Council of the
European Union

Brussels, 10 December 2021
(OR. en)

14910/21

JAI 1401
FREMP 296

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	10 December 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2021) 819 final
Subject:	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Protecting Fundamental Rights in the Digital Age - 2021 Annual Report on the Application of the EU Charter of Fundamental Rights

Delegations will find attached document COM(2021) 819 final.

Encl.: COM(2021) 819 final

EUROPEAN
COMMISSION

Brussels, 10.12.2021
COM(2021) 819 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Protecting Fundamental Rights in the Digital Age -

2021 Annual Report on the Application of the EU Charter of Fundamental Rights

Protecting Fundamental Rights in the Digital Age –

2021 Annual Report on the Application of the EU Charter of Fundamental Rights

Contents

1. Introduction

The EU Charter of Fundamental Rights[1] is a powerful tool used to protect, promote and further strengthen peoples' rights in the European Union. Fundamental rights do not only protect people from undue interferences such as censorship or mass surveillance, they also empower people to make full use of their rights and opportunities in life. It is always possible to improve the conditions and the extent to which people can enjoy their rights. The Charter can guide policy activities across the EU. The more people know about the rights guaranteed in the Charter and how to rely on them, the more powerful they become.

The COVID-19 pandemic has put the protection and guarantees of our fundamental rights and freedoms to the test. Any restrictions to fundamental rights must be necessary and proportionate. This is required by the EU Charter of Fundamental Rights, which is binding EU law. It protects and promotes a broad range of rights linked to human dignity, freedom, equality and solidarity, and all national courts can apply it in cases where EU law is implemented and relevant for the final judgment.

Since 2009, the Charter has had the same legal status as the Treaties, the primary EU law on which EU legislation is based. European institutions must comply with it in all their actions, and EU Member States must comply with it when they implement EU law.

When do Member States need to comply with the Charter?

- When Member States agree in the Council and with the European Parliament to adopt new EU legislation, it is often necessary to give effect to such legislation by national measures implementing that legislation.

- When Member States adopt or change laws on a matter where EU law imposes concrete obligations, their laws may not contravene EU law, including the Charter, because such legislative action would constitute implementation of EU law.

- EU funding programmes are enshrined in EU legislation. Member States must ensure that this money is spent according to the rules in that legislation. When they implement funding programmes, they are implementing EU law.

- Where Member States adopt or change laws in a field where the EU has no competence and where no EU law exists, they are not implementing EU law. In such cases, they are not bound by the Charter. However, many fundamental rights enshrined in the Charter are at the same time set out in national constitutions and case-law as well as in the European Convention on Human Rights to which all EU Member States are signatories.

To increase everyone's knowledge of the Charter, the European Commission has been publishing reports on its application since 2010. This edition is the first to follow a new approach announced in the **Strategy to strengthen the application of the Charter of Fundamental Rights in the EU** (the Charter Strategy)[2]. The annual report will focus on a specific topic governed by EU law and it will look more closely at best practices and challenges in the Member States in this area. This allows systemic developments to be

[1] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.
[2] Commission communication 'Strategy to strengthen the application of the Charter of Fundamental Rights in the EU', COM(2020)711.

explored, to illustrate how different rights can strengthen each other, and how political, societal and economic developments can affect a number of rights at the same time.

The topic of the 2021 edition is the **protection of fundamental rights in the digital age**, in line with the European Commission's strategic focus on the digital transition.

What information is this report based on?

This report has been prepared based on:

- contributions from EU Member States, who were invited to provide insights from their respective national perspectives[3];

- a targeted consultation with umbrella organisations of European civil society organisations (CSOs) working in the area of fundamental rights; and

- reports from EU agencies, in particular the annual reports on fundamental rights from the European Union Agency for Fundamental Rights (FRA)[4], which contain a section on fundamental rights and digitalisation.

2. Implementing the new strategy to strengthen the application of the Charter of Fundamental Rights in the EU

The Charter Strategy, adopted by the Commission in 2020, aims at ensuring that the Charter is applied to its full potential, making fundamental rights a reality for all. The Charter Strategy sets the frame for joint work on fundamental rights throughout the EU for the following 10 years and is fully supported by the Member States[5]. The four priorities that guide the implementation of the goals set out in the Charter Strategy are explained below.

2.1 Supporting and monitoring the effective application of the Charter in the Member States

National and local administrations, parliaments and law enforcement authorities are central to promoting and protecting rights under the Charter and creating an enabling environment for civil society organisations and rights defenders. The Commission is working closely with Member States to help them implement EU law and policies effectively, and in full compliance with the Charter.

The Commission is also helping Member States implement **EU funded programmes** in compliance with the Charter. The Common Provisions Regulation[6] sets out the rules that

[3] Member States provided their contributions in the framework of the Council Working Party on Fundamental Rights, Citizens Rights and Free Movement of Persons (FREMP).
[4] https://fra.europa.eu/en/publication/2021/fundamental-rights-report-2021
[5] https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/en/pdf
[6] Regulation (EU) 2021/1060 of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy, OJ L 231, 30.6.2021, p. 159.

must be observed in the use of several EU funds[7]. It requires Member States to set up and use effective mechanisms to ensure the compliance of EU-funded programmes with the Charter, such as reporting arrangements to the monitoring committee regarding cases of complaints concerning the Charter or non-compliance with the Charter of operations supported by the Funds. The Commission will continue to provide technical assistance to help Member States to ensure that programmes supported by EU funds are designed and implemented in a Charter compliant manner.

Under one specific funding scheme, the Citizens Equality Rights and Values (CERV) programme, the Commission created new **opportunities for national, regional, and local authorities** to receive funding for projects that promote a culture of values and strengthen awareness of the Charter[8]. Cities play an important role in promoting such a culture and protecting fundamental rights. A number of cities have joined a network of 'human rights cities' and embed fundamental rights in their policymaking[9]. FRA launched a report entitled 'Human Rights in the EU: a framework for reinforcing rights locally' at its Fundamental Rights Forum in October 2021[10]. The framework includes tools to help mayors, local governments and administrations, and grassroots organisations integrate human rights standards into their work. As a follow-up to the EU anti-racism action plan 2020-2025[11], the Commission launched a 'European capital(s) of inclusion and diversity Award' in November 2021[12]. It will confer awards for best practices that can be a source of inspiration for other European towns, cities and regions in creating more diverse and inclusive environments for their inhabitants.

In the Charter Strategy the Commission invited the Member States to nominate a **Charter focal point** to further facilitate cooperation and the exchange of information on applying the Charter. To date, 17 Member States have nominated such a Charter focal point. Their role is instrumental in disseminating information and best practice on the awareness of the Charter and coordinating capacity building efforts in the country. Their work contributes to the new page on Member States' best practices on the Charter launched on the European e-Justice Portal in December 2021[13].

As Guardian of the Treaties, the Commission has taken concrete steps towards ensuring the respect of the rights enshrined in the Charter in cases where national legislation or practices implementing EU law breach those rights, for example by launching infringement proceedings. In particular, the Commission acted to ensure respect for:

[7] For the 2021-2027 period: the European Regional Development Fund, the Cohesion Fund, the European Social Fund Plus, the Just Transition Fund, the European Maritime and Fisheries Fund, the Asylum and Migration Fund, the Internal Security Fund and the Border Management and Visa Instrument.

[8] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv. Under the Call for proposals for town-twinning and networks of towns, the CERV programme makes 4,2 million euro available in 2021. More information is available here: Funding & tenders (europa.eu).

[9] https://humanrightscities.net/

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

[11] Commission communication 'A Union of equality - EU anti-racism action plan 2020-2025', COM(2020) 565 final.

[12] https://eudiversity2022.eu/the-award/apply/

[13] https://e-justice.europa.eu/37134/EN/member_states_best_practices_on_the_charter.

- the freedom of association of non-governmental organisations and the rights to protect their donors' personal data;
- academic freedom;
- freedom of expression and media pluralism;
- human dignity;
- the right to respect for private life;
- the right of everybody, including LGBTIQ people, not to be discriminated on grounds of sex and sexual orientation.

The Commission has been monitoring in all Member States the emergency measures taken during the COVID-19 pandemic and their impact especially on the rule of law, on fundamental rights, and on compliance with other provisions of EU law, as reflected in the **2021 Rule of Law Report** and country chapters[14].

2.2 Empowering civil society organisations, rights defenders and justice practitioners

Civil society organisations (CSOs) and independent national human rights bodies are key partners for the EU institutions and for the Member States in promoting and protecting fundamental rights, democracy and the rule of law. They are instrumental in raising people's awareness about their rights and helping them receive effective judicial protection. These organisations must be able to work in a supportive environment, free from undue regulatory constraints, obstacles to financing or even smear campaigns[15], and they also need to be able to build their capacities. Some Member States still do not have fully functioning **national human rights institutions**, which are important links between government and civil society[16]. Member States are invited to establish such institutions and to ensure that they have the means to work in full independence.

The Commission is closely **monitoring the situation of CSOs** and it reports about developments related to the framework for civil society in its annual Rule of Law Report. The 2021 Rule of Law Report states that CSOs were affected by the COVID-19 pandemic, not only due to the limits on the freedom of movement and assembly, but also in terms of funding. According to the Report, civil society has generally had limited involvement in designing and implementing COVID-19 measures[17]. The 2020 Rule of Law Report identified measures that restricted the freedom of expression of CSOs[18]. Data collected by FRA[19] shows indeed that many CSOs consider that national pandemic measures had a negative impact on

[14] COM(2021) 700 final, available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report_en.
[15] FRA, Protecting the civic space, 2021, https://fra.europa.eu/en/publication/2021/civic-space-challenges.
[16] See Charter strategy, op.cit., section 2 'Empowering civil society organisations, rights defenders and justice practitioners'. See report from FRA 'Strong and effective national human rights institutions – challenges, promising practices and opportunities', available at: https://fra.europa.eu/en/publication/2020/strong-effective-nhris. The 2021 Rule of Law Report country chapters report on the status of accreditation of national human rights institutions: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report/2021-rule-law-report-communication-and-country-chapters_en.
[17] 2021 Rule of Law Report, p. 24.
[18] 2020 Rule of Law Report, p. 16. EUR-Lex - 52020SC0316 - EN - EUR-Lex (europa.eu)
[19] https://fra.europa.eu/en/news/2021/findings-fra-consultation-covid-19-impact-civil-society; FRA, Protecting the civic space, op. cit., see section 1.3. 'COVID-19 exacerbates challenges faced by civil society', p. 16.

their activities since March 2020. While they reported increasing demand, a majority faced difficulties in being able to continue providing their services. Practical challenges include cancellation of activities, psychological impact on staff and reduced work contribution by volunteers.

The Commission further **supports rights defenders and CSOs** through dedicated funding, such as a call for proposals on protecting and promoting EU values, which is aimed entirely at small and grassroots CSOs and disburses EUR 51 million over 2021-22[20]. A specific call worth EUR 2 million has been launched to support litigation and capacity building linked to the application of the Charter[21].

The Commission is also promoting capacity building and **awareness on the Charter for judges and other justice practitioners**. In December 2020, the Commission adopted a new European judicial training strategy for 2021-2024[22], and in March 2021, the Commission launched a call for proposals to support projects on judicial training including fundamental rights as one of its key priorities[23]. Several judicial training projects on the Charter, co-funded by the Commission under its 2014-2020 Justice Programme were implemented[24]. Judicial training material on fundamental rights is available for justice professionals on a platform launched in December 2020[25].

2.3 Making full use of the Charter of Fundamental Rights in EU decision-making

EU institutions, bodies, offices and agencies must comply with the Charter in all their action. The Commission is boosting its internal capacity on Charter compliance and is updating its Better Regulation Toolbox[26] including the 2011 guidance on taking account of fundamental rights in impact assessments[27]. It is also developing specific training on the Charter and an e-learning tool to help staff assess the impact of the Commission's policies and legislative proposals on fundamental rights. The e-learning tool will be made publicly available and could be a useful resource, together with the updated Better Regulation Toolbox and guidance, for other EU institutions and for law and policymakers in the Member States. The Commission stands ready to support the European Parliament and the Council to ensure that they apply the Charter effectively in their work.

2.4 Strengthening people's awareness

Along with adopting this report, the Commission is launching an awareness-raising campaign on the Charter to inform people about their rights and where to turn to if their rights are breached. The campaign will be carried out online, through media events and social media, using the hashtag **#RightHereRightNow**. It will focus on a number of specific rights, such as

[20] CERV work programme 2021-22.
[21] Call for proposals to promote capacity building and awareness on the EU Charter of Fundamental Rights.
[22] COM(2020) 713 final.
[23] Justice programme, JUST-2021-JTRA call for proposals, available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home
[24] E.g. https://era-comm.eu/charter-of-fundamental-rights/seminar-materials/; http://charterclick.ittig.cnr.it:3000/; http://help.elearning.ext.coe.int/
[25] The European Training Platform.
[26] Better regulation toolbox | European Commission (europa.eu)
[27] Operational guidance on taking account of fundamental rights in European Commission impact assessments | European Commission (europa.eu)

non-discrimination and equality, rights of the child, freedom of expression and information, and effective remedy and fair trial. Key partners will be involved in raising awareness such as CSOs, national human rights institutions and bodies, FRA and other EU bodies and agencies. Links will be made to other information campaigns on rights and with the Conference on the Future of Europe. The Commission has also translated its webpage on the Charter on the Europa website in all official EU languages[28] and launched a new version of the European e-Justice Portal, which contains information on the application of the Charter and where to get help[29].

3. Making the Charter the EU's compass for the digital age

The European Commission has made it a priority to shape the digital transition in a way that benefits everyone and leaves no one behind. What was once described as the 'offline world' and the 'online world' is today becoming indistinguishable. This brings about a number of challenges to ensure that fundamental rights are respected in a rapidly changing digital environment.

Digital technology is increasingly permeating all areas of our society and can be used in many different and often beneficial ways. Digital solutions advance scientific research, increase industrial production, facilitate the sustainability transition, facilitate a variety of services, and are today the main channel for private and public communication. They increase people's possibilities to participate in democratic discourse and to inform themselves on any topic. Artificial intelligence systems, in particular, can serve to foster innovation and wealth and can be used as tools by individuals in all areas of life, for example in healthcare, for translations or to support decision-making. Digital automation helps organise work in a more efficient way and allows for unprecedented levels of coordination. The collection of data on human actions and their effects helps people understand and shape the world.

At the same time, certain uses of technology risk limiting the effectiveness of the protection guaranteed by fundamental rights. The spread of illegal content such as hate speech and child sexual abuse threaten the right to dignity of the victim, and the spread of disinformation challenges the democratic discourse and our right to access to information. Where processes or even decisions are automated, it can be difficult to ensure transparency and accountability for the outcomes, for example when complex software is used to decide on the allocation of work. Where information is lacking or hard to obtain, it can be difficult to assess and address breaches of fundamental rights.

The more an automated tool relies on external factors, such as data, input from people or other systems to produce an outcome, the more difficult it is to ensure that such a tool does not violate rights from the outset, for example because of certain inbuilt biases that may ultimately impact decision-making in work contexts. The more data are captured about people, the easier it is to monitor them and impinge on their privacy. Network effects may reduce the power of individuals vis-à-vis big organisations, for example in online marketplaces or labour platforms, where individuals have little bargaining power or

[28] Your rights in the EU | European Commission (europa.eu).
[29] https://e-justice.europa.eu/581/EN/fundamental_rights

possibilities to organise. At the same time, social media platforms are also used to spread hate and disseminate illegal content, for instance when they spread illegal hate speech, child sexual abuse material or terrorist content. Furthermore, much work is still needed to help everyone benefit from new and useful tools where internet access, equipment or knowledge on how to use these tools are scarce.

These challenges can occur individually or combined, depending on the context. They can reinforce each other and can affect several fundamental rights at once, which needs to be taken into account when addressing these challenges. This report presents some of the key aspects where challenges to fundamental rights arise due to the use of digital technology. It shows which rights are affected in these contexts, how the situation in the EU Member States is developing, and how the Member States and the European Commission use the Charter to overcome the different challenges and safeguard and promote people's rights.

4. Tackling the challenges of online content moderation

Online intermediaries such as social media platforms play an important role in the life of every individual and foster new forms of interactions between individuals, public administrations and businesses. Their use has led to a significant increase in the information that is available to people and provides greater opportunities for people to exercise their right to freedom of expression and to access information, also creating multiple spaces for online activism and assembly of individuals and civil society.

Large platforms – the new town square

- Some online platforms have become so important in facilitating the exchange of information that they play a major role in the democratic debate.
- With over half of the population in the EU using social media, reaching nearly 90% for those aged 16-24, the effects of the design and standards on these platforms have a wide reaching societal impact[30].
- The tools and mechanisms these platforms use to moderate content and encourage people to spend as much time as possible using their service play a major role in shaping the information and the opinions people encounter online.
- Tackling illegal content on these large platforms is challenging because they have become public spaces for exchange of information without being legally responsible for considerations of public interest.

At the same time, the use of online platforms is amplifying societal problems like polarization[31] or the dissemination of illegal content, often with significantly negative effects on fundamental rights, such as the protection of the rights of the child, consumer protection, the freedom to receive and impart information, and the protection of intellectual property.

[30] https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i

[31] See examples of emerging systemic societal risks posed by online platforms in the impact assessment accompanying the proposal for a regulation on a Single Market For Digital Services (Digital Services Act), SWD(2020) 348 final, p 40 ('DSA impact assessment').

The scale and speed of the spread of online content that is not in itself illegal, such as disinformation and conspiracy theories, may affect the democratic discourse, trust in institutions and, as seen in the wake of the COVID-19 pandemic, health, safety and equal treatment.

Democracy in the EU faces many challenges, including populism, an increasingly polarised political debate and the erosion of public trust in democratic processes caused by disinformation[32]. These phenomena are exacerbated by coordinated interference in elections by third countries or private interests, dissemination of disinformation and a lack of transparency and accountability of targeted political ads. Concerns are also voiced about certain groups not being sufficiently included or engaged with, such as young or older people or persons with disabilities. Ethnic minorities, including Roma communities, LGBTIQ people and women hesitate to a varying degree and depending on the context to engage as political candidates due to fear of intimidation, threats, harassment and hate speech. In those circumstances, measures to protect fundamental rights directly contribute to uphold EU values for a sustainable, equal, democratic and participatory society where tolerance, non-discrimination and pluralism prevail.

Freedom of expression, including online, is at the heart of any democracy. Any legislative or non-legislative measures relating to content moderation and the responsibility of online intermediaries for the content on their services must take into account that the right to free speech includes the right to express ideas that may be regarded as critical, offensive, insulting or controversial, and that the right to free speech can only be limited under very strict conditions including in respect of dissemination of allegedly illegal content such as hate speech material. The European Court of Human Rights has however also made clear that States are permitted and may even have a positive duty to counter all forms of expression that spread, incite, promote or justify hatred directed to persons or groups belonging to a particular ethnicity or religion[33].

More often than not, disinformation and misinformation are not illegal, even though they may be disturbing or offensive. While for speech protected by the freedom of expression the State's primary obligation is to refrain from interference and censorship, the State also has a positive obligation to ensure a favourable environment for inclusive and pluralistic public debate, in particular in relation to elections, and for the exercise of media freedom. Such measures go beyond the sphere of content moderation and are linked to more fundamental education and information actions.

Private actors, such as online platforms, define their own terms and business model in the exercise of their rights to freedom of contract and to carry out a business without State instructions as to the type of the content that they would be obliged to host. Within this context, they could take measures that significantly affect users and their rights. There is not always a legal remedy available against such private decisions that would allow for such decisions to be balanced against individuals' rights and legitimate interests and ensure a

[32] European Parliament study requested by the DROI subcommittee 'The impact of disinformation on democratic processes and human rights in the world', Carme Colomina, Héctor Sánchez Margalef, Richard Youngs, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

[33] Erbakan v. Turkey, judgment of 6 July 2006, § 56.

certain degree of predictability. Where online platforms overly remove legal content, they may significantly restrict the freedom of expression and information.

4.1 Situation at Member State level

In the **targeted consultation** for the purposes of this report, civil society actors reported on problems in the Member States caused by certain illegal content online, such as smear campaigns and attacks on those that work to protect the rights of others. Women, especially women of colour or those belonging to vulnerable groups such as migrants and Roma, as well as LGBTIQ people, were reported to be disproportionately targeted. Children using online platforms are exposed to inappropriate, harmful and violent content, and online predators, also increasing the risks for grooming and recruitment into extremist environments. Sexual violence against children was reported to be amplified through the internet, for example due to increased demand for child sexual abuse material.

Disinformation was also identified by civil society organisations as a problem affecting health and safety, as well as the democratic discourse in several Member States. There was widespread concern about a lack of transparency (labels, sharing alerts, exposure notifications) and a lack of media literacy regarding false or misleading content.

While the spread of illegal content and disinformation was seen as a threat, the CSOs consulted also warned about the effects on freedom of expression when poorly calibrated moderation policies are used to tackle such threats. CSOs indicated that copyright protection has been misused to silence voices online and that laws on defamation and glorification of terrorism have been used to repress individuals. The low accuracy of automated content moderation systems, in particular when deployed on content where the assessment of its legality depends on a high level of contextualisation, raised concerns about unjustified impacts on freedom of expression through overly broad content take-downs and silencing of certain statements and opinions, including from minorities. According to academics and respondents to the targeted consultation, the use of algorithms for customizing the display of content for users can also distort the democratic discourse, since it is often geared towards amplifying advertising revenues, rather than being guided by the objective of providing the public with reliable information in the public interest. Similar claims that algorithms used to tailor the content that users see are causing harm, have also been made by whistle-blowers through the press[34]. Beyond the effects of the use of such systems on fundamental rights, they were claimed, by respondents to the target consultation, to often be deployed in a non-transparent or not fully transparent manner, and with little accountability for their outcomes.

Several EU Member States have regulated digital services established on their territories. These laws aim at ensuring that service providers comply with certain procedural rules when users or authorities report illegal content. They sometimes cover specific categories of illegal content such as copyright infringements or illegal hate speech. However, the precise requirements of these laws often diverge on a number of points, such as:

- the information required for reporting illegal content;
- the possibility for those who published that content to react;

[34] See for instance https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero

- the timeframe for service providers to react;
- potential mandatory measures against abusive reports; or
- the possibility to submit contentious cases to an independent third party.

More recently, faced with growing concerns about the spread of hate speech and terrorist content, several Member States adopted, proposed, or envisage the adoption of additional rules, focusing in particular on certain categories of illegal content, and sometimes also covering service providers established outside of their territory. However, there is significant legal fragmentation resulting from the individual efforts of Member States to tackle illegal content online and to provide varying types of safeguards for freedom of expression. Several Member States[35], as well as the Council[36] and European Parliament[37], have called for these shared concerns to be addressed at EU level. Furthermore, a number of Member States observed that a lack of cross-border cooperation between national authorities hinders effective oversight of online platforms that operate across borders[38].

4.2 The EU policy response

Based on calls from Member States, there have been several sectorial initiatives adopted at EU level to tackle the problem of specific types of illegal content such as that related to terrorism, child sexual abuse, incitement to hatred and violence, trafficking in human beings, unsafe products, and copyright infringements while at the same time guaranteeing the protection of fundamental rights.

The Audiovisual Media Services Directive

The revised **Audiovisual Media Services Directive** (AVMSD) was adopted in 2018. The Directive includes measures to protect minors from audiovisual content and commercial communications that could cause physical, mental or moral detriment to them. Also, Member States must ensure that audiovisual media services do not contain any incitement to violence or hatred against people based on any of the grounds referred to in Article 21 of the EU Charter of Fundamental Rights. The transposition deadline for this directive was on 19 September 2020. In November 2020, the Commission opened infringement procedures (letters of formal notice) against 23 Member States that had not transposed the Directive and many transposed it in the following year. In September 2021, the Commission sent a second warning (reasoned opinions) to nine Member States for failure to notify complete transposition. The implementation of the revised AVMSD is essential not only for market players, but also for individuals (including viewers and minors).

[35] https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package
[36] Council Conclusions of 9 June 2020, 'Shaping Europe's Digital Future' and Conclusions of Special meeting of the European Council of 1 and 2 October 2020.
[37] European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL); European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL).
[38] DSA impact assessment, section 2.3.6. Limited cooperation among Member States and lack of trust.

The Directive on Copyright in the Digital Single Market

The **Copyright Directive**[39] was adopted in April 2019 and aims to ensure that rights holders receive a fair compensation for the use of their work. In doing so, it strikes a balance between competing fundamental rights such as the right to intellectual property, freedom of expression and information, the freedom of sciences and the right to education and cultural diversity. The Directive introduces mandatory exceptions to copyright that protect the freedom of expression of users that generate and upload content on online content-sharing services. The Directive required the Commission to organise a stakeholder dialogue to discuss best practices for cooperation between online content-sharing service providers and rights holders, taking special account of the need to balance fundamental rights and of the use of exceptions and limitations. Following this dialogue, in June 2021, the Commission adopted guidance to support the coherent application of Article 17 of the Directive, which establishes new rules on the use of protected content by online content-sharing services[40]. The guidance provides practical indications on the main provisions of Article 17, helping market players to better comply with national laws that are based on the Directive and taking into account the views gathered from the Member States and stakeholders.

The code of conduct on countering illegal racist and xenophobic hate speech

In 2016, the Commission signed a voluntary **code of conduct** with major online platforms to ensure that notifications of **illegal racist and xenophobic hate speech** are rapidly assessed, not only against the companies' terms of service but also against Member State laws used to implement EU law criminalising racist and xenophobic hate speech[41]. The adherence to the code of conduct is monitored regularly[42]. It yields good results and has also fostered a collaborative approach between online platforms, Member States and civil society to ensure high quality content moderation where an in-depth understanding of the cultural, linguistic and historical context of the disputed content is required.

Recommendation on the safety of journalists and other media professionals

Safety has become a major concern for journalists due to online incitement to hatred, threats of physical violence, but also cybersecurity risks and illegal surveillance. On 16 September 2021, the European Commission issued a **Recommendation for the Protection, Safety and Empowerment of Journalists.**[43] The Recommendation encourages Member States to promote the cooperation between online platforms and organisations with expertise in tackling threats against journalists, for instance by encouraging their potential role as trusted flaggers. Journalists and other media professionals are not only targets of online incitement to hatred and threats of physical violence, but can also be subject to illegal surveillance and the recommendation indicates that relevant national cybersecurity bodies should, upon request,

[39] Directive 2019/790 (EU) on copyright and related rights in the Digital Single Market, OJ L 130, 17.5.2019.
[40] Commission Communication, Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market, COM/2021/288 final.
[41] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008.
[42] The latest monitoring exercise took place in 2021: The EU Code of conduct on countering illegal hate speech online | European Commission (europa.eu)
[43] Commission Recommendation on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union, 16.9.2021, C(2021) 6650 final.

assist journalists who seek to determine whether their devices or online accounts have been compromised, in obtaining the services of cybersecurity forensic investigators. Member States should also promote a regular dialogue between such cybersecurity bodies, media and industry, in particular in view of fostering cyber-awareness and digital skills among journalists.

Regulation on addressing the dissemination of terrorist content online

Security and respect for fundamental rights are not conflicting aims, but consistent and complementary ones. Security of both online and physical environments requires countering illegal content online. To ensure that terrorist content is removed, the European Parliament and the Council adopted a **Regulation addressing the dissemination of terrorist content online** in 2021[44]. It contains a number of safeguards for fundamental rights, in particular the freedom of expression. For example, removal orders by national authorities can only be issued for terrorist content as defined by the Regulation and such orders must justify why the material is considered terrorist content. The Regulation exempts content disseminated for educational, journalistic, artistic or research purposes and content that is disseminated for awareness-raising purposes against terrorist activity. There is no obligation for online platforms to use automated tools to proactively identify or remove terrorist content but if technical measures are used, safeguards, in particular human oversight and verification, should be provided to ensure accuracy. As of March 2023, Member States and online platforms will also have to issue annual reports on measures taken to remove terrorist content and on the functioning of any automated tools that may have been used.

Legislation on addressing online child sexual abuse

While regulatory action to tackle illegal content largely focused on publicly available content such as that posted on social media or websites, the challenge of tackling **child sexual abuse material** shared through interpersonal communications, including in the interpersonal communication tools on social media services also has to be addressed. An **interim legislation**[45], that entered into force in August 2021, ensures that certain online communication services, such as webmail or messaging services, may continue to use – to the extent strictly necessary – specific technologies to detect child sexual abuse material, to report it and to remove it, while ensuring a number of guarantees to safeguard privacy and the protection of personal data in accordance with the General Data Protection Regulation. Mechanisms to detect child sexual abuse in interpersonal communications risk impacting fundamental rights, in particular the confidentiality of communications, the protection of personal data, or the freedom of expression. The interim Regulation aims to mitigate that impact by limiting the use to the least privacy-intrusive technologies in line with the state of the art in the industry. The Regulation also provides for redress mechanisms that must be put in place to ensure that individuals can lodge complaints with providers if their content is wrongly removed. The Commission is also preparing a **proposal for legislation** to replace

[44] Regulation 2021/784 on addressing the dissemination of terrorist content online, OJ L 172, 17.5.2021.
[45] Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, OJ L 274, 30.7.2021.

this interim measure and to give service providers legal certainty and ensure a uniform approach to detecting, removing and reporting child sexual abuse material, while providing for the right balance between the rights of the child and the need to protect children from sexual abuse, and the right to private life and communications of all users of online services.

EU Strategy on Combatting Trafficking in Human Beings 2021-2025

Tackling the digital business model of traffickers is one of the priorities of the EU Strategy on Combatting Trafficking in Human Beings 2021-2025[46], presented by the Commission in April 2021. Internet service providers and related companies are part of the solution to support anti-trafficking efforts with identification and removal of online material associated with exploitation and abuse of trafficked victims. The Commission will conduct a dialogue with relevant internet and technology companies to reduce the use of online platforms for the recruitment and exploitation of victims. The Commission will also facilitate possible similar dialogues to be conducted by Member States at national level.

The proposal for a Digital Services Act Regulation

The proposal for a **Digital Services Act** Regulation[47], adopted by the Commission in December 2020, and which is currently under discussion by the co-legislators, frames the responsibilities of online intermediaries. Without prejudice to sector-specific EU rules such as those on copyright or terrorist content online, it provides a single horizontal set of rules in the EU for a balanced governance of online content moderation.

The proposal caters for the appropriate protection of all fundamental rights, including users' freedom of expression and right to private life, the platforms' freedom to conduct a business and freedom of contract and intellectual property rights. It also aims to mitigate risks for people in vulnerable situations and vulnerable groups to protect them from threats, intimidation or discriminatory behaviour and it aims to protect the right to human dignity of all users of online services.

The proposal for a Regulation aims to achieve these objectives by:

- Largely preserving the existing liability regime for online intermediaries, including the prohibition of general monitoring or fact-finding obligations. This approach builds on the existing E-Commerce Directive.[48] It seeks to cater for: (i) the proportionate and appropriate protection of the right to freedom of expression by limiting incentives to remove legal content, and the right to conduct a business, ensuring proportionality in the efforts requested from online intermediaries and protecting their legitimate business users; and (ii) public policy concerns linked to disseminating different types of illegal content, by ensuring that it is swiftly removed by intermediaries within the conditions provided by the law.

[46] Communication on the EU Strategy on combatting trafficking in human beings 2021-2025, COM(2021) 171 final.
[47] Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.
[48] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

- Setting clear and proportionate due diligence obligations for online intermediaries to ensure that illegal content is appropriately and transparently tackled and that users can assert their rights. The proposal also provides for a rigorous set of safeguards for content moderation processes, including those based on privately set terms and conditions.

- Imposing an obligation on very large online platforms – those that due to their reach have acquired a central, systemic role in facilitating the public debate – to assess and mitigate risks their services pose, including for certain fundamental rights: respect for private and family life, freedom of expression and information, non-discrimination, and the rights of the child. The risk mitigation strategies also need to account for the potentially negative effects of the platforms' content amplification algorithms, such as recommender or advertising systems. Very large online platforms are also subject to increased accountability, giving more choices to users in their online interactions and allowing for independent auditors and vetted researchers to scrutinize their systems.

Fighting disinformation and regulating political advertisement online

The spread of disinformation, misinformation and conspiracy myths can result in polarising debates and put health, security and the environment at risk. Disinformation can also hamper the ability of people to take informed decisions based on correct facts. In some cases, disinformation constitutes speech that the State can legitimately restrict (such as racist and xenophobic incitement to violence and hatred). However, very often it is protected by the right to freedom of expression, even if it lacks any scientific evidence or basis in real events. When it comes to protected speech, States must refrain from censorship. To be effective, actions to limit the reach of disinformation and conspiracy myths needs to be accompanied by the fostering of a favourable environment for inclusive and pluralistic public debate. This is especially relevant in relation to elections.

Against this background the Commission continued in 2020-2021 to develop several actions aiming to make the online environment more transparent and its actors accountable, to empower users, and to foster open democratic debate online. These actions included (i) support for independent fact-checkers and academic researchers, particularly through the **European Digital Media Observatory**[49]**,** (ii) measures to improve media literacy, and (iii) the monitoring of a self-regulatory **Code of Practice on Disinformation**[50]. Based on the outcome of these monitoring activities the Commission has also issued guidance on how current and new signatories to the Code of Practice, including private messaging apps, the advertising sector and other relevant stakeholders, could strengthen the Code's scope and application, and ensure a more robust monitoring framework[51].

To promote democratic discourse, the **European Democracy Action Plan**[52] sets out measures to promote free and fair elections, strengthen media freedom and counter disinformation. This includes the proposal on transparency and targeting of political

[49] EDMO – United against disinformation
[50] Code of Practice on Disinformation | Shaping Europe's digital future (europa.eu)
[51] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585
[52] European Democracy Action Plan | European Commission (europa.eu)

advertising, adopted in November 2021[53], as part of measures aimed at protecting election integrity and open democratic debate. These proposed rules would require any political advertisement to be clearly labelled as such and include information such as who paid for it and how much. Political targeting and amplification techniques would need to be explained publicly in unprecedented detail and would be banned when using sensitive personal data without the explicit consent of the individual. Lastly, the **new Digital Education Action Plan (2021-2027)[54]** proposes the development of guidelines for teachers and educators on tackling disinformation and promoting digital literacy.

The proposal for a new General Product Safety Regulation

In addition, to cater for further sectoral requirements, the Commission, as part of the review of the EU product safety framework, adopted and published a proposal for a new **General Product Safety Regulation** in June 2021[55]. This proposal, building on the Digital Services Act proposal, would introduce additional requirements for online marketplaces regarding unsafe products as a specific category of illegal content. The proposal is currently under discussion by the co-legislators.

5. Safeguarding fundamental rights where AI is used

The use of artificial intelligence (AI) technologies can have significant positive effects on our societies. It can increase the efficiency of processes or drive innovation and research. It can also be used to promote a range of fundamental rights, such as the rights to freedom of expression and information or healthcare, and to foster important issues of public interest like public security or public health.

On the other hand, where AI is used without adequate safeguards and quality controls to automate or support decision-making processes or for activities such as surveillance, this may also violate the rights of individuals. Such violations can occur at great scale, depending on how broadly a system is used, and they can be difficult to prevent or detect when the AI system is not sufficiently transparent or people remain unaware of its use. For example, the use of AI to infer information about people can affect data protection and privacy. Bias in algorithms or training data, such as gender bias or bias in relation to ethnic or racial origin, can lead to unjust and discriminatory outcomes. If a system to estimate potential success at work is trained mostly with data about men, it is likely to perform less well when used to analyze data of women, likely leading to discrimination. In addition, the use of AI can also affect the rights to human dignity, good administration, consumer protection, social security and assistance, freedom of expression, freedom of assembly, education, asylum, collective bargaining and action, fair and just working conditions, access to preventive care, cultural and linguistic diversity, rights to data protection and respect of private life as well as rights of vulnerable groups such as children. If those systems are used in the context of law

[53] Proposal for a regulation on the transparency and targeting of political advertising, COM(2021) 731 final.
[54] Digital Education Action Plan (2021-2027) | Education and Training (europa.eu)
[55] Proposal for a regulation on general product safety, amending Regulation (EU) No 1025/2012, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, COM(2021)346 final.

enforcement or the judiciary, they can also affect the presumption of innocence and the right to fair trial and defence. Furthermore, inaccessibility or non-existence of relevant information on automated systems impedes effective enforcement of fundamental rights obligations and individuals' access to legal remedies.

What is AI and what are the specific characteristics that can lead to risks?

- AI is a term for a set of technologies that have undergone rapid development in recent years. In the case of certain types of AI systems, their functions follow rules that are automatically generated and not explicitly programmed by people. This can sometimes lead to impressive results, but can also pose challenges. Building on the OECD's definition of AI, the proposed Artificial Intelligence Act (AIA) defines AI as software that is developed with machine learning, logic-and knowledge-based, or statistical approaches and can, for a set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments it interacts with.

- The opacity (lack of transparency) and complexity (operation with many different components and processes) of certain AI systems make it difficult to identify and prove possible breaches of law, including provisions ensuring respect for fundamental rights, and trace back possible errors or malfunctioning of the system.

- A specific subset of AI applications can undergo continuous adaptation, even during their use, and change and evolve in unforeseen ways, which cannot be easily monitored. This leads to a certain degree of unpredictability, which can affect safety or fundamental rights.

- Autonomous performance of systems can affect safety, as some AI systems require little to no human intervention in carrying out tasks.

- The dependence on data of certain systems and possible biases embedded in algorithms can cause or increase systemic biases and errors. If these systems are not properly designed, tested and used, they can exacerbate adverse results such as discrimination.

5.1 Situation and actions at Member State level

In recent years, EU Member States have sought to address the challenges posed by the use of AI technologies. Many have developed national AI-strategies[56], in which they emphasize the need to ensure respect for fundamental rights. In addition, Member States have developed or plan to develop guidelines and ethical standards that help those who deploy AI tools to ensure transparency, traceability and robustness, address potential biases and find effective ways to comply with their obligations to respect fundamental rights. In some cases, guidelines and expertise are developed by academics[57] or expert groups established for this purpose[58].

[56] By June 2021, 20 Member States and Norway had published their national AI strategies, while 7 Member States were in the final drafting phase. https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en

[57] For example, academics from the University of Utrecht developed in April 2021 a Code for Good Digital Public Administration for Dutch authorities that is grounded in fundamental rights. https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur

[58] An example for this is the German "Data Ethics Commission" and the expertise it produced in 2019: https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html

Also when acting together at EU level, Member States underlined the need to ensure that the rights in the Charter are fully respected and called for a review of existing relevant legislation to make it fit for purpose in order to address the new opportunities and challenges raised by AI[59]. In October 2020, 26 of the 27 Member States adopted a document entitled "The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change"[60], in which they called for addressing the opacity, complexity and bias, as well as the certain degree of unpredictability and partially autonomous behaviour of certain AI systems, to ensure their respect of fundamental rights and to facilitate the enforcement of legal rules. The Member States underlined the importance of involving various stakeholders, including those from civil society, to benefit from their expertise.

At the time of adoption of this report, no EU Member State had adopted specific legislation to address the fundamental rights challenges raised by the use of AI[61]. Rather, it appears that authorities in the Member States relied on existing legislation. In 2017, an Italian court ordered the Italian Ministry of Education to disclose an automated decision-making algorithm that it used for workers mobility management based on the right of access to documents, which also enables the right to an effective legal remedy[62]. In 2018, the Finnish National Non-Discrimination and Equality Tribunal considered a case of credit-scoring based on statistics relating to gender, place of residence, age and language rather than an individual assessment to be discriminatory[63]. In February 2020, a Dutch court invalidated Dutch legislation that had established a fraud detection system, based on the fundamental right to private life as enshrined in the European Convention of Human Rights[64]. The 'System Risk Indication' (SyRi) was used to analyse data collected by different public authorities to detect people who potentially commit benefits fraud. The Dutch court found that the use of SyRi was not sufficiently transparent and its interference with the right to privacy was not proportionate to the aim of fraud detection.

These examples show that the Member States have already confronted challenges raised by the use AI in relation to fundamental rights. The Commission's proposed approach to AI related challenges aims to strengthen the effective protection of fundamental rights, while at the same time fostering innovation in AI.

5.2 The Commission proposal to regulate high-risk AI

In April 2021, the Commission presented a proposal for a Regulation on AI (AIA)[65]. Key objectives of the proposed AIA are the protection of fundamental rights and safety and the

[59] European Council meeting (19 October 2017) – Conclusion EUCO 14/17, p. 8. and Conclusions on the coordinated plan on artificial intelligence- (11 February 2019) 6177/19, 2019.
[60] https://www.consilium.europa.eu/media/46496/st11481-en20.pdf
[61] Finland reported that work is ongoing to prepare a draft legislative proposal on automated administrative decision-making by the end of 2021. The inclusion of examples for Member State actions (legislation, funding or others) in this report aims to illustrate different types of actions. Not all initiatives can be named for every topic and the selection is to a large extent based on information submitted by the Member States in June 2021.
[62] T.A.R., Rome, sect. III-bis, 22 mars 2017, n° 3769.
[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] Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.

creation of a single market for trustworthy AI systems. The proposal aims to ensure that high-risk AI systems are designed and used in compliance with fundamental rights and that competent national authorities and courts can more effectively investigate and address possible breaches of fundamental rights obligations.

The proposal follows a risk-based approach. Certain AI systems are prohibited outright, such as those deploying subliminal techniques and those used by public authorities for social scoring, due to their contravention of EU values. The use of remote biometric identification systems in publicly accessible spaces for law enforcement purposes is also prohibited, unless clearly defined exceptions and safeguards apply.

High-risk AI systems will need to comply with a set of requirements and follow conformity assessment procedures before being placed on the market or put into service. Those requirements ensure appropriate documentation and testing of high-risk AI systems, as well as adequate data quality, traceability, human oversight, robustness, accuracy and cybersecurity. They will apply where AI systems are used in critical areas, such as biometric identification, education, employment, essential public and private services, such as credits, or public assistance benefits, law enforcement, migration and border control, and the judiciary. AI systems that are safety components of certain regulated products (e.g. machinery, medical devices) will also be covered by the same requirements and have to be checked before they can be placed on the EU market or put into service.

The proposal ensures that the users of AI systems, such as companies interacting with clients, or public authorities taking decisions, are provided with adequate information from the developers of the systems to ensure suitable use of their applications and to enable them to fulfil their obligations under fundamental rights law.

Should infringements of fundamental rights occur through the use of AI systems, effective redress for affected persons will be facilitated by means of transparency and traceability of AI systems, coupled with strong ex post controls by competent authorities. Supervisory authorities in charge of enforcing fundamental rights, such as data protection authorities, equality bodies or consumer bodies, will have access to all documentation on high risk AI systems that fall within their mandate. They will be able to cooperate with market surveillance authorities to test the respective AI systems where needed.

For specific AI systems, transparency obligations towards affected people will minimise the risk of manipulation, in particular in the case of chat bots (computer programs that can answer questions in an online chat) or ‘deep fakes’ (artificially generated or manipulated image, audio or video content that resembles existing people, objects, places or other entities or events and which falsely appear to be authentic or truthful). People should also be informed when emotion recognition or biometric categorisation systems are used, which will help them enforce their rights under the existing data protection legislation.

The proposal is currently under negotiation with the co-legislators.

5.3 Interplay with sectoral legislation – the example of creditworthiness and credit scoring

The AIA proposal will work jointly with other legislation laying down substantive rules for the use of AI systems in clearly targeted contexts. For example, credit providers often use automated decision-making techniques, including AI systems, for creditworthiness assessments or credit scoring. Such providers rely on different data, many of which are not provided by the consumer or are unknown to them. This raises concerns over the protection of personal data, direct or indirect discrimination,[66] and consumer protection.[67] The **Consumer Credit Directive**[68] and the **Mortgage Credit Directive**[69] contain provisions on creditworthiness assessments. In June 2021, the Commission adopted a **new proposal for a Directive on consumer credits** repealing and replacing the current Consumer Credit Directive. It proposes rules in relation to granting credits to consumers according to which Member States will have to ensure documentation of procedures and information used in creditworthiness assessments. In addition, the assessments will have to be based on relevant and accurate information on financial and economic circumstances (e.g. income and expenses) and should not be based on data such as social media data. Consumers will also have the right to an explanation on how a decision on their creditworthiness was reached, to express their point of view and to obtain human intervention, mirroring the principles of the General Data Protection Regulation (GDPR)[70] concerning automated decision-making. The new proposal also includes an article on non-discrimination, specifying that the conditions to be fulfilled for being granted a credit must not discriminate against consumers legally resident in the Union on ground of their nationality or place of residence or on any ground as referred to in Article 21 of the EU Charter of Fundamental Rights. The proposal is currently under negotiation with the co-legislators.

5.4 Skills

Where AI systems are used, workers need to be adequately skilled to ensure respect of fundamental rights and appropriate human oversight. Supervisory authorities will also need staff with specific technical skills to effectively fulfil their mandates. In September 2020, the Commission adopted a **Digital Education Action Plan** for 2021-2027[71]. It aims at promoting digital skills, including in relation to AI[72], and includes the development of ethics guidelines in the field of AI and data in education and training. Moreover, all Member States that have

[66] For example, in April 2019, the Finnish Data Protection Ombudsman ordered financial credit company Svea Ekonomi to correct its creditworthiness assessment practices, considering that an upper age limit was not acceptable as a factor, since age does not describe solvency or willingness to pay.
[67] Impact assessment report accompanying the Proposal for a Directive on credit agreements for consumers repealing and replacing Directive 2008/48/EC, COM(2021) 347 final.
[68] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ L 133, 22.5.2008, p. 66.
[69] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 Text with EEA relevance, OJ L 60, 28.2.2014, p. 34.
[70] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[71] Digital Education Action Plan (2021-2027) | Education and Training (europa.eu)
[72] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8_en

adopted national AI strategies have integrated a skills component into their strategies, for example via reforms of the education systems to strengthen computational thinking or initiatives to adapt lifelong learning and reskilling policies[73].

6. Addressing the digital divide

Being digitally connected and competent enables active participation in society. An increasing number of essential activities are moving to the online sphere, ranging from looking for a job, performing work by means of teleworking, pursuing an education, to interacting with a public administration or making a doctor's appointment. But not everyone is online. Not being online can affect people in the exercise of their rights. For instance, it can affect people's rights in a democratic society, including their right to freedom of expression and information, and their right to stand as a candidate in municipal elections since political campaigns are increasingly run online. The outbreak of the COVID-19 pandemic has exacerbated these difficulties in accessing public services for those without the necessary equipment or digital knowledge, with offices being closed and people being asked to communicate with their national administrations online.

This phenomenon is often called 'the digital divide'. Still today, 46% of Europeans lack basic digital skills[74]. This is recognised by the **European Pillar of Social Rights** that includes digital communications among the essential services everyone should have access to and call for support measures for those in need[75]. Those who lack regular access to the internet, the necessary skills to make use of these services, or cannot access a digital product or service due to physical or cognitive disability, increasingly risk being excluded and face difficulties in making use of their rights.

In the case of public services that are exclusively accessible by digital means, those who are not connected may find themselves unable to exercise their rights or would need help to do so. By way of example, the *Haut Conseil du Travail*, an advisory body to the French Ministry for Social Affairs, estimates that 1 in 5 people in France encounter difficulties trying to complete administrative procedures online, and warn that digitalisation can jeopardise the principle of equal access to public services if alternative means of access are not maintained[76]. Similarly, as more and more economic activities have a digital component, exercising the right of access to services of general economic interest has become increasingly conditional on internet access. Children without a connected device at home have difficulties participating remotely in school, which affects the rights of the child and the right to education. Furthermore, where websites and mobile applications are not adapted to the needs of people with disabilities, their right to integration can be hampered.

[73] https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en
[74] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624 and Statistics | Eurostat (europa.eu)
[75] The European Pillar of Social Rights in 20 principles | European Commission (europa.eu), see principle 20.
[76] https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi_et_comment_les_travailleurs_sociaux_se_saisissent_des_outils_numeriques.pdf, p.4.

In view of the challenges posed by the digital divide, Member States and the Commission are pursuing a series of measures to ensure that nobody is left behind. As announced in the **European Pillar of Social Rights Action Plan**[77], in 2022 the Commission will publish a Report on access to essential services, which will also cover access to digital communications, presenting an overview of the state of play in the EU27 as well as a mapping of existing national and EU measures and good practices supporting access for people in need.

6.1 General reduction of the digital divide

The fact that during the pandemic many activities moved to the online sphere is not only a challenge, but also an opportunity. Member States have developed projects that the EU will finance to help the economy recover from the downturn caused by the pandemic. These projects include measures to tackle the digital divide and achieve inclusive digital rights, and to address the digitalisation of work. Two national plans can be mentioned as examples. **Romania** plans to invest in the creation of educational content and accessible resources, such as videos and interactive lessons, and to develop accessible digital literacy programmes for students with disabilities. **Germany** aims to help acquire digital devices for teachers nationwide. In addition, it will create a platform for digital lifelong learning and particular attention will be paid to supporting the formally least qualified people.

More generally, there are a number of promising initiatives in different Member States[78]. In February 2021, **Belgium** launched a public call for projects supporting female entrepreneurs affected by the COVID-19 pandemic including by offering guidance towards digitalization. Belgium is also investing in local organisations which aim at increasing the digital skills of young people in precarious economic situations.

Portugal is mobilising young volunteers to help educate adults about the digital transition, based on a national network of 1 500 training centres and a number of free tools and resources. This digital inclusion programme is expected to reach 1 million people and will be implemented in partnership with local authorities and local organisations[79].

On a similar logic to the WiFi4EU[80] initiative, **Italy** subsidises internet access for certain people and has started the 'Piazza Wifi Italia' project[81] that allows over 400 000 people to easily connect, free of charge through a dedicated app, to a free wifi network spread throughout the country. In March 2020, this project was extended to health facilities including hospitals.

Digital infrastructure is likely to continue to evolve and the EU has taken action in a range of areas to improve connectivity. The main goal for connectivity in the **Digital Decade** is for every European household to have access to high-speed internet coverage by 2025 and

[77] The European Pillar of Social Rights Action Plan (europa.eu)
[78] Not all initiatives can be named in this report and the following selection aims to illustrate different types of actions. It is based on information submitted by the Member States in June 2021.
[79] Resolução do Conselho de Ministros n.º 30/2020 - DRE
[80] https://digital-strategy.ec.europa.eu/en/activities/wifi4eu
[81] https://www.wifi.italia.it/it/

gigabit connectivity by 2030[82]. The Commission and Member States agreed in March 2021 on a **Connectivity Toolbox** to foster the deployment of digital networks and facilitate access to the 5G spectrum. The review of the Broadband Cost Reduction Directive, planned for 2022, aims at further supporting the roll-out of digital networks by reducing the administrative burden and the cost and speed of such deployments. Moreover, the Commission's long-term **Vision for rural areas**[83] of June 2021 aims to address the urban/rural divide by enabling access to fast internet connectivity, 5G (including via EU funding[84]) and digital technology, as well as strengthening digital competencies. High speed broadband connectivity is a key enabler for the digital transition and the post-COVID-19 recovery. The Commission is committed to reduce the digital gaps of accessibility in rural areas and the EU will invest in network infrastructure, a standard for wireless data transmission, and fibre to ensure that everyone in the EU has access to energy efficient and future proof digital connectivity infrastructure.

6.2 Public administration

Digital technology allows people to benefit from wider access to public services and information that can help them manage their daily lives and exercise their rights, in particular the freedoms to establish and provide services. Since the **Malmö Declaration**, signed at a summit in Sweden in 2009, the EU Member States have made steady progress to modernise public administrations[85]. The **Tallinn Declaration** of 2017 gave an impetus to digitalise public services for people and cross-border public services for businesses[86]. Most recently, the **Berlin Declaration** of December 2020 included steps to take for the protection of fundamental rights online among the commitments of the Member States[87] and the **Lisbon Declaration** of June 2021 aims to ensure that 'no one is left behind'. The efforts made by Member States also include the digitalisation of Justice[88].

Member States are pursuing different approaches to ensure access to public services, trying to reduce this digital divide while at the same time meeting the demands of this digital age. For example, **France** has chosen to maintain several ways of ensuring access to public services in order to avoid any obstacles. People are not obliged to contact the administration electronically. **Denmark** has been following a different path setting a 'digital by default' strategy, and, in 2014, made the use of electronic means compulsory for all contacts with the administration. To address the digital divide, the State is funding measures such as free

[82] Commission Communication '2030 Digital Compass: The European way for the Digital Decade, COM(2021) 118 final.
[83] A long-term vision for the EU's rural areas | European Commission (europa.eu)
[84] Funding from the European Regional Development Fund, the European Agricultural Fund for Rural Development, from the Connecting Europe Facility 2 and from the Recovery and Resilience Facility will be available to reach the connectivity objectives of the EU for 2025.
[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] Advances in this area are reflected in the Commission's Rule of Law Report 2021: https://ec.europa.eu/info/sites/default/files/communication_2021_rule_of_law_report_en.pdf.
See also Commission Communication on the digitalisation of justice in the EU, COM (2020) 710 final and accompanying SWD(2020) 540 of 2 December 2020.

personalised support in libraries[89], assistance with purchasing equipment and contributions to internet subscriptions. In a similar vein, in **the Netherlands** the government and local libraries have started the 'Information Point Digital Government', an initiative in which a trained library employee answers questions and helps people with traditional digital governmental services, such as tax declarations and social services, as well as newer services such as corona-apps.

6.3 Healthcare

The pandemic caused an increase in healthcare provision online, e.g. through virtual consultations or through apps and software developed for diagnostic or therapeutic purposes. For some, such as people in rural areas or on small islands, this trend makes it easier to receive medical support, whereas for others it presents a new barrier. For those who lack access or competencies, measures to bridge the digital divide can improve the situation. For example, **Poland** has introduced 'the Patient's Internet Account', an online tool, which gives patients access to information about their past, current or planned medical treatment and allows them to settle a number of matters (e-prescription, visit history records, e-referral, e-medical leaves, and entitlements) without the need to visit a healthcare facility in person.

6.4 Education

Several Member States have policies and programmes to foster access to technology and strengthen digital competencies in the context of formal education. **Greece**, for example, provides pupils and students who need it with vouchers to purchase equipment like tablets or computers and provides relevant educational programmes through a virtual 'Digital Skills Academy' launched in 2020.

At the EU level, the **Digital Education Action Plan**[90] (2021-2027), launched in September 2020, set out a long-term strategic vision for a sustainable and inclusive digital transformation in education and training. It promotes the right of access to high-quality digital education for all and equal access to infrastructure, with a particular focus on encouraging the participation of girls and women in STEM (science, technology, engineering and mathematics) subjects.

6.5 Integration of persons with disabilities

The **European Electronic Communications Code**[91] ensures equivalent access to and choice of electronic communications services for end-users with disabilities, facilitating participation in the digital society. The **European Accessibility Act**[92] will come into effect in 2025 and expand the inclusion of people with disabilities and older people in the digital world by making a set of key products and services from both the private and public sector more

[89] Such support also exists elsewhere, but for the purpose of illustrating the approach, selected examples are sufficient. The objective of this report is not an exhaustive mapping of measures, but rather to provide an overview of ideas and approaches.
[90] Digital Education Action Plan (2021-2027) | Education and Training (europa.eu)
[91] Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018.
[92] Directive (EU) 2019/882 on the accessibility requirements for products and services, OJ L 151, 7.6.2019.

accessible. The **Web Accessibility Directive** of 2016[93] requires Member States to ensure that websites and mobile applications of public sector bodies are accessible to people with disabilities, such as people with visual, hearing or motor impairments. In this way, it promotes freedom of expression and information, the right to education, freedom to choose an occupation and the right to work, non-discrimination, integration of people with disabilities, access to services of general economic interest, the right of access to documents, the right to move and reside freely within the territory of the Union, the freedom of establishment and their freedom to provide services.

The Directive can be implemented in different ways. For example, **Slovenia** modernised its e-government state portal in such a way that it can be used by the blind and visually impaired, the deaf and hard of hearing, people with dyslexia and users with impaired understanding. Text-based descriptions of procedures are for instance accompanied by short videos, which also feature interpretations in sign language. In **Greece**, during the pandemic, digital school books were adapted so people with all categories of disability could access them.

7. Protecting people working through platforms

Online platforms include a wide array of marketplaces, social media, creative content outlets, app stores, price comparison websites, platforms for the collaborative economy as well as search engines. They facilitate interaction between users and businesses. Digital labour platforms, as a distinct subset of online platforms, have emerged as a characteristic feature of the digital economy.

Platform work has generated new economic opportunities for people, enabling them for instance to pursue part-time activities and access the labour market in general. However, at the same time it poses challenges to fundamental rights, including the protection of personal data, privacy, workers' rights to information and consultation, the right to collective bargaining and action, and fair and just working conditions. Among the 28 million people who are estimated to work through digital labour platforms, there may be up to 5.5 million people who are "false" self-employed.[94] While their contracts with the platforms they work through describe them as self-employed, in reality they are subject to control and supervision, which are characteristic of the 'worker' status. There are also challenges stemming from the algorithm-based business models, such as lack of information and consultation with people working through platforms and their representatives on how algorithms are used and affect working conditions in platform work. There are also insufficient means of redress and unclear responsibility regarding the use of algorithms.

[93] Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies, OJ L 327, 2.12.2016.

[94] See Impact Assessment report accompanying the proposal for a Directive on improving working conditions in platform work, SWD(2021) 396 final.

Platform work

Platform work usually involves three parties: the **platform**, the **person working through it** and the **client** (private individuals or businesses). In certain instances, a fourth party could also be involved, for example restaurants that deliver food.

Digital labour platforms usually define themselves as intermediaries and characterise the relationship between the parties as one of self-employment. Tasks performed on digital labour platforms can vary from complex tasks such as computer programming and graphic design, to simple tasks such as tagging images.

The Commission President Ursula von der Leyen announced in her Political Guidelines the need to improve working conditions in platform work[95]. This has been further highlighted by the COVID-19 crisis and the accelerated uptake of platform business models. A recent European Parliament resolution[96] stresses that platform work has raised concerns about precariousness and poor working conditions, lack of or difficult access to adequate social protection, fragmented and unpredictable income, and a lack of occupational health and safety measures. It calls for strong EU action to address employment status misclassification and improve transparency in the use of algorithms, including for workers' representatives.

7.1 Situation and actions at Member State level

In order to prevent unfair competition to the detriment of workers and a race to the bottom in employment practices and social standards, the EU has created a minimum floor of labour rights that apply to workers across all Member States. The EU's body of law concerning labour and social affairs has grown throughout the years. In addition to that, national responses to the challenges posed by platform work differ across Member States. Some have adopted national legislation to improve working conditions or access to social protection in platform work. Courts have ruled on the issue of misclassification of the employment status in a substantial number of Member States. In some Member States social partners and platform companies have engaged in negotiations on collective agreements.

In 2016, **France** adopted legislation providing for labour and social rights for people working through platforms irrespective of the sector of economic activity, by means of revising the Labour Code. The law applies to technologically and economically dependent self-employed individuals. It grants access to a voluntary insurance scheme against work-related accidents, obliges platforms to pay insurance premiums or provide collective insurance for their workers, and guarantees the right to take collective actions and to further pursue education. In addition, the highest court for private labour issues (Court of Cassation) stressed in two rulings that platform workers in the area of ride-hailing must be recognised as having worker status where the platform can make and enforce instructions[97]. However, there continues to be debate over the actual status of people working through platforms, also in other sectors.

[95] COM(2021) 762.
[96] European Parliament resolution of 16 September 2021 on fair working conditions, rights and social protection for platform workers – new forms of employment linked to digital development (2019/2186(INI)).
[97] Take Eat Easy (18 November 2018, case 17-20.079) and Uber (4 March 2020, case 19-13.316).

The region of Lazio in **Italy** enacted legislation[98] in 2019 to improve working conditions and social protection for all platform workers irrespective of their employment status. This legislation comprises safeguards for work-related accidents, adequate safety training and liability and accident insurance. It also forbids payment per task. In addition, in 2019, Italy adopted national legislation to improve working conditions of self-employed food delivery riders[99]. Moreover, in July 2021, the Italian data protection authority ordered Deliveroo Italy to pay a fine of EUR 2.5 million due to non-transparent use of algorithms and disproportionate collection of workers' data. The authority found violations of some provisions of the General Data Protection Regulation and national privacy legislation, the Italian Workers' Statute and the above-mentioned legislation protecting the workers[100].

Spain adopted legislation in May 2021, introducing a presumption that people working through platforms in both food and parcel delivery are deemed workers, shifting the burden of proof to the platforms to show that they are not[101]. Moreover, this law obliges platforms to provide trade unions with information on algorithmic management, including digital monitoring of performance and automated allocation of assignments. This law stipulates that all companies (not only delivery platforms) must inform their workers about the parameters and rules on which automated systems, that may affect working conditions, access to and maintenance of employment, are based.

Germany published policy papers on the future of work, concerning the inclusion of self-employed individuals engaging in platform work in pension and insurance schemes, and upgrades to their work-related accidents insurance.

In November 2020, **Portugal** also published a policy document on the future of work, related to the creation of a legal presumption on the status of people working through platforms, ways to augment social protection for the self-employed and ways to foster collective representation of platform workers. In 2018, Portugal adopted legislation on individual paid transport of passengers, setting limits on working time for drivers[102].

7.2 A common EU approach

In the light of national approaches being developed to address different challenges related to platform work, there is a risk of fragmentation between different national legislative initiatives. The Commission has identified a number of challenges in platform work and has consulted the European social partners in two stages on the need for an initiative on platform work and its possible direction. European social partners concurred on the challenges to be addressed but differed on the need for concrete action at EU level. In addition, the Commission held exchanges with many stakeholders, including dedicated and bilateral meetings with platform companies, platform workers' associations, trade unions, Member States' representatives, experts from academia and international organisations and

[98] Regione Lazio, Legge Regionale 12 aprile 2019, n.4, available online.
[99] L. 2 novembre 2019, n. 128, Conversione in legge, con modificazioni, del decreto-legge 3 settembre 2019, n. 101, available online.
[100] Italian DPA decision, available online.
[101] Royal Decree-Law 9/2021 of 11 May, available online.
[102] Lei n°45/2018 Regime jurídico da atividade de trasporte individual e remunderado de passageiros em veículos descaracterizadosa partir de plataforma electrónica. Available online.

representatives of civil society[103]. The Commission has proposed a directive to improve working conditions for platform workers at the EU level by ensuring correct determination of their employment status, by promoting transparency, fairness and accountability in algorithmic management in platform work and by improving transparency in platform work, including in cross-border situations, while supporting the conditions for the sustainable growth of digital labour platforms in the Union.

8. Supervising digital surveillance

Data protection and privacy are key fundamental rights in the digital age. They are also 'enabling' rights that facilitate and increase the protection of other fundamental rights that can be affected by state or private party surveillance, such as human dignity, the freedom of expression, freedom of thought, conscience and religion or freedom of assembly, the right to a fair trial and an effective remedy or non-discrimination. The General Data Protection Regulation (GDPR), the Law Enforcement Data Protection Directive and the ePrivacy Directive have put Europe at the forefront when it comes to protecting fundamental rights online. The increasing digitalisation in all areas of life poses challenges for data protection and for private and family life. Other legislation, such as the Data Governance Act, on which political agreement between the co-legislators has been reached recently, aim to foster the emergence of a strong data economy by regulating data intermediary services, data altruism and the re-use of protected public data, in line and compliance with the data protection regime.

What is the relation between the rights to privacy and to data protection?

They are separate but overlapping fundamental rights, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights.

- Respect for private and family life (privacy) protects the private sphere against unlawful intrusions. For instance, the confidentiality of interpersonal communications as well as the users' electronic terminal devices against unauthorised intrusions are protected under this right.

- 'Data protection' applies only when personal data are being processed either by automated means or in manually structured form. The right is not limited to the information relating to one's private sphere but covers any personal data of an individual, including on their professional life. Cornerstone principles of data protection is the transparency, fairness and lawfulness of personal data processing activities. Data protection also means that personal data should be processed only for specified and explicit purposes, they should be accurate, limited to what is necessary and kept safe and only for as long as necessary.

In practice, the strong EU legal framework is constantly put to the test. Consumer organisations and CSOs focusing on fundamental rights deplore a lack of enforcement in

[103] See Annex A.3.1 of the Impact Assessment report accompanying the proposal for a Directive on improving working conditions in platform work, SWD(2021) 396 final.

cases of GDPR infringements[104]. In recent years, the EU and the Member States have adopted a number of measures to safeguard public security and to address security challenges making use of modern technology. In this context, concerns are voiced by civil society organisations about the proportionality of surveillance and security policies, for example on the monitoring of the EU borders[105], or in the case of enacted or proposed legislation that would allow authorities to scan private communications for security purposes[106]. Civil society and industry organisations have also expressed worries about what they perceive as attempts by the Member States to weaken encryption[107].

DPAs and national courts ensured an effective remedy wherever surveillance measures both by private and public actors constitute a breach of fundamental rights. Examples of this are: (i) the Swedish DPA's decision on the use of body-worn cameras by ticket inspectors in Stockholm public transport, which criticised the lack of transparency and excessive data collection, resulting in a fine of SEK 16.1 million[108]; or (ii) France's *Conseil d'Etat* (Council of State) deciding that the police had to stop using drones to check whether social distancing rules were being observed, because these drones had the technical capacity to identify individual people and were not used in compliance with data protection law[109].

The proposed European Digital Identity Framework will offer every EU citizen and resident on a voluntary basis a trusted and secure digital wallet under full user control as a 'self-sovereign' enabler of access to digital public and privates services and to share a variety of attributes and credentials.[110]

8.1 Data retention

Since 2014, national laws providing for the retention of telecommunications metadata (traffic and location data) for law enforcement and intelligence purposes have been found not to meet the requirements of EU law by the Court of Justice of the EU. The Court has considered these national laws to constitute a serious and disproportionate interference with the rights to privacy and data protection because communication metadata may reveal information on a significant number of aspects of the private life of persons concerned[111]. While recognising

[104] E.g. 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 and https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf

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

[106] See for example https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf or https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/

[107] See for example https://www.statewatch.org/news/2020/november/eu-council-set-to-adopt-declaration-against-encryption/ or 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_grundsatzerklarung-verschlusselung_0.pdf auto&utm_medium=email&utm_campaign=Encryption%3A+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption

[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

[111] See for example Judgment of 2 March 2021, Prokuratuur, case C-746/18 ECLI:EU:C:2021:152.

that data retention measures pursue legitimate public interest objectives, the Court has often found that, with some exceptions[112], EU law precludes legislative measures which impose on providers of electronic communications services, as a preventive measure, an obligation requiring the general and indiscriminate retention of traffic and location data. In the **EU Strategy to tackle Organised Crime 2021-2025** of 14 April 2021, the Commission announced that it would analyse and outline possible approaches to data retention aligned with the Court's judgments to respond to law enforcement and judiciary needs in a way that is operationally useful, technically possible and legally sound, including by fully respecting fundamental rights, and to consult the Member States before the end of June 2021. The Commission is currently in a consultation process and will carefully consider the results of that consultation before taking a decision on the possible way forward.

8.2 Encryption

Encryption is essential for protecting fundamental rights and securing systems and transactions. EU legislation provides for encryption as a measure to ensure protection for fundamental rights such as privacy, protection of personal data,[113] and freedom of expression, as well as to ensure cybersecurity[114]. Furthermore, encryption is also important for the protection of business secrets and thereby helps people benefit from their right to conduct a business. Since the Covid-19 pandemic began, along with the growing use of digital tools in all areas of life, the number of cyberattacks has increased. Such attacks have caused major damages to companies and critical services, including healthcare systems, and have jeopardized people's rights, highlighting the importance of encryption for public and private actors since it protects the confidentiality of information[115].

However, the use of encryption also allows criminals to mask their identity and hide the content of their communications. Following calls from the Member States, the Commission committed to explore balanced technical, operational and legal solutions to these challenges. These solutions need to maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism[116]. The Commission intends to suggest a way forward in 2022 to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions that shall be based on a thorough mapping of how Member States deal with

[112] See Judgment of 6 October 2020, La Quadrature du Net and others, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, where the Court the allowed general retention of traffic and location data to safeguard against serious threats to national security, of IP addresses assigned to the source of a communication to combat serious crimes, and of civil identity data to combat crime in general.
[113] Article 32(1a), 34(3a), 6(4e), recital (83) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; recital (60), article 31(3a) of the Law Enforcement Directive; recital (20) in conjunction with article 4 of the ePrivacy Directive 2002/58/EC.
[114] Article 40(1) European Electronic Communications Code and recital (96); recital (40) of Regulation (EU) 2019/881 (Cybersecurity Act).
[115] The European Data Protection Board (EDPB) adopted its Guidelines 1/2021 on Examples regarding Data Breach Notification (version for public consultation). Encryption plays an important role in minimising the risks of personal data breaches.
[116] The commitment is part of the Security Union Strategy of July 2020.

encryption together with a multi-stakeholder process to explore and assess the concrete options (legal, ethical and technical)[117].

8.3 Remote biometric identification

EU data protection rules prohibit in principle the processing of biometric data for the purpose of uniquely identifying a natural person, except under specific conditions[118]. The processing of such data must have a legal basis grounded in data protection legislation. Such a legal basis could be the freely given consent of all people concerned, which is difficult to obtain in practice, or alternatively an EU or Member State law that pursues a substantial public interest, such as the prevention of a concrete and immediate threat of a terrorist attack. In the area of law enforcement, the processing shall be authorised by law. When processing of biometric data is based on law, then this law must be proportionate to the aim pursued, respect the essence of the right to data protection and other fundamental rights and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the people concerned.

CSOs voiced concerns over the increasing use of remote biometric identification technologies in several Member States and have called for a ban of their use[119]. The use of remote biometric systems has also been criticised by the European Data Protection Supervisor, the European Data Protection Board comprising the national data protection authorities (DPAs)[120], and other national fundamental rights bodies such as the *Defenseur des Droits* in France[121]. There are a number of examples where data protection authorities intervened to stop unlawful use of such technology, for example in a school in France, by the police in Sweden, or by a Dutch supermarket[122].

In addition to the existing framework, the AI Regulation that the Commission proposed in April 2021 (see chapter 4) includes a prohibition of real-time remote biometric identification in publicly accessible places and allows it for law enforcement purposes in three limited exceptions and under the condition that specific safeguards apply[123].

[117] Organised crime strategy, adopted on 14 April 2021.
[118] See Article 9 of the General Data Protection Regulation and Article 10 of the Law Enforcement Data Protection Directive. Under the GDPR, such processing can only take place on a limited number of grounds, the main one being for reasons of substantial public interest. In that case, the processing must take place on the basis of EU or national law, subject to the requirements of proportionality, respect for the essence of the right to data protection and appropriate safeguards. Under the Law Enforcement Directive, there must be a strict necessity for such processing, in principle an authorisation by EU or national law as well as appropriate safeguards.

[119] https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/ and 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/communique-de-presse/2021/07/technologies-biometriques-la-defenseure-des-droits-appelle-au-respect
[122] NL DPA: Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology | European Data Protection Board (europa.eu); SE DPA fine to the police for the use of Clearview Sweden fines police for illegal facial recognition tech use - POLITICO Pro FR DPA on the use of biometric recognition at schools: French privacy watchdog says facial recognition trial in high schools is illegal - POLITICO Pro
[123] Article 5(1)(d) of the Proposal provides that such use must be strictly necessary for (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; or (iii) the detection of perpetrator or suspect of a criminal offence referred to in the European Arrest Warrant (EAW) and punished in

8.4 Education

During the COVID-19 pandemic, education and training institutions used different online platforms and tools. Often implemented as 'quick fixes', the use of commercial digital learning solutions and software to monitor students taking exams remotely, gave rise to the concern that their design might leverage user data for profitmaking, rather than meaningful pedagogical practices.

The European Digital Education Hub, set up under the Digital Education Action Plan, is a forum to develop measures to ensure stronger cross-sectoral collaboration, promote exchange between educators, develop means for quality assurance and ensure respect for data protection and privacy. Among those quality assurance and trust will play a crucial role: the former to promote a shared understanding of key quality standards for digital education; the latter to ensure respect of key principles regarding data use, ethics and privacy. These two elements, besides boosting the level of digital preparedness of Europe's education and training institutions, can increase the cooperation improve the overall quality of the digital solutions available.

8.5 Health

Many parts of the **response to the COVID-19 pandemic** involve the processing of personal data, including health data, which due to its sensitivity is subject to further rules under the GDPR. Processing of personal data has to be limited to what is necessary and proportionate to achieve the aim and comply with the requirements of GDPR. This has guided the EU's approach. For example, the Commission has provided guidance[124] to Member States on apps to fight the pandemic, and supported their work on a toolbox with requirements for apps[125] and technical specifications for the interoperability[126] between national warning apps in the EU. The Commission has set up a gateway to allow such warnings to be sent across borders and between the different Member States' applications. The Commission has also put forward a platform for the exchange of data from passenger locator forms[127] to support cross-border contact tracing in transport settings. As a next step, it committed to propose an EU legal framework for a coordinated approach to recording recent travel history to the extent necessary to stem the spread of COVID-19, building on the experience of passenger locator forms.

Furthermore, the European Parliament and the Council adopted, on 14 June 2021, a Regulation establishing the EU Digital COVID Certificate system, which aims to facilitate free movement during the COVID-19 pandemic[128]. An infrastructure was established supporting the issuance and verification of vaccination, test, and recovery certificates, to streamline the checking of public health measures when travelling (e.g. for exemptions from quarantine requirements). For ease of use, the certificates are available both in digital and

---

the Member State concerned for a maximum period of at least three years. The use is also subject to authorisation by a judicial or other independent body and to appropriate limits in time, geographic reach and the data bases searched.

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

[125] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.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/EN/TXT/?uri=CELEX%3A02017D0253-20210726

[128] http://data.europa.eu/eli/reg/2021/953/oj, accompanied by https://eur-lex.europa.eu/eli/reg/2021/954/oj

paper-based formats. In all cases, the data categories and the processing are limited to what is necessary for the purpose at hand, for example, those who verify the certificates are prohibited from keeping their content after verification. Furthermore, the trust framework set up for the EU Digital COVID Certificate ensures that the certificates can be verified in an offline manner, without the issuer or any other third party being informed about the verification. Transparency is always key, both to ensure legal compliance with the Charter and applicable legislation, and to create and maintain trust. The outcome shows that when measures are carefully designed, data protection is consistent with and can help promote acceptance of effective public health measures and ensure that the EU data protection framework provides the required flexibility.

The Commission is currently preparing a legislative proposal on the **European Health Data Space (EHDS)**, which is expected to be adopted at the beginning of 2022. The EDHS aims to facilitate the provision of digital health services and at promoting access to health data for research, innovation, policy-making and regulatory activities, while further improving the control that people have over their personal data. The EHDS initiative will fully comply with the applicable EU data protection rules.

8.6 Enforcement

Competent national supervisory authorities for the monitoring and enforcement of data protection and privacy rules are the cornerstone of the governance system for EU data protection. These authorities and national courts are responsible for monitoring and enforcing the rules under the GDPR, national laws transposing the Law Enforcement Data Protection Directive[129] and the ePrivacy Directive. For the Commission, one of the key objectives is that Member States implement those rules correctly and effectively. Member States have an obligation under EU law to ensure their data protection authorities are independent and to allocate them with sufficient resources to carry out their supervisory tasks[130]. The Commission follows the developments concerning the independence, tasks, powers and resources of supervisory authorities and in the case of non-compliance with EU rules by Member States, resorts to infringement proceedings to ensure these rules are enforced effectively.

Data protection authorities work together within the European Data Protection Board (EDPB) to ensure consistency in enforcing the GDPR, in particular in cross-border cases. After 3 years of applying the GDPR, the effectiveness of this cooperation has attracted criticism[131], and the EDPB will continue its work to increase efficiency[132]. The Commission shares the view of the Council[133], the European Parliament and the EDPB[134] that the focus must now be

[129] http://data.europa.eu/eli/dir/2016/680/2016-05-04
[130] EDPB overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions buy the Data Protection Authorities of 5 August 2021, published on 11 August at https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf
[131] See e.g. European Parliament resolution (2020/2717(RSP)).
[132] 2021-2023 EDPB strategy, adopted on 15 December 2020, at edpb_strategy2021-2023_en.pdf (europa.eu).
[133] Council position a findings on the application of the General Data Protection Regulation (GDPR) – Adoption, 14994/1/19 REV 1, 19 December 2019 at pdf (europa.eu).
[134] EDPB Annual report 2020, 2 June 2021, at EDPB Annual Report 2020 | European Data Protection Board (europa.eu).

on improving implementation and on actions to strengthen the enforcement of EU data protection law.

8.7 Protecting personal data beyond the EU

An essential aspect of protecting fundamental rights in an online environment lies in ensuring continuity of protection for individuals when their data leaves the EU. As personal data moves easily across borders in today's interconnected world and data flows have become an integral part of trade, regulatory cooperation and even social interaction, the protections guaranteed by the GDPR and the Law Enforcement Directive would be ineffective if they were limited to processing inside the EU.

Against that background, the Commission continued to pursue its ambitious agenda aimed at promoting a high level of protection when the data of Europeans is transferred abroad, while, at the same time, facilitating data flows. This included engaging with key partners to reach an 'adequacy finding', which establishes that a non-EU country provides a level of data protection that is 'essentially equivalent' to that in the EU. This yielded important results, such as the adoption of two adequacy decisions for the United Kingdom (under the GDPR and the Law Enforcement Directive) and the conclusion of adequacy talks with South Korea.

Furthermore, following the invalidation of the earlier adequacy finding on the Privacy Shield by the Court of Justice, the EU and the U.S. have intensified negotiations on a new EU-U.S. privacy framework for transatlantic data transfers that ensures full compliance with the judgment of the Court.

In addition, in June 2020, the Commission adopted modernised standard contractual clauses for the transfer of personal data to non-EU countries, which reflect new requirements under the GDPR and are adapted to the needs of the modern digital economy. These are model data protection clauses which a data exporter and data importer can – on a voluntary basis – incorporate into their contractual arrangements (e.g. a service contract requiring the transfer of personal data) and that seek to ensure appropriate data protection safeguards.

The Commission also continues its involvement in a 'Data Free Flow with Trust' initiative, launched by Japan in 2019 and subsequently endorsed by the G20 and the G7. One central part of this concept, currently discussed at the OECD with the active participation of the EU and its Member States, is to draw a line between legitimate government access, with appropriate limitations and safeguards, and abusive state surveillance.

9. Joining forces to make the digital age an opportunity for fundamental rights

Looking at the interrelated challenges and the corresponding measures examined in this report, there is no doubt that the EU and its Member States are committed to protecting and promoting fundamental rights in the digital age and that they are working together to identify the best ways to do so. The examples mentioned in the preceding chapters are some of many opportunities to learn from one another and to shape the changes brought about by the digital transition in a positive way.

The Commission uses many tools to ensure the rights enshrined in the Charter are respected – both in the design of its legislative and policy initiatives as well as when enforcing EU law. In particular, the Commission will closely assess the effects on fundamental rights and aim to balance those effects in the upcoming Commission initiatives in 2022, such as legislative proposals on:

- a right to repair,
- cyber resilience,
- digital mobility services,
- instant payment,
- reciprocal access to security-related information for frontline officers between the EU and key non-EU countries,
- a Media Freedom Act, and
- binding standards for Equality Bodies.

Furthermore, in the context of the Digital Decade, the Commission will propose to include a set of digital principles in an inter-institutional solemn declaration between the European Commission, the European Parliament and the Council. This declaration will inform users and guide policy makers and digital operators about the European way to the digital transformation.

The Commission calls on the European Parliament, the Council and Member States to use this Annual Report on the Application of the EU Charter of Fundamental Rights to engage in exchanges about the challenges and opportunities for protecting fundamental rights in the digital age. It welcomes the Council's commitment to exchange views based on the Commission's reports[135] and would also welcome a discussion in the European Parliament. In particular, these exchanges could help to better address the challenges ahead, in particular the fight against hate speech and disinformation, how to ensure checks and balances on surveillance measures, and more generally how to effectively enforce laws to protect fundamental rights in the digital environment. These exchanges can help frame policy developments in a constructive and beneficial way.

These joint efforts to render the Charter effective in the digital age, together with the European Democracy Action Plan[136] and the European rule of law mechanism[137], illustrate the EU's commitment to promoting and protecting the values on which it is founded.

[135] Council conclusions on strengthening the application of the Charter of fundamental rights in the EU of 8 March 2021, paragraph 26.
[136] Commission Communication on the European Democracy Action Plan, COM (2020)790.
[137] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism_en