



Rat der
Europäischen Union

Brüssel, den 10. Dezember 2021
(OR. en)

14910/21

JAI 1401
FREMP 296

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	10. Dezember 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2021) 819 final
Betr.:	BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Schutz der Grundrechte im digitalen Zeitalter – Jährlicher Bericht über die Anwendung der Charta der Grundrechte der Europäischen Union 2021

Die Delegationen erhalten in der Anlage das Dokument COM(2021) 819 final.

Anl.: COM(2021) 819 final



EUROPÄISCHE
KOMMISSION

Brüssel, den 10.12.2021
COM(2021) 819 final

**BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT,
DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN
AUSSCHUSS DER REGIONEN**

Schutz der Grundrechte im digitalen Zeitalter –

**Jährlicher Bericht über die Anwendung der Charta der Grundrechte der Europäischen
Union 2021**

Schutz der Grundrechte im digitalen Zeitalter –
Jährlicher Bericht über die Anwendung der
Charta der Grundrechte der Europäischen Union 2021

Inhalt

1. Einleitung	2
2. Durchführung der neuen Strategie für eine verstärkte Anwendung der Grundrechtecharta in der EU	3
3. Die Charta als Kompass der EU für das digitale Zeitalter	8
4. Bewältigung der Probleme bei der Moderation von Online-Inhalten	10
5. Schutz der Grundrechte im Zusammenhang mit dem Einsatz von KI	20
6. Überwindung der digitalen Kluft	26
7. Schutz von Menschen, die über Plattformen arbeiten	31
8. Überwachung der digitalen Überwachung	34
9. Mit vereinten Kräften: das digitale Zeitalter als Chance für die Grundrechte	43

1. Einleitung

Die Charta der Grundrechte der Europäischen Union¹ ist ein wirksames Instrument für den Schutz, die Förderung und weitere Stärkung der Rechte der Bürgerinnen und Bürger in der Europäischen Union. Grundrechte dienen nicht nur dem Schutz der Menschen vor unrechtmäßigen Eingriffen wie beispielsweise Zensur oder Massenüberwachung, sondern befähigen die Bürgerinnen und Bürger auch, vollen Gebrauch von allen Rechten zu machen und alle Chancen auszuschöpfen, die ihnen das Leben bietet. Es gibt immer die Möglichkeit, dafür zu sorgen, dass die Menschen ihre Rechte umfänglicher und unter besseren Bedingungen wahrnehmen können. Die Charta kann als Richtschnur für die politische Arbeit in der Union dienen. Je mehr die Menschen über die in der Charta verankerten Rechte und ihre Wahrnehmung wissen, desto mehr Handlungskompetenz gewinnen sie.

Die COVID-19-Pandemie hat den Schutz und die Garantien aus unseren Grundrechten auf die Probe gestellt. Einschränkungen von Grundrechten müssen stets notwendig und verhältnismäßig sein. Dieses Erfordernis ist in der Charta der Grundrechte der Europäischen Union verankert, die verbindliches Unionsrecht darstellt. Die Charta dient dem Schutz und der Förderung eines breiten Spektrums von Rechten im Zusammenhang mit der Würde des Menschen sowie mit Freiheit, Gleichheit und Solidarität; alle einzelstaatlichen Gerichte können sie immer dann heranziehen, wenn es um die Durchführung des Unionsrechts geht und dieses für das endgültige Urteil von Bedeutung ist.

Seit dem Jahr 2009 hat die Charta denselben Rechtsstatus wie die Verträge, die das Primärrecht der Union darstellen, auf denen die EU-Rechtsvorschriften basieren. Die Charta ist für die europäischen Organe bei allen ihren Maßnahmen und für die EU-Mitgliedstaaten bei der Durchführung des Unionsrechts verbindlich.

Wann müssen die Mitgliedstaaten die Bestimmungen der Charta einhalten?

- Wenn sich die Mitgliedstaaten im Rat und mit dem Europäischen Parlament auf die Verabschiedung neuer EU-Rechtsvorschriften einigen, müssen diese oftmals durch nationale Maßnahmen zur Durchführung dieser Rechtsvorschriften umgesetzt werden.
- Wenn die Mitgliedstaaten Gesetze verabschieden oder ändern, die Fragen berühren, zu denen das Unionsrecht konkrete Verpflichtungen vorsieht, dürfen diese Gesetze nicht im Widerspruch zum Unionsrecht, einschließlich der Charta, stehen, da diese legislativen Maßnahmen als Durchführung des Unionsrechts gelten.
- Die Finanzierungsprogramme der Union sind in EU-Rechtsvorschriften verankert. Die Mitgliedstaaten müssen sicherstellen, dass die entsprechenden Mittel nach Maßgabe der Bestimmungen dieser Rechtsvorschriften verwendet werden. Die Durchführung von Finanzierungsprogrammen kommt der Durchführung von Unionsrecht gleich.
- Wenn die Mitgliedstaaten Gesetze in einem Bereich verabschieden oder ändern, in dem die Union keine Zuständigkeit hat und für den es keine EU-Rechtsvorschrift gibt, stellt dies keine Durchführung von Unionsrecht dar. In diesen Fällen sind sie nicht an die Charta gebunden. Jedoch sind viele der in der Charta verankerten Grundrechte zugleich in der Verfassung und

¹ [Charta der Grundrechte der Europäischen Union](#) (ABl. C 326 vom 26.10.2012, S. 391).

der Rechtsprechung der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte festgeschrieben, die von allen EU-Mitgliedstaaten unterzeichnet wurde.

Um dafür zu sorgen, dass alle Bürgerinnen und Bürger besser über die Charta Bescheid wissen, veröffentlicht die Europäische Kommission seit 2010 Berichte über ihre Anwendung. Im vorliegenden Bericht wird erstmals ein neuer Ansatz verfolgt, der in der **Strategie für eine verstärkte Anwendung der Grundrechtecharta in der EU** (im Folgenden „Charta-Strategie“)² angekündigt wurde. Im jährlichen Bericht wird nun schwerpunktmäßig ein bestimmtes Thema beleuchtet, das unter das Unionsrecht fällt, wobei die bewährten Verfahren sowie die Probleme in den Mitgliedstaaten in diesem Bereich eingehender betrachtet werden. So ist es möglich, systemische Entwicklungen zu untersuchen und aufzuzeigen, wie sich unterschiedliche Rechte gegenseitig verstärken können und wie sich politische, gesellschaftliche und wirtschaftliche Entwicklungen gleichzeitig auf eine Reihe von Rechten auswirken können.

Das Thema des Berichts 2021 ist im Einklang mit dem strategischen Schwerpunkt des digitalen Wandels der Europäischen Kommission der **Schutz der Grundrechte im digitalen Zeitalter**.

Welche Informationen liegen diesem Bericht zugrunde?

Für diesen Bericht wurden die folgenden Quellen herangezogen:

- Beiträge der EU-Mitgliedstaaten, die gebeten wurden, Informationen aus ihrer jeweiligen einzelstaatlichen Perspektive bereitzustellen;³
- eine gezielte Konsultation von Dachorganisationen der im Bereich der Grundrechte tätigen europäischen zivilgesellschaftlichen Organisationen; und
- Berichte von EU-Agenturen, insbesondere die jährlichen Grundrechteberichte der Agentur der Europäischen Union für Grundrechte (FRA)⁴, die einen Abschnitt zu Grundrechten und Digitalisierung beinhalten.

2. Durchführung der neuen Strategie für eine verstärkte Anwendung der Grundrechtecharta in der EU

Mit der Charta-Strategie, die im Jahr 2020 von der Kommission angenommen wurde, soll sichergestellt werden, dass die Charta vollumfänglich Anwendung findet, um die Grundrechte für alle Menschen Wirklichkeit werden zu lassen. In der Charta-Strategie, die von den Mitgliedstaaten uneingeschränkt mitgetragen wird, wird der Rahmen für die gemeinsamen Bemühungen um die EU-weite Anwendung der Grundrechte in den nächsten

² Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Strategie für eine verstärkte Anwendung der Grundrechtecharta in der EU ([COM\(2020\) 711](#)).

³ Die Beiträge der Mitgliedstaaten wurden im Rahmen der Gruppe „Grundrechte, Bürgerrechte und Freizügigkeit“ (FREMP) des Rates eingebracht.

⁴ <https://fra.europa.eu/en/publication/2021/fundamental-rights-report-2021>

zehn Jahren gesteckt.⁵ Die vier Bereiche, in denen die in der Charta-Strategie festgelegten Ziele vorrangig verwirklicht werden sollen, werden nachstehend erläutert.

2.1 Förderung und Überwachung der wirksamen Anwendung der Charta in den Mitgliedstaaten

Nationale und lokale Behörden sowie die Parlamente und Strafverfolgungsbehörden spielen bei der Förderung und beim Schutz der in der Charta verankerten Rechte sowie bei der Schaffung günstiger Rahmenbedingungen für zivilgesellschaftliche Organisationen und Institutionen, die sich für die Grundrechte einsetzen, eine entscheidende Rolle. Die Kommission arbeitet eng mit den Mitgliedstaaten zusammen, um sie dabei zu unterstützen, das Recht und die Strategien der Union wirksam und unter uneingeschränkter Einhaltung der Charta umzusetzen.

Darüber hinaus unterstützt die Kommission die Mitgliedstaaten bei der Durchführung **EU-finanzierter Programme** im Einklang mit der Charta. In der Dachverordnung⁶ sind die bei der Nutzung verschiedener EU-Fonds⁷ einzuhaltenden Vorschriften festgelegt. Demnach sind die Mitgliedstaaten verpflichtet, wirksame Mechanismen zu schaffen und einzusetzen, um die Einhaltung der Charta im Rahmen EU-finanzierter Programme sicherzustellen; hierzu zählen beispielsweise Vorkehrungen zur Berichterstattung an den Begleitausschuss über Beschwerden bezüglich der Charta und über Verstöße gegen die Charta bei der Durchführung von aus den Fonds unterstützten Vorhaben. Die Kommission wird die Mitgliedstaaten auch in technischer Hinsicht weiterhin dabei unterstützen, sicherzustellen, dass die aus den EU-Fonds unterstützten Programme unter Einhaltung der Charta konzipiert und durchgeführt werden.

Im Rahmen des Förderprogramms „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ (CERV) hat die Kommission neue **Möglichkeiten für nationale, regionale und kommunale Behörden** geschaffen, Finanzmittel für Projekte zu erhalten, die auf die Förderung einer Wertekultur und die Sensibilisierung für die Charta abzielen.⁸ Städte spielen bei der Förderung einer solchen Kultur und beim Schutz der Grundrechte eine wichtige Rolle. Mehrere Städte haben sich dem Netz der „Human Rights Cities“ (Menschenrechtsstädte) angeschlossen und berücksichtigen die Grundrechte im Rahmen ihrer Politikgestaltung.⁹ Die FRA veröffentlichte bei ihrem Grundrechteforum im Oktober 2021 einen Bericht mit dem Titel „Human Rights in the EU: a framework for reinforcing rights locally“ (Menschenrechte

⁵ <https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/de/pdf>

⁶ Verordnung (EU) 2021/1060 des Europäischen Parlaments und des Rates vom 24. Juni 2021 mit gemeinsamen Bestimmungen für den Europäischen Fonds für regionale Entwicklung, den Europäischen Sozialfonds Plus, den Kohäsionsfonds, den Fonds für einen gerechten Übergang und den Europäischen Meeres-, Fischerei- und Aquakulturfonds sowie mit Haushaltsvorschriften für diese Fonds und für den Asyl-, Migrations- und Integrationsfonds, den Fonds für die innere Sicherheit und das Instrument für finanzielle Hilfe im Bereich Grenzverwaltung und Visumpolitik (ABl. L 231 vom 30.6.2021, S. 159).

⁷ Für den Zeitraum 2021 bis 2027: Europäischer Fonds für regionale Entwicklung, Kohäsionsfonds, Europäischer Sozialfonds Plus, Fonds für einen gerechten Übergang, Europäischer Meeres- und Fischereifonds, Asyl- und Migrationsfonds, Fonds für die innere Sicherheit und Instrument für Grenzmanagement und Visa.

⁸ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv>. Im Wege der [Aufforderung zur Einreichung von Vorschlägen für Städtepartnerschaften und Städtenetzwerke](#) werden im Rahmen des Programms „Bürgerinnen und Bürger, Gleichstellung, Rechte und Werte“ (CERV) im Jahr 2021 4,2 Millionen EUR bereitgestellt. Weitere Informationen sind verfügbar unter [Funding & tenders \(europa.eu\)](#).

⁹ <https://humanrightscities.net/>

in der EU: ein Rahmen für die Stärkung von Rechten auf lokaler Ebene)¹⁰. Dieser Rahmen beinhaltet Instrumente, die Bürgermeisterinnen und Bürgermeister, kommunale Behörden und Gebietskörperschaften sowie Basisorganisationen bei der Einbeziehung von Menschenrechtsstandards in ihre Arbeit unterstützen sollen. Als Folgemaßnahme zum EU-Aktionsplan gegen Rassismus 2020–2025¹¹ rief die Kommission im November 2021 die Auszeichnung „Europäische Hauptstadt/Hauptstädte für Inklusion und Vielfalt“ ins Leben.¹² Diese Auszeichnung wird für bewährte Verfahren verliehen, die andere europäische Städte und Regionen dazu inspirieren können, für ihre Einwohnerinnen und Einwohner ein von Vielfalt und Inklusion geprägtes Umfeld zu schaffen.

In der Charta-Strategie forderte die Kommission die Mitgliedstaaten auf, eine **Charta-Kontaktstelle** einzurichten, um die Zusammenarbeit und den Informationsaustausch mit Blick auf die Anwendung der Charta weiter zu erleichtern. Bislang haben 17 Mitgliedstaaten eine solche Charta-Kontaktstelle benannt. Diese Kontaktstellen spielen eine entscheidende Rolle bei der Verbreitung von Informationen und bewährten Verfahren zur Sensibilisierung für die Charta und bei der Koordinierung der Anstrengungen zum Kapazitätsaufbau im Land. Ihre Arbeit fließt in die neue Seite über bewährte Verfahren der Mitgliedstaaten im Hinblick auf die Charta ein, die im Dezember 2021 im europäischen E-Justizportal freigeschaltet wurde.¹³

Als Hüterin der Verträge unternahm die Kommission in Fällen, in denen mit einzelstaatlichen Rechtsvorschriften oder Verfahren zur Durchführung des Unionsrechts gegen die in der Charta verankerten Rechte verstoßen wird, konkrete Schritte, um die Wahrung dieser Rechte sicherzustellen, indem sie beispielsweise Vertragsverletzungsverfahren einleitete. Insbesondere wurde die Kommission tätig, um die folgenden Rechte und Freiheiten zu gewährleisten:

- die Vereinigungsfreiheit von Nichtregierungsorganisationen und das Recht auf Schutz der personenbezogenen Daten ihrer Geber;
- die akademische Freiheit;
- die Freiheit der Meinungsäußerung und den Medienpluralismus;
- die Würde des Menschen;
- das Recht auf Achtung des Privatlebens;
- das Recht jeder Person, einschließlich LGBTIQ-Personen, nicht aufgrund ihres Geschlechts oder ihrer sexuellen Ausrichtung diskriminiert zu werden.

Die Kommission beobachtet in allen Mitgliedstaaten die während der COVID-19-Pandemie ergriffenen Notfallmaßnahmen und ihre Auswirkungen insbesondere auf die Rechtsstaatlichkeit, die Grundrechte und die Einhaltung anderer Bestimmungen des

¹⁰ <https://fra.europa.eu/en/publication/2021/human-rights-cities-framework>

¹¹ Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine Union der Gleichheit: EU-Aktionsplan gegen Rassismus 2020–2025 ([COM\(2020\) 565 final](https://eur-lex.europa.eu/COM(2020)565_final)).

¹² <https://eudiversity2022.eu/de/preise/bewerben/>

¹³ https://e-justice.europa.eu/37134/DE/member_states_best_practices_on_the_charter

Schwierigkeiten, ihre Dienstleistungen weiter zu erbringen. Zu den praktischen Problemen zählten unter anderem die Absage von Aktivitäten, die psychischen Auswirkungen auf das Personal und die geringere Freiwilligentätigkeit.

Des Weiteren **unterstützt** die Kommission **Institutionen, die sich für die Grundrechte einsetzen, und zivilgesellschaftliche Organisationen** durch die gezielte Bereitstellung von Finanzmitteln, beispielsweise im Wege einer Aufforderung zur Einreichung von Vorschlägen für den Schutz und die Förderung der Werte der Union, die ausschließlich für kleine und Basisorganisationen der Zivilgesellschaft bestimmt ist und in deren Rahmen im Zeitraum 2021–2022 51 Millionen EUR vergeben werden.²⁰ Darüber hinaus wurde eine mit 2 Millionen EUR ausgestattete spezifische Aufforderung zur Einreichung von Vorschlägen für die Unterstützung von Rechtsstreitigkeiten und den Kapazitätsaufbau im Zusammenhang mit der Anwendung der Charta auf den Weg gebracht.²¹

Ferner fördert die Kommission den Kapazitätsaufbau und die **Sensibilisierung von Richtern und anderen Angehörigen der Rechtsberufe für die Charta**. Die Kommission verabschiedete im Dezember 2020 eine neue Strategie für die justizielle Aus- und Fortbildung auf europäischer Ebene für den Zeitraum 2021–2024²² und veröffentlichte im März 2021 eine Aufforderung zur Einreichung von Vorschlägen für die Unterstützung von Projekten zur justiziellen Aus- und Fortbildung, in der die Grundrechte eine der zentralen Prioritäten darstellen.²³ Mehrere Projekte wurden durchgeführt, die die justizielle Aus- und Fortbildung zur Charta zum Gegenstand haben und von der Kommission im Rahmen ihres Programms „Justiz“ für den Zeitraum 2014–2020 kofinanziert wurden.²⁴ Auf einer im Dezember 2020 eingerichteten Plattform kann Material für die justizielle Aus- und Fortbildung von Angehörigen der Rechtsberufe zu Grundrechten abgerufen werden.²⁵

2.3 Uneingeschränkte Anwendung der Charta der Grundrechte bei Entscheidungen auf Unionsebene

Die Organe, Einrichtungen und sonstigen Stellen der Union sind bei allen ihren Tätigkeiten zur Achtung der Charta verpflichtet. Die Kommission baut derzeit ihre internen Kapazitäten zur Einhaltung der Charta aus und aktualisiert ihr Instrumentarium für eine bessere Rechtsetzung²⁶, einschließlich der Leitlinien zur Berücksichtigung der Grundrechte bei Folgenabschätzungen aus dem Jahr 2011²⁷. Darüber hinaus erarbeitet sie spezifische Schulungen zur Charta sowie ein E-Learning-Tool, das die Bediensteten bei der Prüfung der Auswirkungen der Strategien und Legislativvorschläge der Kommission auf die Grundrechte

²⁰ [CERV-Arbeitsprogramm 2021–2022](#).

²¹ [Call for proposals to promote capacity building and awareness on the EU Charter of Fundamental Rights](#) (Aufforderung zur Einreichung von Vorschlägen für die Förderung des Kapazitätsaufbaus und der Sensibilisierung für die Charta der Grundrechte der EU).

²² [COM\(2020\) 713 final](#).

²³ Programm „Justiz“, Aufforderung zur Einreichung von Vorschlägen JUST-2021-JTRA, verfügbar unter <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>.

²⁴ Z. B. <https://era-comm.eu/charter-of-fundamental-rights/seminar-materials/>; <http://charterclick.ittig.cnr.it:3000/>; <http://help.elearning.ext.coe.int/>.

²⁵ [Die Europäische Plattform für Aus- und Fortbildung](#).

²⁶ [Bessere Rechtsetzung: Leitlinien und Instrumentarium | Europäische Kommission \(europa.eu\)](#).

²⁷ [Operational guidance on taking account of fundamental rights in European Commission impact assessments | Europäische Kommission \(europa.eu\)](#) (Operative Leitlinien zur Berücksichtigung der Grundrechte bei Folgenabschätzungen der Europäischen Kommission).

unterstützen soll. Das E-Learning-Tool wird öffentlich verfügbar sein und könnte gemeinsam mit dem aktualisierten Instrumentarium für eine bessere Rechtsetzung und den aktualisierten Leitlinien für die übrigen Unionsorgane sowie für die Gesetzgeber und politischen Entscheidungsträger der Mitgliedstaaten ein wertvolles Hilfsmittel darstellen. Die Kommission ist bereit, das Europäische Parlament und den Rat dabei zu unterstützen, die Charta bei ihrer Arbeit wirksam anzuwenden.

2.4 Stärkere Sensibilisierung der Bürgerinnen und Bürger

Zeitgleich mit der Annahme des vorliegenden Berichts bringt die Kommission eine Sensibilisierungskampagne zur Charta auf den Weg, um die Bürgerinnen und Bürger über ihre Rechte und darüber zu informieren, an wen sie sich wenden können, wenn ihre Rechte verletzt werden. Die Kampagne wird online, im Rahmen von Medienveranstaltungen und über die sozialen Medien unter dem Hashtag **#RightHereRightNow** durchgeführt. Ihr Schwerpunkt wird auf einer Reihe spezifische Rechte liegen, wie beispielsweise dem Recht auf Nichtdiskriminierung und Gleichheit, den Rechten des Kindes, der Freiheit der Meinungsäußerung und der Informationsfreiheit sowie dem Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht. An der Sensibilisierungskampagne werden wichtige Partner beteiligt sein, wie etwa zivilgesellschaftliche Organisationen, nationale Menschenrechtsinstitutionen und -gremien, die FRA sowie weitere Einrichtungen und sonstige Stellen der EU. Es werden Verbindungen zu anderen Informationskampagnen, die Rechte zum Gegenstand haben, sowie zur Konferenz zur Zukunft Europas hergestellt. Des Weiteren hat die Kommission ihre Webseite zur Charta auf der Europa-Website in alle EU-Amtssprachen übersetzt²⁸ und eine neue Version des europäischen E-Justizportals freigeschaltet, das Informationen über die Anwendung der Charta sowie über die Einrichtungen bietet, die Unterstützung leisten.²⁹

3. Die Charta als Kompass der EU für das digitale Zeitalter

Die Europäische Kommission hat sich das vorrangige Ziel gesetzt, den digitalen Wandel so zu gestalten, dass er allen Bürgerinnen und Bürgern zugutekommt und niemand zurückgelassen wird. Was einst als „Offline-Welt“ und „Online-Welt“ beschrieben wurde, ist heute immer schwerer unterscheidbar. Die Gewährleistung der Wahrung der Grundrechte in einem sich rasant verändernden digitalen Umfeld bringt eine Reihe von Herausforderungen mit sich.

Digitale Technologien durchdringen zunehmend alle Bereiche unserer Gesellschaft und können auf vielfältige und oftmals vorteilhafte Weise eingesetzt werden. Digitale Lösungen treiben die wissenschaftliche Forschung voran, bewirken eine Steigerung der Industrieproduktion, erleichtern den Übergang zur Nachhaltigkeit, vereinfachen die Erbringung zahlreicher Dienstleistungen und stellen mittlerweile den wichtigsten Kanal der privaten und öffentlichen Kommunikation dar. Des Weiteren verbessern sie die Möglichkeiten der Bürgerinnen und Bürger, am demokratischen Diskurs teilzunehmen und sich über jedes beliebige Thema zu informieren. Insbesondere Systeme künstlicher

²⁸ [Ihre Rechte in der EU | Europäische Kommission \(europa.eu\)](https://e-justice.europa.eu/581/DE/fundamental_rights).

²⁹ https://e-justice.europa.eu/581/DE/fundamental_rights

Intelligenz können zur Förderung von Innovation und Wohlstand eingesetzt und in allen Lebensbereichen genutzt werden, wie beispielsweise im Gesundheitswesen, für Übersetzungen oder als Hilfsmittel für Entscheidungen. Die digitale Automatisierung trägt zu einer effizienteren Arbeitsorganisation bei und ermöglicht ein beispielloses Maß an Koordinierung. Die Erhebung von Daten über das menschliche Handeln und seine Auswirkungen hilft den Menschen, die Welt zu begreifen und zu gestalten.

Zugleich besteht bei bestimmten Nutzungsformen dieser Technologie die Gefahr, dass die Wirksamkeit des durch Grundrechte garantierten Schutzes eingeschränkt wird. Die Verbreitung illegaler Inhalte wie Hassreden und Darstellungen von sexuellem Missbrauch von Kindern bedrohen das Recht des Opfers auf Würde, und die Verbreitung von Desinformation stellt den demokratischen Diskurs und unser Recht auf Zugang zu Informationen infrage. Werden Prozesse oder sogar Entscheidungen automatisiert, ist es mitunter schwer, die Transparenz der Ergebnisse und die diesbezügliche Rechenschaftspflicht zu gewährleisten; dies ist beispielsweise der Fall, wenn für Entscheidungen über die Zuteilung von Arbeit eine komplexe Software verwendet wird. Wenn Informationen fehlen oder schwer zu beschaffen sind, kann es schwierig sein, Verstöße gegen Grundrechte zu prüfen und dagegen vorzugehen.

Je mehr ein automatisiertes Tool auf externe Faktoren, wie etwa auf Daten oder den Input von Personen oder anderen Systemen, angewiesen ist, um ein Ergebnis zu generieren, desto schwerer ist es sicherzustellen, dass dieses Tool nicht von Grund auf gegen Rechte verstößt, beispielsweise aufgrund bestimmter integrierter Verzerrungen, die letztlich die Entscheidungsfindung in der Arbeitswelt beeinflussen können. Je mehr Daten über die Menschen erfasst werden, desto einfacher ist es, sie zu überwachen und in ihre Privatsphäre einzugreifen. Netzwerkeffekte können die Position des Einzelnen gegenüber großen Organisationen schwächen, beispielsweise auf Online-Marktplätzen oder Arbeitsplattformen, wo die einzelnen Bürgerinnen und Bürger nur eine geringe Verhandlungsmacht und kaum Möglichkeiten haben, sich zu organisieren. Zugleich werden Plattformen sozialer Medien auch genutzt, um Hass und illegale Inhalte zu verbreiten, beispielsweise illegale Hassreden, Darstellungen von sexuellem Missbrauch von Kindern oder terroristische Inhalte. Darüber hinaus muss noch viel unternommen werden, um Menschen, die keinen Internetzugang haben oder nicht über die erforderliche Ausstattung oder die notwendigen Kenntnisse für die Nutzung neuer und hilfreicher Tools verfügen, dabei zu helfen, die Vorteile dieser Tools in Anspruch zu nehmen.

Alle diese Probleme können je nach Kontext einzeln oder gemeinsam auftreten. Sie können einander verstärken und sich auf mehrere Grundrechte zugleich auswirken. Dies muss bei der Bewältigung dieser Probleme berücksichtigt werden. In diesem Bericht werden einige der wichtigsten Aspekte vorgestellt, bei denen der Einsatz digitaler Technologien Probleme für den Schutz der Grundrechte mit sich bringt. Es wird aufgezeigt, welche Rechte in diesen Kontexten betroffen sind, wie sich die Lage in den EU-Mitgliedstaaten entwickelt und wie die Mitgliedstaaten und die Europäische Kommission die Charta nutzen, um die unterschiedlichen Probleme zu bewältigen und die Rechte der Bürgerinnen und Bürger zu bewahren und zu fördern.

4. Bewältigung der Probleme bei der Moderation von Online-Inhalten

Online-Vermittler, wie beispielsweise Plattformen sozialer Medien, spielen im Leben jedes Einzelnen eine wichtige Rolle und ermöglichen neue Formen der Interaktion zwischen Einzelpersonen, Behörden und Unternehmen. Dank ihrer Nutzung verfügen die Bürgerinnen und Bürger nicht nur über einen größeren Fundus von Informationen, sondern haben auch mehr Möglichkeiten, ihr Recht auf freie Meinungsäußerung und auf Zugang zu Informationen wahrzunehmen; darüber hinaus bieten diese Plattformen vielfältige Räume, in denen sich die Menschen online engagieren können, und ermöglichen es Einzelpersonen und der Zivilgesellschaft, zusammenzufinden.

Große Plattformen – die neuen Marktplätze

- Einige Online-Plattformen sind mittlerweile so wichtig für den Informationsaustausch, dass sie in der demokratischen Debatte eine zentrale Rolle spielen.
- Mehr als die Hälfte der Gesamtbevölkerung der EU und 90 % der 16- bis 24-Jährigen nutzen soziale Medien, sodass Konzeption und Standards dieser Plattformen weitreichende gesellschaftliche Auswirkungen haben.³⁰
- Die Tools und Mechanismen, die diese Plattformen einsetzen, um Inhalte zu moderieren und den Nutzern Anreize zu bieten, ihre Leistungen möglichst lange in Anspruch zu nehmen, sind von entscheidender Bedeutung dafür, auf welche Informationen und Meinungen die Bürgerinnen und Bürger im Internet stoßen.
- Es ist schwierig, gegen auf diesen Plattformen veröffentlichte illegale Inhalte vorzugehen, weil sie öffentliche Räume für den Informationsaustausch darstellen, ohne rechtlich für Aspekte des öffentlichen Interesses verantwortlich zu sein.

Zugleich werden gesellschaftliche Probleme wie die Polarisierung³¹ oder die Verbreitung illegaler Inhalte durch die Nutzung von Online-Plattformen verschärft, oftmals mit schwerwiegenden negativen Auswirkungen auf Grundrechte wie den Schutz der Rechte des Kindes, den Verbraucherschutz, die Freiheit, Informationen zu empfangen und weiterzugeben, und den Schutz der Rechte des geistigen Eigentums.

Ausmaß und Tempo der Verbreitung von Online-Inhalten, die an sich nicht rechtswidrig sind, wie beispielsweise von Desinformation und Verschwörungstheorien, können sich nachteilig auf den demokratischen Diskurs, das Vertrauen in die Institutionen und – wie zu Beginn der COVID-19-Pandemie zu beobachten war – die Gesundheit, die Sicherheit und die Gleichbehandlung auswirken.

Die Demokratie in der EU sieht sich zahlreichen Herausforderungen gegenüber, darunter Populismus, einer immer stärker von Polarisierung geprägten politischen Debatte und der durch Desinformation verursachten Erosion des öffentlichen Vertrauens in demokratische

³⁰ https://ec.europa.eu/eurostat/de/web/products-datasets/product?code=isoc_sk_dskl_i

³¹ Beispiele für neu entstehende systemische Risiken für die Gesellschaft durch Online-Plattformen sind in der Folgenabschätzung zum Vorschlag für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) ([SWD\(2020\) 348 final](#), S. 40) („Folgenabschätzung zum Gesetz über digitale Dienste“) zu finden.

Prozesse.³² All dies wird verschärft durch die koordinierte Einflussnahme auf Wahlen durch Drittländer oder private Interessenträger, Desinformation sowie die mangelnde Transparenz und Rechenschaftspflicht im Bereich der gezielten politischen Werbung. Des Weiteren wurden Bedenken darüber geäußert, dass bestimmte Gruppen nicht ausreichend einbezogen oder beteiligt werden, wie beispielsweise junge oder ältere Menschen oder Menschen mit Behinderungen. Ethnische Minderheiten, wie etwa die Roma-Gemeinschaften, LGBTIQ-Personen und Frauen zögern in unterschiedlichem Maße und abhängig vom jeweiligen Kontext, für politische Ämter zu kandidieren, weil sie Angst vor Einschüchterung, Drohungen, Belästigung und Hassreden haben. Angesichts dessen tragen Maßnahmen zum Schutz der Grundrechte unmittelbar dazu bei, eine von Nachhaltigkeit, Gleichbehandlung und Teilhabe geprägte demokratische Gesellschaft zu bewahren, in der den Werten der EU entsprechend Toleranz, Nichtdiskriminierung und Pluralismus von vorrangiger Bedeutung sind.

Die Freiheit der Meinungsäußerung, auch online, bildet den Kern jeder Demokratie. Bei legislativen und nicht-legislativen Maßnahmen, die die Moderation von Inhalten und die Verantwortung der Online-Vermittler für die über ihre Dienste verbreiteten Inhalte zum Gegenstand haben, ist zu berücksichtigen, dass die Redefreiheit auch das Recht einschließt, Ideen zu äußern, die unter Umständen als kritisch, anstößig, beleidigend oder kontrovers betrachtet werden könnten, und dass die Redefreiheit nur unter ganz bestimmten Bedingungen eingeschränkt werden darf, die beispielsweise die Verbreitung von mutmaßlich illegalen Inhalten, beispielsweise Hassrede, betreffen. Der Europäische Gerichtshof für Menschenrechte hat jedoch klargestellt, dass die Staaten die Befugnis und womöglich sogar die positive Pflicht haben, gegen jegliche Ausdrucksformen vorzugehen, durch die Hass gegen Personen oder Gruppen mit einer bestimmten ethnischen Herkunft oder Religion verbreitet, geschürt oder gerechtfertigt oder dazu angestiftet wird.³³

In den meisten Fällen sind Desinformation und Fehlinformation nicht rechtswidrig, auch wenn sie verstörend oder anstößig erscheinen mögen. Während für den Staat im Falle von durch die Freiheit der Meinungsäußerung geschützten Äußerungen das oberste Gebot gilt, nicht einzugreifen und keine Zensur zu üben, hat er andererseits die positive Pflicht, ein günstiges Umfeld für eine inklusive und pluralistische öffentliche Debatte sicherzustellen, insbesondere wenn es um Wahlen geht, und für die Ausübung der Medienfreiheit Sorge zu tragen. Dies geht über den Bereich der Moderation von Inhalten hinaus und steht mit grundlegenden Bildungs- und Informationsmaßnahmen in Zusammenhang.

Private Akteure wie etwa Online-Plattformen legen ihre Konditionen und ihr Geschäftsmodell in Ausübung ihrer Rechte auf Vertragsfreiheit und auf unternehmerische Freiheit selbst fest, ohne dass der Staat Einfluss auf die Art der Inhalte nimmt, die sie hosten müssten. In diesem Zusammenhang könnten sie Maßnahmen ergreifen, die erhebliche Auswirkungen auf die Nutzer und deren Rechte haben. Nicht immer sind Rechtsbehelfe gegen diese privaten Entscheidungen verfügbar, die es ermöglichen würden, die

³² Studie des Europäischen Parlaments im Auftrag des Unterausschusses Menschenrechte: „The impact of disinformation on democratic processes and human rights in the world“ (Die Auswirkungen von Desinformation auf demokratische Prozesse und Menschenrechte in der Welt), Carme Colomina, Héctor Sánchez Margalef, Richard Youngs, verfügbar unter [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU\(2021\)653635_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf).

³³ Urteil des EGMR vom 6. Juli 2006, Erbakan/Türkei, Rn. 56.

Entscheidungen gegen Rechte und berechnigte Interessen von Einzelpersonen abzuwägen und eine gewisse Vorhersehbarkeit zu gewährleisten. Entfernen Online-Plattformen zu viele legale Inhalte, schränken sie unter Umständen die Freiheit der Meinungsäußerung und die Informationsfreiheit erheblich ein.

4.1 Die Situation in den Mitgliedstaaten

Im Rahmen der **gezielten Konsultation**, die für die Zwecke dieses Berichts durchgeführt wurde, berichteten Akteure der Zivilgesellschaft über Probleme in den Mitgliedstaaten im Zusammenhang mit bestimmten illegalen Online-Inhalten, wie beispielsweise mit Hetzkampagnen und Angriffen auf Personen, die sich für den Schutz der Rechte anderer einsetzen. Dabei wurden unverhältnismäßig häufig Frauen, insbesondere aufgrund ihrer Hautfarbe oder ihrer Zugehörigkeit zu einer schutzbedürftigen Bevölkerungsgruppe, wie Migrantinnen oder Roma-Frauen, sowie LGBTIQ-Personen ins Visier genommen. Minderjährige, die Online-Plattformen nutzen, sind unangemessenen, schädlichen und gewalttätigen Inhalten ausgesetzt; darüber hinaus besteht aufgrund der Aktivitäten von Cyberkriminellen die Gefahr, dass sie Opfer von Grooming oder für extremistische Gruppen rekrutiert werden. Sexuelle Gewalt gegen Kinder wird den Berichten zufolge durch das Internet verstärkt, beispielsweise aufgrund der gestiegenen Nachfrage nach Darstellungen von sexuellem Missbrauch von Kindern.

Darüber hinaus wurde von zivilgesellschaftlichen Organisationen festgestellt, dass Desinformation in mehreren Mitgliedstaaten ein Problem darstellt, das sich nachteilig auf Gesundheit und Sicherheit und den demokratischen Diskurs auswirkt. Es wurden vielfach Bedenken hinsichtlich mangelnder Transparenz (Kennzeichnungen, Warnmeldungen beim Versuch, falsche Inhalte zu teilen, Benachrichtigungen über für falsch befundene Inhalte) und einer unzureichenden Medienkompetenz im Hinblick auf falsche oder irreführende Inhalte geäußert.

Zwar wurden die Verbreitung illegaler Inhalte und Desinformation durchaus als Bedrohung wahrgenommen, jedoch warnten die zivilgesellschaftlichen Organisationen zugleich davor, welche Auswirkungen es auf die Freiheit der Meinungsäußerung haben könnte, wenn unausgewogene Moderationsstrategien verfolgt werden, um dieser Bedrohung zu begegnen. Zivilgesellschaftliche Organisationen berichteten, dass der Urheberrechtsschutz missbraucht wird, um im Internet Stimmen zum Schweigen zu bringen, und Gesetze gegen Verleumdung sowie gegen die Verherrlichung von Terrorismus herangezogen wurden, um gegen Einzelpersonen vorzugehen. Automatisierte Systeme zur Moderation von Inhalten weisen eine geringe Genauigkeit auf, insbesondere wenn sie auf Inhalte angewendet werden, bei denen die Prüfung der Rechtmäßigkeit ein hohes Maß an Kontextualisierung erfordert; angesichts dessen wurde die Sorge geäußert, dass diese Systeme eine ungerechtfertigte Beeinträchtigung der Freiheit der Meinungsäußerung bewirken könnten, indem sie übermäßig viele Inhalte sowie bestimmte Aussagen und Meinungen, darunter auch von Minderheiten, entfernen. Von der Wissenschaft und von Befragten im Rahmen der gezielten Konsultation wurde darauf hingewiesen, dass auch der Einsatz von Algorithmen für die personalisierte Anzeige von Inhalten zu einer Verzerrung des demokratischen Diskurses führen kann, da er nicht darauf ausgerichtet ist, den Nutzern im öffentlichen Interesse zuverlässige Informationen zur Verfügung zu stellen, sondern auf die Steigerung der Werbeeinnahmen.

Ähnlich wurde auch von Hinweisgebern über die Presse geäußert, dass Algorithmen zur maßgeschneiderten Anpassung der für Nutzer angezeigten Inhalte schädlich wirken.³⁴ Neben den Auswirkungen des Einsatzes solcher Systeme auf die Grundrechte wurde von Befragten im Rahmen der gezielten Konsultation auch die oftmals intransparente oder nicht vollkommen transparente Nutzung der Algorithmen und die Tatsache beanstandet, dass für die durch sie generierten Ergebnisse kaum Rechenschaftspflicht besteht.

Mehrere EU-Mitgliedstaaten haben eine Regulierung der von in ihrem Hoheitsgebiet ansässigen Anbietern erbrachten digitalen Dienste vorgenommen. Diese Gesetze sollen sicherstellen, dass die Diensteanbieter bestimmte Verfahrensvorschriften einhalten, wenn ihnen von Nutzern oder Behörden illegale Inhalte gemeldet werden. Mitunter beziehen sie sich auf bestimmte Kategorien illegaler Inhalte, wie beispielsweise Urheberrechtsverletzungen oder illegale Hassreden. Zwischen den konkreten Bestimmungen dieser Gesetze bestehen jedoch häufig Unterschiede im Hinblick auf:

- die für die Meldung illegaler Inhalte erforderlichen Informationen;
- die Möglichkeit für eine Reaktion derer, die diese Inhalte veröffentlicht haben;
- den zeitlichen Rahmen, innerhalb dessen die Diensteanbieter reagieren müssen;
- die möglichen obligatorischen Maßnahmen gegen missbräuchliche Meldungen;
- die Möglichkeit, strittige Fälle einem unabhängigen Dritten vorzulegen.

Angesichts einer wachsenden Besorgnis über die Verbreitung von Hassreden und terroristischen Inhalten haben mehrere Mitgliedstaaten in jüngster Zeit weitere Regelungen verabschiedet oder vorgeschlagen oder planen, weitere Regelungen zu verabschieden, deren Schwerpunkt insbesondere auf bestimmten Kategorien illegaler Inhalte liegt und die mitunter auch für außerhalb des Hoheitsgebiets des betreffenden Staates ansässige Diensteanbieter gelten. Diese individuellen Bemühungen der Mitgliedstaaten, gegen illegale Online-Inhalte vorzugehen und unterschiedliche Garantien für die Freiheit der Meinungsäußerung zu gewährleisten, haben jedoch dazu geführt, dass es keinen einheitlichen einschlägigen Rechtsrahmen gibt. Mehrere Mitgliedstaaten³⁵ sowie der Rat³⁶ und das Europäische Parlament³⁷ forderten, sich auf Unionsebene mit diesen gemeinsamen Anliegen zu befassen. Darüber hinaus wiesen einige Mitgliedstaaten darauf hin, dass aufgrund der mangelnden grenzüberschreitenden Zusammenarbeit zwischen den einzelstaatlichen Behörden keine wirksame Überwachung von über Grenzen hinweg betriebenen Online-Plattformen möglich ist.³⁸

4.2 Die strategische Reaktion der EU

³⁴ Siehe beispielsweise <https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero>.

³⁵ <https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package>

³⁶ [Schlussfolgerungen des Europäischen Rates](#) vom 9. Juni 2020, „Gestaltung der digitalen Zukunft Europas“, und [Schlussfolgerungen](#) der Außerordentlichen Tagung des Europäischen Rates vom 1. und 2. Oktober 2020.

³⁷ Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zum Gesetz über digitale Dienste: Verbesserung der Funktionsweise des Binnenmarkts (2020/2018(INL)); Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zum Gesetz über digitale Dienste: Anpassung der handels- und zivilrechtlichen Vorschriften für online tätige Unternehmen (2020/2019(INL)).

³⁸ Folgenabschätzung zum Gesetz über digitale Dienste, Abschnitt 2.3.6. Eingeschränkte Zusammenarbeit der Mitgliedstaaten und mangelndes Vertrauen.

Nach entsprechenden Forderungen der Mitgliedstaaten wurden auf Unionsebene mehrere sektorspezifische Maßnahmen ergriffen, um gegen bestimmte Formen illegaler Inhalte unter anderem im Zusammenhang mit Terrorismus, sexuellem Missbrauch von Kindern, Anstiftung zu Hass und Gewalt, Menschenhandel, unsicheren Produkten und Urheberrechtsverletzungen vorzugehen und zugleich den Schutz der Grundrechte zu gewährleisten.

Richtlinie über audiovisuelle Mediendienste.

Die überarbeitete **Richtlinie über audiovisuelle Mediendienste** wurde im Jahr 2018 verabschiedet. In dieser Richtlinie sind Maßnahmen zum Schutz Minderjähriger vor audiovisuellen Inhalten und kommerzieller Kommunikation vorgesehen, die ihre körperliche, geistige und seelische Entwicklung beeinträchtigen könnten. Des Weiteren müssen die Mitgliedstaaten dafür sorgen, dass audiovisuelle Mediendienste nicht zu Hass oder Gewalt aus den in Artikel 21 der Charta der Grundrechte der EU genannten Gründen anstiften. Diese Richtlinie war bis zum 19. September 2020 in nationales Recht umzusetzen. Im November 2020 leitete die Kommission Vertragsverletzungsverfahren (Aufforderungsschreiben) gegen 23 Mitgliedstaaten ein, die die Richtlinie noch nicht umgesetzt hatten, und viele setzten diese im folgenden Jahr um. Im September 2021 sendete die Kommission eine zweite Warnung (mit Gründen versehene Stellungnahmen) an neun Mitgliedstaaten wegen Nichtmitteilung der vollständigen Umsetzung. Die Umsetzung der überarbeiteten Richtlinie über audiovisuelle Mediendienste ist von wesentlicher Bedeutung nicht nur für die Marktteilnehmer, sondern auch für Einzelpersonen (einschließlich Zuschauer und Minderjährige).

Richtlinie über das Urheberrecht im digitalen Binnenmarkt

Die **Urheberrechtsrichtlinie**³⁹ wurde im April 2019 angenommen und zielt darauf ab sicherzustellen, dass Rechteinhaber einen gerechten Ausgleich für die Nutzung ihres Werkes erhalten. Dabei soll ein Gleichgewicht zwischen widerstreitenden Grundrechten geschaffen werden, wie beispielsweise dem Recht auf geistiges Eigentum, der Freiheit der Meinungsäußerung und der Informationsfreiheit, der Freiheit der Wissenschaft und dem Recht auf Bildung und kulturelle Vielfalt. Mit der Richtlinie wurden verbindliche Ausnahmen vom Urheberrecht eingeführt, durch die die Freiheit der Meinungsäußerung von Nutzern geschützt wird, die Inhalte generieren und über Dienste für das Teilen von Online-Inhalten hochladen. In Übereinstimmung mit der Richtlinie veranstaltete die Kommission einen Dialog zwischen den Interessenträgern, in dessen Rahmen bewährte Verfahren für die Zusammenarbeit zwischen den Diensteanbietern für das Teilen von Online-Inhalten und Rechteinhabern erörtert wurden, wobei die notwendige Ausgewogenheit zwischen den Grundrechten und die Inanspruchnahme von Ausnahmen und Beschränkungen besonders berücksichtigt wurden. Im Anschluss an diesen Dialog nahm die Kommission im Juni 2021 Leitlinien zur einheitlichen Anwendung des Artikels 17 der Richtlinie an; darin sind neue Regelungen für die Nutzung geschützter Inhalte durch Diensteanbieter für das Teilen von

³⁹ [Richtlinie \(EU\) 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG](#) (ABl. L 130 vom 17.5.2019).

Online-Inhalten festgelegt.⁴⁰ Diese Leitlinien, in denen die Standpunkte der Mitgliedstaaten und Interessenträger berücksichtigt werden, beinhalten praktische Hinweise zu den wichtigsten Bestimmungen des Artikels 17 und unterstützen die Marktteilnehmer bei der Einhaltung der nationalen Gesetzgebung, die auf den Vorgaben der Richtlinie beruht.

Verhaltenskodex zur Bekämpfung illegaler rassistischer und fremdenfeindlicher Hassreden im Internet

Im Jahr 2016 unterzeichneten die Kommission sowie mehrere große Online-Plattformen einen freiwilligen **Verhaltenskodex**, mit dem sichergestellt werden soll, dass Meldungen **illegaler rassistischer und fremdenfeindlicher Hassreden** zeitnah geprüft werden, wobei nicht nur die Nutzungsbedingungen der Unternehmen herangezogen werden, sondern auch die von den Mitgliedstaaten zur Umsetzung der EU-Rechtsvorschriften gegen rassistische und fremdenfeindliche Hassreden verabschiedeten Gesetze.⁴¹ Die Einhaltung des Verhaltenskodex wird regelmäßig bewertet.⁴² Mit dem Kodex werden gute Ergebnisse erzielt, wobei auch eine Zusammenarbeit zwischen Online-Plattformen, Mitgliedstaaten und der Zivilgesellschaft aufgebaut wurde, die es ermöglicht, eine hochwertige Moderation von Inhalten sicherzustellen, wenn ein tiefgehendes Verständnis der kulturellen, sprachlichen und kulturellen Hintergründe der beanstandeten Inhalte erforderlich ist.

Empfehlung zur Sicherheit von Journalisten und anderen Medienschaffenden

Die Sicherheit ist aufgrund der Anstiftung zu Hass im Internet und der Androhung körperlicher Gewalt, aber auch aufgrund von Cybersicherheitsrisiken und illegaler Überwachung zu einem großen Anliegen von Journalisten geworden. Am 16. September 2021 legte die Europäische Kommission eine **Empfehlung zur Gewährleistung des Schutzes, der Sicherheit und der Handlungskompetenz von Journalisten** vor.⁴³ In dieser Empfehlung werden die Mitgliedstaaten aufgefordert, die Zusammenarbeit zwischen Online-Plattformen und Organisationen mit Fachwissen zur Bekämpfung der Bedrohungen, denen Journalisten ausgesetzt sind, zu fördern, indem sie diese beispielsweise in ihrer potenziellen Rolle als vertrauenswürdige Hinweisgeber bestärken. Journalisten und andere Medienschaffende sind nicht nur Ziele der Online-Aufstachelung zu Hass und der Androhung körperlicher Gewalt, sondern können auch Gegenstand illegaler Überwachung sein, und in der Empfehlung wird darauf hingewiesen, dass einschlägige nationale Cybersicherheitseinrichtungen Journalisten auf Anfrage dabei unterstützen sollten, Angriffe auf ihre Geräte oder Online-Konten zu ermitteln, indem die Dienste kriminaltechnischer Ermittler im Bereich der Cybersicherheit in Anspruch genommen werden. Die Mitgliedstaaten sollten sich auch für einen regelmäßigen Dialog zwischen diesen

⁴⁰ Mitteilung der Kommission an das Europäische Parlament und den Rat – Leitlinien zu Artikel 17 der Richtlinie (EU) 2019/790 über das Urheberrecht im digitalen Binnenmarkt ([COM\(2021\) 288 final](#)).

⁴¹ [Rahmenbeschluss 2008/913/JI des Rates vom 28. November 2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit](#) (ABl. L 328 vom 6.12.2008).

⁴² Die letzte Bewertungsrunde fand im Jahr 2021 statt: [The EU Code of conduct on countering illegal hate speech online | Europäische Kommission \(europa.eu\)](#) (EU-Verhaltenskodex zur Bekämpfung illegaler Hassreden im Internet).

⁴³ Empfehlung der Kommission vom 16.9.2021 zur Gewährleistung des Schutzes, der Sicherheit und der Handlungskompetenz von Journalisten und anderen Medienschaffenden in der Europäischen Union ([C\(2021\) 6650 final](#)).

Cybersicherheitseinrichtungen, den Medien und der Industrie einsetzen, insbesondere im Hinblick auf die Förderung des Cybersicherheitsbewusstseins und der digitalen Kompetenzen von Journalisten.

Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte

Sicherheit und Achtung der Grundrechte sind keine widersprüchlichen Ziele, sondern stehen miteinander in Einklang und ergänzen einander. Um die Sicherheit in virtuellen und physischen Umgebungen zu gewährleisten, muss gegen illegale Online-Inhalte vorgegangen werden. Um sicherzustellen, dass terroristische Inhalte entfernt werden, verabschiedeten das Europäische Parlament und der Rat im Jahr 2021 eine **Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte**.⁴⁴ Diese Verordnung beinhaltet eine Reihe von Garantien zum Schutz der Grundrechte, insbesondere der Freiheit der Meinungsäußerung. So können beispielsweise Entfernungsanordnungen der einzelstaatlichen Behörden nur für terroristische Inhalte im Sinne der Verordnung erlassen werden und müssen eine Begründung für die Einstufung des Materials als terroristischer Inhalt enthalten. Inhalte, die für Bildungs-, Presse-, Forschungszwecke oder künstlerische Zwecke verbreitet werden, sowie Inhalte, die für die Zwecke der Sensibilisierung für terroristische Aktivitäten verbreitet werden, sind vom Anwendungsbereich der Verordnung ausgenommen. Online-Plattformen sind nicht verpflichtet, automatisierte Verfahren zur proaktiven Ermittlung oder Entfernung terroristischer Inhalte zu verwenden; werden jedoch technische Maßnahmen eingesetzt, sollten Schutzvorkehrungen getroffen werden – insbesondere durch menschliche Beaufsichtigung und Überprüfung –, um für Fehlerfreiheit zu sorgen. Ab März 2023 müssen die Mitgliedstaaten und Online-Plattformen darüber hinaus jährliche Berichte über die zur Entfernung terroristischer Inhalte ergriffenen Maßnahmen und die Funktionsweise der möglicherweise genutzten automatisierten Verfahren vorlegen.

Rechtsvorschriften zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet

Der Schwerpunkt der Rechtsvorschriften zur Bekämpfung illegaler Inhalte lag weitestgehend auf öffentlich verfügbaren Inhalten, die beispielsweise in den sozialen Medien oder auf Websites veröffentlicht werden; zugleich wurde jedoch auch gegen die Verbreitung von **Darstellungen von sexuellem Missbrauch von Kindern** über interpersonelle Kommunikationsdienste, auch in den interpersonellen Kommunikationsinstrumenten in sozialen Medien, vorgegangen. Im August 2021 trat eine **Übergangsregelung**⁴⁵ in Kraft, mit der sichergestellt wird, dass die Anbieter bestimmter Online-Kommunikationsdienste, wie Webmail und Messenger-Dienste, weiterhin bestimmte Technologien einsetzen dürfen, jedoch nur in dem unbedingt erforderlichen Maße, um Darstellungen von sexuellem Missbrauch von Kindern zu ermitteln, zu melden und zu entfernen, wobei sie gleichzeitig eine Reihe von Garantien zum Schutz der Privatsphäre und zum Schutz personenbezogener

⁴⁴ [Verordnung \(EU\) 2021/784 vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte](#) (ABl. L 172 vom 17.5.2021).

⁴⁵ [Verordnung \(EU\) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet](#) (ABl. L 274 vom 30.7.2021).

Daten gemäß der Datenschutz-Grundverordnung gewährleisten müssen. Der Einsatz von Mechanismen zur Aufdeckung von sexuellem Missbrauch von Kindern in der interpersonellen Kommunikation ist mit dem Risiko verbunden, dass dabei Grundrechte beeinträchtigt werden, insbesondere des Rechts auf Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten sowie der Freiheit der Meinungsäußerung. Mit der Übergangsregelung soll diese Beeinträchtigung eingedämmt werden, indem lediglich die Verwendung von Technologien zugelassen wird, die am wenigsten in die Privatsphäre eingreifen und dem Stand der Technik in der Branche entsprechen. Des Weiteren sieht die Verordnung Beschwerdemechanismen vor, die eingerichtet werden müssen, um sicherzustellen, dass Einzelpersonen Beschwerden bei Anbietern einlegen können, wenn Inhalte zu Unrecht entfernt werden. Die Kommission erarbeitet derzeit einen **Vorschlag für eine Rechtsvorschrift**, welche die Übergangsregelung ersetzen, Rechtssicherheit für die Diensteanbieter gewährleisten und einen einheitlichen Ansatz für die Ermittlung, Entfernung und Meldung von Darstellungen von sexuellem Missbrauch von Kindern sicherstellen soll; gleichzeitig sollen die Rechte des Kindes sowie die Notwendigkeit, Kinder vor sexuellem Missbrauch zu schützen, und das Recht der Nutzer von Online-Diensten auf Achtung des Privatlebens und ihrer Kommunikation, in ein ausgewogenes Verhältnis zueinander gesetzt werden.

Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025

Die Bekämpfung des digitalen Geschäftsmodells von Menschenhändlern ist eine der Prioritäten der von der Kommission im April 2021 vorgelegten Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025⁴⁶. Internetdiensteanbieter und einschlägige Unternehmen sind Teil der Lösung zur Unterstützung der Bekämpfung des Menschenhandels durch Identifizierung und Entfernung von Online-Material, das mit der Ausbeutung und dem Missbrauch von Opfern des Menschenhandels in Verbindung gebracht wird. Die Kommission wird einen Dialog mit einschlägigen Internet- und Technologieunternehmen führen, um die Nutzung von Online-Plattformen für die Anwerbung und Ausbeutung von Opfern einzudämmen. Die Kommission wird darüber hinaus ähnliche Dialoge der Mitgliedstaaten auf nationaler Ebene fördern.

Vorschlag für eine Verordnung für ein Gesetz über digitale Dienste

In ihrem im Dezember 2020 vorgelegten Vorschlag für eine Verordnung für ein **Gesetz über digitale Dienste**⁴⁷, der derzeit von den gesetzgebenden Organen beraten wird, formulierte die Kommission die Zuständigkeiten von Online-Vermittlern. Unbeschadet sektorspezifischer EU-Bestimmungen wie den Bestimmungen zum Urheberrecht oder zu terroristischen Online-Inhalten werden in diesem Verordnungsvorschlag einheitliche horizontale EU-Vorschriften für eine ausgewogene Regulierung der Moderation von Online-Inhalten bereitgestellt.

⁴⁶ Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025 ([COM\(2021\) 171 final](#)).

⁴⁷ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG ([COM\(2020\) 825 final](#)).

In dem Vorschlag ist ein angemessener Schutz aller Grundrechte vorgesehen, einschließlich des Rechts der Nutzer auf freie Meinungsäußerung und Achtung des Privatlebens, der unternehmerischen Freiheit der Plattformen sowie der Vertragsfreiheit und des Schutzes der Rechte des geistigen Eigentums. Des Weiteren soll mit dem Vorschlag das Risiko gemindert werden, dass schutzbedürftige Personen und Gruppen Opfer von Drohungen, Einschüchterung oder diskriminierendem Verhalten werden, und das Recht aller Nutzer von Online-Diensten auf Menschenwürde geschützt werden.

Um diese Ziele zu erreichen, sieht der Vorschlag für eine Verordnung Folgendes vor:

- Die bestehende Haftungsregelung für Online-Vermittler wird weitgehend beibehalten, einschließlich des Verbots einer allgemeinen Verpflichtung zur Überwachung oder aktiven Nachforschung. Dieser Ansatz baut auf der bestehenden Richtlinie über den elektronischen Geschäftsverkehr auf.⁴⁸ Mit der Verordnung soll Folgendes sichergestellt werden: i) der verhältnismäßige und angemessene Schutz des Rechts auf freie Meinungsäußerung durch die Einschränkung der Anreize für die Entfernung legaler Inhalte und des Rechts auf unternehmerische Freiheit durch die Gewährleistung der Verhältnismäßigkeit der von den Online-Vermittlern geforderten Bemühungen und den Schutz ihrer rechtmäßigen gewerblichen Nutzer; ii) die Ausräumung ordnungspolitischer Bedenken im Zusammenhang mit der Verbreitung unterschiedlicher Formen illegaler Inhalte, indem sichergestellt wird, dass diese von den Vermittlern zügig und im Einklang mit den gesetzlich vorgesehenen Bedingungen entfernt werden.
- Mit der Festlegung klarer und verhältnismäßiger Sorgfaltspflichten von Online-Vermittlern soll sichergestellt werden, dass auf angemessene und transparente Weise gegen illegale Inhalte vorgegangen wird und die Nutzer ihre Rechte wahrnehmen können. Des Weiteren sieht der Vorschlag eine Reihe strenger Schutzvorkehrungen für die Verfahren zur Moderation von Inhalten vor, die auch für die privaten Geschäftsbedingungen gelten.
- Sehr große Online-Plattformen, die aufgrund ihrer Reichweite eine zentrale, systemische Rolle bei der Förderung der öffentlichen Debatte spielen, werden verpflichtet, die mit ihren Diensten verbundenen Risiken zu bewerten und zu mindern, einschließlich der Risiken für bestimmte Grundrechte: Achtung des Privat- und Familienlebens, Freiheit der Meinungsäußerung und Informationsfreiheit, Nichtdiskriminierung und Rechte des Kindes. Die Maßnahmen zur Risikominderung müssen zudem den möglichen nachteiligen Auswirkungen der von den Plattformen zur Verstärkung von Inhalten eingesetzten Algorithmen Rechnung tragen, wie beispielsweise von Empfehlungs- oder Werbesystemen. Darüber hinaus unterliegen sehr große Plattformen einer erhöhten Rechenschaftspflicht, müssen ihren Nutzern bei ihren Online-Interaktionen eine größere Auswahl ermöglichen und zulassen, dass unabhängige Prüfer sowie zugelassene Forscher ihre Systeme prüfen.

Bekämpfung von Desinformation und Regulierung von politischer Werbung im Internet

⁴⁸ [Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt](#) („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000).

Desinformation, Fehlinformation und die Verbreitung von Verschwörungsmythen können zu einer Polarisierung von Debatten führen und eine Gefährdung der Gesundheit, der Sicherheit und der Umwelt nach sich ziehen. Darüber kann Desinformation die Fähigkeit der Menschen beeinträchtigen, informierte Entscheidungen auf der Grundlage korrekter Fakten zu treffen. Mitunter erfolgt Desinformation in Form von Äußerungen, gegen die der Staat rechtmäßig vorgehen kann (wie beispielsweise rassistische und fremdenfeindliche Anstiftung zu Gewalt und Hass). Sehr häufig ist sie jedoch durch das Recht auf freie Meinungsäußerung geschützt, auch wenn sie jeglicher wissenschaftlichen oder realen Grundlage entbehrt. Im Falle solcher geschützten Äußerungen darf der Staat keine Zensur üben. Um wirksam zu sein, müssen Maßnahmen, mit denen die Reichweite von Desinformation und Verschwörungsmythen eingeschränkt werden soll, von Maßnahmen zur Förderung eines günstigen Umfelds für eine inklusive und pluralistische öffentliche Debatte begleitet sein. Dies ist insbesondere im Zusammenhang mit Wahlen relevant.

Vor diesem Hintergrund befasste sich die Kommission im Zeitraum 2020–2021 weiterhin mit der Erarbeitung mehrerer Maßnahmen, um Online-Umgebungen transparenter zu gestalten, die Rechenschaftspflicht der beteiligten Akteure zu erhöhen, die Handlungskompetenz der Nutzer zu stärken und eine offene demokratische Debatte im Internet zu fördern. Zu diesen Maßnahmen zählten unter anderem i) die Unterstützung unabhängiger Faktenprüfer und Wissenschaftler, insbesondere im Rahmen der **Europäischen Beobachtungsstelle für digitale Medien**⁴⁹, ii) Maßnahmen zur Verbesserung der Medienkompetenz und iii) die Überwachung des **Verhaltenskodex zur Bekämpfung von Desinformation**⁵⁰. Auf der Grundlage der Ergebnisse dieser Überwachungstätigkeit legte die Kommission zudem Leitlinien vor, in denen aufgezeigt wird, wie die gegenwärtigen und künftigen Unterzeichner des Verhaltenskodex, darunter die Anbieter privater Messaging-Apps, die Werbebranche und andere relevante Interessenträger, den Geltungsbereich und die Anwendung des Kodex erweitern könnten und wie ein zuverlässigerer Überwachungsrahmen geschaffen werden kann.⁵¹

Um den demokratischen Diskurs zu fördern, wurden im **Europäischen Aktionsplan für Demokratie**⁵² Maßnahmen zur Förderung freier und fairer Wahlen, zur Stärkung der Medienfreiheit und zur Bekämpfung von Desinformation festgelegt. Dies umfasst den im November 2021 vorgelegten Vorschlag für eine Verordnung über die Transparenz und das Targeting politischer Werbung⁵³, der Teil von Maßnahmen ist, die dazu beitragen sollen, die Integrität von Wahlen zu schützen und die demokratische Teilhabe zu fördern. Mit diesem Vorschlag soll vorgeschrieben werden, dass jede politische Werbeanzeige eindeutig als solche gekennzeichnet sein und Angaben darüber enthalten muss, wer wie viel dafür bezahlt. Techniken für das Targeting (Ausrichten) und die Amplifikation von politischer Werbung sollen so genau wie noch nie öffentlich gemacht und die Verwendung sensibler personenbezogener Daten soll ohne ausdrückliche Zustimmung der Betroffenen verboten

⁴⁹ [EDMO – United against disinformation.](#)

⁵⁰ [Code of Practice on Disinformation | Shaping Europe's digital future \(europa.eu\)](#) (Verhaltenskodex zur Bekämpfung von Desinformation, Gestaltung der digitalen Zukunft Europas).

⁵¹ https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2585

⁵² [Europäischer Aktionsplan für Demokratie | Europäische Kommission \(europa.eu\).](#)

⁵³ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung ([COM\(2021\) 731 final](#)).

werden. Im **neuen Aktionsplan für digitale Bildung (2021–2027)**⁵⁴ schließlich wird vorgeschlagen, Leitlinien für Lehrkräfte und Bildungspersonal zur Bekämpfung von Desinformation und zur Förderung digitaler Kompetenzen zu erarbeiten.

Vorschlag für eine neue Verordnung über die allgemeine Produktsicherheit

Um weiteren branchenspezifischen Erfordernissen Rechnung zu tragen, hat die Kommission im Rahmen der Überprüfung der Produktsicherheitsvorschriften der EU im Juni 2021 einen Vorschlag für eine neue **Verordnung über die allgemeine Produktsicherheit**⁵⁵ angenommen und veröffentlicht. Dieser Vorschlag, der auf dem Vorschlag für das Gesetz über digitale Dienste aufbaut, sieht für Online-Marktplätze die Einführung zusätzlicher Anforderungen bezüglich unsicherer Produkte vor, die als eine bestimmte Art illegaler Inhalte gelten. Der Vorschlag wird derzeit von den gesetzgebenden Organen beraten.

5. Schutz der Grundrechte im Zusammenhang mit dem Einsatz von KI

Der Einsatz von Technologien künstlicher Intelligenz (KI) kann für unsere Gesellschaft erhebliche Vorteile mit sich bringen. Mithilfe dieser Technologien ist es möglich, die Effizienz von Prozessen zu steigern oder Innovation und Forschung voranzutreiben. Des Weiteren können sie eingesetzt werden, um unterschiedliche Grundrechte, wie etwa das Recht auf freie Meinungsäußerung und Informationsfreiheit sowie auf Gesundheitsschutz, zu fördern und in wichtigen Bereichen des öffentlichen Interesses wie der öffentlichen Sicherheit oder Gesundheit Verbesserungen zu bewirken.

Andererseits kann jedoch die Nutzung von KI ohne angemessene Schutzvorkehrungen und Qualitätskontrollen für die Automatisierung oder Unterstützung von Entscheidungsprozessen oder im Zusammenhang mit bestimmten Tätigkeiten, wie beispielsweise bei der Überwachung, auch Verstöße gegen die Rechte der Bürgerinnen und Bürger zur Folge haben. Solche Verstöße können in Abhängigkeit davon, wie umfassend ein System eingesetzt wird, ein erhebliches Ausmaß annehmen und sind mitunter schwer zu verhindern oder aufzudecken, wenn das KI-System nicht hinreichend transparent ist oder sein Einsatz den Betroffenen nicht bekannt ist. So kann beispielsweise die Nutzung von KI für die Erschließung von Informationen über Einzelpersonen den Datenschutz und die Privatsphäre beeinträchtigen. Verzerrungen in Algorithmen oder Trainingsdaten, wie beispielsweise geschlechtsspezifische oder rassistische Verzerrungen oder Verzerrungen aufgrund der ethnischen Herkunft, können zu ungerechtfertigten und diskriminierenden Ergebnissen führen. Wird ein System, das für die Einschätzung des möglichen Erfolgs am Arbeitsplatz eingesetzt wird, vorwiegend mit Daten über Männer trainiert, wird es wahrscheinlich schlechter funktionieren und diskriminierende Ergebnisse hervorbringen, wenn es für die Analyse von Daten über Frauen verwendet wird. Darüber hinaus kann der Einsatz von KI die Menschenwürde, das Recht auf eine gute Verwaltung, Verbraucherschutz sowie soziale

⁵⁴ [Aktionsplan für digitale Bildung \(2021–2027\) | Allgemeine und berufliche Bildung \(europa.eu\)](#).

⁵⁵ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 87/357/EWG des Rates und der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates ([COM\(2021\) 346 final](#)).

Sicherheit und Unterstützung, die Freiheit der Meinungsäußerung, die Versammlungsfreiheit, das Recht auf Bildung, Asyl, Tarifverhandlungen und Kollektivmaßnahmen, gerechte und angemessene Arbeitsbedingungen, Zugang zur Gesundheitsvorsorge, Vielfalt der Kulturen und Sprachen, Datenschutz und Achtung des Privatlebens sowie die Rechte von schutzbedürftigen Personengruppen wie beispielsweise Kindern beeinträchtigen. Werden solche Systeme im Bereich der Strafverfolgung oder der Justiz verwendet, können sie sich zudem die Unschuldsvermutung, die Verteidigungsrechte und das Recht auf ein unparteiisches Gericht auswirken. Sind keine einschlägigen Informationen über automatisierte Systeme zugänglich oder verfügbar, beeinträchtigt dies die wirksame Durchsetzung der Pflicht zur Wahrung der Grundrechte und den Zugang der Bürgerinnen und Bürger zu wirksamen Rechtsbehelfen.

Was ist KI und welche ihrer besonderen Merkmale bergen Risiken?

- KI ist ein Oberbegriff für eine Reihe von Technologien, bei denen sich in den letzten Jahren rasante Entwicklungen vollzogen haben. Bestimmte Formen von KI-Systemen funktionieren nach Regeln, die automatisch generiert und nicht von Menschen programmiert werden. Dies kann mitunter zu beeindruckenden Ergebnissen führen, aber auch Probleme mit sich bringen. Aufbauend auf der von der OECD vorgenommenen Definition wird KI im Gesetz über künstliche Intelligenz definiert als Software, die mithilfe von maschinellem Lernen, logik- und wissensgestützten Konzepten oder statistischen Ansätzen entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren.
- Bei bestimmten KI-Systemen ist es aufgrund ihrer Undurchsichtigkeit (mangelnde Transparenz) und Komplexität (Betrieb mit zahlreichen unterschiedlichen Komponenten und Prozessen) schwer, mögliche Verstöße gegen Rechtsvorschriften, darunter auch gegen Bestimmungen, die die Achtung der Grundrechte sicherstellen sollen, zu erkennen und nachzuweisen und mögliche Fehler oder Fehlfunktionen des Systems zurückzuverfolgen.
- Bei einer bestimmten Kategorie von KI-Anwendungen kann sogar während ihres Einsatzes eine kontinuierliche Anpassung erfolgen, sodass sie sich auf eine unvorhersehbare, mitunter nicht ohne Weiteres zu überwachende Weise verändern und weiterentwickeln. Dies führt zu einem gewissen Maß an Unberechenbarkeit, das den Schutz der Grundrechte beeinträchtigen kann.
- Die autonome Leistung der Systeme kann Sicherheitsprobleme bergen, da manche KI-Systeme kaum oder keine menschliche Intervention erfordern, um Aufgaben auszuführen.
- Die Abhängigkeit mancher Systeme von Daten sowie mögliche Verzerrungen innerhalb der Algorithmen können systemische Verzerrungen und Fehler verursachen oder verstärken. Werden diese Systeme nicht ordnungsgemäß konzipiert, getestet und eingesetzt, können sie negative Folgen, wie beispielsweise Diskriminierung, verschärfen.

5.1 Situation und Maßnahmen in den Mitgliedstaaten

In den letzten Jahren haben die EU-Mitgliedstaaten versucht, die mit dem Einsatz von KI-Technologien verbundenen Probleme in Angriff zu nehmen. Viele haben nationale KI-

Strategien⁵⁶ erarbeitet, in denen die Notwendigkeit unterstrichen wird, die Achtung der Grundrechte sicherzustellen. Darüber hinaus wurden in den Mitgliedstaaten Leitlinien und ethnische Normen erarbeitet oder sind geplant, die die Nutzer von KI-Tools dabei unterstützen, deren Transparenz, Rückverfolgbarkeit und Robustheit sicherzustellen, mögliche Verzerrungen zu beseitigen und wirksame Wege zu finden, um ihrer Verpflichtung zur Achtung der Grundrechte nachzukommen. In einigen Fällen werden Leitlinien und Fachwissen von Wissenschaftlern⁵⁷ oder eigens eingerichteten Sachverständigengruppen⁵⁸ erarbeitet.

Auch im Rahmen ihres gemeinsamen Handelns auf Unionsebene wiesen die Mitgliedstaaten nachdrücklich darauf hin, dass die uneingeschränkte Achtung der in der Charta verankerten Rechte gewährleistet sein muss, und riefen dazu auf, die maßgeblichen geltenden Rechtsvorschriften zu überprüfen, um sicherzustellen, dass sie im Hinblick auf die neuen Chancen und Herausforderungen, die sich durch KI ergeben, zweckdienlich sind.⁵⁹ Im Oktober 2020 billigten 26 der 27 Mitgliedstaaten ein Dokument mit dem Titel „Die Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandel“⁶⁰, in dem sie forderten, dass Probleme wie Undurchsichtigkeit, Komplexität, der sogenannte „Bias“, ein gewisses Maß an Unberechenbarkeit und teilweise autonomes Verhalten einiger KI-Systeme angegangen werden müssen, um deren Vereinbarkeit mit den Grundrechten sicherzustellen und die Durchsetzung der Rechtsvorschriften zu erleichtern. Die Mitgliedstaaten unterstrichen, dass es wichtig ist, verschiedene Interessenträger, unter anderem aus der Zivilgesellschaft, einzubeziehen, um ihr Fachwissen zu nutzen.

Zum Zeitpunkt der Annahme des vorliegenden Berichts hatte kein EU-Mitgliedstaat Rechtsvorschriften verabschiedet, um die mit dem Einsatz von KI verbundenen grundrechtlichen Probleme zu lösen.⁶¹ Stattdessen stützen sich die Behörden der Mitgliedstaaten offenbar auf die geltenden Rechtsvorschriften. Im Jahr 2017 ordnete ein italienisches Gericht die Offenlegung eines Algorithmus zur automatisierten Entscheidungsfindung im Zusammenhang mit der Verwaltung der Mobilität von Arbeitskräften durch das italienische Bildungsministerium an; Grundlage dieser Anordnung war das Recht auf Zugang zu Dokumenten, das auch eine Voraussetzung für die Ausübung

⁵⁶ Bis Juni 2021 hatten 20 Mitgliedstaaten und Norwegen ihre nationalen KI-Strategien veröffentlicht, während sieben Mitgliedstaaten in der abschließenden Phase der Ausarbeitung waren.

https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.

⁵⁷ So haben beispielsweise Wissenschaftler der Universität Utrecht im April 2021 einen Kodex für die digitale öffentliche Verwaltung für niederländische Behörden entwickelt, der sich auf die Grundrechte stützt.

<https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur>.

⁵⁸ Ein Beispiel dafür sind die deutsche „Datenethikkommission“ und das von ihr im Jahr 2019 erarbeitete Fachwissen:

https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html.

⁵⁹ Tagung des Europäischen Rates (19. Oktober 2017) – [Schlussfolgerungen, EUCO 14/17](#), S. 8, und [Schlussfolgerungen zu dem koordinierten Plan für künstliche Intelligenz](#) (11. Februar 2019) 6177/19, 2019.

⁶⁰ <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/de/pdf>

⁶¹ Den Angaben Finnlands zufolge wird dort gegenwärtig ein Legislativvorschlag zur automatisierten Entscheidungsfindung in der Verwaltung erarbeitet, der bis Ende 2021 fertiggestellt sein soll. In diesem Bericht werden einige Beispiele für von Mitgliedstaaten ergriffene Maßnahmen (Rechtsvorschriften, Finanzierung und andere) vorgestellt, um die unterschiedlichen Formen von Maßnahmen zu verdeutlichen. Es können nicht zu jedem Thema alle Initiativen genannt werden, und die Auswahl basiert weitestgehend auf den von den Mitgliedstaaten im Juni 2021 vorgelegten Informationen.

des Rechts auf einen wirksamen Rechtsbehelf darstellt.⁶² Im Jahr 2018 befand das finnische nationale Gericht für Nichtdiskriminierung und Gleichbehandlung, dass die Kreditpunktebewertung auf der Grundlage statistischer Daten zu Geschlecht, Wohnort, Alter und Sprache eher zu Diskriminierung führt als eine individuelle Bewertung.⁶³ In den Niederlanden verwarf ein Gericht im Februar 2020 eine niederländische Rechtsvorschrift, mit der ein System zur Aufdeckung von Betrug eingeführt worden war, und begründete dies mit dem in der Europäischen Konvention zum Schutze der Menschenrechte verankerten Grundrecht auf Achtung des Privatlebens.⁶⁴ Im Rahmen dieses Systems, des sogenannten „System Risk Indication“ (SyRi), wurden von unterschiedlichen Behörden erhobene Daten analysiert, um Personen zu ermitteln, die möglicherweise Sozialleistungsbetrug begehen. Das niederländische Gericht befand, dass der Einsatz von SyRi nicht hinreichend transparent war und der damit verbundene Eingriff in das Recht auf Privatsphäre in keinem angemessenen Verhältnis zum Ziel der Aufdeckung von Betrug stand.

Diese Beispiele zeigen, dass sich die Mitgliedstaaten bereits mit den Herausforderungen auseinandergesetzt haben, die sich aus dem Einsatz von KI mit Blick auf die Grundrechte ergeben. Der von der Kommission vorgeschlagene Ansatz für die Bewältigung der mit KI verbundenen Herausforderungen zielt darauf ab, den wirksamen Schutz der Grundrechte zu verbessern und zugleich Innovationen im Bereich der KI zu fördern.

5.2 Vorschlag der Kommission zur Regulierung von Hochrisiko-KI-Systemen

Im April 2021 legte die Kommission einen Vorschlag für eine Verordnung über KI (Gesetz über KI)⁶⁵ vor. Zentrale Ziele des vorgeschlagenen Gesetzes über KI sind der Schutz der Grundrechte und der Sicherheit sowie die Schaffung eines Binnenmarkts für vertrauenswürdige KI-Systeme. Die vorgeschlagene Verordnung zielt darauf ab sicherzustellen, dass Hochrisiko-KI-Systeme unter Einhaltung der Grundrechte konzipiert und eingesetzt werden und die zuständigen nationalen Behörden und Gerichte mögliche Verstöße gegen die Pflicht zur Wahrung der Grundrechte wirksam untersuchen und dagegen vorgehen können.

Mit dem Vorschlag wird ein risikobasierter Ansatz verfolgt. Bestimmte KI-Systeme sind gänzlich verboten, wie beispielsweise Systeme, die Techniken der unterschweligen Beeinflussung einsetzen oder von den Behörden zur Bewertung des sozialen Verhaltens genutzt werden, weil sie den Werten der EU zuwiderlaufen. Der Einsatz biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken ist ebenfalls verboten, sofern nicht klar definierte Ausnahmen greifen und Schutzvorkehrungen getroffen werden.

Hochrisiko-KI-Systeme müssen einer Reihe von Anforderungen entsprechen und Konformitätsbewertungsverfahren unterzogen werden, bevor sie in Verkehr gebracht oder in Betrieb genommen werden. Diese Anforderungen stellen eine angemessene Dokumentation

⁶² Urteil Nr. 3769 des TAR Lazio – Roma, Kammer III bis, vom 22. März 2017.

⁶³ https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf

⁶⁴ <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>

⁶⁵ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union ([COM\(2021\) 206 final](#)).

und geeignete Tests sowie eine angemessene Datenqualität, Rückverfolgbarkeit, menschliche Aufsicht, Robustheit, Präzision und Cybersicherheit von Hochrisiko-KI-Systemen sicher. Sie kommen zur Anwendung, wenn KI-Systeme in kritischen Bereichen eingesetzt werden, wie beispielsweise zur biometrischen Identifizierung, in Bildung und Beschäftigung, im Zusammenhang mit grundlegenden öffentlichen und privaten Diensten, wie beispielsweise Krediten oder staatlichen Unterstützungsleistungen, bei der Strafverfolgung, in den Bereichen Migration und Grenzkontrolle sowie in der Justiz. KI-Systeme, die als Sicherheitskomponenten bestimmter regulierter Produkte (z. B. Maschinen, medizinische Geräte) eingesetzt werden, unterliegen denselben Anforderungen und müssen geprüft werden, bevor sie in der EU in Verkehr gebracht oder in Betrieb genommen werden.

Mit der vorgeschlagenen Verordnung wird sichergestellt, dass die Nutzer von KI-Systemen, wie beispielsweise Unternehmen, die mit Kunden interagieren, oder Behörden, die Entscheidungen treffen, von den Entwicklern der Systeme geeignete Informationen erhalten, um die zweckmäßige Verwendung der Anwendungen sicherzustellen und die ihnen aus den die Grundrechte betreffenden Rechtsvorschriften erwachsenden Verpflichtungen zu erfüllen.

Führt der Einsatz von KI zur Verletzung von Grundrechten, werden die betroffenen Personen die Möglichkeit haben, wirksame Rechtsmittel einzulegen, da für Transparenz und Rückverfolgbarkeit der KI-Systeme im Verbund mit starken Ex-post-Kontrollen durch die zuständigen Behörden gesorgt ist. Die für die Durchsetzung von Grundrechten zuständigen Aufsichtsbehörden oder Stellen, wie beispielsweise Datenschutzbehörden, Gleichstellungsstellen oder Verbraucherorganisationen, werden Zugang zu der gesamten Dokumentation über Hochrisiko-KI-Systeme haben, die in ihren Zuständigkeitsbereich fallen. Sie werden die Möglichkeit haben, mit Marktüberwachungsbehörden zusammenzuarbeiten, um die betreffenden KI-Systeme gegebenenfalls zu testen.

Bei einigen KI-Systemen wird das Manipulationsrisiko durch die Transparenzpflichten gegenüber den betroffenen Personen gemindert; dies gilt insbesondere für Chatbots (Computerprogramme, die in Online-Chats Fragen beantworten können) oder „Deepfakes“ (künstlich erzeugte oder manipulierte Bild-, Audio- oder Video-Inhalte, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen ähneln und fälschlicherweise als echt oder wahrhaftig erscheinen). Darüber hinaus sollten die betroffenen Personen informiert werden, wenn Emotionserkennungssysteme oder Systeme zur biometrischen Kategorisierung eingesetzt werden, sodass sie die ihnen nach den geltenden Datenschutzbestimmungen zustehenden Rechte durchsetzen können.

Über den Vorschlag wird gegenwärtig im Parlament und im Rat beraten.

5.3 Beispiel für das Zusammenspiel mit sektorspezifischen Rechtsvorschriften: Kreditwürdigkeit und Kreditpunktebewertung

Das vorgeschlagene Gesetz über KI wird mit anderen Rechtsvorschriften zusammenwirken, in denen materiellrechtliche Bestimmungen für den gezielten Einsatz von KI-Systemen in bestimmten Kontexten festgelegt sind. So setzen beispielsweise Kreditgeber im Rahmen der Kreditwürdigkeitsprüfung oder Kreditpunktebewertung oftmals Techniken der automatisierten Entscheidungsfindung ein, darunter auch KI-Systeme. Dabei greifen sie auf unterschiedliche Daten zurück, die ihnen zu einem Großteil nicht von den Verbrauchern zur Verfügung gestellt werden oder diesen unbekannt sind. Dies gibt Anlass zu Bedenken hinsichtlich des Schutzes personenbezogener Daten, der unmittelbaren oder mittelbaren

Diskriminierung⁶⁶ und des Verbraucherschutzes⁶⁷. Die **Richtlinie über Verbraucherkreditverträge**⁶⁸ und die **Richtlinie über Wohnimmobilienkreditverträge für Verbraucher**⁶⁹ beinhalten Bestimmungen zur Kreditwürdigkeitsprüfung. Im Juni 2021 nahm die Kommission einen **neuen Vorschlag für eine Richtlinie über Verbraucherkredite** an, mit der die derzeit geltende Richtlinie über Verbraucherkreditverträge aufgehoben und ersetzt werden soll. Dieser Vorschlag sieht Vorschriften über die Gewährung von Verbraucherkrediten vor, nach denen die Mitgliedstaaten dafür sorgen müssen, dass alle bei der Kreditwürdigkeitsprüfung herangezogenen Verfahren und Informationen dokumentiert werden. Darüber hinaus muss diese Prüfung auf der Grundlage sachdienlicher und genauer Informationen über die finanziellen und wirtschaftlichen Umstände (z. B. Einkommen und Ausgaben) der Verbraucher vorgenommen werden und darf nicht auf Daten beruhen, die beispielsweise den sozialen Medien entnommen wurden. In Übereinstimmung mit den Grundsätzen der Datenschutz-Grundverordnung⁷⁰ werden die Verbraucher zudem das Recht haben, eine Erläuterung des Zustandekommens der Entscheidung über ihre Kreditwürdigkeit zu erhalten, ihren Standpunkt darzulegen und das Eingreifen einer Person zu erwirken. Der neue Vorschlag beinhaltet einen Artikel zum Diskriminierungsverbot, in dem festgelegt ist, dass die für die Gewährung eines Kredits zu erfüllenden Bedingungen Verbraucher, die ihren rechtmäßigen Wohnsitz in der Union haben, nicht aufgrund ihrer Staatsangehörigkeit oder ihres Wohnsitzes oder aus einem der in Artikel 21 der Charta der Grundrechte der Europäischen Union genannten Gründe diskriminieren dürfen. Über den Vorschlag wird gegenwärtig im Parlament und im Rat beraten.

5.4 Kompetenzen

Werden KI-Systeme eingesetzt, müssen die Arbeitskräfte über geeignete Kompetenzen verfügen, um die Achtung der Grundrechte und eine angemessene menschliche Aufsicht zu gewährleisten. Darüber hinaus benötigen die Aufsichtsbehörden Personal mit spezifischen Fachkompetenzen, um ihren Aufgaben wirksam nachkommen zu können. Im September 2020 nahm die Kommission einen **Aktionsplan für digitale Bildung** für den Zeitraum 2021–2027⁷¹ an. Dieser Aktionsplan hat die Förderung der digitalen Kompetenzen unter anderem im Bereich der KI⁷² zum Ziel und sieht die Erarbeitung von Ethik-Leitlinien

⁶⁶ Beispielsweise wies der finnische Datenschutzbeauftragte im April 2019 das Finanzinstitut Svea Ekonomi an, seine Verfahren der Kreditwürdigkeitsprüfung zu berichtigen, und begründete dies damit, dass ein Höchstalter kein akzeptables Kriterium darstelle, da das Alter keinen Aufschluss über die Solvenz oder die Zahlungsbereitschaft gebe.

⁶⁷ Bericht über die Folgenabschätzung zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Verbraucherkredite zur Aufhebung und Ersetzung der Richtlinie 2008/48/EG (COM(2021) 347 final).

⁶⁸ Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (ABl. L 133 vom 22.5.2008, S. 66).

⁶⁹ Richtlinie 2014/17/EU des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Wohnimmobilienkreditverträge für Verbraucher und zur Änderung der Richtlinien 2008/48/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010, Text von Bedeutung für den EWR (ABl. L 60 vom 28.2.2014, S. 34).

⁷⁰ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

⁷¹ [Aktionsplan für digitale Bildung \(2021–2027\) | Allgemeine und berufliche Bildung \(europa.eu\)](#).

⁷² https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8_de

für KI und Daten im Bereich der allgemeinen und beruflichen Bildung vor. Darüber hinaus haben alle Mitgliedstaaten, die nationale KI-Strategien verabschiedet haben, eine die Kompetenzen betreffende Komponente in ihre Strategien aufgenommen, wie beispielsweise Reformen des Bildungssystems zur Förderung des computergestützten Denkens oder Initiativen zur Anpassung des lebenslangen Lernens oder der Umschulungsstrategien.⁷³

6. Überwindung der digitalen Kluft

Der Zugang zum Internet und die einschlägigen Kompetenzen ermöglichen die aktive Teilhabe an der Gesellschaft. Immer mehr grundlegende Tätigkeiten finden im Online-Umfeld statt, von der Arbeitsuche über die Telearbeit, die Teilnahme am Fernunterricht und die Interaktion mit Behörden bis hin zur Vereinbarung von Arztterminen. Aber nicht jeder hat einen Zugang zum Internet. Ein fehlender Zugang zum Internet kann die Bürgerinnen und Bürger bei der Wahrnehmung ihrer Rechte behindern. Beispielsweise können dadurch die Rechte der Bürgerinnen und Bürger in einer demokratischen Gesellschaft beeinträchtigt werden, darunter ihr Recht auf freie Meinungsäußerung und Informationsfreiheit sowie ihr Recht, bei Kommunalwahlen zu kandidieren, da politische Kampagnen zunehmend online durchgeführt werden. Für Menschen, die nicht über die erforderliche Ausstattung oder die notwendigen digitalen Kenntnisse verfügen, wurden diese Schwierigkeiten beim Zugang zu öffentlichen Diensten durch den Ausbruch der COVID-19-Pandemie verschärft, als Ämter geschlossen und die Bürgerinnen und Bürger aufgefordert wurden, mit ihren nationalen Behörden online zu kommunizieren.

Dieses Phänomen wird häufig als „digitale Kluft“ bezeichnet. Noch heute verfügen 46 % der Europäerinnen und Europäer nicht über grundlegende digitale Kompetenzen.⁷⁴ Dem wird in der **Europäischen Säule sozialer Rechte** Rechnung getragen, in der die digitale Kommunikation als eine der essenziellen Dienstleistungen genannt wird, zu denen jede Person Zugang haben sollte, und Unterstützung für Hilfsbedürftige vorgesehen ist.⁷⁵ Bürgerinnen und Bürger, die keinen regelmäßigen Zugang zum Internet haben, nicht über die für die Nutzung dieser Dienstleistungen erforderlichen Kompetenzen verfügen oder aufgrund einer physischen oder kognitiven Behinderung keinen Zugang zu digitalen Produkten oder Dienstleistungen haben, laufen in zunehmendem Maße Gefahr, ausgeschlossen zu werden und bei der Wahrnehmung ihrer Rechte auf Schwierigkeiten zu stoßen.

Sind öffentliche Dienste ausschließlich auf digitalem Wege zugänglich, so sind Personen ohne Internetzugang nicht in der Lage, ihre Rechte wahrzunehmen, oder benötigen diesbezüglich Hilfe. So gibt beispielsweise der *Haut Conseil du Travail*, ein Beratungsgremium des französischen Ministeriums für soziale Angelegenheiten, an, dass in Frankreich schätzungsweise jeder Fünfte Schwierigkeiten bei der Online-Abwicklung von Verwaltungsverfahren hat, und warnt, dass die Digitalisierung den Grundsatz des gleichberechtigten Zugangs zu öffentlichen Diensten gefährden kann, wenn nicht weiterhin

⁷³ https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.

⁷⁴ <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0624> und [Statistik | Eurostat \(europa.eu\)](#).

⁷⁵ [Die Europäische Säule sozialer Rechte in 20 Grundsätzen | Europäische Kommission \(europa.eu\)](#), siehe Grundsatz 20.

alternative Zugangswege angeboten werden.⁷⁶ Da immer mehr wirtschaftliche Aktivitäten eine digitale Komponente aufweisen, ist auch das Recht auf Zugang zu Dienstleistungen von allgemeinem wirtschaftlichen Interesse zunehmend von einem Internetzugang abhängig. Kinder, die zuhause über kein Gerät mit Internetzugang verfügen, haben Schwierigkeiten, am Fernunterricht teilzunehmen; dies beeinträchtigt die Rechte des Kindes und das Recht auf Bildung. Sind darüber hinaus Websites und mobile Anwendungen nicht an die Bedürfnisse von Menschen mit Behinderungen angepasst, so kann sich dies nachteilig auf deren Recht auf Integration auswirken.

Angesichts der Herausforderungen der digitalen Kluft verfolgen die Mitgliedstaaten und die Kommission eine Reihe von Maßnahmen, um sicherzustellen, dass niemand zurückgelassen wird. Wie im **Aktionsplan zur europäischen Säule sozialer Rechte**⁷⁷ angekündigt, wird die Kommission im Jahr 2022 einen Bericht über den Zugang zu essenziellen Dienstleistungen vorlegen, in dem sie sich unter anderem mit dem Zugang zur digitalen Kommunikation befassen und einen Überblick über den aktuellen Stand in den 27 EU-Mitgliedstaaten sowie eine Bestandsaufnahme der auf einzelstaatlicher und Unionsebene eingeführten Maßnahmen und bewährten Verfahren für die Förderung des Zugangs hilfsbedürftiger Menschen vorlegen wird.

6.1 Allgemeine Verringerung der digitalen Kluft

Die Tatsache, dass während der Pandemie zahlreiche Aktivitäten in das Online-Umfeld verlagert wurden, stellt nicht nur eine Herausforderung, sondern auch eine Chance dar. Die Mitgliedstaaten haben Projekte erarbeitet, für die die EU Finanzmittel bereitstellen wird, um die Erholung der Wirtschaft von dem durch die Pandemie verursachten Konjunkturrückgang zu unterstützen. Die im Rahmen dieser Projekte vorgesehenen Maßnahmen betreffen unter anderem die Überwindung der digitalen Kluft, die Schaffung inklusiver digitaler Rechte und die Auseinandersetzung mit der Digitalisierung der Arbeit. Als Beispiele seien hier zwei nationale Pläne genannt. **Rumänien** plant Investitionen in die Erarbeitung von Bildungsinhalten und barrierefreien Ressourcen wie Videos und interaktiven Unterrichtsstunden sowie die Entwicklung barrierefreier Programme zur Förderung der digitalen Kompetenzen von Schülerinnen und Schülern mit Behinderungen. In **Deutschland** werden landesweit Lehrkräfte beim Erwerb digitaler Geräte unterstützt. Darüber hinaus wird eine Plattform für digitales lebenslanges Lernen eingerichtet und besonderes Augenmerk auf die Unterstützung der Bürgerinnen und Bürger mit der geringsten formellen Bildung gerichtet.

Insgesamt gibt es in unterschiedlichen Mitgliedstaaten eine Reihe vielversprechender Initiativen.⁷⁸ Im Februar 2021 wurde in **Belgien** eine öffentliche Aufforderung zur

⁷⁶ https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi_et_comment_les_travailleurs_sociaux_se_saisissent_des_outils_numeriques.pdf, S. 4.

⁷⁷ [Aktionsplan zur europäischen Säule sozialer Rechte \(europa.eu\)](https://european-council.europa.eu/media/e300042c-327c-47e1-9907-010101010101/attachment_data/data/act_plan_en.pdf)

⁷⁸ In diesem Bericht können nicht alle Initiativen genannt werden; die folgende Auswahl dient der Veranschaulichung der unterschiedlichen Maßnahmen. Sie basiert auf den von den Mitgliedstaaten im Juni 2021 vorgelegten Informationen.

Einreichung von Vorschlägen für Projekte zur Unterstützung von durch die COVID-19-Pandemie betroffenen Unternehmerinnen veröffentlicht, unter anderem durch ein Angebot von Orientierungshilfen zur Digitalisierung. Darüber hinaus investiert Belgien in lokale Organisationen, die sich dafür einsetzen, die digitalen Kompetenzen junger Menschen in prekärer wirtschaftlicher Situation auszubauen.

Portugal mobilisiert junge Freiwillige, die Erwachsene über den digitalen Wandel informieren; hierzu wurde ein nationales Netz aus 1500 Schulungszentren aufgebaut und eine Reihe kostenloser Tools und Ressourcen bereitgestellt. Dieses Programm für digitale Inklusion soll 1 Million Menschen erreichen und wird in partnerschaftlicher Zusammenarbeit mit Kommunalbehörden und örtlichen Organisationen durchgeführt.⁷⁹

Ähnlich dem Grundgedanken der WiFi4EU-Initiative⁸⁰ subventioniert **Italien** den Internetzugang bestimmter Bürgerinnen und Bürger und hat das Projekt „Piazza Wifi Italia“⁸¹ ins Leben gerufen, das es mehr als 400 000 Menschen ermöglicht, sich einfach und kostenlos über eine spezielle App in ein gebührenfreies, landesweites WLAN-Netz einzuloggen. Im März 2020 wurde dieses Projekt auf die Gesundheitseinrichtungen, einschließlich der Krankenhäuser, ausgeweitet.

Die digitale Infrastruktur wird aller Voraussicht nach weiterentwickelt und die EU hat in einer Reihe von Bereichen Maßnahmen zur Verbesserung der Vernetzung ergriffen. In der **digitalen Dekade** soll vor allem dafür gesorgt werden, dass jeder europäische Haushalt bis 2025 eine leistungsfähige Internetverbindung und bis 2030 eine Gigabit-Anbindung hat.⁸² Im März 2021 einigten sich die Kommission und die Mitgliedstaaten auf die sogenannte **Connectivity Toolbox** mit Instrumenten zur Förderung des Ausbaus digitaler Netze und des Zugangs zu 5G-Frequenzen. Die für 2022 geplante Überprüfung der Richtlinie über die Senkung der Breitbandkosten zielt darauf ab, den Ausbau digitaler Netze durch die Verringerung der Verwaltungslasten, die Senkung der Kosten und die Beschleunigung des Ausbaus weiter zu fördern. Darüber hinaus wurde in der im Juni 2021 vorgelegten langfristigen **Vision für die ländlichen Gebiete**⁸³ das Ziel festgelegt, die Kluft zwischen Stadt und Land durch die Bereitstellung schneller Internetverbindungen, die Ermöglichung des Zugangs zu 5G (unter anderem mithilfe von Finanzmitteln der EU⁸⁴) und digitalen Technologien sowie die Stärkung der digitalen Kompetenzen zu überwinden. Hochgeschwindigkeits-Breitbandverbindungen sind für den digitalen Wandel und die Erholung nach der COVID-19-Pandemie von entscheidender Bedeutung. Die Kommission hat zugesagt, die Lücken beim Breitbandzugang in ländlichen Gebieten zu schließen, und die

⁷⁹ [Resolução do Conselho de Ministros n.º 30/2020 – DRE.](#)

⁸⁰ <https://digital-strategy.ec.europa.eu/de/activities/wifi4eu>

⁸¹ <https://www.wifi.italia.it/it/>

⁸² Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Digitaler Kompass 2030: der europäische Weg in die digitale Dekade ([COM\(2021\) 118 final](#)).

⁸³ [A long-term vision for the EU's rural areas | Europäische Kommission \(europa.eu\)](#) (Eine langfristige Vision für die ländlichen Gebiete der EU).

⁸⁴ Um die Konnektivitätsziele der EU für das Jahr 2025 zu erreichen, werden Mittel aus dem Europäischen Fonds für regionale Entwicklung, dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums, der Fazilität „Connecting Europe“ – Digitales sowie der Aufbau- und Resilienzfazilität bereitgestellt.

EU wird in Netzwerkinfrastrukturen, einen Standard für die drahtlose Datenübertragung und Glasfaserverbindungen investieren, um sicherzustellen, dass alle Bürgerinnen und Bürger der EU Zugang zu energieeffizienten und zukunftssicheren digitalen Vernetzungsinfrastrukturen haben.

6.2 Öffentliche Verwaltung

Digitale Technologien ermöglichen den Bürgerinnen und Bürgern einen breiteren Zugang zu öffentlichen Diensten und Informationen, die ihnen bei der Bewältigung ihres Alltags und der Wahrnehmung ihrer Rechte, insbesondere der Niederlassungs- und Dienstleistungsfreiheit, helfen können. Seit im Jahr 2009 bei einer Ministerkonferenz in Schweden die **Erklärung von Malmö** unterzeichnet wurde, haben die Mitgliedstaaten kontinuierlich Fortschritte bei der Modernisierung der öffentlichen Verwaltung erzielt.⁸⁵ Mit der **Erklärung von Tallinn** aus dem Jahr 2017 wurde ein Anstoß für die Digitalisierung öffentlicher Dienste für die Bürgerinnen und Bürger sowie grenzüberschreitender öffentlicher Dienste für Unternehmen gegeben.⁸⁶ In der im Dezember 2020 unterzeichneten **Berliner Erklärung** verpflichteten sich die Mitgliedstaaten unter anderem zu Maßnahmen zum Schutz der Grundrechte im Internet⁸⁷, während die **Erklärung von Lissabon** vom Juni 2021 darauf abzielt sicherzustellen, dass „niemand zurückgelassen wird“. Die von den Mitgliedstaaten unternommenen Bemühungen betreffen auch die Digitalisierung der Justiz.⁸⁸

Die Mitgliedstaaten verfolgen unterschiedliche Ansätze, um den Zugang zu öffentlichen Diensten sicherzustellen und somit diese digitale Kluft zu verringern und gleichzeitig den Anforderungen dieses digitalen Zeitalters gerecht zu werden. So hat beispielsweise **Frankreich** beschlossen, unterschiedliche Wege bereitzuhalten, um den Zugang zu öffentlichen Diensten bereitzustellen, mit dem Ziel, dass diese problemlos zugänglich sind. Die Bürgerinnen und Bürger sind nicht verpflichtet, auf elektronischem Wege zu den Behörden Kontakt aufzunehmen. Einen anderen Weg wird in **Dänemark** mit einer Strategie „standardmäßig digital“ verfolgt: Hier ist seit dem Jahr 2014 die Nutzung elektronischer Hilfsmittel für alle Behördenkontakte verpflichtend vorgeschrieben. Um die digitale Kluft zu überwinden, finanziert der Staat Maßnahmen wie etwa eine kostenlose individuelle Unterstützung in Bibliotheken⁸⁹, Hilfe beim Erwerb von Geräten und Zuschüsse zu Internetgebühren. Auch in den **Niederlanden** haben die Regierung und örtliche Bibliotheken die Initiative „Information Point Digital Government“ ins Leben gerufen, in deren Rahmen ausgebildete Mitarbeiterinnen und Mitarbeiter der Bibliotheken Fragen beantworten und Hilfestellung bei den herkömmlichen digitalen öffentlichen Diensten leisten, wie

⁸⁵ <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf>

⁸⁶ <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>

⁸⁷ https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_en

⁸⁸ Die diesbezüglichen Fortschritte werden im Bericht über die Rechtsstaatlichkeit 2021 der Kommission beleuchtet: https://ec.europa.eu/info/sites/default/files/communication_2021_rule_of_law_report_de.pdf.

Siehe auch Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Digitalisierung der Justiz in der Europäischen Union ([COM\(2020\) 710 final](#)) und die begleitende Arbeitsunterlage der Kommissionsdienststellen vom 2. Dezember 2020 ([SWD\(2020\) 540](#)).

⁸⁹ Solche Unterstützungsdienste gibt es auch in anderen Ländern, jedoch genügen die ausgewählten Beispiele, um den Ansatz zu veranschaulichen. Ziel dieses Berichts ist keine erschöpfende Bestandsaufnahme der Maßnahmen, sondern ein Überblick über die Ideen und Ansätze.

beispielsweise im Zusammenhang mit Steuererklärungen und Sozialleistungen, aber auch bei neueren Diensten wie beispielsweise Corona-Apps.

6.3 Gesundheitsversorgung

Infolge der Pandemie wurde die Gesundheitsversorgung zunehmend online erbracht, beispielsweise im Wege virtueller Sprechstunden oder über Apps und Software, die für diagnostische und therapeutische Zwecke entwickelt wurden. Für manche, wie etwa für die Bewohnerinnen und Bewohner ländlicher Gebiete oder kleiner Inseln, wird es durch diese Entwicklung einfacher, ärztliche Hilfe in Anspruch zu nehmen, während sie für andere ein neues Hindernis darstellt. Für Menschen, die keinen Zugang zum Internet haben oder nicht über die erforderlichen Kompetenzen verfügen, können Maßnahmen zur Überwindung der digitalen Kluft eine Verbesserung bewirken. Beispielsweise hat **Polen** den „Internetaccount für Patienten“ eingeführt, ein Online-Tool, über das Patienten auf Informationen über ihre vergangenen, laufenden oder geplanten medizinischen Behandlungen zugreifen und eine Reihe von Vorgängen erledigen können, ohne persönlich eine Gesundheitseinrichtung aufsuchen zu müssen.

6.4 Bildung

Mehrere Mitgliedstaaten haben Strategien und Programme zur Förderung des Zugangs zu Technologien und zur Stärkung der digitalen Kompetenzen im Rahmen der formalen Bildung eingeführt. In **Griechenland** werden beispielsweise Gutscheine für den Kauf von Geräten wie Tablets oder Computern an bedürftige Schülerinnen und Schüler sowie Studierende ausgegeben und einschlägige Bildungsprogramme über die im Jahr 2020 errichtete virtuelle „Akademie für digitale Kompetenzen“ bereitgestellt.

Auf Unionsebene wurde im **Aktionsplan für digitale Bildung**⁹⁰ (2021–2027), der im September 2020 auf den Weg gebracht wurde, eine langfristige strategische Vision für einen nachhaltigen und inklusiven digitalen Wandel in der allgemeinen und beruflichen Bildung formuliert. Darin wird das Recht auf Zugang zu einer hochwertigen digitalen Bildung für alle und auf einen gleichberechtigten Zugang zur Infrastruktur festgelegt, wobei ein besonderer Schwerpunkt auf der Förderung der Teilhabe von Mädchen und Frauen an MINT-Fächern (Mathematik, Informatik, Naturwissenschaften, Technik) liegt.

6.5 Integration von Menschen mit Behinderungen

Dem **europäischen Kodex für die elektronische Kommunikation**⁹¹ zufolge muss gewährleistet werden, dass Endnutzer mit Behinderungen einen gleichwertigen Zugang zu elektronischen Kommunikationsdiensten und diesbezüglich gleichwertige Wahlmöglichkeiten haben, sodass sie an der digitalen Gesellschaft teilhaben können. Mit dem Inkrafttreten des **europäischen Rechtsakts zur Barrierefreiheit**⁹² im Jahr 2025 wird die Integration von Menschen mit Behinderungen und älteren Menschen in die digitale Welt ausgebaut, indem die Zugänglichkeit einer Reihe zentraler Produkte und Diensten sowohl des

⁹⁰ [Aktionsplan für digitale Bildung \(2021–2027\) | Allgemeine und berufliche Bildung \(europa.eu\)](#).

⁹¹ [Richtlinie \(EU\) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation \(Neufassung\)](#) (ABl. L 321 vom 17.12.2018).

⁹² [Richtlinie \(EU\) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen](#) (ABl. L 151 vom 7.6.2019).

privaten als auch des öffentlichen Sektors verbessert wird. Nach der im Jahr 2016 erlassenen **Richtlinie über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen**⁹³ müssen die Mitgliedstaaten sicherstellen, dass Websites und mobile Anwendungen öffentlicher Stellen für Menschen mit Behinderungen, wie beispielsweise Menschen mit eingeschränktem Seh- oder Hörvermögen oder mit motorischen Beeinträchtigungen, zugänglich sind. Diese Verpflichtung stärkt das Recht auf freie Meinungsäußerung und Informationsfreiheit, das Recht auf Bildung, die Berufsfreiheit und das Recht zu arbeiten, das Recht auf Nichtdiskriminierung, die Integration von Menschen mit Behinderungen, den Zugang zu Dienstleistungen von allgemeinem wirtschaftlichen Interesse, das Recht auf Zugang zu Dokumenten, das Recht, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten, die Niederlassungsfreiheit sowie das Recht, Dienstleistungen zu erbringen.

Für die Umsetzung der Richtlinie gibt es unterschiedliche Möglichkeiten. Beispielsweise hat **Slowenien** sein E-Government-Portal modernisiert, sodass es nun von blinden, sehbehinderten, tauben und schwerhörigen Menschen sowie Nutzern mit Legasthenie oder einer kognitiven Beeinträchtigung verwendet werden kann. So werden etwa die textbasierten Beschreibungen der Verfahren durch kurze Videos ergänzt, die auch Verdolmetschungen in Gebärdensprache beinhalten. In **Griechenland** wurden während der Pandemie digitale Schulbücher so angepasst, dass sie nun allen Schülerinnen und Schülern mit Behinderungen unabhängig von deren Form zugänglich sind.

7. Schutz von Menschen, die über Plattformen arbeiten

Es gibt die unterschiedlichsten Arten von Online-Plattformen, darunter Marktplätze, soziale Medien, Plattformen zur Verbreitung von kreativen Inhalten, App-Stores, Websites zum Vergleich von Preisen, Plattformen für die kollaborative Wirtschaft sowie Suchmaschinen. Diese Plattformen erleichtern die Interaktion zwischen Nutzern und Unternehmen. Digitale Arbeitsplattformen stellen eine besondere Form von Plattformen dar und sind mittlerweile charakteristisch für die digitale Wirtschaft.

Die Plattformarbeit eröffnet den Menschen neue wirtschaftliche Chancen, indem sie es ihnen beispielsweise ermöglicht, in Teilzeit zu arbeiten oder allgemein Zugang zum Arbeitsmarkt zu finden. Zugleich bringt sie jedoch auch Grundrechtsprobleme mit sich, die beispielsweise den Schutz personenbezogener Daten, den Schutz der Privatsphäre, das Recht der Arbeitnehmerinnen und Arbeitnehmer auf Unterrichtung und Anhörung, das Recht auf Tarifverhandlungen und Kollektivmaßnahmen sowie das Recht auf gerechte und angemessene Arbeitsbedingungen betreffen. Von den 28 Millionen Menschen, die Schätzungen zufolge über digitale Arbeitsplattformen arbeiten, sind möglicherweise bis zu 5,5 Millionen Scheinselbstständige.⁹⁴ Sie werden in ihren Verträgen mit den Plattformen,

⁹³ [Richtlinie \(EU\) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen](#) (ABl. L 327 vom 2.12.2016).

⁹⁴ Siehe Bericht über die Folgenabschätzung zum Vorschlag für eine Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit ([SWD\(2021\) 396 final](#)).

über die sie arbeiten, zwar als Selbstständige bezeichnet, unterliegen jedoch in Wirklichkeit Weisung und Aufsicht, was für den „Arbeitnehmerstatus“ kennzeichnend ist. Weitere Probleme entstehen im Zusammenhang mit auf Algorithmen basierenden Geschäftsmodellen, da beispielsweise die Menschen, die über Plattformen arbeiten, und ihre Vertreter weder darüber unterrichtet noch dazu angehört werden, wie die Algorithmen eingesetzt werden und sich auf die Bedingungen der Plattformarbeit auswirken. Darüber hinaus sind im Zusammenhang mit dem Einsatz von Algorithmen die verfügbaren Rechtsmittel unzureichend und die Zuständigkeiten unklar.

Plattformarbeit

An Plattformarbeit sind in der Regel drei Parteien beteiligt: die **Plattform**, die **Person, die über die Plattform arbeitet**, und der **Kunde** (Privatpersonen oder Unternehmen). In bestimmten Fällen kann auch eine vierte Partei beteiligt sein, beispielsweise Restaurants, die Speisen liefern.

Digitale Arbeitsplattformen definieren sich selbst für gewöhnlich als Vermittler und bezeichnen die Plattformarbeit als selbstständige Tätigkeit. Die über digitale Arbeitsplattformen erbrachten Tätigkeiten reichen von komplexen Aufgaben wie Computerprogrammierung und Grafikdesign bis hin zu einfachen Aufgaben wie Bildtagging.

Kommissionspräsidentin Ursula von der Leyen hat in ihren politischen Leitlinien auf die Notwendigkeit hingewiesen, die Arbeitsbedingungen der auf Online-Plattformen Beschäftigten zu verbessern.⁹⁵ Diese Notwendigkeit wurde durch die COVID-19-Krise und die beschleunigte Einführung von Plattform-Geschäftsmodellen weiter verdeutlicht. In einer vor Kurzem angenommenen Entschließung des Europäischen Parlaments⁹⁶ wird unterstrichen, dass Plattformarbeit Bedenken in Bezug auf prekäre und schlechte Arbeitsbedingungen, den fehlenden oder erschwerten Zugang zu angemessenem sozialem Schutz, fragmentierte und unvorhersehbare Einkommen sowie einen Mangel an Maßnahmen zur Verbesserung des Gesundheitsschutzes und der Sicherheit am Arbeitsplatz hervorgerufen hat. In der Entschließung werden starke Maßnahmen der EU gefordert, um gegen Fälle falscher Einstufungen des Beschäftigungsstatus vorzugehen und die Transparenz bei der Verwendung von Algorithmen, auch für Arbeitnehmervertreter, zu verbessern.

7.1 Situation und Maßnahmen in den Mitgliedstaaten

Um einen unlauteren Wettbewerb zum Nachteil der Arbeitskräfte und einen „Abwärtswettlauf“ bei Beschäftigungspraktiken und Sozialstandards zu verhindern, hat die EU ein Mindestmaß an Arbeitnehmerrechten festgelegt, die Arbeitskräften in allen Mitgliedstaaten zustehen. Die Rechtsvorschriften der EU in den Bereichen Beschäftigung und Soziales sind über Jahre hinweg entstanden. Darüber hinaus haben die Mitgliedstaaten auf nationaler Ebene unterschiedliche Maßnahmen ergriffen, um den mit der Plattformarbeit verbundenen Herausforderungen zu begegnen. Einige Staaten haben einzelstaatliche

⁹⁵ COM(2021) 762.

⁹⁶ Entschließung des Europäischen Parlaments vom 16. September 2021 zu dem Thema „Gerechte Arbeitsbedingungen, Rechte und soziale Sicherung für auf Online-Plattformen beschäftigte Arbeitnehmer – Neue Beschäftigungsformen im Zusammenhang mit der digitalen Entwicklung“ (2019/2186(INI)).

Rechtsvorschriften verabschiedet, um die Arbeitsbedingungen oder den Zugang zum Sozialschutz im Rahmen der Plattformarbeit zu verbessern. In zahlreichen Mitgliedstaaten haben sich Gerichte in ihren Urteilen mit dem Problem der falschen Einstufung des Beschäftigungsstatus befasst. In einigen Mitgliedstaaten haben Sozialpartner und Plattformunternehmen Tarifverhandlungen geführt.

Im Jahr 2016 wurde in **Frankreich** im Rahmen einer Änderung des Arbeitsgesetzbuches die Vorschrift eingeführt, dass Menschen, die über Plattformen arbeiten, unabhängig von der Branche ihrer Tätigkeit Arbeitnehmer- und soziale Rechte zustehen. Das Gesetz gilt für technisch und wirtschaftlich abhängige Selbstständige. Es gewährt ihnen Zugang zu einer freiwilligen Versicherung gegen Arbeitsunfälle, verpflichtet die Plattformen, Versicherungsprämien zu bezahlen oder den über sie tätigen Arbeitskräften eine Kollektivversicherung anzubieten, und garantiert das Recht auf Sammelklagen sowie auf Fort- und Weiterbildung. Darüber hinaus betonte das höchste für private Arbeitsstreitigkeiten zuständige Gericht (der Kassationsgerichtshof) in zwei Urteilen, dass Personen, die über Plattformen als Kurier oder Fahrer arbeiten, als Arbeitnehmer anerkannt werden müssen, wenn die Plattform ihnen Anweisungen erteilen und diese durchsetzen kann.⁹⁷ Allerdings wird sowohl in dieser als auch in anderen Branchen weiterhin über den tatsächlichen Status von Menschen, die über Plattformen arbeiten, diskutiert.

In der **italienischen** Region Lazio wurde im Jahr 2019 ein Gesetz⁹⁸ verabschiedet, mit dem die Arbeitsbedingungen und der Sozialschutz für alle Plattformbeschäftigten unabhängig von ihrem Beschäftigungsstatus verbessert wurden. Das Gesetz schreibt Schutzvorkehrungen für Arbeitsunfälle, angemessene Sicherheitsschulungen sowie eine Haftpflicht- und Unfallversicherung vor. Darüber hinaus verbietet es eine Bezahlung pro Aufgabe. Des Weiteren wurde in Italien im Jahr 2019 ein nationales Gesetz zur Verbesserung der Arbeitsbedingungen für selbstständige Lebensmittelzusteller verabschiedet.⁹⁹ Zudem verhängte die italienische Datenschutzbehörde im Juli 2021 gegen Deliveroo Italien eine Geldbuße in Höhe von 2,5 Millionen EUR wegen des intransparenten Einsatzes von Algorithmen und der unverhältnismäßigen Erfassung von Arbeitskräftedaten. Die Behörde stellte Verstöße gegen einige Bestimmungen der Datenschutz-Grundverordnung und die nationalen Vorschriften über den Schutz der Privatsphäre, das italienische Arbeitnehmerstatut und das vorstehend genannte Gesetz über den Arbeitnehmerschutz fest.¹⁰⁰

In **Spanien** wurde im Mai 2021 eine Rechtsvorschrift verabschiedet, nach der Menschen, die über Plattformen Lebensmittel und Pakete ausliefern, grundsätzlich als Arbeitnehmer gelten, wobei die Beweislast für den Nachweis des Gegenteils den Plattformen auferlegt wurde.¹⁰¹ Darüber hinaus sind die Plattformen nach diesem Gesetz verpflichtet, den Gewerkschaften Informationen über das algorithmische Management zur Verfügung zu stellen, darunter auch über die digitale Leistungsüberwachung und die automatisierte Zuteilung von Aufträgen.

⁹⁷ Take Eat Easy (28. November 2018, Rechtssache 17-20.079) und Uber (Urteil vom 4. März 2020, Rechtssache 19-13.316).

⁹⁸ Regione Lazio, Legge Regionale 12 aprile 2019, n. 4, [online](#) verfügbar.

⁹⁹ Legge 2 novembre 2019, n. 128, Conversione in legge, con modificazioni, del decreto-legge 3 settembre 2019, n. 101, [online](#) verfügbar.

¹⁰⁰ Entscheidung der italienischen Datenschutzbehörde, [online](#) verfügbar.

¹⁰¹ Königliches Gesetzesdekret 9/2021 vom 11. Mai, [online](#) verfügbar.

Zudem ist in dem Gesetz festgelegt, dass alle Unternehmen (nicht nur Lieferplattformen) ihre Beschäftigten über die Parameter und Regeln unterrichten müssen, auf denen automatisierte Systeme basieren, die Einfluss auf die Arbeitsbedingungen sowie auf die Aufnahme und den Erhalt der Beschäftigung haben.

In **Deutschland** wurden Strategiepapiere zur Zukunft der Arbeit veröffentlicht, in denen die Einbeziehung Selbstständiger, die über Plattformen arbeiten, in Renten- und Versicherungssysteme sowie Verbesserungen ihrer beruflichen Unfallversicherung vorgesehen sind.

Im November 2020 veröffentlichte auch **Portugal** ein Strategiepapier zur Zukunft der Arbeit, das die Einführung einer Rechtsvermutung für den Status von Menschen, die über Plattformen arbeiten, sowie Möglichkeiten für die Verbesserung des Sozialschutzes für Selbstständige und die Förderung der kollektiven Vertretung von Plattformbeschäftigten zum Gegenstand hat. Im Jahr 2018 wurde in Portugal ein Gesetz über die individuelle Personenbeförderung verabschiedet, in dem Obergrenzen für die Arbeitszeiten der Fahrer festgelegt wurden.¹⁰²

7.2 Gemeinsamer Ansatz der EU

Da die Ansätze zur Bewältigung der unterschiedlichen mit der Plattformarbeit verbundenen Probleme auf einzelstaatlicher Ebene erarbeitet werden, besteht die Gefahr einer Fragmentierung der nationalen Gesetzesinitiativen. Die Kommission hat eine Reihe von Problemen im Zusammenhang mit der Plattformarbeit ermittelt und eine zweiphasige Konsultation der europäischen Sozialpartner über die Notwendigkeit einer Initiative zur Plattformarbeit und zu deren möglichen Ausrichtung durchgeführt. Die europäischen Sozialpartner waren sich über die zu bewältigenden Herausforderungen einig, hatten jedoch unterschiedliche Standpunkte in Bezug auf die Notwendigkeit konkreter Maßnahmen auf EU-Ebene. Darüber hinaus stand die Kommission im Austausch mit vielen Interessenträgern; so fanden unter anderem gezielte und bilaterale Treffen mit Plattformunternehmen, Verbänden von Plattformarbeitern, Gewerkschaften, Vertretern der Mitgliedstaaten, Sachverständigen aus Hochschulen und internationalen Organisationen sowie Vertretern der Zivilgesellschaft statt.¹⁰³ Die Kommission hat einen Vorschlag für eine Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit auf Unionsebene vorgelegt, der darauf abzielt, die ordnungsgemäße Feststellung des Beschäftigungsstatus sicherzustellen, die Transparenz bei der Plattformarbeit, einschließlich in grenzüberschreitenden Situationen, zu verbessern und gleichzeitig das nachhaltige Wachstum digitaler Arbeitsplattformen in der EU zu fördern.

8. Überwachung der digitalen Überwachung

Den Grundrechten auf Datenschutz und Privatsphäre kommt im digitalen Zeitalter zentrale Bedeutung zu. Zudem handelt es sich dabei um „befähigende“ Rechte, die den Schutz anderer Grundrechte ermöglichen und stärken, die durch eine staatliche oder private Überwachung beeinträchtigt werden können, wie etwa des Rechts auf Menschenwürde, der

¹⁰² Lei n°45/2018 Regime jurídico da atividade de transporte individual e remunerado de passageiros em veículos descaracterizados a partir de plataforma electrónica, [online](#) verfügbar.

¹⁰³ Siehe Anhang A.3.1 des Berichts über die Folgenabschätzung zum Vorschlag für eine Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit ([SWD\(2021\) 396 final](#)).

Freiheit der Meinungsäußerung, der Gedanken-, Gewissens- und Religionsfreiheit, der Versammlungsfreiheit, des Rechts auf ein unparteiisches Gericht und einen wirksamen Rechtsbehelf sowie des Rechts auf Nichtdiskriminierung. Mit der Datenschutz-Grundverordnung (DSGVO), der Richtlinie zum Datenschutz bei der Strafverfolgung und der Datenschutzrichtlinie für elektronische Kommunikation ist Europa führend beim Schutz der Grundrechte im Internet. Die zunehmende Digitalisierung aller Lebensbereiche birgt Probleme für den Datenschutz sowie für den Schutz des Privat- und Familienlebens. Andere Rechtsvorschriften, wie etwa das Daten-Governance-Gesetz, über das die beiden gesetzgebenden Organe kürzlich eine politische Einigung erzielt haben, sind darauf ausgerichtet, die Entstehung einer starken Datenwirtschaft zu fördern, indem Datenvermittlungsdienste, Datenaltruismus und die Weiterverwendung geschützter öffentlicher Daten im Einklang mit der Datenschutzregelung und deren Einhaltung reguliert werden.

Welcher Zusammenhang besteht zwischen dem Recht auf Privatsphäre und dem Recht auf Datenschutz?

Es handelt sich dabei um eigenständige, in Artikel 7 bzw. 8 der Charta der Grundrechte verankerte Rechte, zwischen denen es jedoch Überschneidungen gibt.

– Das Recht auf Achtung des Privat- und Familienlebens schützt die Bürgerinnen und Bürger vor unrechtmäßigen Eingriffen in ihre Privatsphäre. Es gewährleistet beispielsweise die Vertraulichkeit der zwischenmenschlichen Kommunikation und den Schutz der elektronischen Endgeräte der Nutzer vor unrechtmäßigen Eingriffen.

– Das Recht auf „Datenschutz“ ist nur anwendbar, wenn personenbezogene Daten mithilfe automatisierter Verfahren oder in strukturierter Form manuell verarbeitet werden. Es ist nicht auf Informationen über die Privatsphäre der Bürgerinnen und Bürger beschränkt, sondern erstreckt sich auf alle ihre personenbezogenen Daten, einschließlich der Daten über ihr Berufsleben. Die Transparenz und Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie der Grundsatz, dass diese nach Treu und Glauben zu erfolgen hat, bilden die Grundpfeiler des Datenschutzes. Datenschutz bedeutet auch, dass personenbezogene Daten ausschließlich für festgelegte und eindeutige Zwecke verarbeitet werden und sachlich richtig sowie auf das erforderliche Maß beschränkt sein sollten; darüber hinaus sollten sie sicher und nicht länger aufbewahrt werden als notwendig.

In der Praxis wird der starke Rechtsrahmen der EU kontinuierlich auf die Probe gestellt. Verbraucherorganisationen und zivilgesellschaftliche Organisationen, die sich in erster Linie mit Grundrechten befassen, beklagen eine unzureichende Durchsetzung der Rechtsvorschriften bei Verstößen gegen die DSGVO.¹⁰⁴ In den letzten Jahren haben die EU und die Mitgliedstaaten eine Reihe von Maßnahmen zum Schutz der öffentlichen Sicherheit und zur Bewältigung der Herausforderungen im Sicherheitsbereich unter Einsatz moderner

¹⁰⁴ Z. B. https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf und <https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf>.

Technologien ergriffen. In diesem Zusammenhang zeigen sich zivilgesellschaftliche Organisationen besorgt über die Verhältnismäßigkeit von Überwachungs- und Sicherheitsstrategien, wie beispielsweise die Überwachung der EU-Grenzen¹⁰⁵ oder verabschiedete oder vorgeschlagene Gesetze, die es den Behörden gestatten, private Kommunikation zu Sicherheitszwecken zu überwachen¹⁰⁶. Darüber hinaus äußerten zivilgesellschaftliche Organisationen und Branchenverbände Bedenken über Maßnahmen, die sie als Versuche der Mitgliedstaaten wahrnehmen, die Verschlüsselung zu schwächen.¹⁰⁷

Datenschutzbehörden und nationale Gerichte sorgten für einen wirksamen Rechtsbehelf, wann immer Überwachungsmaßnahmen privater oder öffentlicher Akteure einen Verstoß gegen Grundrechte darstellten. Beispiele hierfür sind i) die Entscheidung der schwedischen Datenschutzbehörde über das Tragen von Körperkameras durch Kontrolleure im Stockholmer öffentlichen Nahverkehr, in der die mangelnde Transparenz und die übermäßige Erhebung von Daten kritisiert wurden und aufgrund derer eine Geldbuße in Höhe von 16,1 Millionen SEK verhängt wurde;¹⁰⁸ ii) die Entscheidung des französischen *Conseil d'Etat* (Staatsrat), nach der die Polizei den Einsatz von Drohnen bei der Überwachung der Einhaltung der Regeln für die räumliche Distanzierung beenden musste, weil diese Drohnen technisch in der Lage waren, Einzelpersonen zu identifizieren, und nicht im Einklang mit dem Datenschutzgesetz eingesetzt wurden.¹⁰⁹

Mit dem Vorschlag für einen Rahmen für eine europäische digitale Identität wird allen Unionsbürgerinnen und -bürgern sowie in der EU ansässigen Personen eine vertrauenswürdige und sichere digitale Brieftasche angeboten, über die die Nutzer die volle Kontrolle haben und die es ihnen ermöglicht, „selbstsouverän“ auf digitale und private Dienste zuzugreifen und eine Vielzahl von Berechtigungsnachweisen und Attributen weiterzugeben.¹¹⁰

8.1 Vorratsspeicherung von Daten

Seit 2014 befand der Gerichtshof der Europäischen Union in mehreren Fällen, dass einzelstaatliche Rechtsvorschriften über die Vorratsspeicherung von Telekommunikations-Metadaten (Verkehrs- und Standortdaten) zu Strafverfolgungs- und nachrichtendienstlichen Zwecken nicht den Anforderungen des Unionsrechts entsprachen. Nach Auffassung des Gerichtshofs stellen die betreffenden einzelstaatlichen Maßnahmen einen schwerwiegenden und unverhältnismäßigen Eingriff in das Recht auf Privatsphäre und Datenschutz dar, da

¹⁰⁵ <https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/>

¹⁰⁶ Siehe z. B. <https://edri.org/wp-content/uploads/2020/10/20201020-EDRI-Open-letter-CSAM-and-encryption-FINAL.pdf> oder <https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/>.

¹⁰⁷ Siehe z. B. <https://www.statewatch.org/news/2020/november/eu-council-set-to-adopt-declaration-against-encryption/> oder https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf?utm_source=dsms-or https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsaterklärung-verschlüsselung_0.pdf

https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsaterklärung-verschlüsselung_0.pdf [auto&utm_medium=email&utm_campaign=Encryption%3A+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption](https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsaterklärung-verschlüsselung_0.pdf)

¹⁰⁸ https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en; <https://www.imy.se/tillsyner/storstockholms-lokaltrafik-sl/>

¹⁰⁹ <https://www.conseil-etat.fr/actualites/actualites/le-conseil-d-etat-ordonne-a-l-etat-de-cesser-immEDIATEMENT-la-surveillance-par-drone-du-respect-des-regles-sanitaires>

¹¹⁰ [COM\(2021\) 281 final](#).

Kommunikations-Metadaten Informationen über zahlreiche Aspekte des Privatlebens der betroffenen Personen offenbaren können.¹¹¹ Der Gerichtshof räumte zwar ein, dass mit Maßnahmen zur Vorratsspeicherung von Daten legitime, im öffentlichen Interesse liegende Zwecke verfolgt werden, stellte jedoch häufig fest, dass das Unionsrecht mit wenigen Ausnahmen¹¹² Rechtsvorschriften entgegensteht, mit denen den Betreibern elektronischer Kommunikationsdienste präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten auferlegt wird. Wie in der **EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025** vom 14. April 2021 angekündigt, wird die Kommission im Einklang mit den Urteilen des Gerichtshofs mögliche Ansätze und Lösungen analysieren und umreißen, die den Erfordernissen der Strafverfolgung und der Justiz in einer Weise entsprechen, die operativ sinnvoll, technisch möglich und rechtlich einwandfrei ist, wobei auch die Grundrechte in vollem Umfang gewahrt bleiben, und die Mitgliedstaaten vor Ende Juni 2021 konsultieren. Die Kommission führt derzeit ein Konsultationsverfahren durch und wird die Ergebnisse dieser Konsultation sorgfältig prüfen, bevor sie über das mögliche weitere Vorgehen entscheidet.

8.2 Verschlüsselung

Verschlüsselung ist für den Schutz der Grundrechte und die Sicherung der Systeme und Transaktionen von entscheidender Bedeutung. Im Unionsrecht ist die Verschlüsselung als eine Maßnahme zur Gewährleistung des Schutzes der Grundrechte vorgesehen, wie beispielsweise des Rechts auf Privatsphäre, des Schutzes personenbezogener Daten¹¹³, der Freiheit der Meinungsäußerung und der Cybersicherheit¹¹⁴. Des Weiteren ist die Verschlüsselung wichtig für den Schutz von Geschäftsgeheimnissen und trägt somit dazu bei, dass die Bürgerinnen und Bürger ihr Recht auf unternehmerische Freiheit wahrnehmen können. Seit dem Ausbruch der COVID-19-Pandemie ist mit dem zunehmenden Einsatz digitaler Instrumente in allen Lebensbereichen auch die Zahl der Cyberangriffe gestiegen. Diese Angriffe verursachten gravierende Schäden sowohl für Unternehmen als auch im Bereich kritischer Dienstleistungen, einschließlich der Gesundheitssysteme; sie stellten eine Gefahr für die Rechte der Bürgerinnen und Bürger dar und machten deutlich, wie wichtig die

¹¹¹ Siehe beispielsweise das Urteil des Gerichtshofs vom 2. März 2021, Prokuratuur, C-746/18, ECLI:EU:C:2021:152.

¹¹² Siehe das Urteil des Gerichtshofs vom 6. Oktober 2020, La Quadrature du Net u. a., verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791, in dem der Gerichtshof die allgemeine Vorratsspeicherung von Verkehrs- und Standortdaten zur Verhütung ernster Bedrohungen der nationalen Sicherheit, der IP-Adressen von Kommunikationsquellen zur Bekämpfung schwerer Straftaten und von die Identität betreffenden Daten zur Bekämpfung der Kriminalität im Allgemeinen für zulässig befand.

¹¹³ Artikel 32 Absatz 1 Buchstabe a, Artikel 34 Absatz 3 Buchstabe a, Artikel 6 Absatz 4 Buchstabe e sowie Erwägungsgrund 83 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; Erwägungsgrund 60 und Artikel 31 Absatz 3 Buchstabe a der Richtlinie zum Datenschutz bei der Strafverfolgung; Erwägungsgrund 20 in Verbindung mit Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG).

¹¹⁴ Artikel 40 Absatz 1 und Erwägungsgrund 96 der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation; Erwägungsgrund 40 der Verordnung (EU) Nr. 2019/881 (Rechtsakt zur Cybersicherheit).

Verschlüsselung für öffentliche und private Akteure ist, weil sie die Vertraulichkeit von Informationen schützt.¹¹⁵

Andererseits können Kriminelle ihre Identität mithilfe der Verschlüsselung verschleiern und die Inhalte ihrer Kommunikation verbergen. Nach entsprechenden Forderungen der Mitgliedstaaten sagte die Kommission zu, ausgewogene technische, operative und rechtliche Lösungen für diese Herausforderungen zu prüfen. Diese Lösungen müssen sowohl die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit bei der Kommunikation als auch eine wirksame Reaktion auf Kriminalität und Terrorismus gewährleisten.¹¹⁶ Die Kommission beabsichtigt, „im Jahr 2022 einen Vorschlag für ein künftiges Vorgehen in Bezug auf den rechtmäßigen und gezielten Zugriff auf verschlüsselte Informationen im Rahmen von strafrechtlichen Ermittlungen und Strafverfolgungen [zu] unterbreiten, der auf einer sorgfältigen Bestandsaufnahme der Art und Weise, wie die Mitgliedstaaten mit Verschlüsselung umgehen, sowie auf einem Prozess mit mehreren Interessenträgern zur Untersuchung und Bewertung der konkreten Optionen (rechtlich, ethisch und technisch) basieren soll“¹¹⁷.

8.3 Biometrische Fernidentifizierung

Die Verarbeitung biometrischer Daten zum Zwecke der eindeutigen Identifizierung natürlicher Personen ist nach den Datenschutzvorschriften der EU grundsätzlich verboten, sofern nicht bestimmte Bedingungen erfüllt sind.¹¹⁸ Die Verarbeitung dieser Daten muss auf einer in den Datenschutzvorschriften vorgesehenen Rechtsgrundlage beruhen. Eine solche Rechtsgrundlage könnte beispielsweise die freiwillige Einwilligung aller betroffenen Personen sein, die in der Praxis jedoch schwer einzuholen ist; alternativ könnte eine Rechtsvorschrift der EU oder eines Mitgliedstaates herangezogen werden, mit der ein wichtiges öffentliches Interesse verfolgt wird, wie beispielsweise die Verhütung einer konkreten und unmittelbaren terroristischen Bedrohung. Im Bereich der Strafverfolgung muss die Verarbeitung durch eine Rechtsvorschrift erlaubt sein. Bei der Verarbeitung biometrischer Daten auf der Grundlage einer Rechtsvorschrift muss die betreffende Rechtsvorschrift in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsehen.

¹¹⁵ Der Europäische Datenschutzausschuss (EDSA) veröffentlichte Leitlinien mit Beispielen für die Meldung von Verstößen gegen Datenschutzvorschriften (Guidelines 1/2021 on Examples regarding Data Breach Notification, Fassung für die öffentliche Konsultation). Verschlüsselung spielt eine wichtige Rolle bei der Eindämmung des Risikos von Verstößen gegen den Schutz personenbezogener Daten.

¹¹⁶ Diese Zusage ist Teil der im Juli 2020 vorgelegten EU-Strategie für eine Sicherheitsunion.

¹¹⁷ Strategie zur Bekämpfung der organisierten Kriminalität, angenommen am 14. April 2021.

¹¹⁸ Siehe Artikel 9 der Datenschutz-Grundverordnung (DSGVO) und Artikel 10 der Richtlinie zum Datenschutz bei der Strafverfolgung. Eine solche Verarbeitung kann nach der DSGVO nur auf Basis einer begrenzten Zahl von Gründen erfolgen, typischerweise aus Gründen eines wichtigen öffentlichen Interesses. In diesem Fall muss die Verarbeitung auf der Grundlage der Rechtsvorschriften der EU oder nationaler Rechtsvorschriften erfolgen, wobei die Anforderungen an die Verhältnismäßigkeit, die Achtung des Wesensgehalts des Rechts auf Datenschutz und geeignete Garantien einzuhalten sind. Gemäß der Richtlinie zum Datenschutz bei der Strafverfolgung muss für eine solche Verarbeitung eine unbedingte Erforderlichkeit vorliegen, sowie ferner im Prinzip eine Genehmigung nach EU-Recht oder nationalem Recht sowie geeignete Garantien.

Zivilgesellschaftliche Organisationen zeigten sich besorgt angesichts der zunehmenden Verwendung biometrischer Fernidentifizierungssysteme in mehreren Mitgliedstaaten und haben ein Verbot ihres Einsatzes gefordert.¹¹⁹ Der Einsatz biometrischer Fernidentifizierungssysteme wurde auch vom Europäischen Datenschutzbeauftragten, vom Europäischen Datenschutzausschuss¹²⁰, in dem die nationalen Datenschutzbehörden vertreten sind, sowie von anderen für Grundrechte zuständigen nationalen Stellen kritisiert, wie beispielsweise von Frankreichs *Defenseur des Droits*¹²¹. In mehreren Fällen wurden Datenschutzbehörden tätig, um den unrechtmäßigen Einsatz dieser Technologie zu unterbinden, beispielsweise in einer französischen Schule, bei der schwedischen Polizei oder in einem niederländischen Supermarkt.¹²²

Über den bestehenden Rahmen hinaus verbietet die von der Kommission im April 2021 vorgeschlagene KI-Verordnung (siehe Kapitel 4) die biometrische Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen und erlaubt diese für Strafverfolgungszwecke in drei konkreten Ausnahmefällen, die bestimmte Schutzvorkehrungen voraussetzen.¹²³

8.4 Bildung

Während der COVID-19-Pandemie kamen in den Einrichtungen der allgemeinen und beruflichen Bildung unterschiedliche Online-Plattformen und -Tools zum Einsatz. Oftmals wurden kommerzielle Anwendungen und Programme für das digitale Lernen als „schnelle Lösungen“ eingeführt, um Schüler und Studierende bei Online-Prüfungen zu überwachen; dies gab Anlass zu der Sorge, dass diese Programme und Anwendungen eher darauf ausgelegt sein könnten, Nutzerdaten zu verwenden, um Gewinne zu erzielen, als darauf, sinnvolle pädagogische Verfahren zu ermöglichen.

Bei der Plattform für digitale Bildung, die im Rahmen des Aktionsplans für digitale Bildung eingerichtet wurde, handelt es sich um ein Forum für die Erarbeitung von Maßnahmen zur Gewährleistung einer engeren sektorübergreifenden Zusammenarbeit zur Förderung des Austauschs zwischen Lehrkräften, zur Entwicklung von Qualitätssicherungsmaßnahmen und

¹¹⁹ <https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/> und <https://reclaimyourface.eu/>.

¹²⁰ https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

¹²¹ <https://www.defenseurdesdroits.fr/fr/communiqu%C3%A9-de-presse/2021/07/technologies-biometriques-la-defenseur-des-droits-appelle-au-respect>

¹²² Niederländische Datenschutzbehörde erlässt förmliche Verwarnung gegen einen Supermarkt wegen des Einsatzes von Gesichtserkennungstechnologie: [Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology | European Data Protection Board \(europa.eu\)](#) (Europäischer Datenschutzausschuss); Schwedische Datenschutzbehörde verhängt Geldbuße gegen die Polizei wegen des Einsatzes von Clearview: [Sweden fines police for illegal facial recognition tech use – POLITICO Pro](#); französische Datenschutzbehörde zum Einsatz biometrischer Erkennung an Schulen: [French privacy watchdog says facial recognition trial in high schools is illegal – POLITICO Pro](#).

¹²³ Gemäß Artikel 5 Absatz 1 Buchstabe d des Vorschlags muss eine solche Verwendung unbedingt erforderlich sein für i) die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern; ii) das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags; oder iii) das Erkennen eines Täters oder Verdächtigen einer Straftat im Sinne des Europäischen Haftbefehls (EuHb), der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Strafe im Höchstmaß von mindestens drei Jahren bedroht ist. Die Nutzung bedarf auch der Genehmigung einer Justizbehörde oder einer anderen unabhängigen Stelle und unterliegt angemessenen Beschränkungen in Bezug auf die zeitliche und geografische Geltung und die abgefragten Datenbanken.

zur Sicherstellung der Achtung des Datenschutzes und der Privatsphäre. Qualitätssicherung und Vertrauen werden dabei eine entscheidende Rolle spielen: Die Qualitätssicherung soll ein gemeinsames Verständnis der wichtigsten Qualitätsstandards für die digitale Bildung fördern, während das Vertrauen die Achtung der wichtigsten Grundsätze in Bezug auf Datennutzung, Ethik und Privatsphäre sicherstellen soll. Diese beiden Elemente können nicht nur das Ausmaß steigern, in dem die europäischen Einrichtungen für die allgemeine und berufliche Bildung digitalfähig sind, sondern auch die Zusammenarbeit stärken und die Qualität der verfügbaren digitalen Lösungen insgesamt verbessern.

8.5 Gesundheit

Bei zahlreichen Maßnahmen, die als **Reaktion auf die COVID-19-Pandemie** ergriffen wurden, werden personenbezogene Daten verarbeitet, darunter auch Gesundheitsdaten, die aufgrund ihrer Sensibilität nach der DSGVO weiteren Vorschriften unterliegen. Die Verarbeitung personenbezogener Daten muss auf das für die Erreichung des betreffenden Ziels erforderliche und verhältnismäßige Maß beschränkt sein und den Anforderungen der DSGVO entsprechen. An diesem Grundsatz orientiert sich der von der EU verfolgte Ansatz. So hat beispielsweise die Kommission für die Mitgliedstaaten Leitlinien¹²⁴ zum Datenschutz bei Mobil-Apps zur Bekämpfung der COVID-19-Pandemie erarbeitet und sie bei der Erarbeitung eines Instrumentariums der für diese Apps geltenden Anforderungen¹²⁵ und der technischen Spezifikationen für die Interoperabilität¹²⁶ zwischen den nationalen Warn-Apps innerhalb der EU unterstützt. Die Kommission hat ein Gateway eingerichtet, über das Warnungen grenzüberschreitend und zwischen den unterschiedlichen Anwendungen der Mitgliedstaaten übermittelt werden können. Des Weiteren hat die Kommission eine Plattform für den Austausch von Daten aus Reiseformularen vorgeschlagen¹²⁷, um die grenzüberschreitende Kontaktnachverfolgung im Verkehrswesen zu unterstützen. Die Kommission hat sich verpflichtet, als nächsten Schritt einen EU-Rechtsrahmen für einen koordinierten Ansatz zur Erfassung der jüngsten Reiseaktivitäten vorzuschlagen, insoweit dies notwendig ist, um der Ausbreitung von COVID-19 Einhalt zu gebieten; dabei soll auf den Erfahrungen mit den Reiseformularen aufgebaut werden.

Darüber hinaus haben das Europäische Parlament und der Rat am 14. Juni 2021 eine Verordnung zur Einrichtung des Systems des digitalen COVID-Zertifikats der EU angenommen, mit dem die Freizügigkeit während der COVID-19-Pandemie erleichtert werden soll.¹²⁸ Eine Infrastruktur für die Unterstützung der Ausstellung und Überprüfung von Impf-, Test- oder Genesungszertifikaten wurde geschaffen, um die Überprüfung der Einhaltung von Maßnahmen im Bereich der öffentlichen Gesundheit bei Reisenden zu vereinfachen (z. B. mit Blick auf Ausnahmen von Quarantänevorschriften). Im Sinne der Benutzerfreundlichkeit sind die Zertifikate sowohl in digitaler als auch in Papierform verfügbar. In jedem Fall sind die Datenkategorien und die Verarbeitung auf das für den gegebenen Zweck erforderliche Maß begrenzt, sodass beispielsweise die Personen, die die Zertifikate prüfen, deren Inhalt nach der Überprüfung nicht speichern dürfen. Darüber hinaus

¹²⁴ [https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020XC0417\(08\)](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020XC0417(08))

¹²⁵ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_de.pdf

¹²⁶ https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

¹²⁷ <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02017D0253-20210726>

¹²⁸ <http://data.europa.eu/eli/reg/2021/953/oj>, ergänzt durch <https://eur-lex.europa.eu/eli/reg/2021/954/oj>.

ist dank des für das digitale COVID-Zertifikat der EU errichteten Vertrauensrahmens sichergestellt, dass die Überprüfung der Zertifikate offline und ohne dass der Emittent oder Dritte über die Überprüfung unterrichtet werden erfolgen kann. Transparenz ist stets von zentraler Bedeutung, um zum einen die Einhaltung der Charta und der geltenden Rechtsvorschriften sicherzustellen und zum anderen Vertrauen zu schaffen und zu pflegen. Das Ergebnis zeigt, dass der Datenschutz in Einklang mit wirksamen Maßnahmen im Bereich der öffentlichen Gesundheit stehen und zur Förderung von deren Akzeptanz beitragen, wenn diese sorgfältig konzipiert sind, und dass sichergestellt ist, dass der EU-Datenschutzrahmen die erforderliche Flexibilität bereitstellt.

Die Kommission erarbeitet gegenwärtig einen Legislativvorschlag zum **europäischen Gesundheitsdatenraum**, der voraussichtlich Anfang 2022 verabschiedet wird. Der europäische Gesundheitsdatenraum soll die Erbringung digitaler Gesundheitsdienste erleichtern, den Zugang zu Gesundheitsdaten für die Zwecke von Forschung und Innovation, Politikgestaltung und Regulierungsmaßnahmen fördern und zugleich die Kontrolle der Bürgerinnen und Bürger über ihre personenbezogenen Daten weiter verbessern. Die Initiative für den europäischen Gesundheitsdatenraum wird den geltenden EU-Datenschutzbestimmungen uneingeschränkt entsprechen.

8.6 Durchsetzung

Die für die Überwachung und Durchsetzung der Vorschriften über den Datenschutz und den Schutz der Privatsphäre zuständigen einzelstaatlichen Aufsichtsbehörden bilden die Eckpfeiler des Governance-Systems für den Datenschutz in der EU. Diese Behörden und die nationalen Gerichte sind für die Überwachung und Durchsetzung der Vorschriften der DSGVO sowie der nationalen Rechtsvorschriften zur Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung¹²⁹ und der Datenschutzrichtlinie für elektronische Kommunikation zuständig. Es ist eine der wichtigsten Zielsetzungen der Kommission, dass die Mitgliedstaaten diese Vorschriften ordnungsgemäß und wirksam anwenden. Die Mitgliedstaaten sind nach dem Unionsrecht verpflichtet, die Unabhängigkeit ihrer Datenschutzbehörden sicherzustellen und diese mit den für die Wahrnehmung ihrer Aufsichtsaufgaben erforderlichen Ressourcen auszustatten.¹³⁰ Die Kommission verfolgt die Entwicklungen im Hinblick auf die Unabhängigkeit sowie die Aufgaben, Befugnisse und Ressourcen der Aufsichtsbehörden und leitet im Falle der Nichteinhaltung der Unionsvorschriften durch die Mitgliedstaaten Vertragsverletzungsverfahren ein, um die wirksame Durchsetzung dieser Vorschriften sicherzustellen.

Die Datenschutzbehörden arbeiten im Europäischen Datenschutzausschuss (EDSA) zusammen, um für eine einheitliche Durchsetzung der DSGVO insbesondere in grenzüberschreitenden Fällen zu sorgen. Drei Jahre nach dem Inkrafttreten der DSGVO

¹²⁹ <http://data.europa.eu/eli/dir/2016/680/2016-05-04>

¹³⁰ Europäischer Datenschutzausschuss: Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities, 5. August 2021, veröffentlicht am 11. August unter https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf (Überblick über die von Mitgliedstaaten den Datenschutzbehörden verfügbar gemachten Ressourcen und über Durchsetzungsmaßnahmen der Datenschutzbehörden).

wurde Kritik an der Wirksamkeit dieser Zusammenarbeit laut¹³¹, und der EDSA wird sich diesbezüglich weiter um Verbesserungen bemühen.¹³² Die Kommission teilt die Auffassung des Rates¹³³, des Europäischen Parlaments und des EDSA¹³⁴, dass der Schwerpunkt nun auf der Verbesserung der Umsetzung der EU-Datenschutzvorschriften sowie auf Maßnahmen zur Stärkung ihrer Durchsetzung liegen muss.

8.7 Datenschutz außerhalb der EU

Ein wesentlicher Aspekt des Schutzes der Grundrechte in einer Online-Umgebung besteht darin, dass die Personen auch nach einer Übertragung ihrer Daten außerhalb der EU und des EWR fortgesetzt geschützt bleiben. Da personenbezogene Daten in der heutigen vernetzten Welt problemlos über Grenzen hinweg bewegt werden können und der Datenverkehr zu einem integralen Bestandteil des Handels, der Zusammenarbeit in Regulierungsfragen und sogar der sozialen Interaktion geworden sind, wären die durch die DSGVO und die Richtlinie zum Datenschutz bei der Strafverfolgung garantierten Schutzmaßnahmen unwirksam, wenn sie auf die Verarbeitung innerhalb der EU beschränkt wären.

Angesichts dessen verfolgte die Kommission weiterhin ihre ehrgeizige Agenda, die darauf abzielt, ein hohes Schutzniveau zu gewährleisten, wenn Daten der europäischen Bürgerinnen und Bürger in Drittländer übertragen werden, und zugleich den Datenverkehr zu erleichtern. In diesem Zusammenhang einigte sie sich mit wichtigen Partnern auf eine „Angemessenheitsfeststellung“, mit der erklärt wird, dass ein Drittland ein Datenschutzniveau gewährleistet, das dem in der EU garantierten Niveau „der Sache nach gleichwertig“ ist. Dies führte zu wichtigen Ergebnissen, wie beispielsweise zur Annahme von zwei Angemessenheitsbeschlüssen für das Vereinigte Königreich (nach der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung) und zum Abschluss der Angemessenheitsgespräche mit Südkorea.

Darüber hinaus haben die EU und die USA nach der Ungültigerklärung der früheren Angemessenheitsfeststellung zum Datenschutzschild durch den Gerichtshof die Verhandlungen über einen neuen EU-US-Datenschutzrahmen für transatlantische Datenübermittlungen intensiviert, der die vollständige Einhaltung des Urteils des Gerichtshofs sicherstellt.

Zudem nahm die Kommission im Juni 2020 modernisierte Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer an, die den neuen Anforderungen nach der DSGVO Rechnung tragen und an die Bedürfnisse der modernen digitalen Wirtschaft angepasst wurden. Dabei handelt es sich um Musterdatenschutzklauseln, die Datenexporteure und Datenimporteure – auf freiwilliger Basis – in ihre vertraglichen Vereinbarungen (beispielsweise in Dienstleistungsverträge, in deren Rahmen die Übertragung personenbezogener Daten erforderlich ist) aufnehmen können, mit denen angemessene Vorkehrungen für den Datenschutz getroffen werden.

¹³¹ Siehe z. B. die Entschließung des Europäischen Parlaments (2020/2717(RSP)).

¹³² Strategie des EDSA für die Jahre 2021–2023, angenommen am 15. Dezember 2020, verfügbar unter [edpb_strategy2021-2023_de.pdf \(europa.eu\)](https://ec.europa.eu/edpb_strategy2021-2023_de.pdf).

¹³³ Standpunkt und Feststellungen des Rates zur Anwendung der Datenschutz-Grundverordnung (DSGVO) – Annahme, 14994/1/19 REV 1, 19. Dezember 2019, verfügbar unter [pdf \(europa.eu\)](https://ec.europa.eu/edpb_strategy2021-2023_de.pdf).

¹³⁴EDPB Annual Report 2020, 2. Juni 2021, verfügbar unter [EDPB Annual Report 2020 | European Data Protection Board \(europa.eu\)](https://edpb.europa.eu/annual-report/2020) (Jahresbericht 2020 des Europäischen Datenschutzausschusses).

Des Weiteren beteiligt sich die Kommission weiterhin an einer Initiative für den „vertrauensvollen, freien Datenverkehr“, die im Jahr 2019 von Japan vorgeschlagen und später von den G20 und den G7 gebilligt wurde. Ein zentrales Element dieses Ansatzes, der gegenwärtig bei der OECD unter aktiver Beteiligung der EU und ihrer Mitgliedstaaten erörtert wird, besteht darin, eine Grenze zwischen dem rechtmäßigen Datenzugriff der Behörden mit geeigneten Einschränkungen und Garantien einerseits und missbräuchlicher staatlicher Überwachung andererseits zu ziehen.

9. Mit vereinten Kräften: das digitale Zeitalter als Chance für die Grundrechte

Angesichts der miteinander verflochtenen Herausforderungen und der diesbezüglichen Maßnahmen, die in diesem Bericht untersucht wurden, steht außer Zweifel, dass sich die EU und ihre Mitgliedstaaten für den Schutz und die Förderung der Grundrechte im digitalen Zeitalter einsetzen und gemeinsam daran arbeiten, die hierfür am besten geeigneten Wege zu ermitteln. Die in den vorstehenden Kapiteln beleuchteten Beispiele zeigen nur einige der vielen Möglichkeiten auf, voneinander zu lernen und die mit dem digitalen Wandel verbundenen Veränderungen positiv zu gestalten.

Die Kommission bedient sich zahlreicher Instrumente, um die Achtung der in der Charta verankerten Rechte zu gewährleisten – sowohl im Rahmen ihrer legislativen und politischen Initiativen als auch bei der Durchsetzung des Unionsrechts. Insbesondere wird die Kommission die Auswirkungen ihrer im Jahr 2022 anstehenden Initiativen auf die Grundrechte sorgfältig prüfen und ist bestrebt, diese Auswirkungen in das richtige Verhältnis zu bringen, beispielsweise in Legislativvorschlägen zu folgenden Themen:

- Recht auf Reparatur,
- Cyberabwehrfähigkeit,
- digitale Mobilitätsdienste,
- Sofortzahlungen,
- gegenseitiger Zugang zu sicherheitsrelevanten Informationen für vor Ort tätige Beamte der EU und wichtige Drittländer,
- ein Rechtsakt über die Medienfreiheit und
- verbindliche Standards für Gleichstellungsstellen.

Darüber hinaus wird die Kommission im Rahmen der digitalen Dekade den Vorschlag machen, dass eine Reihe digitaler Grundsätze und Rechte in eine interinstitutionelle feierliche Erklärung der Europäischen Kommission, des Europäischen Parlaments und des Rates aufgenommen werden. Diese Erklärung wird Informationen für Nutzer und Orientierung für politische Entscheidungsträger und Betreiber digitaler Dienste in Bezug auf den europäischen Weg hin zum digitalen Wandel bieten.

Die Kommission fordert das Europäische Parlament, den Rat und die Mitgliedstaaten auf, diesen jährlichen Bericht über die Anwendung der Charta der Grundrechte für ihren Austausch über die Herausforderungen und Chancen für den Schutz der Grundrechte im

digitalen Zeitalter heranzuziehen. Sie begrüßt die Zusage des Rates für einen Gedankenaustausch auf der Grundlage der Berichte der Kommission¹³⁵ und würde auch eine Erörterung im Europäischen Parlament befürworten. Ein solcher Austausch könnte hilfreich sein, um die anstehenden Herausforderungen besser zu bewältigen, insbesondere mit Blick auf die Bekämpfung von Hassreden und Desinformation, die Gewährleistung von Kontrolle und Gegenkontrolle bei Überwachungsmaßnahmen und insgesamt die wirksame Durchsetzung der Rechtsvorschriften zum Schutz der Grundrechte im digitalen Umfeld. Darüber hinaus kann er zu einer konstruktiven und sinnvollen Gestaltung politischer Entwicklungen beitragen.

Diese gemeinsamen Bemühungen um die Wirksamkeit der Charta im digitalen Zeitalter, der Europäische Aktionsplan für Demokratie¹³⁶ sowie der europäische Mechanismus zur Wahrung der Rechtsstaatlichkeit¹³⁷ sind Belege für die Entschlossenheit der EU, ihre Grundwerte zu fördern und zu schützen.

¹³⁵ [Schlussfolgerungen des Rates](#) zu einer verstärkten Anwendung der Grundrechtecharta in der Europäischen Union, 8. März 2021, Rn. 26.

¹³⁶ Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Europäischer Aktionsplan für Demokratie ([COM\(2020\) 790](#)).

¹³⁷ https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism_de