Schutzbehauptungen –
wer schützt uns vor den Beschützern?

Ein philosophisch-juristischer Essay über digitale Selbstbestimmung, Schutz und Macht

Gerd Raudenbusch

Fachbereich für Rechtsphilosophie / Digital Ethics

December 8, 2025

Zusammenfassung

Deutsch: Der Essay beleuchtet die Ambivalenz des Schutzbegriffs im digitalen Zeitalter. Staatliche und private Akteure beanspruchen, das Individuum vor Risiken zu bewahren, verschieben dabei aber Machtverhältnisse und entziehen Selbstbestimmung. In Anlehnung an Arendt, Foucault und Galtung zeigt der Text, dass Schutz über seine Intention in Gewalt umschlagen kann, wenn er Autonomie ersetzt. Er entwickelt die Idee eines *Grundrechts auf digitale Selbstbestimmung (Art. 2a GG)*, das Schutz als Ermächtigung statt Bevormundung versteht – und skizziert, wie die Rechtsordnung der Zukunft Freiheit nicht vor Risiken, sondern durch Verantwortung sichern sollte.

English: This essay examines the ambivalence of the concept of protection in the digital age. State and corporate actors claim to safeguard individuals from risk while undermining autonomy. Drawing on Arendt, Foucault, and Galtung, it argues that "protection" becomes a form of violence when it replaces agency with control. It proposes a *constitutional right to digital self-determination (Art. 2a of the Basic Law)* as a normative response, redefining protection as empowerment rather than paternalism.

1. Der Schutz als politisches Paradigma

Es gibt kaum ein Wort, das in unserer Zeit häufiger bemüht wird als „Schutz". Schutz ist zu einem der mächtigsten Begriffe der modernen Politik und Technologie geworden. Der Staat will seine Bürger schützen, Unternehmen wollen ihre Nutzer schützen, Algorithmen wollen uns vor uns selbst schützen – vor falschen Informationen, schlechten Entscheidungen, gefährlichem Verhalten.

Schutz ist eine klassische Rechtfertigungsfigur von Macht. Schon in der politischen Philosophie des Gesellschaftsvertrags galt: Der Bürger überträgt einen Teil seiner Freiheit an den Souverän, um im Gegenzug Schutz zu erhalten. Hobbes' *Leviathan* verkörperte diesen Pakt – ein notwendiges Übel, um das Chaos des Naturzustands zu überwinden. Doch was, wenn er vom Mittel zum Zweck wird und Freiheitsräume absorbiert? Was Hobbes als Zwang zur Ordnung beschrieb, ist heute zur Normalität verschleierten Zwangs geworden. Der Schutz, der einst Vertrauen bedeutete, ist zu einem Machtinstrument geworden. Ob Cyberabwehr, Pandemiebekämpfung oder Content-Moderation – Schutz scheint zwar unzweifelhaft gut, doch:

Wer schützt uns vor den Beschützern?

2. Die Logik des Schutzes als Machttechnik

Schutz erzeugt immer ein asymmetrisches Verhältnis: Wer schützt, entscheidet, wovor geschützt wird und wie viel Freiheit dafür aufgegeben werden darf. Diese Logik findet sich in der digitalen Welt in ihrer reinsten Form. BigTech-Konzerne erklären, sie sammelten Daten, um das Nutzererlebnis zu verbessern, um Sicherheit und Komfort zu gewährleisten. Der Staat wiederum fordert Überwachung aus Gründen der nationalen Sicherheit, des Seuchenschutzes oder der öffentlichen Ordnung. Doch hinter all diesen Begründungen steht dieselbe Struktur – sie verschiebt Verantwortung vom Individuum zur Institution.

Mediale Gewalt liegt nicht im Medium, solange das Medium selbst gewaltlos ist, sondern in seiner Benutzung. Technologien sind neutral. Gewalt entsteht erst durch Intention und Zweck – durch die politischen, wirtschaftlichen und kulturellen Absichten, die sie leiten. Dann können aus Werkzeugen Waffen werden, wenn sie eingesetzt werden, um den Einzelnen zu infiltrieren, sein Verhalten zu lenken, Abweichung zu sanktionieren oder Kontrolle zu legitimieren.

Ein „sicheres“ Internet, das intransparent moderiert, oder eine KI-gestützte Überwachung, die Prävention zur Dauerdiagnose erhebt, illustrieren diese Paradoxie. Die Gewalt der Beschützer liegt nicht im Datensatz, sondern in der **Übernahme der Deutungshoheit** über Risiko und Gefahr. Unter dem Vorwand des Schutzes wird Zwang unsichtbar: aus Werkzeugen werden Waffen. Filterung, Scoring-Systeme oder Überwachung transformieren Schutz in Disziplinierung. Das paternalistische Element dabei ist altbekannt: Die Behauptung, man wisse besser, was gut für uns sei. Aber während im analogen Zeitalter Schutz durch Regeln oder physische Grenzen stattfand, geschieht er heute durch unsichtbare Mechanismen – durch Algorithmen, Filterblasen, Verhaltensprofile. Der Schutz ist digital geworden, ebenso wie die Bevormundung. BigTech und Staat bilden gemeinsam eine neue Schutzfigur: den digitalen Leviathan. Seine Macht stützt sich nicht auf Gewalt, sondern auf Information. Er kennt uns besser, als wir uns selbst kennen sollen. Wer seine Dienste nutzt, stimmt implizit einer Herrschaftsform zu, die auf Datenhoheit basiert – nicht mehr auf Gesetzen, sondern auf Algorithmen. Damit verschiebt sich die klassische Rechtsordnung: Der Schutz wird nicht mehr als öffentlich-rechtliches Versprechen verstanden, sondern als technologische Dienstleistung. Das Problem liegt darin, dass dieser Schutz nicht gefragt, sondern vorausgesetzt wird. Er wird zum Dogma – freundlich in der Oberfläche, doch total in der Logik.

3. Die Illusion des Vertrauens

Die heutigen digitalen Schutzversprechen ersetzen Vertrauen nicht, sie verlangen es. Jedes „Cookie-Zustimmen“, jedes Einloggen bei einem Cloud-Dienst, jeder Fingerabdruck im Smartphone ist eine stillschweigende Kapitulation: Wir akzeptieren Überwachung, weil sie in bequeme Interfaces verpackt ist. Die Beschützer arbeiten nicht gegeneinander, sondern miteinander – eine Allianz aus Staat und Plattformökonomie, die die Zirkulation von Daten legitimiert, normiert und schließlich monopolisiert.

Diese Kooperation wird meist als Fortschritt verkauft. Doch sie führt zur schleichenden Entmündigung: Wir verlieren nicht nur die Kontrolle über unsere Daten, sondern auch über die Regeln, nach denen wir leben. Die Machtverhältnisse verschieben sich still – weg vom selbstbestimmten Bürger, hin zum überwachten, digital enteigneten und entmündigten, optimierten Nutzer, der sich auch vermarkten und verkaufen lässt.

Die Datenschutz-Grundverordnung (DSGVO) institutionalisiert Schutz als Fürsorgepflicht, nicht als Autonomiegarantie. Sowohl Staat als auch BigTech

schaffen damit ein Schutzsystem, das Abhängigkeit strukturell reproduziert.

4. Zwischen Autonomie und Fürsorgepflicht

Das liberale Rechtsdenken gründet auf der Würde und Autonomie der Person. Artikel 1 und 2 des Grundgesetzes sichern sowohl das Recht auf Selbstbestimmung als auch den Schutz der Persönlichkeit. Doch die Spannungen zwischen Fürsorgepflicht des Staates und Selbstbestimmungsrecht des Individuums sind im digitalen Zeitalter neu zu denken. Digitale paternalistische Praktiken – etwa algorithmische Inhaltssteuerung, verhaltensorientierte Werbung oder staatliche Vorratsdatenspeicherung – verletzen das Kernprinzip der Rechtsstaatlichkeit: dass der Mensch nie bloß Mittel staatlicher oder wirtschaftlicher Ziele werden darf. Kant formulierte diesen Grundsatz in der „Formel des Selbstzwecks“: Der Mensch besitzt einen unveräußerlichen Anspruch darauf, Zweck seiner eigenen Vernunft zu bleiben. Das digitale Schutzregime durchbricht genau diese Grenze, indem es Verhalten steuert, Entscheidungsspielräume verkleinert und Abweichung sanktioniert. Das *Volkszählungsurteil* (1983) etablierte das Recht auf informationelle Selbstbestimmung. Im digitalen Raum jedoch kollidiert dieses Ideal mit algorithmischer Steuerung und ökonomischer Datenlogik.

5. Die Ethik des Nicht-Schützens

Der moderne Staat und die technologischen Mächte müssen lernen, dass Nicht-Intervention oft der radikalste Ausdruck des Respekts ist. Schutz ohne Zustimmung ist Gewalt unter sanftem Anstrich. Die Ethik des Nicht-Schützens bedeutet nicht Gleichgültigkeit, sondern Anerkennung von Freiheit als Risiko – ein Risiko, das zum Menschsein gehört.

In dieser Perspektive wird der Ruf nach weniger „Schutz“ zu einem Ruf nach mehr Verantwortung. Es ist kein Protest gegen Sicherheit, sondern gegen den Verlust der Souveränität. Denn die Frage, wer uns schützt, darf nie die Antwort verdrängen, dass nur wir selbst über uns verfügen dürfen.

6. Philosophische Begründung

Hannah Arendt unterschied zwischen Macht und Gewalt: Macht gründet auf Zustimmung, Gewalt auf Zwang.
Michel Foucault analysierte „Regierbarkeit durch Sicherheit“ – die stillschweigende Steuerung durch Wissen.
Johan Galtung beschrieb strukturelle Gewalt als systemische Einschränkung menschlicher Möglichkeiten.

Diese Theorien bündeln sich im digitalen Kontext: Beschützer agieren als Machttechniker einer Sicherheit, die den Menschen formt, statt ihn zu schützen.

7. Das Recht auf digitale Autonomie

Die Antwort kann nicht in technologischem Fatalismus liegen, sondern in einer Neuinterpretation bestehender Grundrechte. Datenschutz ist dabei nur der Ausgangspunkt, nicht das Ziel. Was notwendig ist, ist ein **Recht auf digitale Selbstverteidigung** – abgeleitet aus dem Prinzip personaler Autonomie. Dieses Recht müsste drei Dimensionen erfassen:

8. Thesen zur Neuordnung der digitalen Freiheit

1. **Informationssouveränität**: Jeder Mensch hat Anspruch auf volle Kontrolle über seine digitalen Spuren. Daten, die ohne klare Zweckbindung erhoben werden, verletzen die Willensfreiheit.

2. **Algorithmische Nachvollziehbarkeit**: Entscheidungen, die das Individuum betreffen, dürfen nicht im „Black Box“-Modus getroffen werden. Recht muss erklärbar bleiben.

3. **Resistenzrecht gegen Bevormundung**: Der Bürger darf digitale Eingriffe abwehren, selbst wenn sie vermeintlich zu seinem Schutz erfolgen. Schutz darf niemals Pflicht sein.

9. Vom Schutz zur Souveränität

Wahrer Schutz schützt Freiheit, nicht Ordnung. Autonomie verlangt das Recht, Risiken zu tragen. Eine freiheitliche Verfassung darf den Bürger nicht zur Sicherheit erziehen, sondern zur Verantwortung. Ein demokratischer Schutzmechanismus muss das Individuum ermächtigen, nicht entmächtigen. Die derzeitige Praxis – permanente Einwilligung, intransparente AGBs, algorithmische Steuerung – verkehrt dieses Prinzip. Es braucht ein Recht auf Selbstverteidigung in der digitalen Sphäre, ähnlich dem Recht auf Notwehr. Dieses Recht müsste enthalten:

1. **Datenautonomie**: Volle Kontrolle über Erhebung, Nutzung und Löschung persönlicher Daten.
2. **Algorithmische Transparenz**: Offenlegung, wenn Entscheidungen über mich durch automatisierte Systeme getroffen werden.
3. **Digitale Selbstverteidigungsfreiheit**: Das Recht, Verschlüsselung zu nutzen, sich der Datensammlung zu entziehen und digitale Werkzeuge zu verwenden, die Privatsphäre wahren.
4. **Haftungspflicht der Beschützer**: Institutionen, die eingreifen, müssen Verantwortung übernehmen, wenn ihre „Schutzmaßnahmen“ Freiheit oder Würde verletzen.

Sich selbst zu schützen, ist kein Ausdruck von Misstrauen, sondern von Mündigkeit. Kant hätte gesagt: Der Mensch darf nie nur als Objekt des Schutzes behandelt werden, sondern muss immer auch Subjekt seiner eigenen Sicherheit bleiben. Die digitalen Beschützer – ob staatlich oder privat – würden gut daran tun, diesen Grundsatz wiederzuentdecken. So wird Schutz erst dann legitim, wenn er Wahlfreiheit bewahrt. Sobald er Zwang oder Kontrolle impliziert, entlarvt er sich als „Schutzbehauptung“ – als Rationalisierung von Macht. Das Ziel wäre ein Schutzverständnis, das Verantwortung teilt, statt sie zu monopolisieren.

10. Thesen zur Neuordnung der digitalen Freiheit

1. Digitales Selbstbestimmungsrecht als Grundrecht.
2. Transparenzpflicht und algorithmische Nachvollziehbarkeit.
3. Subsidiarität digitaler Eingriffe.
4. Recht auf digitale Selbstverteidigung.
5. Demokratische Rückbindung der Datenmacht.

11. Entwurf Art. 2a GG – Digitale Selbstbestimmung

(1) Jeder Mensch hat das Recht, über die Erhebung, Verarbeitung und Verwendung seiner personenbezogenen und verhaltensbezogenen Daten frei zu verfügen.
(2) Informationstechnische Systeme dürfen nur in einer Weise eingesetzt werden, die selbstbestimmtes Handeln gewährleistet.
(3) Der Staat schützt die digitale Integrität des Menschen vor Eingriffen öffentlicher und privater Stellen.
(4) Algorithmische Entscheidungen mit gesellschaftlicher Wirkung bedürfen demokratischer Kontrolle und Transparenz.

12. Rechtspolitische und internationale Bezugspunkte

Der Entwurf eines **Artikel 2a GG** fügt sich nicht in ein luftleeres Konzept, sondern knüpft an bereits begonnene Entwicklungen im europäischen

und internationalen Recht an. Die Vorschläge knüpfen an die DSGVO, den *Digital Services Act*, den *AI Act* sowie die UNESCO-Empfehlung (2021) an. Ein solcher Artikel 2a GG würde den europäischen Grundrechtekatalog erweitern und die UNESCO-Forderung nach digitaler Selbstbestimmung rechtlich verankern.

1. **EU-Ebene – Von der DSGVO zur Digital Rights Charta**:
   Die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) war ein paradigmatischer Schritt hin zur Kodifizierung individueller Kontrollrechte im digitalen Raum. Ihre Grenzen sind jedoch offenkundig: Die auf Einwilligung basierende Schutzlogik übersieht strukturelle Abhängigkeitsverhältnisse. Der von der Europäischen Kommission 2023 zur Diskussion gestellte *European Declaration on Digital Rights and Principles for the Digital Decade* betont zwar Würde, Freiheit und Solidarität, bleibt aber programmatisch. Ein verfassungsrechtlich verankerter Artikel 2a würde dieses Programm rechtsverbindlich verdichten.

2. **Digital Services Act (DSA) und AI Act**:
   Der **DSA** (Verordnung (EU) 2022/2065) und der 2024 verabschiedete **AI Act** führen Schutzpflichten und Transparenzanforderungen für Anbieter digitaler Dienste und KI-Systeme ein. Sie adressieren, was bisher fehlte: die strukturelle Verantwortlichkeit von Plattformen. Doch auch diese Regelwerke bleiben im Modus des Verwaltungsrechts. Eine Grundrechtsnorm zur digitalen Selbstbestimmung würde daraus ein subjektives, justiziables Abwehrrecht formen.

3. **UNESCO und Ethik der KI**:
   Die UNESCO-Empfehlung über die Ethik der Künstlichen Intelligenz (2021) formuliert die Verpflichtung, algorithmische Systeme an Menschenwürde und Partizipation zu binden. In Artikel 23 verlangt sie, dass Staaten „die Fähigkeit der Individuen zum selbstbestimmten Handeln in digitalen Umgebungen“ schützen. Diese Formulierung deutet bereits auf ein universelles Menschenrecht auf digitale Selbstbestimmung hin, das national-konstitutionell verankert werden könnte.

4. **Deutscher Ethikrat und Datenethikkommission**:
   Sowohl der **Deutsche Ethikrat** (Stellungnahme 2023: „Mensch und Maschine – Herausforderungen durch KI“) als auch die **Datenethikkommission der Bundesregierung** (2019) haben betont, dass ein Mehr an Regulierung nicht automatisch mehr Freiheit schafft. Beide Gremien plädieren für eine „Ethik der Transparenz und Teilhabe“, die die Bürger befähigt, technologische Strukturen kritisch zu hinterfragen. Dieses Denken steht im Einklang mit der hier formulierten Idee einer „Rechtsordnung der Mündigkeit“.

5. **UN Digital Compact und kommende UN-Konvention über digitale Menschenrechte**:
   Der derzeit im Entstehen befindliche *Global Digital Compact* der Vereinten Nationen (geplant für 2025) dient als völkerrechtlicher Rahmen für digitale Menschenrechte. Die deutsche bzw. europäische Verfassungspraxis könnte mit einem Artikel 2a ein Modell schaffen, das innerhalb dieser Debatte Vorbildfunktion hat – ähnlich der Rolle, die das Volkszählungsurteil 1983 für das globale Verständnis von Datenschutz spielte.

Diese Systematik erlaubt es, den Begriff der Freiheit über physische Grenzen hinaus zu erweitern – in den digitalen Raum, der längst konstitutiver Teil des öffentlichen Lebens geworden ist.

13. Normative Perspektive: Das Recht als Raum der Selbstbehauptung

Wenn das 20. Jahrhundert die juristische Institutionalisierung von Sozialrechten brachte, dann könnte das 21. Jahrhundert die Kodifizierung der **digitalen Selbstrechte** einleiten. Ein Grundrecht auf digitale Selbstbestimmung wäre kein Luxus der Informationselite, sondern ein Schutzrecht gegen strukturelle Entmündigung – gegen algorithmische Autorität ohne Verantwortung.

Politisch würde eine solche Norm zwei Funktionen erfüllen:

1. **Legitimationsfunktion**: Staatliches und privatwirtschaftliches Handeln muss sich künftig an einem klaren Maßstab messen lassen: Dient das System der Befähigung oder der Steuerung des Bürgers?

2. **Emanzipationsfunktion**: Bürgerinnen und Bürger erhielten ein einklagbares Recht auf Widerstand gegen Formen digitaler Fremdverwaltung – sei es durch Überwachung, algorithmische Diskriminierung oder manipulative Gestaltung sozialer Medien.

So verstanden, würde Artikel 2a GG nicht nur Schutz garantieren, sondern Souveränität schaffen. Er wäre Ausdruck einer neuen Staatsraison, in der nicht der Schutz des Bürgers vor der Welt, sondern der Schutz der Freiheit vor ihren Beschützern den normativen Kern des Rechts bildet.

Juristisch-theoretisch lässt sich das vorgeschlagene Grundrecht auf digitale Selbstbestimmung in die drei Dimensionen *Autonomie*, *Transparenzpflicht* und *Integrität* einordnen.

Dimension	**Kerngedanke**	**Bezugssystem**
Autonomie	Individuelle Verfügung über Daten und Entscheidungen	Kant, Grundrecht auf Selbstbestimmung (Art. 2 GG)
Transparenzpflicht	Verpflichtung von Institutionen zur Nachvollziehbarkeit algorithmischer Steuerung	Rule of Law, DSA/AI Act
Integrität	Schutz der digitalen Würde und Handlungsfähigkeit als Ausdruck der Menschenwürde	Art. 1 GG, UNESCO AI Ethics, UN Charter of Digital Rights

Tabelle 1: Dimensionen der digitalen Rechte

14. Schluss

Schutz ist kein Selbstzweck. Er wird gewaltsam, wenn er den Menschen entmündigt. Das Recht des 21. Jahrhunderts muss den Schutzbegriff revolutionieren: nicht Schutz *vor* Freiheit, sondern Schutz *der* Freiheit selbst.

Literatur

[1] Hannah Arendt. *On Violence*. New York: Harcourt, Brace & World, 1970.

[2] Stefanie Bublitz. *Digitale Würde: Eine rechtsethische Grundlage für KI-Regulierung*. Tübingen: Mohr Siebeck, 2022.

[3] Bundesverfassungsgericht. *Volkszählungsurteil vom 15. Dezember 1983, BVerfGE 65, 1*. Entscheidungssammlung des Bundesverfassungsgerichts. 1983.

[4] Datenethikkommission der Bundesregierung. *Gutachten zur Regulierung algorithmischer Systeme*. Berlin, 2019.

[5] Deutscher Ethikrat. *Mensch und Maschine – Herausforderungen durch KI*. Berlin, 2023.

[6] Europäische Kommission. *Europäische Erklärung über digitale Rechte und Grundsätze für das digitale Jahrzehnt*. Brüssel, 2023.

[7] Europäische Union. *Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO)*. Amtsblatt der Europäischen Union. 2016.

[8] Europäische Union. *Verordnung (EU) 2022/2065 – Digital Services Act (DSA)*. Amtsblatt der Europäischen Union. 2022.

[9] Europäische Union. *Verordnung (EU) 2024/1685 – Artificial Intelligence Act (AI Act)*. Amtsblatt der Europäischen Union. 2024.

[10] Luciano Floridi. *The Ethics of Information*. Oxford: Oxford University Press, 2013.

[11] Michel Foucault. *Sécurité, territoire, population: Cours au Collège de France, 1977–1978*. Paris: Gallimard / Seuil, 2004.

[12] Michel Foucault. *Surveiller et punir: Naissance de la prison*. Paris: Gallimard, 1975.

[13] Günter Frankenberg. *Autorität und Recht*. Frankfurt am Main: Suhrkamp, 2020.

[14] Johan Galtung. "Violence, Peace, and Peace Research". In: *Journal of Peace Research* 6.3 (1969), S. 167–191.

[15] Byung-Chul Han. *Psychopolitik: Neoliberalismus und die neuen Machttechniken*. Berlin: Matthes & Seitz, 2017.

[16] Marshall McLuhan. *Understanding Media: The Extensions of Man*. New York: McGraw-Hill, 1964.

[17] UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris, 2021.

[18] Vereinte Nationen. *Entwurf des Global Digital Compact*. New York, 2025.