



– 09.04.2020 –

## „Digitalisierung und Menschenrechte“

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41

Die Auswirkungen der Corona-Pandemie auf Gesellschaft und Wirtschaft sind zum jetzigen Zeitpunkt nicht absehbar. Die volle Aufmerksamkeit gilt weltweit der Gesundheit der Menschen. Aber auch die Sorge um mögliche wirtschaftliche Folgen wächst – Folgen für jeden und jede ganz persönlich wie auch für unsere Gesellschaften. Digitale Technik hat in dieser Krisenzeit rasant an Aufmerksamkeit und Bedeutung gewonnen. Es zeichnet sich ab, dass die Corona-Pandemie das Tempo der digitalen Transformation beschleunigen wird. Jedoch ist die Frage unbeantwortet, ob dabei alle – auch Menschen ärmerer Regionen Asiens, Afrikas und Lateinamerikas – mitgenommen oder vielleicht sogar abgehängt werden.

Der digitale Wandel inspiriert seit vielen Jahren zu Bildern und Phantasien einer Zukunft, die erwartungsvoll euphorisch aber auch beängstigend zerstörerisch sein können. Bilder, die manchmal noch in eine ferne Zukunft weisen, immer häufiger aber auch schon die Gegenwart spiegeln. Das Internet startete mit einem großen Freiheitsversprechen: Alle Menschen würden ihre Stimme erheben und Informationen einholen können, frei von staatlicher Zensur. Kommunikation würde über weite Distanzen vereinfacht und damit Vernetzung und Verständigung im Land und über nationale Grenzen hinweg gefördert. Der Arabische Frühling schien in seinen ersten Tagen viel von diesem Bild zu bestätigen. Jedoch zeichneten sich bald drei Entwicklungen ab, die als Backlashes gegen dieses Freiheitsversprechen bezeichnet werden können: globale Massenüberwachung, Einschränkung der zivilgesellschaftlichen Handlungsmöglichkeiten im Netz (Shrinking Spaces online) und wachsende Datenkartelle.

Ein erster Paradigmenwechsel konnte 2001 als Reaktion auf die Anschläge auf das World Trade Center beobachtet werden – in den USA, dann in immer mehr Staaten weltweit. Statt der gezielten Überwachung Verdächtiger setzen Nachrichtendienste auf anlasslose digitale Massenüberwachung ganzer Bevölkerungen.

Massenüberwachung durch staatliche Stellen höhlt das Menschenrecht auf Privatsphäre aus und führt durch Einschüchterung und vorausseilendem Gehorsam dazu, dass auch weitere Menschenrechte weniger Beachtung finden („Chilling Effects“). Denn eine geschützte Privatsphäre ist die Grundlage für die Wahrung von Menschenrechten, für politisches Engagement und für eine Teilhabe am gesellschaftlichen Leben. Wer Sorge hat, überwacht zu werden, äußert die eigene Meinung weniger frei oder traut sich nicht, im Internet nach sensiblen Informationen zu suchen.

Als Reaktion auf den Arabischen Frühling und ähnliche Bewegungen in anderen Ländern entwickelten Regierungen knapp 10 Jahre später Baukästen repressiver Werkzeuge, um die Internetfreiheit weiter einzuschränken. „Shrinking Spaces“ sind auch online ein großes Problem für Zivilgesellschaft und Menschenrechte geworden.

Dazu gehört eine weltweit zunehmende Anzahl spezieller „Cyber-Laws“, die die freie Meinungsäußerung und das Teilen von Informationen online einschränken oder Telekommunikations-Unternehmen verpflichten, sensible Daten über ihre Nutzerinnen und



42 Nutzer ohne hinreichende unabhängige Kontrolle an Behörden weiterzugeben. Ein besonders  
43 drastisches Beispiel stellt das chinesische Cyber-Security-Law dar. Auch durch das Blockieren  
44 einzelner Webseiten oder digitaler Dienste und Anwendungen, durch Upload-Filter oder gar  
45 vollständige Internet-Shutdowns – etwa im Vorfeld von Wahlen – wird es Menschen  
46 erschwert, sich online zu informieren, ihre Meinung zu äußern oder sich etwa zu  
47 Kundgebungen zu verabreden. Ein besorgniserregender Trend zu Internet-Shutdowns lässt  
48 sich in Asien (insbesondere in Indien und Pakistan) und einigen afrikanischen Ländern  
49 beobachten. Technische Werkzeuge wie VPN-Netzwerke und Ende-zu-Ende-Verschlüsselung  
50 ermöglichen das Umgehen staatlicher Zensur und werden daher zunehmend kriminalisiert,  
51 etwa in China und Russland. Der zunehmende Einsatz von Gesichtserkennungstechnologie  
52 gefährdet die Versammlungsfreiheit. In besonderer Weise trifft der „Baukasten“ repressiver  
53 digitaler Werkzeuge Menschenrechtsaktivisten. Durch Phishing-Angriffe werden persönliche  
54 Passwörter abgegriffen, um etwa Korrespondenz mitzulesen. Spähsoftware wird verdeckt auf  
55 Smartphones und Computern installiert, um Nachrichten und Telefonate mitzuschneiden, die  
56 Kamera unbemerkt eine Videoaufnahme machen zu lassen und Adressbuch und Dateien  
57 heimlich auszuleiten. Häufig wird die benötigte Technik in Ländern des globalen Nordens  
58 produziert und aufgrund mangelhafter Exportkontrolle für digitale Technologie in Länder mit  
59 besorgniserregender Menschenrechtsbilanz exportiert.

60 Hinzukommt fehlende staatliche Regulierung großer Datenkartelle. Internetplattformen wie  
61 Facebook und Google haben geradezu eine Monopolstellung eingenommen und haben eine  
62 enorme Macht über die Ausübung von Menschenrechten im digitalen Raum. Sie diktieren die  
63 Bedingungen, unter denen Meinungs- und Informationsfreiheit online ausgeübt werden – und  
64 welchen Preis Nutzerinnen und Nutzer in Bezug auf Privatsphäre dafür zahlen. Die  
65 Wissenschaftlerin Shoshana Zuboff hat das Modell dieser Konzerne als „Überwachungs-  
66 Kapitalismus“ bezeichnet. Profiling und gezielte Werbung ermöglichen, gezielt Menschen in  
67 schwierigen Lebenssituationen oder solche mit Radikalisierungspotenzial anzusprechen oder  
68 eine Immobilienanzeige nur bestimmten Schichten, Geschlechtern oder ethnischen Gruppen  
69 anzuzeigen. Gezielte Werbung kann etwa im Vorfeld von Wahlen missbraucht werden. Nicht  
70 zuletzt können politische Manipulationen und Algorithmen Nutzerinnen und Nutzern eine  
71 ausgewählte Weltsicht präsentieren und damit das Menschenrecht auf Meinungs- und  
72 Informationsfreiheit, Gedanken-, Gewissens- und Religionsfreiheit untergraben. Die freie  
73 Meinungsbildung im digitalen Zeitalter zu schützen, ist daher eine der entscheidenden  
74 politischen Herausforderungen unserer Zeit.

75 Um einen gleichberechtigten Zugang zum Internet für alle Menschen weltweit zu  
76 gewährleisten, darf der Anschluss der sogenannten „next billion“ an das Internet nicht allein  
77 Unternehmen überlassen werden. Facebook kooperiert in 65 Ländern mit  
78 Mobilfunkanbietern, um „Free Basics“ zur Verfügung zu stellen. In manchen Regionen ist  
79 Facebook so zum Synonym für das Internet geworden. Doch die fehlende Netzneutralität  
80 solcher Angebote macht die Zielgruppen abhängig von den Bedingungen der Unternehmen,  
81 was eine Ausbeutung persönlicher Daten erleichtert und auf der anderen Seite die  
82 gleichberechtigte Nutzung der Vielfalt des gesamten Internets erschwert. Der „digitale  
83 Spaltung“ ist zudem nicht nur eine Frage des technischen „Angeschlossenenseins“, sondern  
84 hängt von Faktoren wie Geschlecht, Alter oder Behinderung, von Konto- und Bildungsstand  
85 und den politischen Rahmenbedingungen ab.



86 Digitale Plattformen wie Amazon, Google, Facebook oder auch Uber lehnen es ab,  
87 Verantwortung für die Überwindung digitaler Spaltungen innerhalb von Gesellschaften oder  
88 auch zwischen Kontinenten zu übernehmen – mit dem Argument, nicht mehr als ein  
89 „Marktplatz“ zu sein. Für das Ziel „Daten für alle“ (Daten sollen allen Menschen  
90 zugutekommen kommen und nicht großen Konzernen vorbehalten bleiben), braucht es eine  
91 Regulierung dieser Geschäftsmodelle. Es muss deshalb die Daten-Eigentumsfrage gestellt  
92 werden. In der digitalen Transformation kommt es zur Verschiebung von Macht- und  
93 Kooperationsverhältnissen. Auswirkungen auf die Gesellschaft zeichnen sich deutlich ab. Dem  
94 gilt es entgegenzutreten.

95

96

97 **Wir empfehlen folgende konkrete Handlungsschritte:**

98

- 99 1. Die SPD setzt sich dafür ein, dass digitale Überwachung zum Erreichen eines legitimen  
100 Ziels nur stattfinden darf, wenn ein konkreter Verdacht vorliegt und die  
101 Überwachungsmaßnahme gezielt, verhältnismäßig, durch eine unabhängige Instanz  
102 kontrolliert und notwendig ist. Betroffene einer Überwachungsmaßnahme sollen nach  
103 deren Beendigung umfassend darüber aufgeklärt werden.
- 104 2. Um Verteidigerinnen und Verteidiger von Menschenrechten weltweit zu schützen,  
105 macht sich die SPD auf EU-Ebene für eine Reform der Dual-Use-Verordnung stark, die  
106 den Export von Überwachungstechnologie reguliert – mit Sorgfaltspflichten für  
107 exportierende Unternehmen sowie einer menschenrechtlichen "Catch All Klausel", die  
108 Exporte in Staaten untersagt, bei denen ein Risiko besteht, dass die Technologie dort  
109 zu Menschenrechtsverletzungen beitragen.
- 110 3. Krisensituationen, wie wir sie durch die Corona-Pandemie erleben, stellen den Schutz  
111 von Menschenrechten vor besondere Herausforderungen und Demokratien auf die  
112 Probe. Es gilt die Schaffung eines globalen Systems für Wahrung der Menschenrechte  
113 und der Demokratie durch Zusammenarbeit auf mehreren Ebenen voranzutreiben.  
114 Der Einsatz neuer Technologien soll zur Überwachung von Rechten genutzt werden –  
115 unter Wahrung internationalen Rechts.
- 116 4. Die SPD setzt sich für Ende-zu-Ende Verschlüsselung und Werkzeuge wie VPN und Tor  
117 ein.
- 118 5. Die SPD macht sich für ein umfassendes nationales und internationales Verbot der  
119 Entwicklung, der Herstellung und des Einsatzes von autonomen, potenziell tödlichen  
120 Waffensystemen (sogenannten „Killerrobotern“) stark.
- 121 6. Regierungen haben eine Schutzpflicht und müssen Internet-Plattformen so regulieren,  
122 dass die Menschenrechte gewahrt bleiben. In einem ersten Schritt sollen  
123 Unternehmen verpflichtet werden, die Nutzung ihrer Dienste nicht zu erschweren,  
124 indem sie den Zugang davon abhängig machen, dass Nutzerinnen und Nutzer der  
125 Erhebung und Verwendung ihrer persönlichen Daten zu Werbezwecken „zustimmen“.



- 126 7. Um allen Menschen weltweit einen gleichberechtigten Zugang zum Internet zu  
127 ermöglichen, setzt sich die SPD für Netzneutralität ein. Ein besonderes Augenmerk  
128 beim digitalen Wandel muss auf den Rechten von Frauen liegen, um zu verhindern,  
129 dass sie in dem Digitalisierungsprozess diskriminiert werden.
- 130 8. Unternehmen haben einen starken Einfluss auf die Wahrung von Menschenrechten im  
131 digitalen Raum. Sie sollen verpflichtet werden, menschenrechtliche Sorgfaltspflichten  
132 nach den UN-Leitprinzipien in ihren Geschäftstätigkeiten zu implementieren.  
133 Sorgfaltspflichten lassen sich nicht nur auf Lieferketten anwenden, sondern auch auf  
134 menschenrechtliche Risiken von Datensammlungen auf Internet-Plattformen, bei der  
135 Entwicklung von Künstlicher Intelligenz (KI), bei Maßnahmen gegen Hate Speech auf  
136 Social Media oder bei Verkaufsentscheidungen über Überwachungstechnologie.
- 137 9. Wir brauchen ein „Daten-für-alle-Gesetz“ – eine Demokratisierung der Datennutzung  
138 durch eine allgemeine Datenteilungspflicht: Der Zugang zu vollständig anonymisierten  
139 Daten und zu nicht-personenbezogenen Daten (beispielsweise Mobilitäts- und  
140 Verkehrsdaten, Geodaten und Wetterdaten) muss – wo immer möglich – frei sein.