anzupassen oder allenfalls sogar die Zulassung eines Wirkstoffs oder Pflanzenschutzmittels nachträglich zu entziehen.[42]

2. Überprüfung des Wirkstoffs Chlorothalonil und Widerruf der Zulassung

In den Jahren 2016 und 2017 führte die Europäische Behörde für Lebensmittelsicherheit (EFSA) im Zusammenhang mit dem Antrag auf Erneuerung der Genehmigung von Chlorothalonil in der EU eine Reevaluation des Wirkstoffs durch.[43] In der Folge hat das BLV im Dezember 2018 ebenfalls eine gezielte Überprüfung des Fungizids eingeleitet.[44] Gestützt auf die Erkenntnisse

---

39 Vgl. Art. 5 Abs. 1 PSMV.

40 Art. 71 Abs. 1 PSMV.

41 Vgl. Medienmitteilung des Bundesrats vom 17. November 2021 „Neuorganisation der Pflanzenschutzmittelzulassung", abrufbar unter <www.blw.admin.ch/blw/de/home/services/medienmitteilungen.msg-id-85919.html>.

42 BLV, „Allgemeine Informationen zur Gezielten Überprüfung der bewilligten Pflanzenschutzmittel" (Stand: 1. Januar 2022), abrufbar unter <www.blv.admin.ch/blv/de/home/zulassung-pflanzenschutzmittel/zulassung-und-gezielte-ueberpruefung/gezielte-ueberpruefung.html>.

43 EFSA, 2016, Conclusion on the peer review of the peer review of the pesticide risk assessment of the active substance chlorothalonil, EFSA Journal 2018;16(1):5126, abrufbar unter <www.efsa.europa.eu/en/efsajournal/pub/5126>.

44 BLV, Wirkstoff-Liste GÜ in Bearbeitung und abgeschlossen (Stand: 30.4.2023), abrufbar unter: <www.blv.admin.ch/blv/de/home/zulassung-pflanzenschutzmittel/zulassung-und-gezielte-ueberpruefung/gezielte-ueberpruefung.html>.

der in der EU bereits durchgeführten Reevaluation gelangte es dabei zum Schluss, dass Chlorothalonil als wahrscheinlich krebserregend eingestuft werden müsse. Diese Neueinstufung habe gemäss dem europäischen Leitfaden über die Beurteilung der Relevanz[45] zudem automatisch zur Folge, dass fortan auch alle Metaboliten von Chlorothalonil – und nicht wie bis anhin nur einzelne von ihnen – als trinkwasserrelevant anzusehen seien, für die ein Grenzwert von 0,1 µg/l gilt.[46] Am 11. Dezember 2019 entzog daraufhin das (damals noch zuständige) BLW die Verkaufserlaubnis für die Chlorothalonil-haltigen Pflanzenschutzmitteln mit sofortiger Wirkung und verbot deren Verwendung ab dem 1. Januar 2020.[47] Damit zog das BLW mit der EU-Kommission gleich, welche bereits am 29. April 2019 die Verlängerung der Genehmigung für den Wirkstoff Chlorothalonil verweigert hatte.[48]

Während sich die Bundesbehörden bei der Neubeurteilung des Wirkstoffs Chlorothalonil im Wesentlichen den Ergebnissen der Reevaluation der EFSA bzw. EU-Kommission angeschlossen haben, sind sie dem im Rahmen der gezielten Überprüfung selber erstellten Gutachten zur Relevanz der Chlorothalonil-Metaboliten nicht gefolgt.[49] In diesem Gutachten ist das BLV noch zu teilweise von der Beurteilung der EFSA abweichenden Ergebnissen gelangt. Insbesondere hatte das BLV den Metaboliten „R471811" dort im Unterschied zur EFSA noch als nicht trinkwasserrelevant beurteilt.[50] Der in der Zwischenzeit neu erlassene Art. 24 Abs. 2^{bis} PSMV sieht nunmehr ausdrücklich vor, dass die Schweizer Behörden die Ergebnisse der EFSA und die Erwägungen der EU-Kommission über die Genehmigung der Wirkstoffe des Pflanzenschutzmittels bei der Überprüfung einer Bewilligung für ein Pflanzenschutzmittel überneh-

---

45 Guidance document on the assessment of the relevance of metabolites in groundwater of substances regulated under Regulation (EC) No 1107/2009, Sanco/221/2000 – rev.10- final, vom 25. Februar 2003.

46 Vgl. Medienmitteilung des BLW vom 12. Dezember 2019 (Fn. 1) sowie Weisung Nr. 2020/1 des BLV vom vom 14. September 2020, Ziff. 3.

47 Allgemeinverfügung des BLW vom 11. Dezember 2019 über die Verwendung von Pflanzenschutzmittel mit dem Wirkstoff Chlorothalonil, BBl 2019 8431.

48 Durchführungsverordnung (EU) 2019/677 der Kommission vom 29. April 2019 zur Nichterneuerung der Genehmigung für den Wirkstoff Chlorthalonil, ABl L 114 vom 30. April 2019, 15 ff.

49 Vgl. dazu auch hinten Ziff. V.1.

50 Gutachten des BLV vom 3. Dezember 2019, „Relevanzprüfung der Grundwassermetaboliten der Produkte mit dem Wirkstoff Chlorothalonil im Rahmen der (teil-)gezielten Überprüfung", abrufbar unter <https://files.newsnetz.ch/upload//2/9/291152.pdf>.

men. Gemäss dieser Bestimmung soll die Schweiz zudem neu auf eine eigene Beurteilung der Stoffe verzichten, wenn diese bereits von der EFSA überprüft worden sind.

3. Weisungen des BLV zum Vorgehen bei Grenzwertüberschreitungen

Zur konkreten Umsetzung dieser Neubewertung von Chlorothalonil und seiner Abbauprodukte hat das BLV gestützt auf seine Kompetenz zur Regelung des einheitlichen Vollzugs des Lebensmittelrechts verschiedene Weisungen an die zuständigen kantonalen Behörden erlassen. Dazu gehören insbesondere die Weisung Nr. 2020/1 vom 14. September 2020 mit dem Titel „Anordnung von Massnahmen bei Höchstwertüberschreitungen von Chlorothalonil-Metaboliten im Trinkwasser“[51] sowie die Weisung Nr. 2020/4 vom 10. November 2020 „Interpretation von Höchstwertüberschreitungen chemischer und physikalischer Parameter in Lebensmitteln“[52].

In der Weisung Nr. 2020/4 führt das BLV allgemein aus, dass die verschiedenen Grenzwerte der Lebensmittelgesetzgebung aus unterschiedlichen Gründen festgelegt werden. Sie beruhten zum einen „auf der gesundheitlichen Beurteilung nach heutigem Wissensstand“, andererseits aber auch „auf der technischen Vermeidbarkeit“ (Ziff. 1). Weil sich die Bedeutung der einzelnen Grenzwerte im Hinblick auf allfällige Gesundheitsrisiken unterschieden, seien keine generellen Aussagen über die im Fall einer Grenzwertüberschreitung zu treffenden Massnahmen möglich (Ziff. 3.1). Bei der Beurteilung, ob ein Lebensmittel gesundheitsschädlich ist, sehe das LMG vor, dass die wahrscheinlichen sofortigen, kurzfristigen und langfristigen Auswirkungen auf die Gesundheit, die wahrscheinlichen kumulativen toxischen Auswirkungen und die besondere Empfindlichkeit bestimmter Konsumentengruppen zu berücksichtigen seien (Ziff. 2). Würden die Höchstwerte für die Pflanzenschutzmittel oder ihre Abbauprodukte im Trinkwasser überschritten, bestehe nicht in jedem Fall ein Risiko für die Gesundheit. Vielmehr müsse im Einzelfall eine eingehende Beurteilung des spezifischen Stoffes unter Einbezug des BLV erfolgen. Eine weitere Abgabe an die Konsumentinnen und Konsumenten für einen „definierten Zeit-

---

51 Diese Weisung ist aufgrund der vor Bundesverwaltungsgericht hängigen Beschwerde gegen die Neubeurteilung der Chlorothalonil-Metaboliten auf der Webseite des BLV momentan nicht abrufbar; vgl. dazu hinten Ziff. V.3.

52 Abrufbar unter <www.blv.admin.ch>, Lebensmittel und Ernährung > Rechts- und Vollzugsgrundlagen > Hilfsmittel und Vollzugsgrundlagen > Weisungen.

raum“ sei im Sinn einer Ausnahmeregelung nicht ausgeschlossen, solange kein untragbares Gesundheitsrisiko bestehe und es „keine Alternative“ gebe (Ziff. 3.2.2).

Spezifisch mit Blick auf die Belastung des Trinkwassers durch die Chlorothalonil-Metaboliten hatte das BLV die Kantone in der bereits früher erlassenen Weisung Nr. 2020/1 angewiesen, bei sämtlichen Höchstwertüberschreitung dafür zu sorgen, dass das Trinkwasser die neu eingeführten Grenzwerte einhält (Ziff. 3). Dazu müssen die kantonalen Vollzugsbehörden zunächst Sofortmassnahmen verfügen (Ziff. 4.1). Für den Fall, dass diese Sofortmassnahmen ungenügend sind, sieht die Weisung „weitergehende Massnahmen zur Einhaltung der Anforderungen der Lebensmittelgesetzgebung“ vor, die spätestens innert zweier Jahre ab der Beanstandung zu ergreifen sind (Ziff. 4.2). Ist die Umsetzung solcher weitergehenden Massnahmen innerhalb dieses Zeitraums „aus zeitlichen, finanziellen, politischen oder ökologischen Gründen nicht möglich“, steht es den Kantonen gemäss der Weisung jedoch offen, „eine der Situation angemessene Frist“ festzulegen (Ziff. 4.3). In jedem Fall verlangt das BLV, dass die betroffenen Konsumentinnen und Konsumenten regelmässig über die Ergebnisse der Qualitätskontrolle und die getroffenen Massnahmen zu informieren sind (Ziff. 4.5).

IV. Seitenblick: Rechtslage in der EU und Grenzwerte im benachbarten Ausland

1. EU

Im EU-Recht wird – wie in der PSMV[53] – zwischen der Genehmigung des Wirkstoffs und der Zulassung des Pflanzenschutzmittels unterschieden. Für die Genehmigung der Wirkstoffe ist die EU-Kommission zuständig.[54] Die Kompetenz für die Zulassung der Pflanzenschutzmittel liegt dagegen bei den einzelnen Mitgliedstaaten.[55] Voraussetzung für die Zulassung eines Pflanzenschutzmittels ist aber, dass die Wirkstoffe von der EU-Kommission genehmigt

53 Siehe vorne Ziff. III.1.

54 Art. 13 Abs. 2 Verordnung (EG) Nr. 1107/2009 vom 21. Oktober 2009 über das Inverkehrbringen von Pflanzenschutzmitteln und zur Aufhebung der Richtlinien 79/117/EWG und 91/414/EWG des Rates, ABl L 309, 1 ff.

55 Art. 28 Abs. 1 Verordnung (EG) Nr. 1107/2009.

worden sind.[56] Die Beurteilung der Trinkwasserrelevanz der einzelnen Metaboliten ist ebenso Aufgabe der Mitgliedstaaten.[57] Die EFSA gibt hierzu nur Empfehlungen ab.

2. Unterschiedliche Relevanzbeurteilung in Deutschland/ Österreich und Frankreich

Die Empfehlungen der EFSA in Bezug auf Relevanz-Bewertung des in der Schweiz hauptsächlich problematischen Metaboliten „R471811" wurden in den einzelnen EU-Mitgliedstaaten unterschiedlich umgesetzt:

a) Deutschland und Österreich

In Deutschland[58] und Österreich[59] wird der Metabolit „R471811" nicht als trinkwasserrelevant eingestuft. Für ihn gilt aber ein sog. „gesundheitlicher Orientierungswert" (D) bzw. „Aktionswert" (A) von 3,0 µg/l, der wesentlich weniger streng ist als der neue schweizerische Höchstwert. Diese Grenzwerte sind so angesetzt, dass sie genügend gewährleisten sollen, dass bei lebenslanger täglicher Aufnahme des Stoffes über das Trinkwasser ausreichend sicher keine Gesundheitsschädigungen beim Menschen zu erwarten sind.[60]

---

56 Art. 29 Abs. 1 Verordnung (EG) Nr. 1107/2009.

57 Vgl. aber den Leitfaden der EU-Kommission „Guidance document on the assessment of the relevance of metabolites in groundwater of substances regulated under Regulation (EC) No 1107/2009".

58 Vgl. Umweltbundesamt, Liste der bewerteten nicht relevanten Metaboliten, Fortschreibungsstand: November 2021, abrufbar unter <www.umweltbundesamt.de/sites/default/files/medien/5620/dokumente/gowpflanzenschutzmetabolite-20211109_0.pdf>.

59 Vgl. Bundesministerium Arbeit, Soziales, Gesundheit und Verbraucherschutz, Liste der Aktionswerte bezüglich nicht relevanter Metaboliten von Pflanzenschutzmittel-Wirkstoffen in Wasser für den menschlichen Gebrauch, zuletzt geändert am 4. August 2021, abrufbar unter <www.lebensmittelbuch.at/leitlinien/leitlinien-richtlinien-empfehlungen-usw-der-codexkommission/trinkwasser/aktionswerte-bezueglich-nicht-relevanter-metaboliten-von-pflanzenschutzmittel-wirkstoffen-in-wasser-fuer-den-menschlichen-gebrauch.html>.

60 Vgl. Umweltbundesamt, Leitfaden Gefährdungsbasiertes Risikomanagement für anthropogene Spurenstoffe zur Sicherung der Trinkwasserversorgung, 46 f., abrufbar unter <www.umweltbundesamt.de/themen/wasser/trinkwasser/trinkwasserqualitaet/toxikologie-des-trinkwassers/gesundheitlicher-orientierungswert-gow>.

b) Frankreich

Anders als in Deutschland und Österreich wird der Metabolit „R471811“ in Frankreich dagegen wie in der Schweiz als trinkwasserrelevant eingestuft. Für ihn gilt ebenfalls grundsätzlich ein strenger Höchstwert von 0,1 µg/l im Trinkwasser („limite de qualité réglementaire“).[61] Liegt die Belastung aber noch unterhalb eines Werts von 3,0 µg/l („valeur sanitaire transitoire“), der vom GOW des deutschen Umweltbundesamts übernommen wurde,[62] kann das Trinkwasser mit Zustimmung des Präfekten für eine Übergangsdauer von maximal 6 Jahren nach wie vor an die Konsumentinnen und Konsumenten abgegeben werden.[63]

V. Beschwerdeverfahren vor dem Bundesverwaltungsgericht[64]

1. Argumentation von Syngenta

Die Syngenta Agro AG hat im Januar 2020 beim Bundesverwaltungsgericht sowohl gegen das vom BLW erlassene Chlorothalonil-Verbot (Verfahren B-531/2020) als auch gegen die vom BLV vorgenommene Neubeurteilung der Chlorothalonil-Metaboliten „R417888“, „R419492“, „R471811“ und „R611965“ (Verfahren B-3340/2020) Beschwerde erhoben. Sie macht im Wesentlichen geltend, die Neueinstufung der Abbauprodukte als trinkwasserrelevant sei widersprüchlich, da das BLV in seinem eigenen Gutachten[65] zum Schluss gekommen sei, dass die genannten Abbauprodukte nicht als trinkwasserrelevant zu beurteilen seien. Dass sich das BLV nur kurze Zeit später der abweichenden Beurteilung durch die EFSA angeschlossen habe, sei aus wissenschaftlicher Sicht nicht nachvollziehbar. Darüber hinaus lägen den Behörden Gutachten vor, die

---

61 Agence nationale de sécurité sanitaire de l’alimentation, de l’environnement et du travail, Avis du 26 janvier 2022 relatif à la détermination de la pertinence pour les eaux destinées à la consommation humaine de métabolites de pesticide: chlorothalonil R471811, 2,6-dichlorobenzamide, diméthénamide ESA et diméthénamide OXA, N° de Saisine 2021-SA-0020, abrufbar unter <www.anses.fr/fr/content/avis-de-lanses-relatif-à-la-détermination-de-la-pertinence-pour-les-eaux-destinées-à-la-1>.

62 Direction générale de la Santé (DGS), Instruction du 24 mai 2022 N° DGS/EA4/2022/127, Bulletin officiel Santé - Protection sociale - Solidarité N° 2022/13 du 15 juin 2022 S. 380 ff., abrufbar unter <https://sante.gouv.fr/fichiers/bo/2022/2022.13.sante.pdf>.

63 Siehe Art. R 1321 31-1321 36 Code de la Santé Publique français (CSP).

64 Die Arbeiten zu diesem Artikel wurden im Juli 2023 abgeschlossen.

65 Vgl. dazu vorne Ziff. III.2.

aufzeigten, dass die beiden im Grundwasser hauptsächlich verbreiteten Metaboliten „R471811“ und „R417888“ für Mensch und Umwelt nicht gefährlich seien.[66] Syngenta verlangte zudem in prozessualer Hinsicht, dass das BLV für die Dauer des Verfahrens anzuweisen sei, die Publikationen betreffend Neubeurteilung von Chlorothalonil und dessen Abbaustoffen von seiner Webseite zu entfernen.

2. Zwischenverfügung vom 24. August 2020

Der zuständige Einzelrichter des Bundesverwaltungsgerichts ist mit Zwischenverfügung vom 24. August 2020 zum Schluss gelangt, dass bei einer weiteren Publikation der Informationen, wonach Chlorothalonil „wahrscheinlich krebserregend“ sei und sämtliche Metaboliten als trinkwasserrelevant einzustufen seien, ein allfälliger Schaden für Syngenta als Inhaberin von Bewilligungen für das Inverkehrbringen von Chlorothalonil-haltigen Pflanzenschutzmitteln als wahrscheinlich erscheine und es insbesondere bei längerer Verfügbarkeit und Verbreitung der beanstandeten Informationen schwieriger würde, diese Nachteile im Falle des Obsiegens rückgängig zu machen. Er hat daher das BLV für die Dauer des Verfahrens vorsorglich angewiesen, Chlorothalonil nicht mehr als wahrscheinlich krebserregend und die Chlorothalonil-Metaboliten „R417888“, „R419492“, „R471811“ sowie „R611965“ nicht mehr als trinkwasserrelevant zu bezeichnen.[67]

3. Zwischenverfügung vom 15. Februar 2021

In der Folge entfernte das BLV zwar die beanstandeten Ausführungen von seiner Webseite. Jedoch nahm es diese in die wenig später erlassene Weisung Nr. 2020/1 weitgehend wieder auf. Ausserdem wurde das Dokument „Relevanz von Pflanzenschutzmittel-Metaboliten im Grund- und Trinkwasser“, in dem die fraglichen Metaboliten als trinkwasserrelevant bezeichnet werden, neu auf der Webseite des BLW publiziert.[68] Auf Intervention der Syngenta hat das Bun-

---

66 Vgl. Syngenta, Mitteilung auf der Webseite vom 7. April 2022 „Syngenta begrüsst Zwischenentscheid des Bundesverwaltungsgerichts im Fall Chlorothalonil“, abrufbar unter <www.syngenta.ch/news/schweizer-landwirtschaft/syngenta-begruesst-zwischenentscheid-des-bundesverwaltungsgerichts-im>.

67 Zwischenverfügung vom 24. August 2020 im Verfahren B-3340/2020, Dispositiv-Ziff. 2 und 3, abrufbar unter <www.bvger.ch>.

68 ALDER.

desverwaltungsgericht mit einer zweiten Zwischenverfügung vom 15. Februar 2021 auch diese Publikation einstweilen unterbunden.[69] Der Hauptentscheid in der Sache steht nach wie vor aus.[70]

4. Unsicherheit in Bezug auf die aktuelle Rechtslage

Bis zur endgültigen gerichtlichen Klärung, bleibt vorderhand unklar, ob und wieweit die Trinkwasserversorgungen rechtlich verpflichtet sind, Massnahmen gegen die Belastung ihres Wassers durch Chlorothalonil-Metaboliten zu treffen. Der Bundesrat stellt sich auf den Standpunkt, dass das Bundesverwaltungsgericht mit den Zwischenverfügungen die Weisung 2020/1 nicht explizit widerrufen, sondern lediglich deren Publikation bis zum Hauptentscheid verboten habe. Deshalb seien die Höchstwerte nicht ausser Kraft gesetzt worden. Der Bundesrat wies aber darauf hin, dass das BLV den Kantonen in Bezug auf die Massnahmen, die von der Relevanz der Metaboliten ausgehen, Zurückhaltung empfohlen habe. Dies solle jedoch die Trinkwasserversorger und Kantone nicht daran hindern, Überlegungen und Investitionen für den zukunftsorientierten und nachhaltigen Trinkwasserschutz zu tätigen.[71]

VI. Beschränkte Handlungsoptionen für die Wasserversorgungen

1. Aktuelle Belastungssituation

Nach den jüngsten Angaben des BAFU[72] treten im Grundwasser trotz des seit Anfang 2020 geltenden Chlorothalonil-Verbots nach wie vor vier Metaboliten in Konzentrationen von mehr als 0,1 µg/l auf. Problematisch ist vor allem die anhaltende Belastung durch den Metaboliten „R471811", welcher den neuen Höchstwert landesweit an jeder dritten Grundwassermessstelle und im Mit-

---

69 Zwischenverfügung vom 15. Februar 2021 im Verfahren B-3340/2020, Dispositiv-Ziff. 2, abrufbar unter <www.bvger.ch>.

70 Der Europäische Gerichtshof ist im Urteil vom 6. Oktober 2021 in der Rechtssache T-518/19, ECLI:EU:T:2021:662 – Sipcam Oxon/Kommission, in Rz. 38 ff. zum Schluss gelangt, dass die EU-Kommission von der Trinkwasserrelevanz der umstrittenen Chlorothalonil-Metaboliten ausgehen durfte.

71 Vgl. Antwort von BR Berset anlässlich der Fragestunde im Nationalrat vom 13. Dezember 2021, Frage Nadine Masshardt, ABl 2021 N 2505.

72 BAFU, Bericht „Gewässer in der Schweiz, Zustand und Massnahmen", 2022, Ziff. 3.1.3, S. 28 f., abrufbar unter <www.bafu.admin.ch/bafu/de/home/themen/wasser/publikationen-studien/publikationen-wasser/gewaesserbericht.html>.

telland in 60% der Fälle überschreitet. Für den Metaboliten „R417888" ist dies im Mittelland an mehr als 20% der Messstellen der Fall. Es kann zwar davon ausgegangen werden, dass sich die Belastung im Grund- und Trinkwasser mit der Zeit verringern wird, da unterdessen kein neues Chlorothalonil mehr in die Böden und den Wasserkreislauf gelangt. Da aber gerade die im Trinkwasser hauptsächlich vorgefundenen Chlorothalonil-Metaboliten sehr langlebig sind und sich die Grundwasserreservoire in der Regel nur langsam erneuern, gehen Fachleute und Behörden davon aus, dass die Qualität des Grundwassers noch während Jahren beeinträchtigt bleibt.[73] Immerhin bestehen erste Messresultate, die auf eine leichte Abnahme der Belastung hindeuten.[74]

2. Sofortmassnahmen

Weil die Grundwasservorkommen grossflächig durch Chlorothalonil-Abbauprodukte belastet sind, erweisen sich die Handlungsoptionen der Trinkwasserversorgungen im Fall einer Grenzwertüberschreitung oftmals als beschränkt. In vielen Fällen ist es aus Kapazitätsgründen etwa nicht ohne weiteres möglich, auf die Nutzung der belasteten Fassungen zu verzichten. Es besteht in diesen Fällen zwar grundsätzlich die Möglichkeit, die Grenzwerte im abgegebenen Trinkwasser durch Mischen des Rohwassers von verschiedenen Bezugsorten unter den Grenzwert zu senken. Dies setzt allerdings voraus, dass alternative Wasserbezugsmöglichkeiten überhaupt vorhanden sind (z.B. mehrere Wasserfassungen oder Verbindungsleitungen zu benachbarten Wasserversorgungen). Ferner ist das Wasser von diesen alternativen Bezugsorten oftmals ebenfalls mit Chlorothalonil-Metaboliten belastet. Als Sofortmassnahme reicht das Mischen des Rohwassers deshalb regelmässig nicht aus, um die Höchstwerte einzuhalten.

3. Weitergehende Massnahmen

Neben diesen Sofortmassnahmen kommen nur noch relativ aufwändige Massnahmen wie etwa der Bau von neuen Wasserfassungen oder von Verbindungsleitungen zu anderen Wasserversorgungen in Frage. Dies bedingt jedoch, dass noch ungefasste Wasserressourcen im Einzugsgebiet zur Verfügung stehen bzw. dass benachbarte Trinkwasserversorgungen willens und in der Lage sind, überschüssiges Wasser abzugeben. Hinzu kommt, dass solche Projekte in der

---

73 Vgl. HINTZE et al.

74 Vgl. etwa Baudirektion des Kantons Zürich, Bericht „Wasser und Gewässer 2022", Januar 2023, 114, abrufbar unter <www.zh.ch/de/umwelt-tiere/wasser-gewaesser/gewaesserschutz/gewaesserqualitaet.html>.

Regel mit langen Vorabklärungen und hohen Kosten verbunden sind. Im Übrigen ist es auch möglich, die Chlorothalonil-Rückstände mit technischen Mitteln im Rahmen einer Wasseraufbereitung aus dem Wasser zu entfernen. Gemäss einer Studie der Eawag bietet sich aber hierfür als einzige gut geeignete Methode die sog. Nanofiltration bzw. Umkehrosmose an.[75] Diese Aufbereitungsmethode ist in der Schweiz noch wenig erprobt und ebenfalls sehr teuer. Gemäss einer Studie ist beim Bau einer solchen Anlage mit einer Erhöhung der Trinkwasserkosten von bis zu 50% zu rechnen.[76] In jüngerer Zeit durchgeführte Pilotversuche haben zwar gezeigt, dass sich das Rohwasser ebenfalls mit Aktivkohle säubern lässt.[77] Allerdings ist davon auszugehen, dass auch diese Aufbereitungsmethode nicht wesentlich kostengünstiger ist.[78]

4. Haltung des Fachverbands

Die Schweizerische Verein des Gas- und Wasserfachs (SVGW) stuft die technische Aufbereitung von Grundwasser zur Lösung des Chlorothalonil-Problems lediglich als „Übergangslösung in gewissen Fällen" ein, lehnt „flächendeckende Investitionen" in die Wasseraufbereitung aber grundsätzlich als unverhältnismässig ab. Nach seiner Auffassung würde eine systematische Aufbereitung des Trinkwassers ausserdem zu einer Aushöhlung des Vorsorge- und Verursacherprinzips führen und auch nicht dem Wunsch der Konsumentinnen und Konsumenten nach möglichst natürlichem Trinkwasser entsprechen.[79]

---

75 Vgl. Eawag, Factsheet vom Februar 2020 „Chlorothalonil-Metaboliten: Eine Herausforderung für die Wasserversorg", abrufbar unter <www.eawag.ch/de/info/portal/aktuelles/news/chlorothalonil-fordert-wasserversorger>.

76 Vgl. Rieck et al.

77 Caprez.

78 Jeckelmann.

79 Vgl. SVGW, Positionspapier vom 15. März 2023 „Wasseraufbereitung und Ressourcenschutz", abrufbar unter <www.svgw.ch/media/8965/positionspapier_aufbereitung-und-ressourcenschutz.pdf>; SVGW, Kommentar vom 14. September 2020 zur BLV-Weisung 2020/1, abrufbar unter <www.svgw.ch/wasser/dossiers/dossier-chlorothalonil/weisung-blv>; Blog-Beitrag des SVGW-Direktors vom 27. Dezember 2021 „Gretchenfrage Wasseraufbereitung" vom 27. Dezember 2021, <www.aquaetgas.ch/svgw-news/blog/20211227_gretchenfrage-wasseraufbereitung>.

VII. Chlorothalonil-Problematik als Anwendungsfall des Vorsorgeprinzips

1. Tragweite des Vorsorgeprinzips

Das Vorsorgeprinzip ist für den Bereich des Umweltrechts in Art. 74 Abs. 2 Satz 1 BV und Art. 1 Abs. 2 USG sowie für den Bereich des Lebensmittelrechts in Art. 22 LMG positivrechtlich verankert.[80] In materieller Hinsicht verlangt es, dass jede Einwirkung auf die natürliche Umwelt und mittelbar auf den Menschen, die – allein oder zusammen mit anderen Einwirkungen – schädlich oder lästig sein könnte, frühzeitig am Ort ihres Entstehens zu begrenzen ist. Zudem beinhaltet es eine „Entscheidungsregel für den Fall der Unsicherheit"[81], d.h. für Situationen, in denen eine zuverlässige quantitative Abschätzung des Risikos nicht möglich ist. Gemäss dem Bundesgericht bedeutet das Vorsorgeprinzip, dass „in solchen Situationen der Ungewissheit […] den Unsicherheiten mit einer Sicherheitsmarge Rechnung zu tragen ist"[82].

Beim Vorsorgeprinzip handelt es sich insofern um eine Vorgehensweise zum rechtlichen Umgang mit dem Risiko, die verlangt, dass potenziellen Schädigungen möglichst präventiv am Ort ihres Ursprungs zu begegnen ist. Allerdings gilt dieses Präventionsgebot nicht absolut; vielmehr werden ihm durch andere verfassungsrechtlichen Prinzipien wie namentlich den Grundsatz der Verhältnismässigkeit Grenzen gesetzt. Verlangt wird daher grundsätzlich keine „Null-Risiko-Strategie", sondern nur, dass das Eintreten möglicher Schädigungen auf ein vernünftiges Mass reduziert wird (sog. ALARA-Prinzip, „As Low As Reasonably Achievable").[83] Entsprechend hat auch das Bundesgericht in seiner Rechtsprechung festgehalten, dass das Vorsorgeprinzip „nicht bedeuten [kann], dass alle hypothetischen Risiken unzulässig sind"[84].

Der Grundsatz der Vorsorge gilt sowohl in der Rechtsetzung als auch in der Rechtsanwendung: Die rechtsetzenden Organe sind im Sinne eines Optimierungsgebots gehalten, dem Vorsorgeprinzip im positiven Recht so gut wie möglich Ausdruck zu verleihen. In der Rechtsanwendung wirkt der Grundsatz

---

80 Es ist unklar, ob das Vorsorgeprinzip darüber hinaus als allgemeiner Rechtsgrundsatz gilt. Vgl. BGE 132 II 305 E. 4.3; Griffel/Rausch, Komm. USG Ergänzungsband, Art. 1 N. 20; Thurnherr, Rz. 68.

81 Griffel/Rausch, Komm. USG Ergänzungsband, Art. 1 Rz. 19.

82 BGE 131 II 431 E. 4.4.4, 124 II 219 E. 8a.

83 SGK-BV, Morell/Vallender/Hettich, Art. 74 Rz. 27.

84 BGE 131 II 431 E. 4.4.4.

hauptsächlich als „Auslegungs- und Konkretisierungshilfe", welche die Interpretation der unbestimmten Rechtsbegriffe im Einzelfall in eine bestimmte Richtung lenkt und die vorzunehmenden Interessenabwägungen beeinflusst.[85]

2. Vorsorgeprinzip im Lebensmittelrecht

Für den Bereich der Lebensmittelsicherheit sieht Art. 22 LMG vor, dass die zuständige Bundesbehörde gestützt auf das Vorsorgeprinzip vorläufige Massnahmen zur Sicherstellung eines hohen Gesundheitsschutzniveaus treffen kann, wenn sie nach einer Auswertung der verfügbaren Informationen feststellt, dass ein Lebensmittel oder ein Gebrauchsgegenstand gesundheitsschädliche Auswirkungen haben könnte, aber wissenschaftlich noch Unsicherheit besteht. Im Rahmen der Umsetzung des Vorsorgeprinzips ist gemäss Art. 21 LMG grundsätzlich eine Risikoanalyse vorzunehmen, welche eine Risikobewertung, ein Risikomanagement und eine Risikokommunikation umfasst.[86] Während die Risikobewertung die möglichst gute Abschätzung des Schädigungspotenzials mit Hilfe des naturwissenschaftlichen Sachverstands bezweckt,[87] soll im Rahmen des Risikomanagements vor dem Hintergrund des unvollständigen wissenschaftlichen Kenntnisstands eruiert werden, welche Risiken zu welchem Preis von den Betroffenen bzw. der Gesellschaft akzeptiert werden müssen und welche Massnahmen zur Reduktion der Risikoexposition letztlich zu ergreifen sind. Hierbei sind insbesondere auch gesellschaftliche und wirtschaftliche Gesichtspunkte sowie die Vollziehbarkeit zu berücksichtigen.[88] Die Risikokommunikation verlangt schliesslich, dass die Öffentlichkeit und die Betroffenen transparent darüber zu informieren sind, welche Prämissen der Risikobeurteilung zugrunde gelegt, welche Wirkungen in Betracht gezogen und wie diese gewichtet werden.[89]

3. Umsetzung des Vorsorgeprinzips als Zusammenspiel verschiedener Akteure in Bund und Kantonen

Wie in den vorangehenden Ausführungen aufgezeigt wurde, sind im Kontext der Chlorothalonil-Problematik verschiedene Behörden auf unterschiedlichen Staatsebenen in die Umsetzung des Vorsorgeprinzips involviert. Während die Identifikation des von den Chlorothalonil-Metaboliten ausgehenden Gesund-

85 Thurnherr, Rz. 88.
86 Marti, 241 ff.
87 Marti, 241 ff.
88 Marti, 243 ff.
89 Marti, 245 ff.

heitsrisikos ursprünglich durch die EU-Behörden erfolgte, fand und findet die Risikoanalyse sowie das Festlegen der konkreten Massnahmen innerhalb der Schweiz im Zusammenspiel von verschieden Behörden in Bund und Kantonen sowie den betroffenen Wasserversorgungen statt.

Die Risikobewertung wurde im Wesentlichen vom BLV und dem BAFU sowie den Kantonschemikern durchgeführt. Während das BLV zunächst im Rahmen der Gezielten Überprüfung das Gefährdungspotenzial der im Trinkwasser vorhandenen Chlorothalonil-Metaboliten ermittelte, haben das BAFU und die Kantonschemiker anhand von Grund- und Trinkwasseruntersuchungen zwecks Abschätzung der Risikoexposition eruiert, wie stark die Pflanzenschutzmittelrückstände im Grundwasser verbreitet sind. Aufgrund der Weisungen des BLV[90] ist es nunmehr auch Aufgabe der Wasserversorgungen, im Rahmen der lebensmittelrechtlichen Selbstkontrolle, die konkrete Belastung des Trinkwassers in ihrem Versorgungsgebiet zu überwachen.

Die zentrale Aufgabe des Risikomanagements (Festlegen der konkreten Massnahmen) wurde und wird ebenfalls im Zusammenspiel verschiedener Behörden auf Bundesebene und kantonaler Ebene wahrgenommen: Die vom Vorsorgeprinzip gebotene Beschränkung des Risikos am Ort seiner Entstehung wurde mit dem Chlorothalonil-Verbot von der Zulassungsstelle für Pflanzenschutzmittels (damals BLV) und damit vom Bund verfügt (sog. „Quellenstopp“). Das Risikomanagement im Bereich der Trinkwasserversorgung (sog. „End of pipe-Massnahmen“) obliegt dagegen im Wesentlichen den Kantonen und Wasserversorgungen. Wie im Fall einer Grenzwertüberschreitung vorzugehen ist bzw. welche konkreten Massnahmen zu treffen sind, ist letztlich von ihnen zu entscheiden. Aus den Weisungen des BLV ergeben sich kaum konkrete Anhaltspunkte, wie die verschiedenen zu berücksichtigenden Interessen in einem solchen Fall zu bewerten sind.

Auch die Kommunikation über die mit den Chlorothalonil-Metaboliten im Trinkwasser verbundenen Gesundheitsrisiken obliegt gleichzeitig verschiedenen Akteuren: Gemäss Art. 24 Abs. 1 Bst. b LMG haben die Behörden die Öffentlichkeit über Lebensmittel zu informieren, bei denen ein hinreichender Verdacht besteht, dass sie ein Risiko für die Gesundheit mit sich bringen können. Da im vorliegenden Fall mehrere Kantone von diesen Belastungen betroffen sind, fällt nach Art. 54 Abs. 2 LMG den Bundesbehörden grundsätzlich die Aufgabe zu, die Bevölkerung zu informieren und Verhaltensempfehlungen

[90] Siehe vorne Ziff. III.3.

abzugeben.[91] Entsprechende Informationen zum Thema Chlorothalonil finden sich auf der Webseite des BLV allerdings derzeit keine.[92] Gemäss der BLV-Weisung Nr. 2020/1 sind die Kantone bzw. Wasserversorgungen im Rahmen der Risikokommunikation sodann dazu verpflichtetet, die Bevölkerung über die konkreten Metaboliten-Belastungen in den verschiedenen Versorgungsgebieten zu informieren[93] sowie die Anordnung von bestimmten Massnahmen bzw. den Verzicht auf solche öffentlich zu kommunizieren.[94]

VIII. Auswirkungen für die Kantone und die Gerichte

1. Kantone

Auch wenn das weitere rechtliche Schicksal der neu eingeführten Grenzwerte derzeit noch unklar ist, sind die Kantone gut beraten, sich im Austausch mit den Wasserversorgungen bereits heute damit auseinanderzusetzen, wie sie mit der Chlorothalonil-Problematik umgehen wollen, da sich gezeigt hat, dass die über dem Grenzwert liegenden Konzentrationen vielerorts mit Sofortmassnahmen allein nicht ausreichend gesenkt werden können. Da sich das Problem aufgrund der Langlebigkeit der Chlorothalonil-Metaboliten oftmals auch nicht durch „Aussitzen" lösen lässt, werden die kantonalen Lebensmittelbehörden möglicherweise in zahlreichen Fällen darüber zu befinden haben, ob das belastete Trinkwasser nach wie vor an die Konsumentinnen und Konsumenten abgegeben werden darf oder ob die Trinkwasserversorgung einzuschränken oder gar einzustellen ist. Das BLV hat mit der Weisung Nr. 2020/1 allerdings lediglich einen groben Handlungsrahmen vorgegeben, wie das Vorsorgeprinzip in einem solchen Fall umzusetzen und die zu berücksichtigenden Interessen konkret zu bewerten sind. Da davon auszugehen ist, dass den betroffenen Kantonen und Wasserversorgungen zur Bewältigung des Chlorothalonil-Problems hohe Investitionskosten bevorstehen, werden sie nicht umhinkommen, sich Gedanken darüber zu machen, wie sie bestehenden Zielkonflikte zwischen dem Gesundheitsschutz, dem Trinkwasserversorgungsauftrag und den Massnahmenkosten vornehmen wollen. Dabei werden sie sich insbesondere auch die Frage stellen müssen, wie weit grössere Investitionen in die Versorgungsinfrastruktur auch bei geringen Grenzwertüberschreitungen angesichts des nicht klar nachgewiesenen Gesundheitsrisikos noch ver-

---

91 Art. 54 Abs. 2 LMG.

92 Eine Suche mit dem Stichwort Chlorothalonil im Suchfeld der Webseite ergab keine Treffer.

93 Vgl. auch Art. 5 TBDV.

94 Siehe vorne Ziff. III.3.

hältnismässig sind bzw. ab welcher Belastung dies grundsätzlich der Fall ist. In der Bundesversammlung wurden in diesem Zusammenhang bereits Vorstösse eingereicht, die eine Mitfinanzierung des Bundes verlangen.[95] Da die Trinkwasserqualität in weiten Teil der Bevölkerung ein sensibles Thema ist und entsprechende Ängste vor den Auswirkungen von solchen Verunreinigungen bestehen, bedarf der Umgang der Kantone und deren Wasserversorgungen mit dem Chlorothalonil-Problem „Fingerspitzengefühl". Im Falle der Bestätigung der neuen Grenzwerte wird es ihnen obliegen, in diesem auch politisch heiklen Bereich mit Augenmass zusammen mit den Trinkwasserversorgungen einzelfallgerechte und verhältnismässige Lösungen zu erarbeiten, die auch von den betroffenen Trinkwasserkonsumentinnen und -konsumenten akzeptiert werden können.

2. Gerichte

Sollten die neuen Grenzwerte gerichtlich standhalten, ist anzunehmen, dass es auch bei der Umsetzung der notwendigen Massnahmen zu Streitigkeiten vor den Gerichten kommen wird. Der Überprüfung durch die Justiz sind allerdings insofern relativ enge Grenzen gesetzt, als mangels solider (naturwissenschaftlicher) Entscheidungsgrundlage rechtlich nur schwer zu beurteilen ist, ob die einzelnen Interessen in einer „Situation der Ungewissheit" vernünftig gewichtet worden sind. Dies gilt umso mehr, da zahlreiche Interessen gleichzeitig zu berücksichtigen sind, die sich durch eine hohe Technizität auszeichnen und eine komplexe Gesamtfolgenabschätzung erfordern. Zudem ist aus rechtlicher Sicht unklar, ob und inwiefern die Ängste bzw. die Risikoaversion in der Bevölkerung zu berücksichtigen sind.[96] Wie die verschiedenen Rechtsgüter im Einzelfall relativ zueinander zu bewerten bzw. welche konkreten Massnahmen zu treffen sind, ist daher normativ nur vage vorgegeben. Die Wahl der im Einzelfall angemessenen Massnahmen dürfte daher weitgehend eine politische und keine rechtliche Frage sein und zu weiten Teilen im Ermessen der Verwaltungsbehörden liegen.[97] Materiell lässt sich in diesem Zusammenhang gerichtlich wohl regelmässig im Wesentlichen nur überprüfen, ob die der Entscheidung zugrunde liegenden Wertungen ausreichend offengelegt wurden und ob aufgezeigt wurde, inwiefern diese auf die Rechtsordnung abgestützt werden können.[98]

---

95 Vgl. etwa Motion 20.3022 Felix Wettstein vom 2. März 2020, „Finanzielle Beteiligung des Bundes an den notwendigen Sanierungsmassnahmen".

96 Dazu THURNHERR, Rz. 109 ff.

97 Vgl. MARTI, 244.

98 Vgl. THURNHERR, Rz. 110.

IX. Fazit

Zusammenfassend lässt sich festhalten, dass der Umgang mit der Chlorothalonil-Problematik auf Ebene des Bundes insbesondere hinsichtlich seiner Auswirkungen für die Kantone bzw. Trinkwasserversorgungen nicht in jeder Hinsicht zu überzeugen vermag. Einerseits ist im Sinne der Vorsorge zwar nicht zu beanstanden, dass der Bund nach dem Bekanntwerden der möglichen Gesundheitsrisikos das Chlorothalonil-Verbot von der EU auch in der Schweiz übernommen hat, zumal für den Schutz der Kulturen offenbar ausreichend andere Wirkstoffe zur Verfügung stehen.[99] Indem er für sämtliche Chlorothalonil-Metaboliten einen neuen strengen Grenzwert eingeführt hat und grundsätzlich deren Einhaltung verlangt, setzt er die Kantone und Trinkwasserversorgungen allerdings unter erheblichen Handlungsdruck, lässt gleichzeitig aber weitgehend offen, welches Gesundheitsrisiko im Fall einer Grenzwertüberschreitung besteht und welche rechtliche Bedeutung dem neuen Grenzwert genau zukommt. Im Unterschied zu Deutschland[100] hat – soweit ersichtlich – keine umfassende Bewertung der verfügbaren wissenschaftlichen Daten bzw. des Grades der wissenschaftlichen Ungewissheit zur Festlegung eines auf das spezifische Risiko abgestimmten Grenzwerts stattgefunden. Da die Risikobewertung Ausgangspunkt und zentrale Grundlage der Entscheidung über die im Einzelfall zu treffenden, zum Teil weitreichenden Massnahmen bildet, wären klarere Vorgaben durch den Bund jedoch wünschenswert, zumal mit den gegebenenfalls anstehenden Infrastrukturmassnahmen möglicherweise wichtige Weichen für die zukünftige Wasserversorgung gestellt werden. Zu denken ist dabei etwa an eine differenziertere Regelung mit abgestuften Grenzwerten und verschiedenen Interventionsstufen. Der Bund könnte so festlegen, ab welcher Belastung zwar ein grundsätzlicher, nicht aber absolut dringender Handlungsbedarf besteht und ab welcher Konzentration von einem nicht mehr hinnehmbaren Gesundheitsrisiko auszugehen ist.

Indem der Bund bisher auf präzisere Handlungsanweisungen verzichtet hat, belässt er die Kantone und Wasserversorgungen nicht nur in einer problematischen Rechtsunsicherheit in Bezug auf die vorzunehmenden komplexen Interessenabwägungen, sondern überlässt ihnen auch weitgehend die (politische) Verantwortung für den konkreten Umgang mit dem Chlorothalonil-Problem. Ausserdem befürchten Trinkwasserexperten, dass ohne aktivere Rolle

---

99 Vgl. Schweizer Bauernverband, Medienmitteilung vom 8. November 2019 „Verzicht auf Chlorothalonil-haltige Pflanzenschutzmittel“, abrufbar unter <www.sbv-usp.ch/de/verzicht-auf-chlorothalonil-haltige-pflanzenschutzmittel>.

100 Vgl. vorne Ziff. IV.2.a), insb. Fn. 62.

des Bundes wichtige Erfahrungen zu wenig ausgetauscht werden und ein föderalistischer „Flickenteppich“ entsteht.[101] Hinzu kommt, dass in den vergangenen Jahren neben den Chlorothalonil-Rückständen weitere unerwünschte und möglicherweise gesundheitsgefährdende Fremdstoffe im Trinkwasser vorgefunden wurden (etwa Arzneimittel-Rückstände oder sog. „Forever chemicals“).[102] Sinnvollerweise sind auch diese Belastungen bei den möglicherweise weitreichenden Investitionsentscheidung in die künftige Trinkwasserversorgungsinfrastruktur mitzuberücksichtigen. Da überdies nicht nur im Hinblick auf die Trinkwasserqualität, sondern auch in Bezug auf die quantitative Versorgungsicherheit verschiedene weitere infrastrukturelle Herausforderungen bestehen,[103] wären differenziertere Leitlinien des Bundes im Rahmen einer kohärenten gesamtschweizerischen Lösungsstrategie auch aus einer ganzheitlichen Sicht auf die Trinkwasserversorgung zu begrüssen, zumal namentlich die kleineren Kantone mit der sich dabei stellenden naturwissenschaftlichen und technischen Komplexität allein oftmals überfordert sind. Dazu müsste auf Bundesebene allerdings eine bereitere politische Diskussion geführt werden, als dies bisher der Fall war.

Literaturverzeichnis

Alder Katrin, Streit um verunreinigtes Trinkwasser: Der Bund wird vom Bundesverwaltungsgericht erneut in die Schranken gewiesen, NZZ vom 18. Februar 2020, <www.nzz.ch/schweiz/verunreinigtes-trinkwasser-bund-wird-in-schranken-gewiesen-ld.1602337>

Caprez Cathrin, Verschmutztes Grundwasser – Mit einem Aktivkohle-Filter lässt sich Trinkwasser säubern, SRF-online vom 2. Februar 2023, abrufbar unter: <www.srf.ch/wissen/nachhaltigkeit/verschmutztes-grundwasser-mit-einem-aktivkohle-filter-laesst-sich-trinkwasser-saeubern>.

Ehrenzeller Bernhard et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 4. A., Zürich/St. Gallen 2023 (zit. SGK BV-Bearbeiter/in, Art. XX Rz. YY).

Griffel Alain/Rausch Heribert, Kommentar zum Umweltschutzgesetz, Ergänzungsband zur 2. A., Zürich 2011 (zit. Griffel/Rausch, Komm. USG Ergänzungsband, Art. XX Rz. YY).

---

101 Vgl. Interview mit Prof. Urs von Gunten von der Eawag, in Wissenschaftsmagazin SRF Kultur vom 28. Januar 2023, abrufbar unter <www.srf.ch/audio/wissenschaftsmagazin/bald-wieder-sauberes-trinkwasser?id=12323020>.

102 Häusler.

103 Vgl. dazu etwa BAFU, Bericht „Grundlagen für die Wasserversorgung 2025, Risiken, Herausforderungen und Empfehlungen“, 2014, abrufbar unter <www.bafu.admin.ch/bafu/de/home/themen/wasser/publikationen-studien.html>.

Häusler Thomas, Chemikalien für die Ewigkeit – PFAS: Das Gift, das in unseren Alltagsgegenständen lauert, SRF-online vom 12.02.2022, abrufbar unter: <www.srf.ch/wissen/chemikalien-fuer-die-ewigkeit-pfas-das-gift-das-in-unseren-alltagsgegenstaenden-lauert>.

Hettich Peter/Jansen Luc/Norer Roland (Hrsg.), Kommentar zum Gewässerschutzgesetz und zum Wasserbaugesetz, Zürich/Basel/Genf 2016 (zit. Komm. GSchG/WBG-Bearbeiter/in, Art. XX Rz. YY).

Hintze et al., Langzeitverhalten von Chlorothalonil-Metaboliten, 5. Juli 2021, Aqua & Gas, abrufbar unter <www.aquaetgas.ch/wasser/trinkwasser/20210705_ag7_langzeitverhalten-von-chlorothalonil-metaboliten-im-grundwasser>.

Jeckelmann Brigitte, Aufbereitung von Trinkwasser im Seeland wird wohl teurer, Bieler Tagblatt vom 31. Mai 2022, abrufbar unter <https://web.bielertagblatt.ch/node/2162083>.

Kiefer Karin et al., Pflanzenschutzmittel-Metaboliten im Grundwasser – Ergebnisse aus der NAQUA-Pilotstudie „Screening", Aqua & Gas, No 11 | 2019, 14-23.

Klauser Lucia, Zusammenfassung der Präsentation: „Zulassung und Überprüfung von Pflanzenschutzmitteln", URP 2022, 711 ff.

Klemm Urs/Uebe Wesselina, Risikoanalyse im Lebensmittelrecht, Sicherheit & Recht 2018, 137 ff.

Lagger Annemarie, Anforderungen an Lebensmittel und Gebrauchsgegenstände in: Daniel Donauer/Hugh Reeves/Celine Weber (Hrsg.), Lebensmittel- und Gebrauchsgegenständerecht, Zürich/Basel/Genf 2020, 33 ff.

Marti Ursula, Das Vorsorgeprinzip im Umweltrecht – Am Beispiel der internationalen, europäischen und schweizerischen Rechtsordnung, Diss., Genf 2011.

Rieck Tobias, Leuzinger Florence, Ehrensberger Hannes, Jacob Axel, Scheel Harald, Grundwasseraufbereitung – Umkehrosmose mit Remineralisierung, 25. November 2021, Aqua & Gas, abrufbar unter <www.aquaetgas.ch/wasser/trinkwasser/20211125_ag12_umkehrosmose-mit-remineralisierung>.

Thurnherr Daniela, Vorsorgeprinzip: Verpflichtungen und Grenzen für die Verwaltung und weitere staatliche Akteure, Rechtsgutachten im Auftrag des BAFU, Basel 2020.

Digital Sovereignty in Switzerland: the laboratory of federalism

Yaniv Benhamou / Frédéric Bernard / Cédric Durand*

This paper analyses the issues of digital sovereignty in Switzerland, particularly from a socio-economic and legal standpoint. It aims to contribute to the general debate on digital sovereignty in Switzerland and abroad, including on a Swiss cloud. Beyond Switzerland, the specificities of the Confederation (federalism and distributed competencies) make its ecosystem an interesting laboratory for digital sovereignty. This analysis follows a complete multidisciplinary study carried out within the framework of the Latin Conference of Digital Directors (CLDN), based on desk research and interviews.

Content

I. Introduction and definitions 68
1. Background 68
2. Definitions 70
a) Concepts 70
b) Components 71
c) Territories 72
d) Actors 72

* Yaniv Benhamou is associate professor of Digital law at the Faculty of Law of the University of Geneva and specialized in data protection, intellectual property, internet and media law. He is admitted to the Geneva Bar and Attorney-at-law Of Counsel in a Geneva law firm. Frédéric Bernard is professor of Public Law at the University of Geneva and is specialized in administrative law, constitutional law, human rights and the fight against terrorism. In 2010, he was a visiting scholar at the University of California, Berkeley. He is admitted to the Geneva Bar and is Of Counsel in a Geneva law firm. Cédric Durand is economist, associate professor at the University of Geneva and member of the Centre d'économie Paris Nord. Working within the tradition of Marxist and French Regulationist Political Economy, he studies globalization, financialization and contemporary mutations of capitalism. The authors would like to thank M. Ammihud Joseph (researcher at the Digital Law Center) for his help in translating and finalizing the text.

3. Digital sovereignty intitiatives 73

II. Socio-economic issues 75
1. Swiss ICT capacities 76
2. Material dependence 76
3. Intellectual dependence 77
4. Recommendations 78

III. Legal issues 82
1. Data Sovereignty 83
a) Extra-territoriality of laws 83
b) Data transfer abroad 84
c) Digital self-determination 86
2. Technological sovereignty 87
3. Cyberadministration 88
a) Federalism and the distribution of powers 88
b) Three steps of the implementation of public policy 89
c) Principle of rule of law 91
d) Public procurement law 92
4. Cybersecurity 93
5. Recommendations 95

Bibliography 96

Executive Summary

Digital sovereignty can be defined as the ability of authorities to maintain their strategic autonomy, i.e. to be able to autonomously use and control the tangible and intangible assets and digital services that impact the economy, society, and democracy. Digital sovereignty has several components, mainly "technological sovereignty" and "data sovereignty". Digital technology redefines the notion of "territory" into "sovereignty on networks", which has several layers (hardware, software, and data), with the State being able to exercise exclusive sovereignty over the 1st layer (hardware) and limited sovereignty over the 2nd and 3rd layers (software and data). Finally, the degree of sovereignty is assessed according to the State's ability to control each layer, which will depend in particular on the location of the data or access to the data, and the nature and links of the service provider with the State in question. Policy and regulatory strategies may also address the different actors in the digital ecosystem (public, industry, and civil society).

From the socio-economic standpoint, the study analyses Switzerland's dependencies on the three layers (hardware, software, data) and from the point of view of the different actors (public, industry, civil society). It concludes that Switzerland has strong digital assets but that there are issues to watch out for, in particular the fact that consumer digital activity and intellectual property are concentrated in the hands of a few companies (with effects on privacy, public policy, and economic development). It also describes an autonomy-sophistication dilemma: dependencies increase in proportion to the intensity of ICT use. Consequently, measures shall be taken according to the degree of criticality. When the use is critical and complex, measures may range from data residency (or data localisation) to diversification of suppliers and shared sovereignty. The analysis also emphasises that sovereignty is not only spatial but also temporal, i.e. in terms of the ability to anticipate and react to a new situation.

From the legal standpoint, the study analyses the main components of digital sovereignty, namely data sovereignty and technological sovereignty, as well as cyberadministration and cybersecurity. Data sovereignty requires to clarify the law, including those that may have extra-territorial effects (e.g. GDPR, Cloud Act, LPD)[1] and rules on international data transfers, which may range from the free flow of data to a requirement for the localisation of data or servers. Technological sovereignty requires an innovation policy with state measures (legal, economic, and technical). This requires a careful assessment of which critical technologies (Key Enabling Technologies or KETs) can be accessed and which data protection laws apply. Cybersecurity requires coordination at different levels, depending on the area concerned (civil cybersecurity, cyberdefense, cybercrime), and requires resilient technology, adequate preparation, appropriate contracts, and compliance monitoring processes. Cyberadministration requires that the State can decide whether and how to digitise its processes and services autonomously while respecting the principles of federalism, legality, and public procurements.

[1] GDPR stands for the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 4.5.2016, 1-88; Cloud Act stands for Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943, 2018); LPD stands for the Swiss Data Protection Act, Loi sur la protection des données of 25 September 2020, FF 2020 7397.

On this basis, several recommendations can be made to guide public action on digital sovereignty (see II.4 and III.5)[2]. At the international level, it is also important to pursue determined diplomatic action to reduce the negative repercussions of digital sovereignty (fragmentation of the Internet, barriers to data sharing and innovation).

I. Introduction and definitions

1. Background

This paper aims to contribute to the general debate on digital sovereignty in Switzerland and abroad, including on Swiss cloud[3]. Beyond Switzerland, the specificities of the Confederation (federalism and distributed competencies) make its ecosystem an interesting laboratory for digital sovereignty[4]. This analysis follows a complete multidisciplinary study carried out within the framework of the Latin Conference of Digital Directors (CLDN), based on desk research and interviews.

Digital sovereignty presupposes that the state, the economy and society have ongoing control over their digital transformation, i.e. that they can determine whether and what information to digitize for re-use[5]. Although governments have technical expertise in this area (as shown in the rapid development of Covid applications), it is often the private sector that has control over ICT. This applies not only to market-dominant economic actors (e.g. GAFAM and BHATX)[6] who decide on the faith of data, or even replace state prerogatives

---

2 For an overview of all recommendations, see the complete report Benhamou/Bernard/Durand, 41 ff.

3 FDF/UPIC, Swiss Cloud Report; Swiss Digital Strategy 2023: These 2 reports consider the issues of Cloud and digital sovereignty as priorities and conclude that there is a need to clarify the concepts (e.g. terminology, degrees of sovereignty) and the legal framework (e.g. to reduce the risks of data access by third parties, such as foreign authorities). The purpose of this contribution is precisely to answer these questions.

4 For an analysis of the EU, see Brunessen, 15 ff; Moghior, 104, highlighting the difficulty of finding a consensus due to the decentralised nature of the institutions and the heterogeneity of the Member States. The Swiss example can be another example of decentralised institutions that neighboring countries could learn from, with its governance and consensus mechanisms.

5 Tan/Chi, 1; FDF/UPIC, Swiss Cloud Report.

6 GAFAM stands for the US tech giants, namely Google (Alphabet), Apple, Facebook (Meta), Amazon and Microsoft; BHATX stands for the Chinese tech giants, namely Baidu, Huawei, Alibaba, Tencent and Xiaomi.

(e.g. via their general terms of use, authentication techniques, or by making states dependent on their services with digital currencies or reliable authentication techniques) but also to non-market-dominant actors who create dependencies with other operators[7]. Economic actors thus acquire *de facto* normative power in cyberspace[8].

Given the emergence of new power relations, politicians frequently use the concept of digital sovereignty in their speeches with the aim of restoring the centrality of the nation-state[9]. However, this concept is not yet clarified, making achieving coherence at the decision-making and operational levels difficult. The rapid proliferation of initiatives in digital sovereignty also complicates the delimitation of the concept and the distribution of powers between the different levels of the state. The diversity of initiatives can be highlighted by models or indexes that quantify digital sovereignty based on indicators, such as the components of digital sovereignty[10]. However, these models vary according to the country and/or entity concerned, and no such model exists in Switzerland at the moment.

It is worth noting that, while it is logical for Switzerland to take a position on digital sovereignty, this debate may also have negative repercussions on society, such as the fragmentation of the Internet, barriers to data sharing for the common good and to innovation (e.g. the development of technologies such as web3)[11].

---

7 COTTIER, N 8; TÜRK and references; JÄGER et al., 189.

8 TÜRK and references; POHLE/THIEL, 6 ff; SEIFRIED/BERTSCHEK, 10 ff.

9 FALKNER et al., 3; AUFRECHTER/KLOSSA, 11, indicating that the concept of digital sovereignty is also used as a pretext for economic protectionism, referring to a US government report of 2021.

10 KALOUDIS, 8 ff; European Commission, Digital Economy and Society Index (DESI) 2022 (<https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>); PUGLIERIN/ZERKA, 5 ff; LU/MAYER, 5, regarding the Digital Dependence Index (DDI).

11 See DIPLOFOUNDATION, Balancing digital sovereignty and the splinternet (event report), Internet Governance Forum, 2022; GANNE, 101; CORY/DASCOLI, stating that data localisation requirements have doubled in 4 years worldwide; WEBER, who talks about "Splinternet", "digital sovereignism".

2. Definitions

The term "digital sovereignty" has not yet been defined in a harmonised way at the international or national level. However, several attempts to define have emerged, notably in the academic world. The concepts (a), components (b) and territories (c) at stake will be analysed to better define the outlines of this concept and to establish terminological benchmarks.

a) Concepts

An initial approach is to define the two terms that make up the concept. "Digital" refers to the infrastructure, the underlying technologies, the data and its contents and their consequences on society, culture and processes[12]. Sovereignty refers to the territory of a state, i.e. sovereign actor that is the nation (external sovereignty) and that has a monopoly on the rules of law and law enforcement (internal sovereignty)[13]. However, this classical approach is criticised because it does not take into account the new power relations exercised by non-state actors (e.g. internet users or platform operators)[14].

Digital sovereignty is also often defined from a technological standpoint, which sometimes distinguishes three degrees of sovereignty (high, medium and low) for each stage of the life cycle of a digital system and data[15]. Beyond technology and given the transversality of the issues, it is interesting to define the notion from a multidisciplinary standpoint, in particular socio-economic and legal. The latter prefers the notion of 'strategic autonomy' to that of digital sovereignty. Strategic autonomy refers to the ability of a state or organisation to decide and act autonomously and over the long term on key digital aspects of its economy, society and democracy[16]. While a state's digital sovereignty has become inseparable from technology, strategic autonomy refers to the means to achieve it, i.e. the state's ability to control ICTs and data[17]. This

---

12 Couture/Toupin, 2306.

13 See art. 2 UN Charter; Pohle/Thiel, 49; Alcaud; INTERNET SOCIETY, Navigating Digital Sovereignty and its Impact on the Internet, december 2022; Norodom, 21 ff: political and economic contexts can create divergent approaches to the same concept by state entities. A "liberal" view is traditionally opposed to a more "protectionist" view of digital sovereignty.

14 See footnote 5.

15 Couture/Toupin, 2313; Pohle/Thiel, 6 ff; Kaloudis, 16.

16 Moerel/Timmers, 8 and references; Tan et al., 4 and references; Danet/Desforges, 179 ff; Schmitz Seidl, 12.

17 Chrétien/Drouard, 15 ff; Danet/Desforges, 184; Moerel/Timmers, 8.

definition seems more precise and better delimited than the notion of "digital sovereignty", in particular because it would avoid the legal controversies linked to the recognition of the "sovereignty" of non-state or supranational actors[18].

b) Components

Digital sovereignty includes several components, mainly "technological sovereignty" and "data sovereignty"[19]. Technological sovereignty refers to the ability of a State and its economic operators to control the layers (hardware, software, data)[20]. Data sovereignty refers to the capacity of the different actors (administration, industry, civil society) to control and use data in a self-determined way[21]. It therefore implies control over the personal and non-personal data stored and processed, including access rights (on a contractual or technological basis)[22].

Data sovereignty (control over data) has become central in an ultra-connected society given the security and privacy issues at stake[23]. As data are strategic assets, states also seek to minimise foreign interference with state or private, sensitive or strategic data (e.g. through espionage methods). In order to protect against intelligence activities and to protect the Swiss economy, the concept of the "*Swiss cloud*" emerged in political circles[24], which evolved into the notion of "*sovereign cloud*".

Sovereign cloud can be defined as a *cloud computing* environment controlled, deployed and/or managed locally within a single jurisdiction. The idea is that the user organisation retains control over the data, systems and applications. The requirements vary according to the degree of control: for some, the provider, data, systems and/or applications must be managed locally; for

---

18 See MOEREL/TIMMERS, 8 and DANET/DESFORGES, 180; SCHMITZ/SEIDL, 31.

19 Other dimensions of sovereignty can also be considered, such as "network sovereignty", "information sovereignty", "platform and infrastructure sovereignty", "economic sovereignty", "energy sovereignty". See KAGERMAN ET AL., 13; POHLE/THIEL, 6 ff; SEIFRIED/BERTSCHEK, 6 ff; TAN ET AL., 4; SWISS DATA ALLIANCE, 2, indicating that "data sovereignty" is central for digital sovereignty.

20 See. *below* III.3; FABIANO, 272; BERTANI ET AL., 7; COUTURE/TOUPIN, 2317; KAGERMAN ET AL., 10.

21 See. *below* III.2; GOLLIEZ, 83; CELESTE, 211 ff; KALOUDIS, 6.

22 GOLLIEZ, 83: distinguishing three axes of data sovereignty: the use of non-personal data by as many actors as possible ("*open data*"), the use of personal data by the persons concerned ("*my data*") and the sharing of sensitive data between companies and administrations under strict conditions ("*shared data*").

23 See *below* III.1; TAN ET AL., 2.

24 FDF/UPIC, Swiss Cloud Report, 22 ff.

others, it is sufficient that the data is inaccessible from abroad. There are thus different degrees of cloud sovereignty according to the following 3 components: (*i*) data sovereignty (controlling who owns and accesses the data) regardless of the data localisation a single territory (data residency), (*ii*) operational sovereignty (controlling operations on services, including business continuity and regulatory compliance), (*iii*) technical sovereignty (performing operations oneself without relying on a provider)[25].

c) Territories

Technologies evolve in a context of interconnected global communications networks without well-defined spatial territories. We are therefore shifting from an approach of "territorial sovereignty" to a notion of "sovereignty over networks"[26].

These networks (new forms of territories) are composed of several layers over which the State can exercise its authority: (*i*) physical layer (ICT components and technical capacities located on a spatial territory) (*ii*) logical layer (codes and standards governing the ICT components, making it possible to exchange information between them) and (*iii*) data layer (data circulating on the networks)[27]. The degree of sovereignty will depend on the State's ability to control each layer. The State can exercise exclusive sovereignty over the 1st layer (physical) and limited sovereignty over the 2nd and 3rd layer (logical and data) which have no spatial limits[28].

d) Actors

Digital sovereignty requires political and regulatory strategies, which may involve various actors in the digital ecosystem (the State through public and semi-public entities, industry, civil society), each of which plays different roles and can be described as "governance and regulatory levers"[29]. The State is the

---

25 CAPGEMINI, referring to a sovereign cloud *continuum* and distinguishing several categories of cloud (from least to most sovereign): (i) Public Cloud (without local providers and without restriction as to the jurisdictions from which services are deployed), (*ii*) Hybrid Cloud (without local providers but with pre-approved data centres), (*iii*) *Open source Cloud* (for software and/or components of foreign origin), (*iv*) Private Cloud (i. e. local providers, and only local data) (*v*) *Full in-house private cloud* (i.e. local providers, data and components).

26 VATANPARAST, 1; CHAPDELAINE/MCLEOD, 66; COTTIER Cyberespace, 205 ff; ROGUSKI, 5.

27 ROGUSKI, 5; DUCHEINE, 458 ff; GOLDMAN, 17-1; SHEIKH, 6.

28 This is subject to a nationalisation of cyberspace (e.g. China and Russia). ROGUSKI, 10 ff.

29 COUTURE/TOUPIN, 2317; TÜRK and references; POHLE, 14; GUEHAM, 12; POHLE/THIEL, 8.

first actor concerned. Through its regalian and regulatory functions, the state plays a key role in protecting state or critical infrastructures, the population and industry[30]. Industry also has a decisive role as technology companies influence innovation and generate skills. Civil society is an essential lever of governance and regulation within a democratic system. The term 'weak sovereignty' is used when these issues are driven by the private sector (e.g. in the form of self-regulation) and 'strong sovereignty' when they are driven by the state (e.g. in the form of strict regulation and safeguarding national security)[31]. The term 'internal sovereignty' is also used when rules and policy are focused on internal processes and 'external sovereignty' when they are internationally oriented[32].

This report defines digital sovereignty as the development of strategic digital autonomy. It is the right and ability of political entities to autonomously (independently and/or self-determinedly) use and control tangible and intangible assets and digital services that significantly impact democracy, the economy and society.

3. Digital sovereignty initiatives

Digital sovereignty is subject to numerous initiatives, both internationally, abroad and in Switzerland.

At the international level, it should be recalled, without going into detail, that digital sovereignty has become a major issue, it being recalled that the debate on digital sovereignty may also have negative consequences and that some people are calling for increased international collaboration to reduce these risks[33].

Abroad, digital sovereignty initiatives vary by region and state. Three approaches to digital sovereignty can be identified: the first one focused on entrepreneurial freedom (e.g. in the US), the second one on the state (e.g. in

30 FABIANO, 270; TAN ET AL., 5.

31 COUTURE/TOUPIN, 2313; POHLE/THIEL, 6 ff; CELESTE, 6; POHLE, 6; KALOUDIS, 7.

32 BENDIEK/STÜRZER, N 20; SWISS DATA ALLIANCE, 3, looking at "digital sovereignty" from an international perspective and asking how Switzerland can promote its objectives (positive approach) and protect itself from interventions by other actors (negative approach).

33 DIPLOFOUNDATION (op.cit.).

China), the third one on the individual (e.g. in the EU)[34]. In the EU, digital sovereignty is mainly envisaged in the strengthening of local European capabilities, in particular in its dimensions of infrastructure and *cloud* platforms (also called "*sovereign cloud*") and cybersecurity[35]. At the strategic level, it focuses on artificial intelligence on the one hand and on data on the other hand[36]. At the regulatory level, it aims to create norms allowing the emergence of global standards (e.g. RGPD with extra-territorial effects) and to limit access to the European market for non-European companies (e.g. by controlling access to data)[37]. At the national level, several Member States (e.g. Germany, France) follow the same approach centred on European values (freedom, tolerance and solidarity), some having a real policy of digital sovereignty[38]. Finally, it is generally observed that the EU is pushing to emancipate itself from foreign technology by creating European "champions", while smaller or more liberal countries want to benefit from the best technologies available.

---

34 DETEC / DFAE, Création d'espaces de données fiables, sur la base de l'autodétermination numérique, 30 March 2022, 35; BENDIEK/STÜRZER; BAISCHEW ET AL., 63 ff; CELESTE, 8 ff; BARRINHA/CHRISTOU, 362: reminding that the concept of digital sovereignty in the EU has appeared for the first time explicitly in the field of cyber security, in particular in the December 2020 EU Cyber Security Strategy. For other jurisdictions, see ERGAS/BRANIGAN, 75 ff (Australia), YEN, 105 ff (Taiwan); YUGUCHI, 75 ff (Japan).

35 As an European sovereign cloud project, mention should be made of the Gaïa-X project launched in 2020. As cybersecurity projects, the "cloud (EUCS)" certification issued by ENISA or "SecNumCloud" issued by the French National Agency for the Security of Information Systems (ANSSI), guarantees a level of cybersecurity, the location and processing of data in the EU, as well as immunity to the extraterritoriality of foreign laws. For critics of the Gaia-X project (notably because of the possible participation of non-European private actors in its board of directors and because of extra-territorial laws), see LUZEAUX, 14 ff.

36 Among many documents, see BURWELL/PROPP, 11: defining data and AI as the Lifeblood of Digital Sovereignty.

37 BURWELL/PROPP, 15.

38 For example, Germany and France are keen to develop indigenous skills in relevant technology areas to counterbalance non-European suppliers and are investing in certain strategic areas (hardware (infrastructure and hardware), software (applications and software), artificial intelligence, cyber security, digital platforms and data). For Germany, see BMWK, Shaping the Digital Transition: SEIFRIED/BERTSCHEK, 6 ff; LAMBACH/OPPERMANN, 7; WEBER H., 15 ff; BURGFRIED/RECKERT-LODDE, 611 ff. For France, WOOD ET AL., 11; BAISCHEW ET AL., 63 ff; AUFRECHTER/KLOSSA, 11, reminding that already in 2006 President Chirac called on Europeans to develop an indigenous information search capacity to respond to the "global challenge posed by Google and Yahoo" and that already in 2010 the French government was alerting about the loss of sovereignty to foreign technology companies.

In Switzerland, public digital policies have already been considered, without defining digital sovereignty or strategic autonomy[39]. As Switzerland is a federal state, reflections on digital sovereignty are conducted at all levels of the state (federal, cantonal, communal and intercantonal)[40] as well as in the academic world[41] and civil society[42]. The difficulty of solving the challenges of digital sovereignty can be illustrated by several concrete cases, such as the electronic patient record or cybersecurity.

II. Socio-economic issues

Digital sovereignty is a concept used in many ways. However, they all refer to a central meaning: to what extent is a political entity able to control the 3 layers (physical, logical and data)[43]. This question of control of the layers arises from the point of view of the various actors, in particular national security, economic development and the capacity of the authorities to preserve the rights of individuals and their autonomy of individual and collective action. These three dimensions of digital sovereignty (regalian, economic and civic) depend on the more or less important capacities to supervise and standardise the design and use of technologies and data[44]. These capacities are themselves a direct function of Swiss ICT capacities (1), and of their material (2) and intellectual (3) dependence.

---

39 MAYER/LU, 5.

40 At the federal level: FDF/UPIC, Swiss Cloud Report. At the cantonal and communal level: for example, in Geneva, the Geneva Digital Policy, 37 ff and in Vaud, the Digital Strategy, 35 ff. At the intercantonal level: see PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, 4.; CLDN.

41 For example, in spring 2022, the University of Geneva set up a "UNIGE Digital Sovereignty" think tank, which is working on drafting a Charter of Good Practice.

42 See SWISS DATA ALLIANCE, which brings together companies, professional associations, civil society organisations, research institutions and individuals to establish a future-oriented data policy in Switzerland.

43 See *above* I.2.c); CHANDER/SUN, 283; FLORIDI, 369 ff; FALKNER ET AL., 3.

44 See *above* I.3.

1. Swiss ICT capacities

Switzerland consistently ranks high in the indexes assessing digital development and ICT usage[45]. This assessment is based on nationally developed infrastructure, services and skills that play a favourable role for innovation. But it is also a potential source of social, economic and political vulnerability. This is the case in the field of cybersecurity, where Switzerland is considered to be lagging behind due to poorly developed legislation and insufficient preparation of public authorities for major incidents[46]. It is also the case of the omnipresence of foreign technological devices, i.e. devices produced, developed and/or controlled outside the country. Thus, the notion of digital sovereignty implies taking into account the degree of dependence of a country on the rest of the world in general and on certain countries in particular with regard to ICTs. This dependence cannot be reduced to a single metric and must be understood in its material and intellectual dimensions[47]. Rather than seeking a state of unattainable and undesirable autarky, it is a question of pointing out the vulnerabilities and potential problems that they pose.

2. Material dependence

The degree of Switzerland's material dependence in the digital domain can be assessed on the one hand through usage data from internet browsing and on the other hand through trade. With regard to usage data (i.e. data from devices such as computers, smartphones and tablets used from Switzerland), the studies show a total dependence on foreign hardware infrastructure (e.g. Apple and Samsung accounting for 85% of the equipment used in Switzerland)[48]. With regard to trade, the studies also show a dependence on certain

---

45 Switzerland was 3rd in 2017, International Telecommunication Union (ITU), ICT Development Index 2017 (website); World Economic Forum (WEF), Global Competitiveness Index 2017-2018 (website); Portulans Institute, Network Readiness Index, Switzerland (<https://networkreadinessindex.org/country/switzerland/>).

46 Switzerland was 23rd in the 2021 edition of the National Cyber Security Index of the Estonian e-Governance Academy. eGovernance Academy, National Cybersecurity Index (website). It should be noted that the Confederation is currently making numerous efforts to improve cybersecurity, in particular with the transformation of the NCSC into the Federal Office for Cybersecurity.

47 See Lu/Mayer, 5 ff.

48 Statcounter GlobalStats, Browser Market Share Worldwide (<https://gs.statcounter.com/vendor-market-share/mobile/switzerland/2022>).

countries (e.g. around 85% of consumer hardware, computers, telephones and components are imported, 95% of which come from China)[49].

3. Intellectual dependence

Dependencies are not limited to hardware, but also refer to intellectual aspects (e.g. computer services and softwares)[50]. This is particularly sensitive for government services, including in their regalian functions, when they have to call on foreign service providers for office suites, specialised software or specific audits, including in the field of technological security.

With regard to usage data, the studies show total dependence on foreign software infrastructure, whether for browsers or platforms, with American companies dominating (e.g. Microsoft, Apple and Google account for 90% of operating systems)[51]. Trade in digital services (e.g. computer services, software and telecommunications) is less unbalanced. At the global level, imports of digital services account for 56% of trade (compared with 76% for ICT goods) and are more geographically diversified. A country's intellectual dependence requires a global view of intellectual property[52]. The concentration of intellectual property in the digital fields on a global scale is a source of vulnerability for Switzerland as for most countries. The United States has the most digital patents in the world (42%), followed by Japan (23%) and South Korea (8%), accounting for three quarters of digital IP. China and Germany account for 8% and 3% respectively, leaving only 15% for the rest of the world. Among the main digital fields (e.g. semiconductors, audiovisual technologies, telecommunications, coding/decoding), Switzerland relies on foreign intellectual property with only 0.9% of Swiss patents.

The development of learning and adaptive algorithms has major implications for human-machine relations, economic competition, and military-police control capabilities[53]. Despite having one of the highest densities of artificial intelligence researchers in the world, this development is a concern for

---

49 DFAE, Strategy China 2021-2024, 28-29.

50 Haskel/Westlake, 153.

51 Statcounter GlobalStats, Browser Market Share Worldwide (<https://gs.statcounter.com/os-market-share/all/switzerland/2022>).

52 Pagano, 1413.

53 Durand/Rikap, emphasising that the dynamics of intellectual monopolisation in the digital age cannot be reduced to patent issues, but also include specific logic relating to returns to scale associated with massive data and the modalities of innovation.

Switzerland's digital sovereignty, as it is for other European countries[54] and most other countries except China and the United States, which are in exclusive rivalry in this area[55].

This duopoly is mostly a success of consumer platform firms in these two countries. Conversely, the lack of consumer platforms comparable to *Big Tech* in Europe and in Switzerland[56] has negative effects. Since user data is one of the main fuel for innovation in this field, without the huge pools of user data generated by consumer platforms it is very difficult to be at the frontier of the evolution of artificial intelligence[57]. Countries such as Switzerland are exposed to the consequences of external developments of these powerful technologies, but over which they have almost no control.

4. Recommendations

As an outcome, Switzerland has strong strengths in the digital field, in particular thanks to the quality of its infrastructure and skills that are reflected in the dynamic and balanced foreign trade in digital services. Such trade is however unbalanced on the hardware side, particularly in terms of the terminals used, but this is part of a more general context of international fragmentation of production processes and is not a concern, at least as long as there are various supply options.

However, a first worrying concern relates to the consumer digital activity on the Internet which is almost entirely in the hands of American companies (Apple, Microsoft, Alphabet, Meta). There is a threefold issue of sovereignty here. Firstly, in terms of control of personal data and respect for privacy. Secondly, in terms of public action, the data controlled by *Big Techs* not only makes it possible to better understand individual behaviour but also to influence it[58]. Thirdly, in terms of long-term economic development. The rise of artificial intelligence is largely driven by the mass harvesting of data by consumer platforms and has implications for the security of individuals, organisations and political institutions based in Switzerland as well as for future economic development.

---

54 GROTH/STRAUBE, 7.

55 LUNDVALL/RIKAP, 2 ff.

56 See *above* II.2.

57 GROTH/STRAUBE, 7.

58 A recent example is the impact of social networking platforms on the health of young and old.

A second important concern relates to intellectual property in digital fields which is concentrated on a global scale in American and Asian companies (Japan, Korea, China). This limits the ability of Swiss-based entities to act, with cumulative effects on innovation, as in the case of data.

	General capabilities	*Physical infrastructure*	*Massive data*	*Intellectual property*
Vulnerability	***low***	***moderate***	***strong***	***strong***
Highlights	– *good quality of infrastructure* – *high competence* – *cybersecurity to be strengthened*	– *unbalanced trade in consumer goods and equipment* – *balanced trade in components (core industrial competencies)*	– *uses of consumer data monopolised by US platforms* – *development of artificial intelligence*	– *concentration of intellectual property* – *limits to innovation capacity* – *economic cost*

Table 1. Summary assessment of sovereignty issues in the field of ICT

These vulnerabilities exposed on the material and intellectual levels result in the existence of an autonomy-sophistication dilemma (Figure 1). Authorities must be aware that being at the forefront of digital uses may result in a loss of autonomy, both in terms of public action and data control by individuals and industry. Indeed, since the State cannot control ICT in all its dimensions given the dependencies exposed, the vulnerability of the various domains grows in proportion to the intensity of ICT use.

This difficulty is unavoidable, but it must be the subject of an assessment of the degree of criticality of the various uses of digital technology within and outside administrations, in order to guide public action in terms of digital sovereignty. This cannot be done *a priori* and requires a multi-criteria assessment of what is critical from a digital sovereignty standpoint, in the regalian, economic and social fields. On the basis of such an assessment by

domain, four configurations can be identified, involving distinct measures depending on the complexity of the systems mobilised and the degree of criticality[59].

1. When the uses are not critical and simple, it is *desirable* to maintain openness (blue zone). This ensures dissemination of the most effective solutions to local actors and allows for learning effects.
2. When the uses are critical and simple (green zone), it is *necessary* to develop local solutions guaranteeing maximum sovereignty, especially as relatively inexpensive solutions allow this.
3. When the uses are critical and complex (red zone), it is *desirable but difficult* to develop local solutions ensuring full sovereignty. When the issues at stake are essential for the community, it is important to preserve a capacity for action that is not hindered by dependence on actors beyond the reach of public action. These solutions can be very costly. In the event that they are completely out of reach, because it is not possible to exercise genuine sovereignty, public action must seek ways of limiting the risks incurred, either through protective measures, or in the selection of the entities with which it contracts, or by seeking cooperation enabling it to exercise shared sovereignty.
4. When the uses are both uncritical and complex (orange zone), the development of autonomous solutions is either out of reach or extremely costly while the issues are not essential. Openness is then *necessary*.

[59] See Luzeaux, 16, who speaks of 3 levels of sovereignty, namely (1) weak with limited control over vital infrastructure, (2) partial with limited control over critical infrastructure and (3) complete with extensive control.

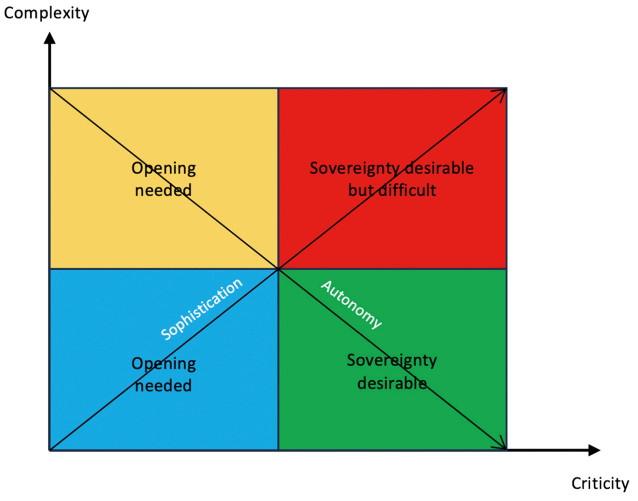

Figure 1. The autonomy-sophistication dilemma in data processing

In sum, with regard to dependencies, it is *recommended* to adapt the measures according to the degree of criticality of the various digital uses within and outside administrations (e.g. critical and simple uses; complex but not very critical; critical but simple; critical and complex). In the latter case (critical and complex uses), measures may range from data residency to diversification of suppliers or the search for cooperation for shared sovereignty[60].

Finally, temporality should be taken into account. Indeed, the question of criticality evolves over time. While some issues are crucial at all times (control of administrative and tax data, confidentiality in military and diplomatic matters), other applications that are *a priori* less sensitive (e.g. in the field of education, transport or health infrastructures) may suddenly become so in a geopolitical crisis. In particular, it should be borne in mind that legal guarantees of data access abroad are not equivalent to political and material control over data on national territory. Only the latter is a real guarantee of sovereignty in the event of a major geopolitical crisis, as the Covid-19 crisis and the war in Ukraine have reminded us.

[60] For the concept of shared and cooperative sovereignty, see Weber, Digital Sovereignty revisited, 77.

Sovereignty is thus not only spatial but also has a temporal dimension[61], i.e. in terms of the ability to anticipate and the time an authority has to react to a new situation. In a field where innovation is very dynamic, it is difficult for public authorities to anticipate relevant problems upstream through regulation alone. Indeed, territorial location requirements are not necessarily a sufficient guarantee, as an entity resident in Switzerland and controlled from abroad could be subject to decisions contrary to the country's interests by the parent company. This is all the more true as the very question of nationality is not self-evident when it comes to effective economic control: is it the address of the head office, the majority of the shareholding, the nationality of the *management*? Based on these uncertainties, public authorities could be led to take shareholdings in the resident entities on which they depend for critical services, so as to have an internal view of the issues that directly concern their sovereignty[62].

III. Legal issues

The legal challenges are numerous, starting with the variety of legal regimes that apply depending on the components, layers and actors involved[63]. Among the main legal regimes, one thinks of personal data protection laws[64] and intellectual property, unfair competition and contractual rights[65]. There are also fundamental rights[66], cybersecurity and secrecy issues (e.g. art. 320 CP;

---

61 JESSOP, 41-61.

62 This would mean going further than the Swiss Cloud Report recommends. See FDF/UPIC, Swiss Cloud Report.

63 For the components, layers and actors, see *above* I.2.

64 The monitoring of compliance with data protection laws by companies and federal bodies is the responsibility of the Federal Commissioner, while the monitoring of compliance with cantonal laws by the cantonal administration is the responsibility of the Cantonal Commissioner, which may lead to divergent interpretations of the legal framework.

65 Beyond personal data, data in general (e.g. industrial and technical data) are at the heart of technologies, which explains why they are subject to several legislative developments in Switzerland and abroad. See DE WERRA, RSDA, 365 ff and the references; BENHAMOU Y., RSDA, 393.

66 At the international level, one thinks first of the general instruments protecting human rights (ECHR; UN Covenant II; Convention 108). At the national level, one thinks of the Cst./CH, in particular the right to personal freedom (art. 10 para. 2 Cst./CH), the rights to privacy, informational self-determination and protection against the misuse of personal data (art. 13 Cst./CH) and the right to freedom of information (art. 13 Cst./) and to freedom of information (art. 16 Cst./CH). One also thinks of the cantonal constitutions, including those revised and containing a catalogue of fundamental rights (e.g. in Geneva art. 14-43 Cst./GE, and Vaud art. 9-38 Cst./VD).

art. 47 LB and 321 CP)[67]. The analysis of legal issues will focus on the two components of data sovereignty (1) and technological sovereignty (2), as well as on cyberadministration (3) and cybersecurity (4) as prerequisites for digital sovereignty.

1. Data Sovereignty

a) Extra-territoriality of laws

The concept of territorial sovereignty has been undermined over the last decade by the extraterritoriality of certain laws that apply to events occurring abroad (e.g. GDPR and *Cloud Act*). This generally serves strategic and economic objectives[68]. For example, the GDPR protection extends to all data subjects who are in the European Union, regardless of the actual location of the data[69]. The *Cloud Act* gives authorities a right of access to data located outside the US but managed by US companies[70]. Swiss law also provides for laws with extra-territorial effect, such as the DPA (art. 3 DPA)[71].

This extraterritoriality of laws leads to a certain decline in territorial sovereignty, or even to a deterritorialisation of law, it being specified that it creates

---

67 CP stands for the Swiss criminal code, code pénal suisse RS 311.0; LB stands for the Swiss banking act, loi sur les banques, RS 952.0. FDF/UPIC, Swiss Cloud Report, 27; FEDERAL COUNCIL, Federal IT Strategy 2020-2023, 6.

68 THELISSON, 524 ff; BRADFORD, who speaks of the "*Brussels effect*" of the GDPR in imposing data protection standards on a global scale consisting of the EU promoting its standards and leading to a Europeanisation of the European legal framework abroad.

69 THELISSON, 524 ff, indicating that the GDPR also serves strategic and economic purposes and influences digital sovereignty as it subjects the data of European individuals to European protection regardless of their location. On the Trans-Atlantic Data Privacy Framework see INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP), Is data localization coming to Europe?, 23 August 2022.

70 THELISSON, 521, stating that the *Cloud Act* is seen as a US response to the extraterritoriality of the RGPD and complements and gives extra-territorial scope to the SCA (for *Stored Communications Act*); CASSART, 41; US DEPARTMENT OF JUSTICE, USA DoJ, White Paper, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *Cloud Act*, April 2019.

71 With the DPA, the Federal Court extended the scope of application of the former DPA by making certain data processing operations that take place abroad subject to it (see in particular ATF 138 II 346, ATF 138 II 346), before the legislator codified this theory of effects in the law, by providing that "this Act applies to facts that have effects in Switzerland, even if they occurred abroad" (art. 3 para. 1 DPA).

competition between jurisdictions[72] and that it must in any case respect international law[73].

b) Data transfer abroad

Given the strategic importance of data, states adopt rules on the transfer of data abroad. These rules can be liberal with free flow of data or restrictive with localisation requirements for data, servers and/or data controllers. These localisation requirements characterise the debate on digital sovereignty. Thus, they pursue both a legal objective (to control compliance with these rules abroad) and a political objective (to strengthen data sovereignty).

Under Swiss law, the rules on data transfer abroad provide for the free flow of data to countries with an adequate level of protection and, in the absence of such a level of protection, for the data transfer abroad subject to additional safeguards (e.g. standard contractual clauses or bilateral agreement)[74]. Thus, where there is a risk that data will be transferred to a country without an adequate level of protection, a risk assessment should be carried out and the contractual relationship should be adapted accordingly. The assessment will take into account the nature of data (e.g. ordinary, sensitive data, secret data) and the existence of a right of access to the data by foreign authorities under foreign law[75].

---

72 See THELISSON, 525, indicating that competing jurisdictions should be resolved according to the conflict of laws rules that determine the applicable law (subject to regional solutions for resolving possible conflicts through governance, such as the designation of a lead authority); PRETELLI, 22.

73 THELISSON, 513-517: *in* Swiss law, the Constitution establishes the principle of respect for international law by the Confederation and the cantons (Art. 5); MAYER, 9 ff; VAN HECKE, 309.

74 FF 2017 6594, stressing that the free flow of data is a cardinal principle of the Swiss Data Protection Act (LPD).

75 E.g. if the data is hosted by a US provider or a Swiss provider under the control of a US group, the US Stored Communications Act respectively the *Cloud Act* may give access to the authorities from US soil. See PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, 4; SCHWARZENEGGER ET AL., 83 ff. Also see FISCHER/PITTET, who distinguishes between a one-off and a general legal right of access and points out that the risk analysis must still assess the likelihood that the authority will assert this right and achieve its ends. It should be noted that the *Cloud Act is not the* only foreign regulation providing for a right of access to foreign authorities. One example is the current debate concerning the TikTok application, whose parent company ByteDance, based in China, could be required to provide access to Chinese authorities from Chinese territory, regardless of the location of the data, on the basis of Chinese law.

In European law, the rules are similar and provide for the free flow of data, even if authorities and courts sometimes limit the possibilities of transferring data abroad through a strict interpretation of the rules (e.g. the Schrems II judgment)[76] and localisation requirements for certain personal data and infrastructures (e.g. the DGA providing for data localisation requirements respectively cybersecurity certification requirements for cloud services)[77].

It should be noted that, even when data is hosted in Switzerland but with a provider controlled by a foreign group (e.g. Swiss Microsoft), some legislations have extra-territorial effects and give access to authorities regardless of the localisation of the data (e.g. *Cloud Act*)[78]. On this basis, in case of data storage and processing in Switzerland, the risk of access by foreign authorities can only be avoided when the Swiss-based data controller has no relationship or contact with foreign companies (e.g. with a US affiliate) or, if it does, when the foreign companies do not have possession, custody, control or responsibility of the Swiss entity. This kind of immunity of the Swiss-based data controller presupposes, in organisational terms, that its registered office and central administration are established in Switzerland and that its share capital and voting rights are not individually or collectively held above a certain threshold (e.g. 24% individually, 39% collectively) by third parties with their registered office, central administration or principal place of business based abroad[79].

For this reason, the use by the public administration of service providers located abroad or belonging to an American group is currently under debate. The Federal Data Protection Commissioner (FDPIC) considers that the use of M365 *cloud* (*Outlook* and *Teams* services) by the Swiss Accident Insurance Fund (SUVA) is contrary to the DPA, even if the data is hosted in Europe, on the grounds that there is a residual risk of access by foreign authorities (zero-risk approach)[80], whereas the Federal and Zurich Cantonal Administrations

---

76 European Court of Justice, 16 July 2020, C-311/18 (Schrems II).

77 See Joint Opinion 03/2021 of the EDPB and the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), adopted on 10 June 2021 (<https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en>); EDPS, Opinion of 28 February 2023 on the adequacy decision on the EU-US Data Privacy Framework.

78 See III.1.a).

79 RAMOS ET AL.

80 See FDPIC, Guide June 2021: contrary to SUVA's assessment of the risk as very unlikely (*höchst unwahrscheinlich*).

consider that such recourse for the administration is permissible provided that certain additional protective measures are taken to limit the risk of access by foreign authorities (risk-based approach)[81].

In both cases, there is a question of risk analysis, in that the lawfulness of the *cloud* is analysed according to whether or not the additional protection measures make it possible to limit the risk of access by foreign authorities[82]. The reluctance of the FDPIC is certainly due to the tightening of the practice of the European authorities regarding transfers to the United States and pending an agreement replacing the *Privacy Shield*[83]. This being said, the risk of access by foreign authorities is reduced, since a data transfer by a Swiss entity to foreign authorities would be a violation of Article 271 of the Swiss Criminal Code, which prohibits activities on behalf of a foreign state (except mutual assistance)[84].

c) Digital self-determination

Digital self-determination is a new approach to strengthening data sovereignty, in particular the control of individuals, businesses and society over their own data. It could be enshrined through the interpretation of fundamental rights[85] or through the recognition of a new right, such as the "right to digital integrity", which has been recently proposed in French-speaking cantons[86].

---

81 Federal Council, La Confédération passe à Microsoft 365, Communiqué de presse, 15 February 2023.

82 The Swiss Lawyers Bar (FSA), follows the risk-based approach but recommends caution (local solutions), at least on tax and ILL issues and if foreign legislation makes it difficult to enforce contracts. Schwarzenegger et al., 30 ff.

83 See Fischer/Pittet, citing the strict decisions in the *Google Analytics* cases.

84 See Fischer/Pittet, recalling other issues that are just as important as the access risk in the case of data outsourcing, such as data security and the need to ensure *business continuity in the event of* the provider's failure.

85 E.g. right to life and personal freedom (Art. 10 Cst./CH), from which personality rights (Art. 27 ff CC) are derived; protection of the private sphere (Art. 13 Cst./CH), from which informational self-determination is derived ATF 148 I 233).

86 Draft constitutional amendments have recently emerged in Geneva, Jura, Neuchâtel, Valais and Vaud, so as to fil the gaps of existing laws (e.g. for a right to offline life and a better cybersecurity). At federal level, the initiative 22.479 "Introduce the right to digital integrity into the Constitution" is currently under consideration, so that one can speak of the "laboratory of federalism".

2. Technological sovereignty

Technological sovereignty requires an innovation policy that includes state measures (legal, economic and technical) and international cooperation[87]. Protectionist measures (e.g. investment controls, repatriation of the value chain) should be avoided, as total independence from exclusively indigenous ICTs is unlikely, given the extreme interweaving of the Swiss digital ecosystem with the infrastructures and services deployed worldwide[88]. An innovation policy aimed at technological sovereignty requires an analysis of which technologies are critical ("*key enabling technologies*", KETs) and what measures are needed to maintain control over these KETs (in the short or medium term)[89]. It will also be necessary to improve the decision-making and operational skills of public and private users in order to strengthen freedom of choice and avoid a concentration of supply (e.g. advanced training to make up for the lack of personnel in the production and/or use of KETs)[90]. The digital transformation of government activities (e.g. e-ID identification and electronic signature) should also be reclaimed[91].

Intellectual property regulation is a key element in strengthening innovation, data protection and trade secrets (e.g. algorithms and data analysis techniques)[92]. However, regulation alone is insufficient, as only an understanding of the technologies and an *ex ante* analysis of the regulation can strike the right balance between protection and free use[93]. It is in this spirit of balance that data flow is at the heart of the development of innovation policy, including

---

87 See CHRÉTIEN/DROUARD, 24 ff; COMCO, Annual Report 2020 of the Competition Commission (COMCO), DPC 2021/1 23 ff, 42, categorising innovation policies according to 3 approaches: the "competition" approach consisting of creating European champions in order to compete with dominant players (1t approach); the "competition" approach consisting of industrial alliances with existing European players (2nd approach); the "cooperation" approach aiming at data openness and interoperability of technologies (e.g. GAIA-X) (3rd approach).

88 ILLGNER, 8 ff; SEIFRIED/BERTSCHEK, 6 ff.

89 EDLER ET AL., 19 ff; WESTPHAL, 7; CHRÉTIEN/DROUARD, 23 ff; MAURER ET AL., 53 ff; ILLGNER, 8; KALOUDIS, Action Plan, 7 ff, pointing out that access to the necessary raw materials and knowledge must also be taken into account.

90 Decision-making skills are understood as the ability to understand, evaluate and verify the reliability of solutions in the market, operational skills as the effective use of technologies to increase one's own competitiveness and innovative capacity. See SEIFRIED/BERTSCHEK, 6 ff and references.

91 TÜRK and references.

92 See MARCH/SCHIEFERDECKER.

93 PAGANO, 1413.

artificial intelligence (AI), which explains why it is the subject of numerous legislative developments in Switzerland and abroad.[94] In addition, complementary support measures (e.g. standard contracts, certification, awareness raising and training) could be used to promote data flows rather than major legislative measures[95].

3. Cyberadministration

a) Federalism and the distribution of powers

Digital sovereignty presupposes that the state can freely decide whether and how to digitise its internal processes and services to the population (*cyberadministration*) under the right conditions and independently[96]. Digital sovereignty can also mean not digitising certain services (e.g. for cybersecurity and/or digital sobriety reasons).

Digital sovereignty is a cross-cutting issue, which requires a common public policy for the Confederation, the cantons and the municipalities[97]. The main constraints stem from the federal nature of the state (federalism). The cantons are sovereign as long as their sovereignty is not limited by the Federal Constitution and their rights are not delegated to the Confederation (art. 3 Cst/CH[98]). Thus, if digital transformation (in the broad sense including administration and society) is considered a new task of the state, it is by default a cantonal task[99]. Consequently, there is a certain tension between

---

94 In European law, one thinks of sectoral or horizontal regulations, such as the GDPR, the Regulation on the free flow of non-personal data, the Open Data Directive, the Data Governance Act, the Digital Services Act, the Digital Market Act, the Data Act proposal. In Swiss law, there are several initiatives that aim to promote access to personal and non-personal data, see INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE (IPI), Rapport concernant l'accès aux données non personnelles dans le secteur privé, 1er March 2021, 4 ff; DE WERRA, RSDA, 365 ff and the numerous references cited.

95 The European certification mechanisms for a sovereign cloud are good examples that Switzerland could learn from, especially given the similar considerations that led the EU to turn to certification mechanisms, see n. 35.

96 The term "cyberadministration" is used here in a broad sense to refer both to the transformation processes of the administration and to the digitised processes themselves providing administrative services. MONTAVON, 25 ff.

97 MONTAVON, 25 ff; FDF, Digital Administration (website); FEDERAL COUNCIL, Swiss Digital Strategy 2020, 12.

98 Cst/CH stands for the Federal Constitution, RS 101.

99 MONTAVON, 53 ff.

power decentralization (which is guided by the cantonal autonomy, Art. 47 Cst/CH) and power centralization (which is guided by the efficiency principle, Art. 170 Cst/CH). This raises the question of how far the Confederation can restrict cantonal competences for the sake of efficiency.

In this context, many voices advocate the introduction of common norms and standards at all levels of the state, while others see the diversity of technical solutions adopted in the various communities that make up the federal state as an asset in terms of cyber security[100]. The cantons will also be better able to take account of their specific characteristics (e.g. large cross-border population)[101]. On the other hand, when a competence has been entrusted to the Confederation by means of a federal constitutional amendment and the Confederation has made use of its competence, the cantons are no longer competent to make certain choices (e.g. in the area of digital transformation) (Art. 49 Cst/CH; primacy of federal law)[102].

b) Principle of rule of law

Digital transformation must comply with the principle of rule of law (Art. 5 para. 1 Cst/CH), which requires that any state action be based on a legal basis (legal basis requirement) and that the latter be sufficiently precise (normative

---

100 This is illustrated by the electronic patient file (EPR) project, for which it was decided to introduce the EPR in a decentralised manner through officially certified regional "communities". See Swiss Confederation and Conference of Cantonal Health Directors, Electronic Patient Record: The introduction phase is underway, 16 August 2022. The EPR is provided for and framed by the LDEP, which was adopted in 2015 and entered into force in 2017. This is also illustrated by the LMETA, a federal law for the digital transformation, for which the federal National council wanted to give the federal government the power to issue federal technical standards, while it finally gave up upon opposition of States Council and Cantons and left the technical standards to cantonal autonomy. See Parliamentary Press Release, 18 October 2022, The elimination of divergences on the LMETA. See Montavon, 53 ff.

101 To take account of these constraints, more flexible modes of collaboration can be used (e.g. Framework Agreement on eGovernment Collaboration in Switzerland).

102 This is illustrated by the debate on the deployment of 5G technology, in respect of which the Constitutional Chamber of the Geneva Court of Justice annulled the Geneva law on buildings and various installations (LCI/GE) on the grounds that both telecommunications (Art. 92 Cst/CH) and the protection of human beings and their natural environment against harmful interference (art. 74 Cst/CH) were federal competences that had been duly implemented (in particular in the LTC, the LPE and more specifically the ORNI with regard to mobile telephone antennas). ACST/11/2012 of 15 April 2021, recitals 6 and 7.

density requirement)[103]. In our view, the digital transformation must be based on formal legal foundations (legal basis requirement), given its importance beyond the organisational measures of the administration[104]. Much of the debate surrounding digital transformation currently focuses on the requirement for a legal basis, as in the case of the LMETA[105], and the awarding of *cloud* contracts to private service providers[106]. However, the requirement for normative density must be equally analysed and well used. The technical complexity of the field and its development make it difficult to regulate exhaustively in law. To a certain extent, therefore, it seems legitimate to allow for clauses delegating powers to the executive[107], as well as references to technical standards[108].

Finally, one could consider experimental legislation, that is to say legislation that is limited in time and to specific sectors, which can be then evaluated and, if necessary, made permanent and extended to other sectors (e.g. the LLExp in Geneva)[109]. This solution would be well suited to the digital transformation of the administration and society, which is currently in the midst of a "learning phase" and characterised by legal uncertainties[110]. This solution would allow time to learn and to develop the elements necessary for the adoption of a final regulation at a later stage[111]. It should also be added that innovations may be

---

103 MALINVERNI ET AL., 683 ff; OFK-BIAGGINI, BV 36 N 13 and BV 164 N 3-4, recalling that the degree of requirement depends on the norm in question (see Art. 36 para. 1 and 164 para. 1 Cst./CH requiring that serious restrictions of fundamental rights be imposed).

104 MONTAVON, 350 ff.

105 Loi fédérale du 4 mars 2022 sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités, FF 2022 804, 2.

106 Federal Supreme Court, Decision 1C_216/2022 of 28 July 2022.

107 MONTAVON, 323: The author also identifies a phenomenon of 'legislative inversion', which reverses the traditional model of elaboration and hierarchy of norms. On this phenomenon, FLÜCKIGER, Légistique, 244.

108 ZUFFEREY, 61 ff.

109 Loi genevoise du 14 décembre 1995 concernant la législation expérimentale (RS/GE A 2 35).

110 MONTAVON, 431 ff. On experimental legislation and the precautions that must accompany its use in a rule of law, FLÜCKIGER, Légistique, 660 ff; FLÜCKIGER, Droit expérimental, 142; COTTIER, Cyberspace, 247 ff.

111 See FOJ, Guide to Legislation, 269, which sets out the principles that must be observed when creating and applying legislation of an experimental nature.

proposed at the cantonal level before being considered at the federal level, which can be called the "laboratory of federalism"[112].

c) Three steps of the implementation of public policy

In the implementation of public policy, it is useful to distinguish between different steps (each of which takes place at the three levels of the state, Confederation, canton, municipalities).

As a first step, a planning phase should be carried out to examine existing technical solutions and the risks they pose to the values and principles of the Swiss rule of law (e.g. massive data collection, concentration of a few *hyperscalers*, extraterritoriality of foreign laws, threat to secrecy), in order to identify strategic choices, such as legislative initiatives at the international or national level[113]. This implies clarifying the division of competences between the different levels of government, the role to be played by public authorities (e.g. service providers and/or issuers of an appropriate legal framework or self-regulation)[114] and the need for dedicated infrastructures (e.g. National infrastructure of network for mobility data, NaDIM in the field of national mobility data infrastructure), cooperation bodies (e.g. Swiss Digital Administration ANS in the field of cyberadministration) and the authority(ies) in charge to support or promote digital transformation within each public authority (e.g. at federal level, the Federal Statistical Office (FSO) for networking AI skills)[115]. In a second phase, the implementation phase begins, which consists of the adaptation of existing legal texts (e.g. LMETA), the creation of new bodies or

---

112 For a recent example, one can think of the draft constitutional amendment in GE for the recognition of a "right to digital integrity" (Cst.-GE) (For a strong protection of the individual in the digital space) (PL 12945), published on 30th September 2022. See above III.1.c).

113 Federal Council, Message of 4 March 2022 on the Federal Act on the Use of Electronic Means for the Execution of the Tasks of the Authorities, FF 2022 804; DETEC/DFAE, Report on the Creation of Trusted Data Spaces, 3; see also FDF/UPIC, Swiss Cloud Report, 7; FDFA, Digital Foreign Policy 2021-2024, 14; FDF/UPIC, 27; Federal Council, Federal IT Strategy 2020-2023, 6.

114 DETEC/DFAE, Report on the Creation of Trusted Data Spaces, 40.

115 At the cantonal and communal level, for example, the digital delegates who meet in the Assembly of Delegates of the Swiss Digital Administration. See Federal Chancellery, Digital Transformation and IT Governance, DTT Sector (website); FSO, New Statistical Information, Artificial Intelligence Competence Network, 25 August 2021 (<https://www.bfs.admin.ch/bfs/en/home/dscc/blog/2022-02-ecosystem.assetdetail.18164964.html>).

the selection of companies to provide the desired services[116]. In a third phase, the measures adopted, and their implementation are **monitored.** This control is carried out by judicial or supervisory bodies and may lead to changes in the adopted legislation in order to comply with the set requirements.

d) Public procurement law

Digital transformation of the administration must also take into account public procurement law, as the procurement of ICT by administrative entities from private companies is in principle subject to public procurement law[117]. This requires an analysis of the scope of application of public procurement law (e.g. which IT services are subject to the Public Procurement Agreement with their classification code).

The application of public procurement law makes the wording of tenders and the requirements set by contracting entities crucial. For example, the tender "*Public Clouds Confederation*" in 2020 for the provision of *cloud* services for a period of five years required that "*[t]he bidder must have data centres on at least 3 continents (including within the European Economic Area*"[118]. This meant that Swiss companies were excluded from the procedure and the award decision selected foreign companies. This being said, public procurement law allows a certain amount of leeway for the use of direct agreement procedures, particularly in the case of an *in-house* solution or the presence of a single company capable of supplying the required goods or services. It should also be noted that the European States are interested in the American procedures for awarding public contracts (e.g. the *Small Business Act*), which have enabled the

116 At the communal level, the Municipal Council of the City of Geneva voted on 28 June 2022, on the proposal of the Administrative Council, a credit of CHF 2,000,000 for the implementation of the Office 365 suite from Microsoft in the City of Geneva.

117 Public procurement law includes the agreements ratified by Switzerland in the field of public procurement, i.e. the WTO Agreement on Government Procurement revised in 2012 ("GPA 2012", RS/CH 0.632.231.422) and the Agreement between the Swiss Confederation and the European Community on certain aspects of government procurement concluded in 1999 (RS/CH 0.172.052.68).

118 See simap.ch, project no. 204859 (call for tender of 7 December 2020).

development of technological giants, by putting in place instruments enabling small and medium-sized enterprises (SMEs) to use public contracts to develop[119].

4. Cybersecurity

Cybersecurity is a key element in a digital society, especially in view of the risks of unauthorised access to data, manipulation of information or other forms of cybercrime, which are amplified in a technology-dependent digital society[120]. Cybersecurity is a cross-cutting issue that concerns all levels of government, especially in Switzerland, where the division of tasks is governed by federalism. However, cybersecurity has several dimensions for which the responsibility lies at different levels: civil cybersecurity requires consultation at different levels, cyberdefence is primarily a matter for the Confederation and the military, and cybercrime for the criminal prosecution authorities[121].

Cybersecurity implies the use of resilient ICT, i.e. technological means to ensure the security, confidentiality and availability of data. The sovereign *cloud* or, more generally, the storage of data in a single territory (*data residency*) is often mentioned for this purpose[122]. However, this approach may be counterproductive, as the more concentrated the data, the more vulnerable it is[123]. Instead, a diversification of hardware and software solution providers

---

119 E.g. the *Small Business Act* has directed a share of public procurement to small businesses, which has allowed innovative companies to rely on creditworthy customers to improve their products and services. For French experts, this type of instrument could be deployed at French level for innovative public procurement without contravening European law. See BENHAMOU B., Souveraineté numérique.

120 FEDERAL COUNCIL, Security Report, 7. See DURAND, 91; National Cyberstrategy, 13 April 2023, 9.

121 National Cyberstrategy, 13 April 2023, 9.

122 TIPPER/KRISHNAMURTHY, 2 ff, distinguish 4 approaches to resilience: isolationist consisting of using domestic components and local labour for a state's digital infrastructure (e.g. Russia's creation of Mir to replace Visa and Mastercard) (1st approach); cooperative consisting of entering into international treaties, agreements and standards to regulate ICT (e.g. GAIA-X within the EU) (2nd approach); competitive consisting of strategic partnerships between domestic industry and government (e.g. China's *Digital Silk Road Initiative*) (3rd approach); military consisting of mobilising military resources to protect the physical and cyber digital infrastructure (4th approach).

123 BAUER/ERIXON, 26 ff.

is needed to reduce dependencies[124], taking into account that imported technologies may contain *backdoors*[125].

Cybersecurity also requires adequate preparedness in case of a cyber incident[126], which implies the development of (production, decision-making and/or operational) skills, the establishment of contracts to maintain (legal and de facto) control over data[127] and of monitoring and *compliance* processes with regard to potential breaches of applicable regulations[128]. Cybersecurity also requires a clear legal framework, possibly by strengthening legal instruments (e.g. criminal offences, obligations to report cyber attacks)[129], by National Cybersecurity Center's (NCSC) recommendations and incentives or constraints to ensure compliance[130].

Internationally, it would be interesting to look for global solutions to protect civilians in case of state cyber attacks[131], to sanction government cyber

---

124 FEDERAL COUNCIL, Product Security and Supply Chain Risk Management in Cyber Security and Cyber Defence, 7; BAUER/ERIXON, 26: Cyber espionage, however, remains undetectable in most cases.

125 And the risk of leakage of critical data or cyber attacks on critical systems. See BERCHTOLD Carina, Have you thought about all the backdoors? *in* ICTJournal, 22 August 2022; The market is mainly dominated by US, Chinese companies and a few isolated players from Korea (Samsung), Russia (Kaspersky) and Germany (SAP). See SATW, Cybersecurity Map, Sovereignty (<https://www.satw.ch/en/cybersecurity/cybersecurity-map>).

126 Adequate cybersecurity preparedness traditionally involves the following 5 phases: identify, protect, detect, respond, recover (*NIST Core Framework*). DEFR/OFAE, IT Resilience, 14 ff.

127 Contractual commitments include the commitment to technical and organisational measures (e.g. data encryption), the absence of liability in the event of a breach of confidentiality, the obligation to inform about the precise location of the servers as well as about possible data requests by foreign authorities (*lawful access*).

128 TAN ET AL., 3; TIPPER/KRISHNAMURTHY, 2 ff.

129 These obligations are provided for in various laws and reinforce the identification of threats, in particular in the NISP (Art. 24 NISP) and in the ISL (Art. 74a ff ISL). See FF 2023 84.

130 See CHAVANNE Yannick / ZÜLLIG Yannick, Cybersecurity: the Confederation launches a prevention campaign, *in* ICTJournal, 5 September 2022; KOLLER Rodolphe, Mobilising employees to report phishing emails: it works, according to a Swiss study, *in* ICTJournal, 14 January 2022.

131 E.g. Digital Geneva Convention was envisaged to protect cyberspace. See Digital Geneva Task Force, A white paper to make Switzerland the core of digital governance in a secure digital world, 9.

attacks[132] and to subject technology companies to humanitarian law rules[133]. It would also be interesting to develop political-legal measures, such as virtual embassies (i.e. *data* storage with immunity/inviolability status like diplomatic missions)[134].

5. Recommendations

On this basis, several recommendations can be made to guide public action on digital sovereignty. With regard to data sovereignty, it is *recommended* that, when foreign laws apply in Switzerland, the courts analyse their compatibility with Swiss sovereignty before admitting their extra-territorial effects in Switzerland. When transferring data abroad (whether personal or non personal), it is also recommended that the contractual relationship be adapted to the risk of access to the data by foreign authorities, and that a local solution be preferred if critical data or infrastructures are involved.

With regard to technological sovereignty, it is *recommended* to favour European and international cooperation (instead of protectionist measures). With regard to state measures, it is recommended to favour complementary support measures (e.g. standard contracts, certification, awareness raising and training) over major legislative measures. It is also recommended to improve the skills of public and private users and to keep full control (e.g. in-sourcing) for the digital transformation of regalian activities (e.g. e-ID identification and electronic signature).

With regard to cyberadministration, it is *recommended* that the digital transformation be planned on an ongoing basis, carefully analysing the need to adapt or enact the necessary legal bases and public procurement law (e.g., wording of calls for tender or competitive bidding procedures). It is also recommended to clarify which cantonal autonomy remains and, in case of doubt, to consider that there is cantonal autonomy by default in the name of the principle of primacy of federal law and subsidiarity.

---

132 BREITENFELDT/JORDAN, 959 ff.

133 E.g. based on the Montreux Document. See DFAE Montreux Document (website) and ICRC, The Montreux Document (website).

134 The Estonian state stores a duplicate of critical data "in a friendly country", in order to ensure system continuity in case of a serious cybercriminal attack on the national state infrastructure. MONTAVON/SCHWAB, 16; ROBINSON ET AL., 391 ff; WGS/OECD, 42 ff.

With regard to cybersecurity, it is *recommended* that contracts with ICT providers that include TOMs be put in place. It is also recommended to ensure a clear legal framework, which calls for the follow-up of the NCSC recommendations and incentives or binding measures to ensure compliance. Internationally, it would be interesting to look for solutions to protect civilians in the event of state cyber attacks, to subject technology companies to the rules of humanitarian law and to develop solutions such as data *embassies*.

Bibliography

Alcaud David, Souveraineté, *in* Encyclopædia Universalis <https://www.universalis-edu.com/encyclopedie/souverainete/> (12 October 2022).

Aufrechter Fabien / Klossa Guillaume, Pour une souveraineté numérique européenne, Concilier indépendance et attractivité, Paris 2022.

Baischew Dajan / Kroon Peter / Lucidi Stefano / Märkel Christian / Sörries Bernd, Digital Sovereignty in Europe – a first benchmark, Bad Honnef 2020 (cited: Baischew et al.).

Barrinha André / Christou George, Speaking sovereignty: the EU in the cyber domain, *in* European Security, 2022, vol. 31, no. 3, 356 ff.

Bauer Matthias / Erixon Fredrik, Europe's quest for technology sovereignty: Opportunities and pitfalls, *in* European Centre for International Political Economy (ECIPE) Occasional Paper, No. 02/2020.

Baur Andreas, European Dreams of the Cloud Imagining Innovation and Political Control, *in* Geopolitics, 2023.

Belli Luca, Structural Power as a Critical Element of Digital Platforms Private Sovereignty (non-final draft), *in* Edoardo Celeste / Heldt Amélie / Iglesias Keller Clara (Ed.), Constitutionalising Social Media, 2022.

Bendiek Annegret / Stürzer Isabella, Advancing European internal and external digital sovereignty: The Brussels effect and the EU-US Trade and Technology Council, *in* Stiftung Wissenschaft und Politik (SWP) Comment, 2022, no. 20.

Benhamou Bernard, Souveraineté numérique: quelles stratégies pour la France et l'Europe? <https://www.vie-publique.fr/parole-dexpert/276126-souverainete-numerique-quelles-strategies-pour-la-france-et-leurope> (cited: Benhamou B., Souveraineté numérique).

Benhamou Yaniv, Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property-like rights, their exceptions and licensing practices, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, no. 4, 393 ff <https://archive-ouverte.unige.ch/unige:145046> (cited: Benhamou Y., RSDA).

Benhamou YAniv / Bernard Frédéric / Durand Cédric, Souveraineté numérique : étude pluridisciplinaire pour la Suisse, 2023, <https://archive-ouverte.unige.ch/unige:168718>.

Bertani Sebastiano / Caccia Andrea / Massimo Fabio / Allard Jean-Luc / Tumietto Daniele, White Paper on Digital Sovereignty, Bruxelles 2021 (cited: Bertani et al.).

Bradford Anu, The Brussels effect: how the European Union rules the world, New York 2020.

Breitenfeldt Friedo / Jordan Sylvain, Atteinte à l'indépendance de la Confédération, *in* AJP/PJA 2022, vol. 9, 959 ff.

Brunessen Bertrand (Ed.), La politique européenne du numérique, Bruxelles 2023.

Büchel Jan / Engels Barbara, The Importance of the Data Economy for Europe's Digital Strategic Autonomy, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 13-18.

Burgfried Andreas / Reckert-Lodde Andreas, Die Deutsche Verwaltungscloud-Strategie, Auf dem Weg zur Digitalen Souveränität, *in* Datenschutz und Datensichercheit (DuD), 2022, vol. 46, no. 10, 611 ff.

Burwell Frances G. / Propp Kenneth, Issue brief – The European Union and the Search for Digital Sovereignty – Building "Fortress Europe" or Preparing for a New World?, *in* Atlantic Council, 22 June 2020.

Cassart Alexandre, Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD, *in* Revue du droit des technologies de l'information, 2018, vol. 73, 41 ff.

Celeste Edoardo, Digital Sovereignty in the EU: Challenges and Future Perspectives, *in* Fabbrini Federico / Celeste Edoardo / Quinn John (Ed.), Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Oxford 2021, 211-228.

Chander Anupam / Sun Haochen, Sovereignty 2.0, *in* Vanderbilt Journal of Transnational Law, 2022, vol. 55, no. 2, 283 ff.

Chapdelaine Pascale / McLeod Rogers Jaqueline, Contested Sovereignties: States, Media Platforms, Peoples, and the Regulation of Media Content and Big Data in the Networked Society, *in* Laws, 2021, vol. 10, no. 66.

Chrétien Jennyfer / Drouard Étienne, European technological sovereignty, Paris 2022, <https://www.renaissancenumerique.org/wp-content/uploads/2022/01/renaissancenumerique_note_souverainetetechnologique.pdf>.

Cory Nigel / Dascoli Luke, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, *in* Information Technology & Innovation Foundation (ITIF), 19 July 2021 <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>.

Cottier Bertil, La privatisation de la fonction législative ou la face sombre de la révolution numérique, *in* LeGes, 2019, vol. 30, no. 3 (cited: Cottier, Privatisation).

Cottier Bertil, Le droit "suisse" du cyberespace ou le retour en force de l'insécurité juridique et de l'illégitimité, *in* ZSR/RDS 2015, vol. 134, no. 2, 205 ff (cited: Cottier, Cyberespace).

Couture Stéphane / Toupin Sophie, What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?, *in* New Media & Society, 2019, vol. 21, no. 10, 2305 ff.

Danet Didier / Desforges Alix, Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques, *in* Hérodote, 2020, vol. 177-178, no 2-3 (2020), 179 ff.

Département fédéral des finances (DFF) / Unité de pilotage informatique de la Confédération (UPIC), Rapport sur l'évaluation des besoins d'un nuage informatique suisse ("Swiss Cloud"), Berne, December 2020 (cited: DFF/UPIC, Swiss Cloud Report).

DE WERRA JACQUES, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non personnelles (par des licences obligatoires ou des licences "FRAND")?, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, vol. 92, no. 4, 365 ff. (cited: DE WERRA, RSDA).

DUCHEINE PAUL A. L., Military Cyber Operations, *in* DIETER Fleck / GILL Terry D. (Ed.), The Handbook of the International Law of Military Operations, 2nd edition, Oxford 2015, 458-475.

DURAND CÉDRIC / RIKAP CECILIA, Intellectual monopoly capitalism – challenge of our times, 5 October 2021 <https://socialeurope.eu/intellectual-monopoly-capitalism-challenge-of-our-times>.

EDLER JAKOB / BLIND KNUT / KROLL HENNING / SCHUBERT TORBEN, Technology Sovereignty as an Emerging Frame for Innovation Policy – Defining Rationales, Ends and Means, Fraunhofer ISI Discussion Papers Innovation Systems and Policy Analysis No. 70, July 2021 (cited: EDLER ET AL.).

ERGAS HENRY / BRANIGAN JOE, Digital Strategic Autonomy: An Australian Perspective, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 75-84.

European Commission, Digital Economy and Society Index (DESI) 2022 (<https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 >).

FABIANO NICOLA, Digital Sovereignty Between "Accountability" and the Value of Personal Data, *in* Advances in Science, Technology and Engineering Systems Journal, 2020, vol. 5, no. 3, 270 ff.

FALKNER GERDA / HEIDEBRECHT SEBASTIAN / OBENDIEK ANKE / SEIDL TIMO, Digital Sovereignty-Rhetoric and Reality, Framework Paper, 2022 (cited: FALKNER ET AL.).

FISCHER PHILIPP / PITTET SÉBASTIEN, Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?, 16 août 2022 in <www.swissprivacy.law/165>.

FLORIDI LUCIANO, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *in* Philosophy & Technology, September 2020, vol. 33, no. 3., 369 ff.

FLÜCKIGER ALEXANDRE, Le droit expérimental : Potentiel et limites en situation épidémiologique extraordinaire, *in* Sécurité et droit, 2020, vol. 3, 142 ff (cited: FLÜCKIGER, Droit expérimental).

FLÜCKIGER ALEXANDRE, (Re)faire la loi : Traité de légistique à l'ère du droit souple, Berne 2019, 244 (cited: FLÜCKIGER, Légistique).

GANNE EMMANUELLE, Can Blockchain revolutionize international trade?, Geneva 2018.

GOLDMAN JAMES E., Network Concepts, *in* WHITAKER Jerry C. (Ed.), Systems Maintenance Handbook, 2nd edition, Boca Raton / London / New York / Washington D.C. 2002.

GOLLIEZ ANDRÉ, Souveraineté des données, in SCHÄRER Claudia (Ed.), Technology Outlook 2021, Zurich / Lausanne (Schweizerische Akademie der Technischen Wissenschaften), April 2021.

GROTH OLAF / STRAUBE TOBIAS, Analysis of current global AI developments with a focus on Europe, Berlin (Konrad-Adenauer-Stiftung), 2020.

GUEHAM FARID, Vers la souveraineté numérique, Paris 2017.

HASKEL JONATHAN / WESTLAKE STIAN, Capitalism without capital: the rise of the intangible economy, Princeton / Oxford 2018.

Illgner Klaus (Ed.), Technological Sovereignty: Methodology and Recommendations, Frankfurt am Main 2020.

Jäger Wilfried / Nentwich Michael / Embacher-Köhle Gerhard / Krieger-Lamina Jaro, Digitale Souveränität und politische Prozesse, *in* Bogner Alexander / Decker Michael / Nentwich Michael / Scherz Constanze (Ed.), Digitalisierung und die Zukunft der Demokratie Beiträge aus der Technikfolgenabschätzung, Baden-Baden (Nomos) 2022, 189-204 (cited: Jäger et al.).

Jessop Bob, Redesigning the state, reorienting state power and rethinking the state, *in* Jenkins Craig / Leicht Kevin (Ed.), Handbook of politics, New York 2010, pp. 41-61.

Kagerman Henning / Streibich Karl-Heinz / Suder Katrin, Souveraineté numérique, Statu quo et champs d'action, Munich 2021 (cited: Kagerman et al.).

Kaloudis Martin, Digital Sovereignty–European Union's Action Plan Needs a Common Understanding to Succeed, *in* History Compass, 2021, vol. 19, no. 12 (cited: Kaloudis, Action plan).

Kaloudis Martin, Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan?, *in* New Global Studies, 25 October 2021 (cited: Kaloudis, Index).

Lambach Daniel / Oppermann Kai, Narratives of digital sovereignty in German political discourse, *in* Governance Journal (early view), 2022, 1 ff.

Lu Yen-Chi / Mayer Maximilian, Illusions of Autonomy? Global Digital Dependence Structures, Bonn 2022.

Lundvall Bengt-Åke / Rikap Cecilia, China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems, *in* Research Policy, 2022, vol. 51, no. 1.

Luzeaux Dominique, *Cloud* souverain: souveraineté et résilience, ou confiance ?, *in* Revue Défense Nationale, 2022, vol. 855, no. 10, 14 ff.

Malinverni Giorgio / Hottelier Michel / Hertig Randall Maya / Flückiger Alexandre, Droit constitutionnel suisse, vol. I : L'Etat, 4th éd., Berne 2021 (cited: Malinverni et al.).

March Christoph / Schieferdecker Ina, Technological Sovereigntyas Ability, Not Autarky, Center for Economic Studies and IfoInstitute (CESifo) Working Paper, 2021, no. 9139.

Maurer Tim / Skierka Isabel / Morgus Robert / Hohmann Mirko, Technological Sovereignty: Missing the Point?, *in* 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, p. 53 ff (cited: Maurer et al.).

Mayer Pierre, Le phénomène de la coordination des ordres juridiques étatiques en droit privé : cours général de droit international privé, *in* RCADI, 2007, vol. 327, 9 ff.

Montavon Michael, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Zurich 2021.

Montavon Michael / Schwab Stéphane, eGovernment : quelques comparaisons et réflexions à partir de l'exemple estonien (1/2), Revue fribourgeoise de jurisprudence (RFJ), 2019.

O'Neil Cathy, Algorithmes, la bombe à retardement, Paris 2018.

Pagano Ugo, The crisis of intellectual monopoly capitalism, *in* Cambridge Journal of Economics, 2014, vol. 38, no. 6, 1409 ff.

Pohle Julia, Digital Sovereignty, A New Key Concept of Digital Policy in Germany and Europe, Berlin 2020.

Pohle Julia / Thiel Thorsten, Digital Sovereignty, *in* Herlo Bianca / Irrgang Daniel / Joost Gesche / Unteidig Andreas (Ed.), Practicing Sovereignty, Digital Involvement in Times of Crises, Bielefeld 2021, 47-67.

Pretelli Ilaria, Conflict of Laws in the Maze of Digital Platforms/Le droit international privé dans le labyrinthe des plate-formes digitales, Zurich 2019.

Puglierin Jana / Zerka Pawel (Ed.), European Sovereignty index, ECFR/451, June 2022 <https://ecfr.eu/wp-content/uploads/2022/06/European-Sovereignty-Index.pdf>.

Ramos Gretchen / Maciejewski Andrea / Jongen Herald (Greenberg Traurig LLP), Application of the CLOUD Act to EU Entities, Memorandum to the Dutch Ministry of Justice and Security, 26th July 2022 <https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo> (cited: Ramos et al.).

Robinson Nick / Kask Laura / Krimmer Robert, The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis, *in* ICEGOV2019, Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, 2019, 391 ff (cited: Robinson et al.).

Roguski Przemysław, Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment, *in* 11th International Conference on Cyber Conflict (CyCon), 2019, 1 ff.

Schmitz Luuk / Seidl Timo, As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy, *in* Journal of Common Market Studies (JCMS), 2022, 1 ff.

Schwarzenegger Christian / Thouvenin Florent / Stiller Burkhard, Avis de droit concernant l'utilisation des services de cloud par les avocates et avocats, 2019 <https://digital.sav-fsa.ch/documents/1060627/1169162/gutachten_sav-franzoesisch.pdf/81740267-8cf0-36b1-6918-c3ddb9c71ee4?t=1618228137307> (cited: Schwarzenegger et al.).

Seifried Mareike / Bertschek Irene, Schwerpunktstudie Digitale Souveränität, Berlin 2021.

Sheikh Haroon, European Digital Sovereignty: A Layered Approach, *in* Digital Society (DISO), 2022, vol. 1, no. 25.

Tan Kheng-Leong / Chi Chi-Hung / Lam Kwok-Yan, Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization, 2022 (cited: Tan et al.).

Thelisson Eva, La portée du caractère extraterritorial du Règlement général sur la protection des données, *in* Revue internationale de droit économique 2019/4, 501 ff.

Tipper David / Krishnamurthy Prashant, Digital Sovereignty and Resilience, 1 August 2022.

Türk Pauline, Définition et enjeux de la souveraineté numérique, 14 September 2020 <https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique>.

Van Hecke George A., Le droit anti-trust : aspects comparatifs et internationaux, *in* Recueil des cours de l'Académie de droit international de La Haye, 1962, vol. 106, 309 ff.

Vatanparast Roxana, Data Governance and the Elasticity of Sovereignty, *in* Brooklyn Journal of International Law (Brook. J. Int'l L), 2020, vol. 46, no. 1, 1 ff.

Weber Herbert, Digitale Souveränität, *in* Informatik Spektrum, 2022, vol. 45, 152 ff (cited: Weber H.).

Weber Rolf H., Digital Sovereignty revisited, new elements for a shared and cooperative concept, jusletter 2023, 73 (cited: Weber R., Digital Sovereignty revisited).

Weber Rolf H., Elements of a Legal Framework for Cyberspace, *in* Swiss Review of International and European Law, 2016, vol. 26, no. 2, 195 ff (cited: Weber R.).

Westphal Kirsten, Strategic sovereignty in energy affairs: reflections on Germany and the EU's ability to act, SWP Comment 7/2021, Berlin 2021.

Wood Sam / Hoffmann Stacie / McFadden Mark / Kaur Akhiljeet / Wongsaroj Sarongrat / Schoentgen Aude / Forsyth Grant / Wilkinson Laura, Digital Sovereignty: the overlap and conflict between states, enterprises and citizens, London 2020, p. 11 (cited: Wood et al.).

Yen Huai-Shing, Digital Autonomy and Taiwan–EU Partnership, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 105-110.

Yuguchi Kiyotaka, Japan: Digital Sovereignty as an Element of the Economic Security, *in* Pogorel Gérard / Nestoras Antonios / Cappelletti Francesco (Ed.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles 2022, 75-84.

Zufferey Jean-Baptiste, Le traitement de l'énergie en droit de la construction : Une belle illustration des problèmes du renvoi aux normes techniques, *in* Hottelier M. / Foëx B. (Ed.), La propriété immobilière face aux défis énergétiques : Du statut juridique de l'énergie au contrôle des loyers, Genève 2016.

6. Fachtagung Bedrohungsmanagement – Umsetzung Istanbul-Konvention

Luca Lehmann / Vivian Stein*

I. Einleitung

Das Zuhause ist für viele Menschen ein Ort der Ruhe, der Entspannung und der Vertrautheit. Leider ist es oftmals auch ein Ort, an dem Gewalt verübt wird. Unter dem Titel „Gewalt gegen Frauen" wurde dieser bedauerliche Umstand durch den Regierungsrat des Kantons Zürich als einer der Schwerpunkte der Legislaturperiode 2019 – 2022 (RRB 184/2019) definiert. Ein zentrales Anliegen war dabei die Umsetzung der Massnahmen des Übereinkommens des Europarates zur Verhütung und Bekämpfung von Gewalt gegen Frauen und Häuslicher Gewalt (Istanbul-Konvention). Die „Fachtagung Bedrohungsmanagement – Umsetzung der Istanbul-Konvention" am 3. November 2022 in Zürich unter der Leitung von Prof Dr. CHRISTIAN SCHWARZENEGGER, Professor für Strafrecht, Strafprozessrecht und Kriminologie an der Universität Zürich, und Major REINHARD BRUNNER, Chef der Präventionsabteilung der Kantonspolizei Zürich, setzte sich mit ebendieser Problematik auseinander. Das Ziel der Veranstalter war die Vermittlung eines Überblickes über die Stossrichtung und den aktuellen Stand der Umsetzungen der Istanbul-Konvention, sowie die Vernetzung zwischen Fachpersonen aus den Bereichen Polizei, Justiz, Bildung, Sicherheit und Soziales.

* MLaw LUCA LEHMANN und BLaw VIVIAN STEIN sind wissenschaftliche Mitarbeitende am Lehrstuhl für Strafrecht, Strafprozessrecht und Kriminologie von Prof. Dr. Christian Schwarzenegger an der Universität Zürich.

II. Die Umsetzung der Istanbul Konvention

Nach einer kurzen Begrüssung durch Prof. Dr. Christian Schwarzenegger und dem Einleitungsreferat von lic. iur. Mario Fehr, Regierungsrat und Vorsteher der Sicherheitsdirektion des Kantons Zürich, informierte lic. phil. Irene Huber Bohnet, wissenschaftliche Mitarbeiterin im Bereich Gewalt am Eidgenössischen Büro für die Gleichstellung von Frau und Mann (EBG), die Teilnehmenden über die aktuelle Umsetzung der Istanbul-Konvention in der Schweiz. Die Zahl der Opferberatungen habe sich in den letzten 20 Jahren verdreifacht. Der Grund für die Zunahme liege aber nicht in der erhöhten Inzidenz solcher Vorfälle, sondern an der verstärkten Inanspruchnahme von Hilfe und einer gesteigerten Anzeigequote. Mit dem Inkrafttreten der Istanbul-Konvention im Jahr 2018 sei auch ein politischer Aufschwung der Themen häusliche Gewalt und Gewalt gegen Frauen einhergegangen. Vor dem Jahr 2018 wurden auf Bundesebene stets weniger als zwei parlamentarische Vorstösse unternommen, seither ist diese Zahl jedoch auf sieben bis zehn Vorstösse pro Jahr gestiegen. In verschiedenen Kantonen und Städten wurden zudem Aktionspläne und Massnahmen zur Prävention von Gewalt gegen Frauen verfasst und umgesetzt. Zusätzlich wurde auf Bundesebene der „Nationale Aktionsplan zur Umsetzung der Istanbul-Konvention" (NAP IK) lanciert. Der NAP IK ist eine prioritäre Massnahme der Gleichstellungsstrategie 2030 und wurde durch die Delegierten aller föderalen Ebenen erarbeitet. Die drei Schwerpunkte des NAP IK liegen auf der Information und Sensibilisierung der Bevölkerung, der Aus- und Weiterbildung von Fachpersonen und ehrenamtlich Tätigen sowie auf dem verstärkten Fokus auf sexualisierte Gewalt. Im Rahmen des NAP IK wurden 44 Massnahmen verabschiedet, darunter 22 auf Bundes- und 15 auf Kantonsebene. Die konkrete Umsetzung des NAP IK erfolgt ab 2022 gemäss föderalen Zuständigkeiten bzw. der Sektoralpolitik des Bundes und wird durch das EGB koordiniert. Mit Hilfe eines jährlichen Monitorings wird im Jahr 2024 ein Zwischen- und im Jahr 2026 ein Abschlussbericht erstellt, auf deren Grundlage die Weiterführung des NAP IK geprüft werden wird. Der Vortrag zur Umsetzung der Istanbul-Konvention im Kanton Zürich wurde im Anschluss durch lic. iur. Regina Carstensen, Rechtsanwältin, und lic. phil. Rahel Ott in ihrer Funktion als Co-Fachverantwortliche für die Interventionsstelle gegen Häusliche Gewalt der Kantonspolizei Zürich (IST) gehalten. Die IST gehört zur Präventionsabteilung der Kantonspolizei Zürich und wird durch §15 des Gewaltschutzgesetzes des Kantons Zürich damit beauftragt, die Zusammenarbeit der mit häuslicher Gewalt und Stalking befassten Behörden und Beratungsstellen zu gewährleisten, zu steuern, zu koordinieren und zu überprüfen. Im Rahmen des Regierungsratsbeschlusses „Gewalt gegen Frauen" wurde die IST daher damit betraut, gestützt auf eine Situationsanalyse Massnahmen zur Umsetzung der

Istanbul-Konvention zu empfehlen. Zu diesem Zweck wurde die Arbeitsgruppe Koordination Istanbul-Konvention (AG KIK) ins Leben gerufen. Diese Arbeitsgruppe wurde der Leitung der IST unterstellt und umfasste unter anderem die Kantonale Opferhilfestelle, die Fachstelle Gleichstellung für Frau und Mann sowie die Bewährungs- und Vollzugsdienste des Kantons Zürich. Am 12. April 2021 konnte der Zürcher Regierungsrat – gestützt auf die Arbeit der AG KIK – 16 prioritäre Massnamen in neun Bereichen präsentieren (RRB 338/2021). Die Aus- und Weiterbildungsmassnahmen stellten dabei den Schwerpunkt des Regierungsratsbeschlusses dar und bezogen sich überwiegend auf Fachpersonen aus dem Bereich des Gesundheitssektors, der Schulsozialarbeit und der Strafverfolgung. Darüber hinaus wurden Massnahmen zur Arbeit mit gewaltausübenden Menschen mit dem primären Ziel, Rückfälle zu verhindern, eingeführt. Weiter soll der Zugang zur Opferhilfe und zu Schutzunterkünften für alle sichergestellt werden, das heisst nicht nur für Betroffene von sexueller oder häuslicher Gewalt, sondern von unmittelbar auch involvierten Kindern. Die Kinder sollen durch schulische Präventionsarbeit über die Problematik informiert und im Fall einer Betroffenheit angemessen unterstützt werden. Auch sollen sich Fachpersonen in der Bildung darauf konzentrieren, Anzeichen häuslicher Gewalt frühzeitig zu erkennen und gezielt Hilfe zu leisten. Als weitere Massnahmen wurde durch die Justizbehörden eine Null-Toleranz-Strategie in Bezug auf Gewalt gegen Frauen und häusliche Gewalt eingeführt. Diese Strategie richtet sich sowohl an die Strafverfolgungsbehörden als auch an die RichterInnen der Straf- und Zwangsmassnahmengerichte. Als letzte Massnahme wurde angeordnet, dass einheitliche Datenerhebungen in allen IK-relevanten Bereichen durchgeführt werden, um eine bessere statistische Grundlage für zukünftig Entscheidungen sicherzustellen. In der ersten Diskussionsrunde wurden die Expertinnen gefragt, welche Probleme sie bei Ihrer Tätigkeit feststellen konnten und welche konkret zu unternehmenden Schritte sie zur Lösung vorschlagen würden. Ein grosses Problem sahen die Expertinnen in der dünnen Datenlage. Bisher mussten sich die ExpertInnen mit den Zahlen zur häuslichen Gewalt in Gerichts-, Strafurteils- und Anzeigestatistiken begnügen. Doch selbst nach der Einführung von Prävalenzstudien, was zurzeit im Parlament besprochen wird, würde das Dunkelfeld weiterhin einen grossen Teil der Gewalterfahrungen umfassen. Eine zusätzliche Problematik ergebe sich daraus, dass nur rund ein Drittel der Anzeigen tatsächlich zur Ausstellung eines Strafbefehls oder einer Anklageerhebung führen. Dass zwei Drittel der Verfahren scheitern, liege gemäss den Angaben der Expertinnen unter anderem daran, dass sich mehr als die Hälfte der Opfer selbst aus dem Verfahren zurückziehe. Darüber hinaus ist die Beweislage bei Vier-Augen-Delikten oftmals schwierig. In einer Gesamtbetrachtung führe das aktuell grosse Dunkelfeld und die tiefen Strafurteilsquoten somit zu einem unbefriedigenden

Ergebnis, welches nicht vermag, die tatsächliche Prävalenz häuslicher Gewalt wiederzugeben. Als konkrete, noch zu unternehmende Schritte nannten die Expertinnen einerseits die Aufnahme von Massnahmen gegen die digitale Gewalt und Hassverbrechen in den NAP IK, und andererseits die Schaffung eines spezifischen StGB[1]-Straftatbestandes für „Stalking". Obwohl der Umgang mit digitaler Gewalt und Hassverbrechen erst noch in der Findungsphase stehe, sei eine Umsetzung spezifischer Massnahmen im NAP IK für den ersten Zwischenbericht im Jahr 2024 geplant. Bereits jetzt würden solche Delikte aber in der polizeilichen Kriminalstatistik erfasst. In Bezug auf die Schaffung eines Straftatbestandes „Stalking" seien aktuelle Bestrebungen im Gange. Denn obwohl das Stalking materiellrechtlich grundsätzlich vom Straftatbestand der Nötigung (Art. 181 StGB) umfasst sei, könne es vorkommen, dass einzelne Tatbestandsmerkmale der Nötigung in einem Stalking-Fall nicht gegeben seien, sodass eine Strafbarkeit nach Art. 181 StGB ausser Betracht falle. Die Schaffung eines eigenen Straftatbestandes „Stalking" sei aber auch nach der Ansicht des Bundesrates auf jeden Fall zu bevorzugen, da dies eine Signalwirkung entfalten würde.

Im Anschluss referierte RAin lic. iur. Sandra Müller, Leiterin der Kantonalen Opferhilfestelle des Kantons Zürich, zur Umsetzung der Istanbul-Konvention und der damit verbundenen Chancen und Herausforderungen aus Sicht der Opferhilfestellen. Sie leitete ihr Referat mit einer Erläuterung von Art. 7 und 9 der Istanbul Konvention ein, der relevanten vertraglichen Grundlagen, welche die Einführung ganzheitlicher Massnahmen gegen häusliche Gewalt verlangen, bei denen die Rechte des Opfers im Zentrum stehen. Ganzheitlich bedeutet hierbei auch, dass nicht nur staatliche, sondern auch nichtstaatliche Akteure zusammenarbeiten und letztere Organisationen anerkannt, gefördert und unterstützt werden sollen. In vielen Kantonen liegt die Opferhilfe auch heute (noch) in privater Hand, da sie erst mit Einführung des Opferhilfegesetzes[2] zur staatlichen Aufgabe wurde und die Auslagerung an Private gesetzlich ausdrücklich möglich ist. Das bietet die Vorteile, dass die Kantone vom bestehenden Erfahrungs- und Wissenspotenzial der, insb. auch spezialisierten, Beratungsstellen profitieren können und es einfacher ist, dem Erfordernis der fachlichen Unabhängigkeit der Opferhilfestellen gerecht zu werden. Da die Hemmschwelle bei Kontaktaufnahme mit privaten Organisationen oft niedriger ist, können aber auch Opfer von der Auslagerung profitieren. Doch nicht nur die Istanbul-Konvention und das OHG, sondern auch sich häufig über-

[1] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

[2] Bundesgesetz über die Hilfe an Opfer von Straftaten (Opferhilfegesetz, OHG) vom 23. März 2007, SR 312.5.

schneidende kantonale, interkantonale und Bundesvorgaben regeln die Tätigkeit der Opferhilfeorganisationen. So sind in der Roadmap von Bund und Kantonen beispielsweise die Einführung einer schweizweiten, rund um die Uhr bedienten, zentralen Beratungshotline (Handlungsfeld 5) und die Sicherstellung von ausreichenden Plätzen in Schutzunterkünften und angemessene Betreuung im Strafverfahren (Handlungsfeld 6) vorgesehen. Der Kanton Zürich verfolgt zusätzlich dazu unter der Organisation der Direktion der Justiz und des Inneren und unter Zusammenarbeit der vielen beteiligten Akteure einen eigenen Massnahmenplan. Dieser unterteilt sich in sechs Teilprojekte, reichend von einer Verbesserung der Kommunikation zwischen den einzelnen Akteuren, über ein kontinuierliches Monitoring, um Verbesserungspotenzial zu erkennen, bis hin zu einer Verbesserung der Finanzierung.

Prof. Beat Reichlin, teilamtlicher Bezirksrichter am Bezirksgericht Zürich und Professor für Familien- und Sozialrecht an der Hochschule Luzern, beschäftigte sich in seinem Vortrag mit dem Thema „Kinder als (Mit-)Betroffene von Häuslicher Gewalt – was ist zu tun?". Die elterliche Streitkultur hat einen grossen Einfluss auf die Gesundheit der Kinder und kann – gerade im Falle elterlicher Paargewalt – sogar dazu führen, dass die Kinder krank werden und beispielsweise an Schlafstörungen, Aggressivität oder Kopf- und Bauchschmerzen leiden. Das durch die Gewalt zwischen den Eltern geschaffene Familienklima hat aber auch psychische Auswirkungen auf die Kinder und verursacht unter anderem Loyalitätskonflikte und Schuldgefühle. Im Umgang mit den betroffenen Kindern ist es daher wesentlich, dass ihnen eine Subjektstellung im Verfahren zukommt, wie es auch die UN-Kinderrechtskonvention verlangt. Um in diesem besonderen Setting für Entscheide im Interesse des Kindes eine Unterstützung für Behörden zu bieten, wurde basierend auf dem Frankfurter Leitfaden zum Umgang nach häuslicher Gewalt ein schweizerischer Leitfaden entwickelt. Der Leitfaden soll einerseits aufzeigen, welche Entscheidungsgrundlagen und Einschätzungen herangezogen werden können und müssen, und andererseits eine Übersicht darüber geben, welche Massnahmen und Möglichkeiten in anderen Bereichen bestehen. Der Schutz des Kindeswohls ist nämlich eine Verbundaufgabe vieler Kräfte. Zentral für alle Beteiligten, und insb. die Eltern, ist es, dass der Fokus weg von einem „Recht haben" im Konflikt hin zu einer Lösung gerichtet wird, bei der das Kind im Zentrum steht. Dies ist besonders anspruchsvoll, wenn es um die Ausgestaltung des Kontakts zwischen dem Kind und dem gewaltausübenden Elternteil geht. Nach einer ersten kontaktfreien Phase stellen sich hier viele Fragen, die nicht nur das Kind, sondern auch beide Elternteile betreffen, z.B. ob durch den Kontakt das Kind retraumatisiert werden könnte, aus welchen Motiven der gewaltausübende Elternteil den Kontakt zum Kind wünscht, oder ob der ge-

waltbetroffene Elternteil stabil genug ist, um allfällige emotionale Reaktionen des Kindes abzufangen. Das Recht ermöglicht hier eine Vielzahl differenzierter Ausgestaltungen des Umgangs, um der individuellen Situation Rechnung zu tragen, reichend von einer vollständigen Verweigerung des persönlichen Verkehrs (Art. 274 Abs. 2 ZGB[3]), über eingeschränkte Kontakte, beispielsweise in Verbindung mit Weisungen, bis hin zu einem völlig uneingeschränkten persönlichen Verkehr. Für das Kind am wichtigsten ist aber, dass die Verantwortung für das Vorgefallene von ihm weggenommen, die Situation offen angesprochen und in klarer Weise Stellung gegen gewalttätige Verhaltensweisen eingenommen wird. In der anschliessenden Diskussion stellte sich die Frage, ob es nicht sinnvoller wäre, die Opferhilfe auf Bundesebene zu konzentrieren, um eine gewisse Einheitlichkeit und Konzentration des „Know Hows" zu erwirken. Dies wurde zwar als grundsätzlich wünschenswert bezeichnet, auch da für die Opfer besser erkennbar wäre, an wen sie sich wenden können. Die unterschiedlichen kantonalen Strukturen und insb. die starke Auslagerung der Opferhilfe in der Deutschschweiz machen ein derartiges Vorhaben jedoch schwer umsetzbar.

III. Umgang mit sexueller Gewalt

Nach dem Mittagessen stellten MLaw Nicole Fernandez, Rechtsanwältin und Fachverantwortliche für Sexualdelikte der Kantonspolizei Bern, und Hauptmann Gérald Pfeifer, Chef der Ermittlungsabteilung Gewaltkriminalität der Kantonspolizei Zürich, in ihren Vorträgen die Modelle ihrer Kantone zum Umgang mit sexueller und häuslicher Gewalt – das Berner und das Zürcher Modell – vor. Das Ziel beider Modelle ist es, betroffenen Frauen und Kindern ein effizientes und professionelles Hilfsangebot zur Verfügung zu stellen, welches die komplexe Situation des Opfers sexueller Gewalt respektiert und dadurch möglicherweise eine weitere Traumatisierung zu verhindern. Beide Modelle setzen auf interdisziplinäre Kooperation. Das Institut für Rechtsmedizin (IRM) arbeitet mit den Spitälern der beiden Kantone, mit den kantonalen Opferberatungsstellen und den Justizbehörden zusammen, um eine korrekte Umsetzung der beiden Modelle zu gewährleisten. Die interdisziplinäre Zusammenarbeit fördert das gegenseitige Verständnis und die Vertrautheit zwischen den Behörden und hilft dabei, im Krisenfall abgesprochene Abläufe bereitzustellen. Das „Berner Modell" funktioniert nach dem Prinzip „von Frauen für Frauen". Zu diesem Zweck steht ein Frauenpikett mit aktuell 47 Polizistinnen jederzeit zur Verfügung, um die Untersuchungen am Körper des Opfers zu orga-

[3] Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB), SR 210.

nisieren, das Opfer einzuvernehmen, über das OHG zu informieren und um den Opfern eine weibliche Bezugsperson zur Verfügung zu stellen. Demgegenüber setzt der Kanton Zürich auf eine strikte Aufgabenteilung. Während die Grundversorgung – also die Entgegennahme von Anzeigen, die Tatortarbeit und die Einleitung von Sofortmassnahmen – den Angehörigen der 60 regionalen Polizeiposten obliegt, wird die weitere Bearbeitung der Fälle schwerer Sexualdelikte durch die spezialisierten Fachdienste der Kantons- und Stadtpolizei Zürich übernommen. Im Gegensatz zum Kanton Bern bestehen diese zwar überwiegend, aber nicht ausschliesslich, aus Frauen. Klare Unterschiede zeigen sich auch bei der Befolgung des Untersuchungsgrundsatzes: Obwohl es sich bei den Sexualdelikten um Offizialdelikte handelt und somit nach den Regeln der Strafprozessordnung die Einleitung eines strafrechtlichen Verfahrens durch die Behörden ohne Anzeige durch das Opfer möglich und erforderlich wäre, eröffnet das Berner Modell dem Opfer die Möglichkeit, selbst über die Erstattung einer Anzeige zu entscheiden. Dies geschieht aus Rücksicht auf die Bedürfnisse des Opfers, da diese oftmals Scham- und Schuldgefühle wegen des sexuellen Übergriffes hätten. Von der Möglichkeit, auf die Einleitung eines strafrechtlichen Verfahrens zu verzichten, werde in der Praxis regelmässig Gebrauch gemacht. Anhand der Zahlen der Jahre 2020 und 2021 wurde aufgezeigt, dass in der Hälfte der Fälle, in denen medizinische Untersuchungen mit Spurensicherung an weiblichen Personen ab 14 Jahren durchgeführt werden, keine Anzeige erstattet wird. Die durch das IRM gesicherten Spuren werden – auch bei einem vorgängigen Verzicht auf eine Strafanzeige – jedoch während 15 Jahren (entsprechend der Verjährungsfristen von Sexualdelikten) aufbewahrt. Im Kanton Zürich ist der Beizug des IRM demgegenüber nur unter der Bedingung einer Strafanzeige möglich. Als Begründung nannte Hauptmann Pfeifer die hohe Dunkelziffer, insbesondere da rund ein Drittel der schweizweiten schweren Sexualdelikte in Zürich begangen würden. Zurzeit geht man davon aus, dass nur 10% der tatsächlich verübten Sexualdelikte später zu einer Anzeige führen. In neun von zehn Fällen bleiben schwere Sexualdelikte somit heute – auch nach dem Inkrafttreten der Istanbul-Konvention – noch unverfolgt und unbestraft.

IV. Präventionsstrategien

Im Anschluss hielt Joder Regli, Diplo. Sozialarbeiter FH, Bereichsleiter Fachsupport & Lernprogramme, Justizvollzug und Wiedereingliederung Kanton Zürich (JuWe), Bewährungs- und Vollzugsdienste (BVD) des Kantons Zürich, einen Vortrag zu dem Thema „Lernprogramme – Eine wirksame und kostengünstige Intervention gegen häusliche Gewalt". Die Istanbul Konvention ver-

pflichtet die Vertragsparteien, Programme einzuführen, die darauf ausgerichtet sind, das Verhaltensmuster der Täter zu ändern. Dies, und das Inkrafttreten des Bundesgesetzes über die Verbesserung des Schutzes gewaltbetroffener Personen, hat dazu geführt, dass seit 2020 schweizweit eine Zunahme solcher, vorher eher dünn gesäten, Programme und auch der verpflichtenden Anordnungen zur Teilnahme an selbigen zu verzeichnen war. Gleichzeitig wurde mit der Inkraftsetzung des Art. 55a StGB für Staatsanwaltschaften und Gerichte die Möglichkeit geschaffen, für die Dauer der Sistierung einer Strafverfolgung wegen häuslicher Gewalt die Teilnahme an diesen Lernprogrammen für die mutmasslichen TäterInnen anzuordnen. In Zürich wird seit 2000 das Programm „Partnerschaft ohne Gewalt" PoG® verwendet, das auf kognitiv-verhaltenstherapeuthischen Grundsätzen beruht. Die Anordnung der Teilnahme am PoG nahm seit 2020 massiv zu, wobei 2/3 der Zuweisungen im Rahmen der Strafuntersuchung erfolgten. Da die meisten Täter nicht rechtskräftig verurteilt sind, wird deshalb im Rahmen des Lernprogramms nicht vom Delikt, sondern von dem „Vorfall in der Beziehung" gesprochen. Ziel des Programms ist es, den Tätern mit Hilfe eines Arbeitshefts, Gruppen- und Einzelsitzungen sowie Nachkontrollgesprächen beizubringen, die Verantwortung für ihr problematisches Verhalten zu übernehmen, ihre Denk- und Verhaltensweisen zu ändern und ein gewaltfreies Vorbeugen und Bewältigen von Risikosituationen zu vermitteln und so Rückfälle vorzubeugen. Damit dies möglich ist, müssen die Teilnehmenden volljährig sein, sich auf Deutsch verständigen können und zumindest eingestehen, dass sie Beziehungsprobleme haben. Nicht erforderlich hingegen ist die Motivation zur Teilnahme, dies ist gerade ein zentraler Bestandteil des Vermittlungsauftrags, oder dass die Person im Sachverhalt geständig ist. Da es etwa zwei Monate dauert, bis eine gewisse Stabilität erzielt werden kann, ist das Programm nicht für Personen mit akuter Ausführungsgefahr geeignet, und auch Personen mit schweren psychischen Erkrankungen oder Selbstmelder sind von der Teilnahme ausgeschlossen. Dass durch die Teilnahme eine erfolgreiche Prävention von häuslicher Gewalt möglich ist, zeigten dabei nicht nur die Rückmeldungen der Absolventen, sondern auch eine Studie zur Rückfälligkeit: Im Beobachtungszeitraum von zwei Jahren wurde die Rückfallrate für (gemeldete) allgemeine Gewaltdelikte halbiert und kein Zwischenfall partnerschaftlicher Gewalt polizeilich registriert. Das Programm überzeugt aber nicht nur aus präventiver, sondern auch aus finanzieller Sicht. So kostet die Teilnahme für eine Person zwischen 2800 und 3600 CHF, die lebenslangen Gesamtkosten eines Rückfalls liegen dagegen bei schätzungsweise CHF 150'000. Die Zukunft des PoGs sieht der Referent in der Digitalisierung und insbesondere der Ausarbeitung einer unterstützenden App. Er kam zu dem Fazit, dass Lernprogramme ein wichtiger Teil

der Umsetzung der Istanbul-Konvention darstellen, bereits in vielen Kantonen vorhanden seien und ihr grosser Vorteil darin liegt, dass sie kostengünstig und effektiv seien.

Im Anschluss gab lic. iur. CLAUDIA WIEDERKEHR, leitende Staatsanwältin, Staatsanwaltschaft Limmatthal/Albis, Kanton Zürich zusammen mit Major REINHARD BRUNNER, Chef der Präventionsabteilung, Kantonspolizei Zürich, einen Rück- und Ausblick zum Thema „Gewalt gegen Frauen", das bereits seit 2012 einen Schwerpunkt der regierungsrätlichen Tätigkeit bildet. Positive Effekte dieser Politik lassen sich beispielsweise an einer Verdoppelung der Anzeigerate im Bereich der Tätlichkeiten (Art. 126 StGB) und damit einer Erhellung des Dunkelfelds verzeichnen. Im Sinne eines Rückblicks zeigten die Referenten auch auf, dass mit 6677 Einsätzen wegen familiärer Differenzen und häuslicher Gewalt im Jahre 2021 und 1217 Massnahmen nach dem Bundesgesetz über die Verbesserung des Schutzes gewaltbetroffener Personen (was auch Stalking durch Drittpersonen erfasst), immer noch Handlungsbedarf besteht. Bis jetzt hat der Regierungsrat in seiner Präventionsstrategie unter anderem auf eine bessere Information und Sensibilisierung der Öffentlichkeit, beispielsweise durch eine gemeinsame Plakat-Kampagne mit Polizei, Staatsanwaltschaft und der kantonalen Opferhilfestelle, sowie der Website <www.stopp-gewalt-gegen-frauen.ch>, gesetzt. Ein weiteres Mittel war der Ausbau von Unterstützungs- und Hilfsangeboten für die Opfer und auch die Anordnung des Zürcher Lernprogramms PoG, als Massnahme zur Senkung der Gewaltbereitschaft der gefährdenden Personen, sowie die Umsetzung der Vorgaben der Istanbul Konvention. Im Anschluss wurde in einem Ausblick aufgezeigt, dass der Schwerpunkt Gewalt gegen Frauen in den Jahren 2023-2026 erweitert werden und unter anderem eine obligatorische Weiterbildungsveranstaltung für alle Fallbearbeitenden eingeführt werden soll. Weiter will sich der Kanton weiterhin an Projekten zur Information und Sensibilisierung der Öffentlichkeit beteiligen und die Stellung des Opfers in Verfahren zu häuslicher Gewalt soll weiter verbessert werden. Weitere Instrumente im Kampf gegen Gewalt gegen Frauen sind die Einführung von schweizweiten Qualitätsstandards im Rahmen des kantonalen Bedrohungsmanagements und die Umsetzung des Roadmaps des nationalen Aktionsplans. In der anschliessenden Diskussion kam die Frage auf, wer in das Lernprogramm PoG aufgenommen werden könne, und es wurde mit Blick auf die Erfolgsrate als wünschenswert erachtet, in der Zukunft alle Täter hier zu integrieren, sofern ihre Risikoevaluation dies zulasse. Mit Blick auf Zürichs Schwerpunkt gegen häusliche Gewalt kam die Frage auf, welche Rolle Electronic Monitoring als Ersatzmassnahme einnehme. Dies ist zwar Teil des Roadmaps, es wurde aber zum Zeitpunkt der Konferenz noch in keinem Fall angewandt. Dies auch, weil es schwere Delikte oder eine Flucht im

Anschluss nicht verhindern kann, sondern einzig erlaubt, festzustellen, ob eine Person sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hat. Im Anschluss an die Diskussion fasste Prof. Dr. CHRISTIAN SCHWARZENEGGER die Erkenntnisse der einzelnen Vorträge noch einmal zusammen und kam zu dem Schluss, dass seit Beginn der Fachtagung Bedrohungsmanagement bereits viel zur Verhinderung der Gewalt gegen Frauen geschafft wurde, das Ziel jedoch noch nicht erreicht worden sei.

1. Jahrgang

HERAUSGEBER

WISSENSCHAFTLICHER BEIRAT

REDAKTION

Dr. Tobias Baumgartner, LL.M., Rechtsanwalt /
MLaw Sophie Tschalèr
Europa Institut an der Universität Zürich
Hirschengraben 56
8001 Zürich
Schweiz

URHEBERRECHTE

ERSCHEINUNGSWEISE

R&R – Risiko & Recht erscheint dreimal jährlich online. Die Ausgaben werden zeitgleich im Wege des print on demand veröffentlicht; sie können auf der Verlagswebseite (www.eizpublishing.ch) sowie im Buchhandel bestellt werden.

ZITIERWEISE

R&R, Ausgabe 1/2023, …

KONTAKT

EIZ Publishing
c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

ISSN

2813-7841 (Print)
2813-785X (Online)

ISBN:

978-3-03805-605-8 (Print – Softcover)
978-3-03805-606-5 (PDF)
978-3-03805-607-2 (ePub)

VERSION

1.01-20230929

DOI

Zeitschrift: https://doi.org/10.36862/eiz-rrz01
Ausgabe: https://doi.org/10.36862/eiz-rr202301
Artikel:
Thomas Noll / David Hans / Michael Weber, Radikalisierung im Bereich des islamistischen Extremismus: Allgemeine Beobachtungen und ausgewählte Modelle, https://doi.org/10.36862/eiz-rr202301-01
Tobias Tschumi / Marc Häusler, Chlorothalonil-Rückstände im Trinkwasser – eine Bestandesaufnahme und rechtliche Einordnung, https://doi.org/10.36862/eiz-rr202301-02
Yaniv Benhamou / Frédéric Bernard / Cédric Durand, Digital Sovereignty in Switzerland: the laboratory of federalism, https://doi.org/10.36862/eiz-rr202301-03

RISIKO

EIZ Publishing

Herausgeber:
Prof. Dr. Tilmann Altwicker
PD Dr. Goran Seferovic
Prof. Dr. Franziska Sprecher
Prof. Dr. Stefan Vogel
Dr. Sven Zimmerlin

RISIKO & RECHT **AUSGABE 01 / 2023**

RECHT