Group of the Progressive Alliance of
Socialists & Democrats
in the European Parliament

European Parliament
Rue Wiertz 60
B-1047 Bruxelles
T +32 2 284 2111
F +32 2 230 6664
www.socialistsanddemocrats.eu

Our Inclusive Digital Europe

Leaving Nobody Behind
Offering Opportunities for Everyone

Table of contents:

Introduction

The accelerating **digital transition of Europe's societies brings along many new opportunities**. Concrete examples range from addressing epidemic diseases and improving medical diagnostics to reducing traffic and workplace accidents, allowing for telework and ICT-based mobile work or increasing system-wide energy efficiency. It will therefore have a considerable impact on people's lives, with the **emergence of new rights and increased efficiency** that the internet and overall digitalisation allow for and blurring the lines between the physical and the virtual world. Such digital transformation encourages us to rethink our social and economic models in line with our social-democratic values.

At the same time, the **growing digitalisation of products and services**, both private and public, presents some challenges, namely job losses due to the automation of tasks and processes. Therefore, throughout this transition, the S&D Group will stand up for all those facing the consequences of digitalisation, in particular vulnerable groups such as **workers, consumers and children**, to ensure that no one is left behind. In particular, it will fight to **defend quality employment**, preventing it from deteriorating and leading to precariousness caused by a strong downward pressure on wages and the spread of bogus self-employment, thereby contributing to the rise of overall social inequality. Accordingly, among other measures outlined in this position paper, we need to insist on **extra financial commitments** at EU level to guarantee **a strong role for workers and their union representatives** at all stages during this transition process.

Moreover, a **just and inclusive transition** means the **respect of fundamental rights**, public investment and support in strategic sectors to ensure green and digital progress for all. It also means **education** (including at elementary and high school level) **and training policies**, instruments on the anticipation of change and restructuring, the guarantee of strong and **effective social protection** systems, and must ensure that such interventions and opportunities are extended to the most remote communities and **promote gender equality**.

We need to develop a **new social contract** by ending and reversing hyper-privatisation and, if necessary, **bringing key sectors and their profits back into public ownership**. This may specifically apply in cases of new digital sectors, which have major societal impacts.

The different crises Europe has faced in recent years have harshly exposed a growing **digital divide between people**. It has also shown the **gap between regions and between urban and rural areas**, highlighting the economic and geographic difficulties that certain territories have in order to deploy technologies and improve their connectivity standards.

As addressing **the digital divide is a key priority for the S&D group**, we believe that initiatives such as the Digital Decade Policy Programme can contribute to achieving a **cohesive digital transformation** of European society by 2030.[1] This should be achieved whilst keeping in mind the need for **tailor-made solutions adapted to the characteristics of every territory** and using the best from existing financial instruments.

[1] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

Ultimately, we believe that digital transformation can work for all. This is why we see equal access to the **Internet as a fundamental right** and believe that digitalisation can contribute to ensuring **inclusive public administration**. To that end, we must promote **sustainable digital policies that empower citizens and businesses, making the EU more competitive,** creating **new opportunities for all**, notably by securing the necessary investments and establishing a governance framework based on cooperation mechanisms to reach targets in digital skills, digital infrastructures, digitalisation of businesses and public services.

Lastly, our political family has significantly contributed to the negotiations of the **European Declaration on Digital Rights and Principles for the Digital Decade**, intended to serve as a guiding reference of the EU's approach to the digital transformation.[2] The **S&D Group has covered many important issues of the progressive agenda**, from the impact of AI on worker's rights, the gender dimension of the current transition or the need for high-quality digital education and training, to the protection of media freedom and pluralism, and privacy against disinformation or profiling. We have thus made sure that those **digital rights and principles safeguarded in the EU leave no one behind and offer opportunities to everyone**.

[2] European Declaration on Digital Rights and Principles for the Digital Decade, 15.12.2022.

1. The social dimension of the digital economy

Nobody should be left behind across the EU

The ongoing digital transition should lead to societal progress, be inclusive and **not lead to a** '**race to the bottom'** with regard to labour and social standards. It should, moreover, **reinforce democracy**, reduce gaps and increase the quality of public services. Technology is a paradigm of opportunity to enhance equality in line with European ethical and human-centric standards and values. It should involve and generate opportunities for everyone, in particular the most vulnerable, through a fair sharing of the profits and prosperity that it generates. It must contribute to socially sustainable development, while striking a balance between economic, ethical and environmental considerations. The European Pillar of Social Rights and the Social Acquis apply to all actors in the offline and online economy and must be implemented and enforced. **Precarious work and new forms of "dumping" are not acceptable.**

We do not yet know if jobs created through new technologies will make up (at least in the medium-term) for those lost, and this uncertainty represents **a considerable social risk**. **The European Digital Agenda must therefore have a strong social dimension**. New types of employment and platform work could offer a **better work-life balance** with improved productivity, additional income and new chances for people not currently within the labour market, as well as be an **instrument to close the gender pay gap**. However, this can only be achieved through adequate regulation and if workers are strongly organised, covered by collective agreements and have their rights protected. With the right policies in place, people can work in **safer environments** with more meaningful tasks. Yet, for the time being, such new working arrangements in the platform economy are often undermining social and employment standards, thus giving rise to precarious forms of employment, labour exploitation and tax fraud that mainly disadvantage vulnerable groups.

New forms of employment

European labour markets are evolving towards 'atypical' or 'non-standard' forms of employment such as occasional work, work on-demand or work intermediated by digital platforms. These new forms of work generally offer poorer working conditions and less protection than traditional employment as they circumvent the application of labour law and labour rights. This may lead to, amongst other things, abuses in working time, lack of social protection and increased fundamental rights, health, safety and occupational risks – especially affecting people who have more difficulty entering the labour market.

Employment and social policies must keep pace with the digitalisation of labour markets. The European Commission's Digital Single Market Strategy, however, has largely disregarded the social dimension of the digital economy and its impact on the life and work of Europeans.

New technologies and **digital trends should benefit all** and contribute to the eradication of social and gender inequalities and discrimination. They should promote the creation of new quality jobs, improving working conditions, providing new opportunities and better-quality local services not least in rural areas, usually the least

well connected. Decent working conditions, professional training (as well as personalised learning pathways) and social protection should be universally available to all working people.

We have been calling for action in this context for a very long time, and in 2021, the European Commission finally proposed a **Directive for improving working conditions in platform work**. We will ensure that this Directive protects the rights of platform workers irrespective of their type of employment or where they are located in the EU.

Minimum wage and social security

The "platformisation" of work is taking place across various sectors of the labour market, of which platform workers form only one part. The EU should therefore take a more **holistic approach towards the future of work and new atypical forms of work**. Some platform workers are driven by a need for additional income (though, importantly for some, these jobs are the main or only source of income) and this fact demonstrates a need for policies to boost people's income from their main job. Therefore, the establishment of **minimum wages and the strengthening of collective bargaining across Europe** are directly linked to the question of the future of work in the digital economy.

Member States and the European Commission must ensure adequate social security for genuinely self-employed people, who are key players in the digital labour market. Adequate social protection coverage of all workers on these platforms as well as non-discrimination and gender equality should be ensured.

The Commission must, consequently, live up to its commitment and present a proposal for a **European Social Security Number (ESSN)** without undue delay. Such an instrument with real time secure data-access and verification would allow the competent national authorities to verify social security coverage for workers at any given point in time and thereby considerably facilitate labour inspections and enforcement of social security coordination. It would guarantee the rights and entitlements of mobile workers in general, and posted workers in particular. It would also make it easier for workers to track their social security contributions and entitlements. Furthermore, it would not only help Member States to hold companies to account for avoiding decent remuneration or social security contributions, but it could also contribute to combatting undeclared work, unsafe work environments or unacceptable working conditions and wages.

AI at the workplace

In general, we advocate for **dignity at work and quality working conditions**. This means that decisions that have an impact on fundamental rights, working conditions, health and safety or on contractual relationships, including their suspension or termination, are only taken by humans and not by automated or semi-automated monitoring and decision-making systems. In addition, the features of automated or semi-automated monitoring and decision-making systems which have an impact on working conditions shall always be the object of collective bargaining and collective agreements between trade unions and employers.

Flexibility and self-determination of new working models in the digital age must not become a synonym of disguised exploitation and **surveillance of workers' performance**, especially in the context of the development of Artificial Intelligence (AI). **AI solutions in the workplace** must respect fundamental rights, be ethical and human-centric, transparent, fair and avoid any negative implications for workers.

We must stop surveillance capitalism! It is critically important to make sure that respect for workers' fundamental rights in the digital environment, including their right to privacy, data protection and protection against pervasive surveillance in any use of digital tools, are respected at their work place. This is why we call on the European Commission to urgently present a Directive to **regulate the use of AI technologies at the workplace** that includes safeguards against the adverse and unethical impacts of algorithmic management on the fundamental rights, health and safety of workers and make the involvement of trade union representatives mandatory in the process.

Biometric surveillance, tracking apps that monitor workers both online and offline, rating mechanisms as well as recruitment discrimination based on algorithms or employment screenings services in breach of data protection represent dangerous and non-efficient trends which have to be urgently addressed. Devices like microchip implants for workers must be entirely banned, as well as software which tracks keyboard or mouse use on remote work.

In order to prevent discrimination in recruitment or at the workplace, there should be a ban on the access, collection or processing of any personal data falling under the scope of Article 9 of the General Data Protection Regulation (hereinafter "GDPR").[3] For example, data revealing racial or ethnic origin, gender, political opinions, religious or philosophical beliefs, disability or state of health, trade union membership, sexual orientation or health status.

Lastly, the EU could consider the creation of an adjustment fund to support Member States in adapting their labour markets to the rapid mass introduction of AI systems that is disrupting specific job sectors.

The right to disconnect and the role of social partners

For the sake of promoting decent working conditions, work-life balance and physical and mental well-being, the S&D Group has called for the **right to disconnect** outside established working hours. We must further examine the different risks that undue additional working time poses to workers. The EU should strive for a mandatory minimum level of disconnected time per day, week and month – a goal as needed today as the establishment of an 8-hour working day. In addition, workers should be compensated or provided with the necessary equipment, utilities, and space to perform their work, in remote mode, in full respect of health and safety requirements.

We need to **strengthen the role of social partners** within the labour market, including with regards to collective bargaining and collective agreements. These require a high degree of membership rate. The EU should give priority to strengthening the ability of workers to organise themselves and, if possible, provide financial incentives or other stimulating measures. In addition, we call for an exclusion of

[3] 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).

individual platform workers from anti-cartel-measures in order to allow them to exercise their fundamental rights to association, collective bargaining and collective action.

Addressing the digital gap and guaranteeing accessibility

The EU must guarantee that the digital services offered by companies are inclusive and can be understood, accessed and used by people of any age, ability, and education level and geographical location in the EU. This will avert the deepening of gaps in our societies maintained by unequal access to technology, especially between generations and between rural and urban areas, particularly when it comes to the upcoming 5G deployment within the EU. We must ensure that **nobody is left behind**. There are still areas and regions in Europe where internet connectivity is limited or non-existent, as well as considerable disparities across Member States as regards access to high-speed internet connection, often affecting rural areas or regions suffering from depopulation, further aggravating such demographic challenges and increasing economic decline. The S&D defends **secure and high-quality internet connection as a universal right** that would justify a social-tariff scheme meant to support its affordability, thereby mitigating new forms of "digital poverty".

Digital connectivity is a key element to address and can possibly reverse these negative trends, since it can reduce the gap between densely and scarcely populated areas. The **EU should urgently address the existing digital divide** and analyse the impact of digital technologies on the depopulation phenomenon in the context of rural-proofing all policy areas and via a modernised cohesion policy. Strategic decentralisation of investments across the EU should become a key principle in this context.

Approximately 80 million Europeans suffer from some kind of disability. New technologies must contribute to **closing the digital gap for persons with disability.** We must support their inclusion in the economy and ensure their access to essential services, including by adapting services' availability to their needs. The use of digital technologies can reduce the barriers which persons with disabilities face to enter the job market, such as completing work tasks, communication, interactions or flexibility.

Digitalisation should also make a positive impact on **people with reduced mobility**, including the elderly. While the European Accessibility Act of 2019 has taken into consideration the digital agenda, its enforcement at national level should be carefully monitored, in line with the European Disability Strategy for 2020-2030.

Transforming public services and public administrations in the EU through digitalisation will be crucial. **High quality digital public services** should be used to increase **equal and easy access** for all. The possibility to vote electronically in elections, for example, will improve equality and accessibility of our democracies. At the same time, access to public services for those who do not wish to use services via digital means cannot be denied, hindered or made more costly. The goal of digitalising public services should go beyond the digitalisation of administrative procedures. It implies redesigning public services and the way we deliver them, and using interoperability to improve their efficiency.

2. Digital education, skills and literacy: towards an inclusive and democratic transition

A new digital culture

All Europeans need the necessary education, understanding and skills to fully embrace the opportunities of the digital transition, as well as to responsibly manage digital tools such as AI, data and media in everyday life and protect their rights. The promotion of a **"digital culture"** will allow for active citizenship; democratic control in the digital world should support specific national initiatives on **digital education, training, obtaining of digital qualifications and the recognition of digital competences**.

To this end, education systems at all levels across the EU, whether public or private, must be fit for purpose and the EU budget should support specific national and European initiatives on digital literacy through education, hybrid learning, training, upskilling and **reskilling of every citizen, and in particular educational staff and workers.** Ensuring that **free access to digital education** is possible in every school and every region of the EU - and in particular, the availability of skilled educational staff, modern digital equipment, connectivity and tools - must be a key priority in line with the 2030 digital decade targets.

We need new education programmes with an approach to learning that uses **STEM** - Science, Technology, Engineering, Arts and Mathematics - in order to support the development of adequate digital literacy, skills and tools and prevent brain drain in some regions. **Education** should not be oriented solely towards the immediate labour market's needs, as it **should support the personal development and critical thinking of every individual**, including in the arts, to promote creativity, innovation and personal development. This is especially relevant for children and adolescents, and particularly **women, whose participation and involvement in digital education** and specialised ICT programmes must be prioritised in order to advance gender equality across all value chains in the digital sectors.

New learning formats and media competence

A broad variety of digital means and **new learning formats** should be used, respecting children's developmental needs and the latest pedagogical consensus on the limits, risks and benefits of digital learning. Therefore, distance and blended learning must be seen as an accompanying tool on all educational levels, but never substitute face-to-face education provided primarily in a physical setting.

AI can play a support role in education systems, namely in the use of interactive technologies or by facilitating access to education by children in special circumstances like, for example, those living in remote areas or experiencing longer periods of hospitalisation. To this end, **digital education curricula** should promote active citizenship and **people's interaction with AI on all levels** - from basic schooling to university, research and innovation. Education must be categorised as a high-risk area for regulatory purposes, and e-proctoring and other AI tools such as those for enrolment assessments of educational institutions should be treated accordingly.

Young people's media competence is essential to ensure that they are able to distinguish facts from opinions. They should understand the opportunities and risks of the technologies they are presented with, including the impact of digitalisation on mental health and how to act against cyberbullying and online harassment. Media and digital competence should be enshrined on all educational levels and for all generations.

Re-skilling and vocational training

Facilitating and supporting the obtaining of digital qualifications and the recognition of digital competence of the adult workforce equally deserves special attention. **The COVID-19 pandemic has radically altered the job market, placing a greater emphasis on digital qualifications and competences and leaving behind those who do not possess them.** These digital skills and qualifications, which are constantly evolving, are now increasingly necessary for citizens to participate in society and benefit from accessible digital services. Therefore, we need solutions for the provision of free **digital literacy training for adults** on a continuous basis, and with a special focus on teachers and educational staff, taking into account existing best practices across the EU.

However, providing people with a minimum set of digital qualifications and competences will not help them to find sustainable jobs. It is crucial to ensure that every individual is encouraged to acquire advanced qualifications and competences in order to better adapt to the future. We need, therefore, to put in place **a progressive Digital Literacy and Qualifications Agenda**, in the context of 2023 European Year of Skills which would guarantee learning and training opportunities for everyone. The agenda should aim at the certification and validation of qualifications and competences providing added value to workers, improving their position in the labour market and transferable in labour market transitions. To this end, achieving the automatic recognition of education qualifications across all EU Member State - as agreed - until 2025 is of highest importance.

Europe needs to retrain workers in all industrial sectors and especially those most affected by the advent of automation and robotisation, in order to safeguard their social rights and decent living standards and to maintain the competitiveness of the European industry and economy. **Educational vocational training** programmes should also focus on developing workers skills through life-long learning and continuous qualified training, especially in the STEM field.

However, **low-income adult workers** can only afford to obtain new qualifications if a new allowance scheme is adopted with EU support in order to enable these workers to enrol in vocational training or tertiary education. In addition to having their educational costs covered, they should have a minimum income, enough to support the household during the period when the person is enrolled in the programme.

The S&D is fighting to introduce, in relevant legislation, general training and knowledge requirements promoting **AI and data literacy** of employees working directly with AI systems operating in the digital single market or with non-personal data sharing at different levels of the data economy.

Life-long learning, research and investment

Life-long learning will become increasingly important as a key factor for companies to succeed in all sectors and for workers to maintain their employability to provide the conditions for a just transition towards the digital economy.

We need a **European-wide strategy** to improve the training and obtaining of qualifications for all workers, including ICT professionals, in order to **close the digital qualifications gap**. To that end, skills-based compensation systems should be established in companies accessing public funds for retraining workers and in agreement with workers' representatives. Such a system would also ensure that there is a return on the public investment in the form of higher wages and promotions for upskilled workers.

The EU should promote the creation and expansion of digital knowledge and support the **research programmes** and networks created among European universities in order to help European businesses and entrepreneurs attract the best talent and become the vanguard of **digital innovation** worldwide. The potential of different EU regions in developing research and knowledge ecosystems to boost their economic growth and human capital whilst avoiding digital economy concentrations must be noted.

Skills shortages and mismatches can be prevented by improving and facilitating connections between the education and training systems and the needs of companies to innovate in all EU regions.

We need harmonised digital growth strategies that involve all levels of public administration, from Member states to local authorities, ensuring that "second tier" cities have the opportunity to become innovation and growth poles, boosting the EU's competiveness in a connected world. Guaranteeing all EU territories can participate in the digital economy of the future is achievable through decentralisation. Achieving these priorities through Cohesion Policy, amongst other policy instruments, is a key priority for the S&D.

We need more attention and **more investments in research & development, science and the scientific community**, which is the driving force of technological development. European entrepreneurs should not feel compelled to relocate to Silicon Valley in order to get the necessary funding to grow their businesses. EU programmes such as Future and Emerging Technologies or European Research Council should play a decisive role.

Empowerment, education and media literacy

Large **online platforms** should put more resources in **tackling bots** which are spreading disinformation, provide more detailed **information about malign actors** and troll factories, and intensify their **cooperation with fact checkers** and researchers whose independence should be undisputed beyond doubt. They should also **empower users** to better detect and flag up disinformation.

Nevertheless, fact-checkers and codes of conduct will not be sufficient on their own. The only effective cure solution for disinformation are **well-educated citizens and a pluralistic media landscape**. We need **media literacy programmes** which should be implemented across the EU and included in the educational systems. Media

literacy education can empower citizens to evaluate and critically assess the disinformation they face. Education and training, starting in primary and secondary schools, should help people obtain the skills and competences to analyse the quality and relevance of information sources, as well as address individual online behaviour (from cyber-bullying to privacy and the right to disconnect from the online learning environment).

Media freedom has long been under threat in Europe and the S&D Group is therefore determined to improve the **Media Freedom Act**[4] proposed by the European Commission to make it an effective tool against attacks on media freedom, while safeguarding what works well in Europe as well as a politically independent media oversight. It also welcomes the revised '**Code of Practice on Disinformation**'.[5] Digital transformation must be turned into a catalyst for a **European digital public sphere** that upholds media freedom and pluralism by ensuring citizens' access to media content they trust whether offline at the newsstand or online, unhindered by profit interests such as those of large online platforms located outside Europe.

Culture, new challenges and protection of intellectual property

We have to promote the introduction of new and innovative digital formats in the **creative and cultural sector** to make culture more tangible for the young by using digital tools in a positive way to encourage people embracing the European cultural diversity.

However, this will depend on the **accessibility of content** throughout the single market taking into account different interests and the cross-border demand for content while **respecting creators' rights**, including through collective bargaining and access to information pertaining to the use of their creative work.

Another challenge that lies ahead is the **regulation of the metaverse** - an immersive digital experience that can be accessed through virtual reality (VR) or augmented reality (AR) devices. Key aspects such as the enforcement of data protection, the combat against illegal, harmful content and manipulation through advertising practices, the protection of children's' privacy and safety and the respect for intellectual property (IP) rights should be addressed, and **digital literacy can and should play an important role** in this context.

Without adequate **protection of intellectual property**, there would be no innovation. At the same time, innovation brings new challenges to such protection. Technology can assist, or even replace, human artists and inventors in the creative process. New digital assets such as NFTs, with their unique form of creative work ranging from music to 3D objects or images, have also emerged. Consequently, over the past few years, the European Commission and the European Parliament have payed closer attention to the establishment and enforcement of intellectual property rights in the digital sphere. It is important to keep assessing whether the current EU legal framework is sufficient to meet the challenges brought about by these developments, and adapt it accordingly, where needed.

[4] Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU.
[5] 2022 Strengthened Code of Practice Disinformation, available at https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

3. Digital gender equality

No to gender biases and no to gender discrimination

Underrepresentation, STEM and online gender violence

Women are under-represented at all levels in the digital sector in Europe, starting as students (32% at Bachelor, Master or equivalent level) up to top academic positions (15%). The Gender Equality Index shows persistent inequalities with only marginal progress. The gap is largest in ICT specialist skills and employment. Women in ICT earn 19% less than their male colleagues.

Closing the gender gap and ensuring women can exercise their digital rights is of paramount importance. In this context, the evolution of the digital sector must go hand-in-hand with other aspects such as education, socialisation, fair working conditions, work-life balance, democracy, good governance and strong public services. **We need real equality, including in achieving high-level positions, not just employability**.

Technologies such as AI have the potential to shape gender relations. Measures must be taken to **promote equal participation of all genders** in the design, implementation, evaluation and debate on ethics and norms of **AI-powered technologies**. Reproduction and amplification of sexism and discrimination by biased data-sets, models and algorithms in AI is not acceptable and must be prevented. A meaningful inclusion of all genders at all stages should result in policies and technologies that make **digital equality a reality**. Gender-aware coding and AI that serves all and does not reproduce stereotypes and inequalities are essential!

The **participation of girls and women** in the field of science, technology, engineering, and mathematics (**STEM**) must be boosted through concrete policy action to foster their full participation and inclusion in the digital economy. At the same time stereotypes, social norms and structural inequalities that lead to discrimination against women must be urgently tackled through, for example, educational campaigns in schools.

Moreover, sexist hate speech, misogyny and online violence against women, homophobia and transphobia are on the rise. All forms of **gender-based violence** in the public and private spheres, including on social media, **must be stopped**. In this context, the ongoing work on a draft Directive which aims to criminalise various forms of cyber violence is of the utmost importance. Policy responses should be formulated in recognition of the fact that violence in the digital space is a form of violence against women as well as against other vulnerable groups such as LGBTIQ.

In the context of the **future cohesion policy**, in particular with regard to the depopulation phenomenon, it is essential to include a **gender dimension** into any future policies considering, among other factors, the limited amount of labour opportunities for women in rural areas.

4. Fundamental rights, democracy and fighting disinformation

Disinformation undermines our democracy

The Facebook/Cambridge Analytica scandal and subsequent revelations made it clear that various actors (state and non-state) are attempting to undermine the foundations of our democracy and European values. **Disinformation** and hate speech influence our democratic discourse and processes and have already affected the outcome of democratic elections. This phenomenon spreads fear and dangerously **diminishes the trust of our citizens in** institutions and **democratic processes**.

Balancing fundamental rights

Fundamental rights to freedom of expression, information and opinion, as well as to the protection of personal data and private life, **cannot be put into question**. At the same time, we need to find adequate ways to preserve those rights while containing the spread and impact of misleading or false content which could otherwise be perceived as factually correct.

Much of the misinformation and disinformation currently witnessed is linked to the lack of transparency and the commercial motives of big online platforms which we use to communicate. Therefore, **transparency for political advertising** would help address these issues, supported by measures such as clear labelling of all political advertisements; universal public repository with additional information on sponsors, funding and targeting; clear **limits on ad delivery algorithms and targeting techniques**. The adoption of the **e-Privacy Regulation** with a strong emphasis on the protection of confidentiality of communications would also be important in this context, and should be strongly supported.

When it comes to the responsibility of online platforms and social media, **self-regulation is not enough** to protect the public from attempts of interference and manipulation and we need a clear set of rules and sanctions for codes of practice to have sufficient impact in the online environment. By imposing **restrictions on content-recommender algorithms** promoting or making politically polarising content or hate speech more visible, we tackle the segmentation of the public debate and encourage plurality online. Just as we can choose in the offline world between different newspapers, we should be able to choose between different content recommender algorithms. Our group shall promote **privacy-friendly verification of online users** whilst respecting the rights to freedom of expression and information - the **EU cannot allow any form of censorship**.

Consumer trust, e-Privacy and the European Charter on Fundamental Rights

Gradually, digital surveillance and online intrusion threaten to dismantle our fundamental rights and to undermine our democratic values. The **right to private life and confidentiality of communications** is a fundamental right protected under the Charter and the current e-Privacy Directive. We must protect it in all electronic communications, content and metadata alike, **against the invasive use and abuse**

of personal data and private communications by private companies and from government surveillance**.** It is vital for our democratic values to secure the **prohibition of generalised monitoring and other forms of mass surveillance, indiscriminate identification or indiscriminate retention of activity records**, to be fully in line with both EU primary and secondary law and the case law of the European Court of Justice. There should be no attempts to weaken digital tools such as end-to-end encryption or to circumvent them in any way. Transparency and accountability in online processes, transactions and algorithms are indispensable in order to earn everyone's trust - an essential requirement for a functioning society, including in its digital dimension.

The **GDPR** is a global milestone for protection of people against abuse of their personal data and the most private details of their lives. However, the best rules only work where the enforcement is effective and guidance is available. Therefore, Member States have a legal obligation to adequately fund and staff their supervisory authorities in order to make this fundamental right a reality in practice. As a political family, we will continue to work on promoting cooperation within the EU, namely through the work of the European Data Protection Board and European Data Protection Supervisor. In addition, we urgently need an update of the EU's **e-Privacy** rules, to protect the confidentiality of communications and information related to peoples' devices.

With regard to **consumers**, EU policies have to guarantee **protection of personal data, privacy and autonomy** when making purchasing decisions. Automated decision-making may alter the relationship between consumers and traders and, therefore, it must be fully transparent and non-discriminatory. As particularly vulnerable consumers, children should never be subject to targeted advertisements for commercial purposes, including through nudging techniques.

Europe should aspire to become the technological powerhouse for **digital technologies** which should be **designed and developed according to European values as enshrined in the EU Charter on Fundamental Rights,** as well as other relevant international instruments, such as those put forward by the United Nations on protecting children's rights in the digital environment. The EU has to ensure that processes in the public digital sphere are driven by democratic decision-making rather than by commercial interests and monopolistic actors. Citizens must enjoy the same level of treatment, protections and rights of expression in the digital and physical spheres.

The Pegasus spyware scandal

Nevertheless, online hate speech and disinformation are circulating at an accelerated pace. Journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors and other actors face surveillance and are subject to frequent online attacks. **Highly intrusive spyware technologies, such as Pegasus or Predator**, are reportedly being used in many countries, often outside any legal framework. Safeguarding human rights and the democratic space in the digital age has thus become more crucial than ever**.** We therefore condemn the massive-scale and illicit use of the NSO group Pegasus surveillance software and welcome the Parliament's inquiry committee to investigate the use of Pegasus and other surveillance spyware**.**

The S&D Group is committed to ensure the confidentiality of communications in particular by **prohibiting any type of unlawful surveillance or interception of**

communications and metadata. The unregulated cyber surveillance industry and the provision of highly intrusive spyware as a service by private companies to governmental actors (and potentially to private ones) poses additional risks to several EU fundamental rights and freedoms, and, overall, to the proper functioning of our democratic systems.

It is thus necessary to develop a **legal framework for the purchase and the use of these spyware technologies** in order to prevent abusive surveillance and to ensure the protection of innocent citizens. Other measures should, moreover, include increased transparency and independent oversight of spyware use by state bodies, strengthened human rights due diligence by companies along the value chain, and the establishment of an independent EU Tech Lab that can identify spyware infections and explore tech solutions to strengthen our e-communications at the EU level. Lastly, required safeguards to prevent abuse of such technologies, and ensure **redress for victims of illegal wiretapping** should be implemented.

5. Consumer protection in the digital internal market

Same rules and equal consumer protection online and offline

Online platforms are shaking up highly regulated traditional business models, raising questions of **equal conditions for all market players** but also of liability, quality of service and safety and protection of consumers.

Consumers' vulnerability

Online consumers are increasingly facing manipulative environments where merchants and service provider use so-called "**dark patterns**", including their accumulated knowledge of consumers' individual choices, preferences and prior online searches and, ultimately, personal characteristics. In such conditions, **consumers have very little bargaining power** because alternatives are limited and interaction with merchants and service providers is therefore mostly carried out on a "take-it-or-leave it" basis. Even for well-informed consumers, it is very difficult to know the extent of or the mere existence of the mechanics at work, or the way in which their personalised environments are structured based on the personal data gathered about them when compared to those of other consumers.

As a consequence, the online consumer is almost-permanently in a state of **digital vulnerability**, a different concept from offline environments since it encompasses virtually all consumers who participate in the data economy and have their freedom of choice compromised. The S&D Group sees the need for a horizontal strategy across digital policies focusing on the **effective protection of all digitally vulnerable consumers**, including a legal definition of vulnerable consumer and ranging from product safety and consumer credit to digital services and markets.

Digital markets

The Digital Markets Act (DMA)[6] creates **a level-playing field** to ensure that there is **no unfair competition between online and offline sectors and to address dominance and overreliance on a small group of tech giants**. The DMA outlaws **unfair commercial and trading practices of platforms**, as general terms are often a non-negotiable condition to use their services.

The **DMA** is also the response to our Group's long-standing call to regulate the unsustainable and continued increase of corporate concentration in and commercialisation of the online economy. The DMA tackles tech giants´ abusive market power by establishing ex-ante rules for dominant digital companies. By establishing fair market conditions, smaller companies will have the chance to compete in the online market. This will drive innovation and creativity and create a real choice for consumers with regard to digital services which are currently concentrated in the hands of very few companies.

[6] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

For widespread messaging services, such as WhatsApp, **the DMA introduces a requirement of interoperability**, whilst fully complying with all personal data protection requirements. It will allow citizens to use a different service while still being able to communicate with friends and family that choose to remain on these platforms. Following the first introduction of mandatory interoperability, the **S&D Group will keep advocating for digital service interoperability beyond messenger systems** to increase the weight of the European market. Examples of sectors to which this interoperability could be extended are, first and foremost, social media platforms, but also payment systems or personal identification systems.

Moreover, the DMA will be added to the Representative Actions Directive Annex.[7] This means that **consumer organisations are empowered to bring actions to court due to infringements of consumer rights** and this too will significantly strengthen the enforcement of this legislation.

The DMA also foresees the possibility to examine **"killer acquisitions"** and takeovers of other market actors that could increase the market strength of big tech companies, including the option of **structural separation** of the services if necessary but only in the event of a continuous violation of DMA obligations. Robust merger control rules are needed to restrict these types of acquisitions and we urge the Commission to make use of this opportunity when necessary and to **assess other legislative and non-legislative tools to tackle such deals**. We will make sure that the **notification obligation** to the Commission for any sort of acquisition will lead to an effective interdiction of these "killer acquisitions". This is of utmost importance to promote the innovative power of digital markets and for **allowing small new competitors to grow** into real challengers of the gatekeepers.

Our Group has secured important achievements for both individual and societal well-being regarding interoperability, the banning of dark patterns and enforcement of personal data protection. Under the GDPR, EU Member States have the legal responsibility to provide adequate funds for their data protection supervisory authorities so that they can **effectively enforce data protection law**. Our group will keep pushing for strong oversight, starting by raising awareness about the **underfunding of data protection authorities** that requires urgent attention.

Furthermore, we will continue to call on the Commission to investigate abuses of power, notably in the advertising market, and to review the **EU's competition framework** in a future-proof manner, including, for example, the definition of 'relevant market' and the data criteria to be used as indicators of consumer welfare during the assessment of mergers and acquisitions.

Digital services

Social media platforms have a huge influence over children and teenagers and can be addictive. The amplification of harmful content by the algorithms underlying social media platform use can lead to increased suicide rates, especially among teenage girls. Too many children and teenagers have been victims of cyberbullying. Social media platforms must take steps to **give back users' autonomy to the users**, respecting their wellbeing regardless of profitability considerations, and give regulators and researchers the necessary tools to analyse the effects of using these platforms.

[7] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

Updating the regulatory framework for digital services, namely the **e-commerce Directive**,[8] was one of the priorities of the S&D Group. The spread of illegal products, harmful algorithms and disinformation were not questions at the centre of policy-making in 2000, when the e-commerce Directive was adopted, nor was it the case for many of the platforms we are using today.

In this context, and through the S&D leadership on this file, the recently adopted **Digital Services Act (DSA)[9]** will, once it enters into force in 2024, set a new global standard on regulating digital services and will ensure a safer and trustworthy online environment to the benefit of our users and businesses, without prejudice to the need for stricter sector specific legislation.[10]

The DSA will ensure **users have better control over how their personal data are used**. Certain types of targeted advertising, such as targeting minors and ads based on profiling using sensitive data such as health or sexual orientation will not be possible anymore. This is the first step towards a ban on the collection and use of personal data for targeted advertising. We need to **break down the business model of micro-targeted advertisements**, by prohibiting it. Minors will benefit from a stronger protection as online platforms accessible to minors will be obliged to put in place measures to ensure a **high level of privacy, safety and security**.

Moreover, transparency provisions in the DSA will help platform users to better understand **how platforms moderate their content and recommend it to them**. Very large online platforms and very large online search engines will be obliged to offer an alternative recommender system which is not based on profiling. We will seek to expand these kinds of obligations in other relevant legislation.

The DMA and the DSA **ban so-called 'dark patterns'**. Currently, consumers are requested to consent to **cookies** on any platform: the 'Consent' option is often put in bold colours or big letters while the 'Reject' option is displayed on a second layer or is less visible. This will no longer be possible. In addition, it will be prohibited to repeatedly request that a recipient of the service consent to data processing, where such consent has been refused, or to make the procedure of terminating a service significantly more difficult than signing up to it.

Taking into account the risks that they pose to society, very large online platforms (VLOPs) and very large online search engines (VLOSEs) will be subject to stronger obligations. They will have to conduct, on a yearly basis, assessments of systemic risks such as the dissemination and amplification of illegal content; **deceptive content, disinformation**, and revenge porn and adopt mitigation measures

With the adoption of the DSA, we are finally opening the black-box of algorithms, allowing researchers and non-for-profit organisations and associations to get access to data.

Enforcement will be extremely important to ensure the proper application of this Regulation. While the European Commission will have the powers for the supervision of VLOPs and VLOSEs, all other platforms and services falling within the

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[10] See, for example, proposal for a Regulation of the European Parliament and of the Council on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724.

scope of the DSA will be under the supervision of the Member State in which they are established or have a legal representative. If the platforms do not comply with obligations, there will be **sanctions**, up to 6% of their annual turnover worldwide. As a political family, we will be actively following the implementation of both the DSA and DMA and where needed lead legislative and public scrutiny.

Product safety

The **development of e-commerce** poses certain **challenges** regarding non-compliant products and the **protection of health and safety of consumers.** A range of those unsafe products, which have been prohibited from sale or recalled from the market or which present inadequate product labelling and safety warnings can remain available for sale online and therefore cause harm. It should be as safe to purchase product online as it is offline. The recently concluded negotiations of the **General Product Safety Directive**[11] aim to ensure that the **EU has a stronger and more harmonised framework** for checks on products entering the EU market.

Intermediaries and online marketplaces profit from their role in the digital supply chain, offering multiple services and generating several income sources that go beyond the traditional role of brick and mortar stores. However, this has not yet been recognized in marketplaces' obligations and responsibilities. Therefore, we should **address this gateway for dangerous products** and fight for direct obligations and responsibilities in product safety and product liability legislation. These should be accompanied by common European market surveillance efforts to address the problem of non-compliant direct imports from third countries. With the help of AI and data science, national market surveillance authorities, such as customs authorities, could benefit from this European agenda.

Special attention should be given to proliferation of Internet of Things devices (**IoT)** and the increasing number of **AI-enabled devices**, taking into account that consumers are increasingly using connected devices in their daily lives. The EU regulatory framework should address the current **security threats of such devices**, which can be hacked and thus present new risks remotely. In the IoT and AI area, both the **safety and security of the products** are key to ensuring the safety of their users. Similarly, the protection of confidentiality of communication should be extended when IoT devices are being used. **Home appliances and smart goods should not become surveillance tools**. It is of utmost importance to have specific rules protecting the confidentiality and security of electronic communications in the EU and to follow a technologically neutral approach that affords effective protection also in the future. Companies whose primary activity revolves around children or provide **services likely to be accessed by children and to have an impact on children should put in place specific measures** to embed safety-by-design features so as to mitigate any potential harm or adverse consequences prior to the development of the product or the service.

Single market legislation should be better enforced and implemented to **avoid loopholes for consumer rights in the digital sphere**. Product safety should be increased, in particular to protect more vulnerable consumer groups and children. The

[11] Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council

rights of consumers are not easily enforceable by individuals against large digital companies. If digital rights are infringed or responsibilities neglected, we have to ensure that access to **collective redress** is possible and efficient.

Connectivity and roaming

With regard to the **Roaming Regulation**,[12] the S&D Group has a long-standing success in securing the "Roam like home" principle that favours European consumers, keeping millions of citizens connected and improving their lives. The new regulation not only prolongs the current rules for another 10 years, but also ensures better roaming services for travellers. Consumers will be entitled to have the same quality and speed of their mobile network connection abroad as at home, where equivalent networks are available. With the new rules, our Group has also secured and strengthened the efficient access to emergency services, including improving awareness about alternative means for people with disabilities, as well as increasing consumer awareness on possible fees from using value-added services.

[12] Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast).

6. Digital taxation

Taxes should be paid where profits are generated

Traditionally, taxation has been heavily reliant on labour. **International taxation** rules, developed in a 'brick-and-mortar' economic environment over a century ago, are not fit for purpose in the modern globalized economy.

The rise of the **digital economy** through technological developments and increased automation has enabled seamless cross-border trade and has changed the way in which **added value is created** and how **benefits** are **redistributed**.

Jurisdiction and fairer allocation

Consequently, the digitalisation of our economy as a whole has brought about serious tax challenges which call for reform of the international tax system. Currently, companies are taxed where they are located. However, within the digital economy, the physical presence of a company in countries where it operates and makes profits is not required. Thus, companies are active 'remotely' in domestic economies, enabled by digital means but they circumvent their tax liability due to lack of a taxable physical presence in the respective jurisdiction.

This is why **tech giants like Google, Apple, Facebook or Amazon**, as well as all large digitalized firms, make enormous profits all around the world while exploiting the possibility to **locate their profits in only a few low tax jurisdictions**. This is **unacceptable** because it distorts the functioning of not only the EU's internal market bur also the global economy, thus exacerbating existing inequalities.

Taxation is core to the functioning of our societies and is used to finance public services from schools, hospitals and public libraries to roads and network infrastructure, therefore providing equal opportunities for citizens. **Tax avoidance leads to the erosion of national and EU budgets, which consequently undermines public services and social protection.** Taxation is also at the core of our social contract as it fights income inequality via its redistribution function.

In light of the foregoing, we welcome the OECD's/G20's deal on the Inclusive Framework on 'base erosion and profit shifting' (BEPS)[13] two-pillar solution that will **ensure that large domestic firms and multinational enterprises (MNEs) pay a fairer share of tax** and that will grant a new taxing right to jurisdictions:

- **Pillar One** directly addresses tax challenges stemming from digitalisation and will ensure a **fairer distribution of profits and taxing rights** among countries with regard to the largest MNEs, mainly including digital companies. It would give back taxing rights to countries where MNEs have business activities and earn profits, irrespective of whether or not these firms have a physical presence there.
- **Pillar Two** will stifle aggressive corporate tax competition through the introduction of a **global minimum effective tax rate of 15%**.

[13] Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy – 8 October 2021, available at https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm.

We ask for a **rapid implementation** of this deal in the EU and among all 137 signatories of the OECD to make this two-pillar solution a reality, address the challenges of the digitalized economy, and to foster greater tax justice.

In addition, we welcome the upcoming European Commission proposal on the 'Business in Europe: Framework for Income Taxation' (**BEFIT**), expected in 2023, which will provide a single corporate tax rulebook for the EU and a fairer allocation of taxing rights between Member States.

Transparency, value creation and the cryptocurrency market

Furthermore, we welcome the recent developments to improve **corporate and tax transparency**, with the adoption of the Directive on public country-by-country-reporting (CBCR) in 2021.[14] However, there is more to be done in this regard and we call for increased transparency measures to better tackle existing abuse of our tax systems.

We are encouraged by the fact, following continued S&D efforts in this regard, that a share of the residual profits from multinationals which will be reallocated to EU Member States under Pillar One of the OECD/G20 agreement will be used as **EU's Own Resources** helping to finance Next-Generation-EU, among other measures such as the Social Climate Fund.

Value creation is and will increasingly be supported by software and AI, which raises the question of sharing and distributing the wealth in an economy where only a few individuals would own the value produced, leading to disproportionate concentrations of wealth. We should take the lead on this complex issue and seek innovative solutions to better define how the **future of taxation in a highly digitalized economy** should look.

Digital tools should not serve for purposes such as the setting-up of letter-box companies which are often used to avoid paying taxes or social fees and which circumvent workers' rights. The big scandals like LuxLeaks, Panama and Paradise papers and most recently the Pandora papers, showed the difficulties of identifying companies' owners due to the amount of opaque corporate structures that established with the assistance of onshore and offshore company service providers in collusion with tax havens. We need to strengthen the full availability of beneficial ownership information worldwide, a field where the EU is already at the forefront. The EU should also create an **Asset Register** to provide public authorities with centralised access to information on the ownership of high value assets and goods throughout the EU and thereby effectively curb efforts to circumvent taxation, and allow proper exchange of information.

Crypto-assets have created yet more avenues for tax evasion. Currently, the identification of tax-relevant activities in the crypto-asset market is very difficult notably due to lack of centralized control for crypto assets, their pseudo-anonymity and difficulties in valuation. Such loopholes need to be urgently addressed in the scope of the **upcoming revision of the Directive on Administrative Cooperation (DAC8).**[15] Tax administrations must obtain information that is necessary to control whether

[14] Directive (EU) 2021/2101 of the European Parliament and of the Council of 24 November 2021 amending Directive 2013/34/EU as regards disclosure of income tax information by certain undertakings and branches.
[15] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

taxpayers pay their fair share, as well as to exchange information**.** Moreover, in some Member States, income derived from **crypto-assets is not necessarily treated as taxable income at the moment**, or enjoys different treatment on a case-by-case basis, depending on the crypto-assets exchanged or their use. This indicates an unjust discrepancy amongst the national tax regimes. Individuals and companies handling crypto-assets should not be exempt from taxation!

As regards online procedures for companies, any further **upgrade of company law into the digital age** must include sufficient safeguards which would ensure a level playing field for all companies in the digital single market, addressing issues such as fraud and money laundering, identity hijacking or counterfeiting.

7. Artificial Intelligence (AI)

No AI without ethics, legal safeguards and fundamental rights

The EU needs an ambitious and enforceable legal framework on AI focusing on upholding **fundamental rights, ethical principles, legal safeguards and liability** and thus promoting a trustworthy, human-centric European ecosystem for AI that protects our democratic societies and our citizens whenever and however they might be subject to AI.

In this context, **our Group welcomes the AI Act** proposed by the European Commission since it provides the means to clearly define the kind of AI we want in Europe and once again gives the EU the role of global standard-setter.[16]

A European approach to trustworthy and ethical AI

AI technologies carry the **risk** of reducing human autonomy - a challenge that must be seriously addressed. AI must become an instrument that serves people and society and pursues the common good, in full respect of people's fundamental rights and freedoms. Accordingly, there have to be significant investments in robotics and AI, including in digital start-ups and scale-ups. Europe is lagging behind regarding the development of AI applications and calls for an urgent need to develop its own **capabilities** and reinforce **its autonomy**. Currently, both China and the US are investing heavily in AI. So far, however, much of that investment has gone into targeted advertisement and automated labour. The EU should increase its investments (through public and private funding) in robotics and AI to drive innovation guided by public interest in line with **European values and legislation**.

The development of AI commercial products in democratic societies implies setting means of control and human oversight and promoting technologies aimed at improving public services with collective benefits.

We support the **risk-based approach** proposed by the Commission in the AI Act which sets out stricter obligations and requirements for so-called 'high-risk' AI. However, the Commission's approach is incomplete. We believe that all AI systems should comply with a set of **common principles to guarantee ethical and trustworthy AI systems** throughout the Union. The S&D will fight to ensure that our citizens interact with fair, robust, transparent and safe AI systems.

It is of paramount importance to ensure that any new legislation in this field does not undermine Europeans' fundamental rights, including **workers' rights** and the rights to **non-discrimination** and the **protection of privacy and personal data**, democracy and protection of the environment, as well as their health and safety.

Moreover, we cannot control what we do not understand, therefore, AI literacy, transparency and independent oversight will be crucial to get a grip on how these technologies function and are used. This implies strong provisions on exhaustive **ex-ante and ex-post risk assessments** and on immediate **redress mechanisms**, which should take into consideration users' vulnerabilities and be easily accessible by

[16] 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.

children and people with disabilities, among other groups, to deal with potential and resulting breaches of fundamental rights.

Moreover, we need a **horizontal and technologically neutral framework on intellectual property rights** applicable to various sectors where AI technologies and robotics will be deployed. The EU has to strike the right balance between the geopolitical dimension of EU innovation in AI technologies and the protection of the right holders' interests, ultimately aiming at protecting jobs and investments in the EU. This framework should also address the global concentration of **patent applications** which could potentially harm innovation in Europe.

Protecting fundamental rights and ensuring non-discrimination

Algorithmic bias reflecting the values and perception of those producing these algorithms can adversely affect people on grounds such as gender, ethnicity, language, age, disability and social/cultural background. **AI must be free of bias** and neither discriminate nor be based on any stereotypes, especially not by use of biometric surveillance systems (i.e. emotion recognition, biometric categorisation, remote biometric identification) and technologies using other types of sensitive personal data.

Certain types of **AI systems must be prohibited when they threaten our fundamental rights.** For instance, the use of AI for real-time biometric recognition and AI systems used for predictive policing can lead to mass surveillance practices and are in direct contradiction with the presumption of innocence, which is a fundamental principle of our democracies. They should therefore not be allowed in the EU. In addition, AI systems used for performing social scoring, emotion recognition, subliminal manipulation, or accessing a person's mental state can be discriminatory and invasive and lead to detrimental effects to our fundamental rights. Therefore, the S&D Group will defend the prohibition of such uses of AI by both private and public entities. In addition, **transparency** and clarity are essential in ensuring that AI products are fair, non-discriminatory and free of bias.

The use of AI in the area of financial services provides other risk examples. When used to assess a person's creditworthiness or credit score or to decide whether to provide insurance, for instance, there is a risk of perpetuating historical patterns of discrimination, including based on racial or ethnic origins, disabilities, age or sexual orientation. The risk to limit individuals or certain groups from **accessing essential financial services that are necessary for their full participation in society** must be mitigated and uses of AI in this context should be considered as high-risk under the AI Act.

Accordingly, the S&D Group will fight to introduce in the AI Act an obligation for public authorities and companies using high-risk AI systems to carry out **a fundamental rights impact assessment**. This will ensure that our fundamental rights are protected, while taking into account the specificities of the context of use, the person or groups of persons to be affected, in particular vulnerable persons, and detailing possible measures to mitigate any risk.

The EU also needs to ensure that none of its official **languages** are discriminated against or made vulnerable by the use of AI, and that there are data and language sets available in all EU languages and accessible language for people and children with disabilities.

Liability, individual and consumer rights, product safety and standardisation

The EU should actively promote **corporate digital responsibility**. It should especially **support SMEs and start-ups** in pursuing **innovative new services and business models** as well as their access to risk capital.

The EU has to set up clear **liability rules** governing AI and machine learning. People **have to** be able to question **and understand new technologies,** as well as to **seek redress when their rights have been harmed by them**. Questions regarding the risks posed by AI (from the development stage on, throughout their lifecycle), or when it comes to the consequences of its possible misuse - all these issues will have to be clearly addressed. The special characteristics of AI, namely its complexity, opacity, vulnerability and the possibility of being modified through updates and self-learning, stress the need to update liability law. Citizens must not be the ones bearing the burden of proving the causal relationship between a damage and the underlying defect of the AI-based product. We need to avoid that persons who suffer harm to their physical or psychological well-being or to their property end up without compensation. We need to ensure that the party that bears the risks also holds the responsibility. For the normal citizen it is impossible to understand, let alone prove, the causal relationship between the harm suffered and the AI system that cause it and the EU legal framework needs to take account of this and include a reversal of the burden of proof to empower those harmed by AI decisions. A proposal updating EU liability rules for AI has finally been proposed by the European Commission, as it is now high time that we have ambitious legislation in place.[17]

The EU has to become the world leader in terms of **product safety and consumer rights** protection when addressing digital challenges, including AI and algorithms. We should promote initiatives related to AI with the objective of safeguarding fundamental rights and increasing product safety and provide more information to people.

We see the **AI Act** as an opportunity to **create a European Single Market for AI** by clarifying the roles and obligations of the different actors involved in the AI supply chain, enhancing innovation to open new technological and economic opportunities and, above all, ensuring harmonized and high-level protection to individuals affected by AI. The proposed AI Act rightly aims at regulating providers and users of AI system and seeks to give a common framework to innovate via sandboxes, but it should do more to protect the people. **The S&D wants to put individuals at the centre of this piece of legislation.**

In order to fully benefit from AI, **the AI Act should award new rights to individuals such as:** a right to information to ensure they are always aware whenever they face an AI system; a right to explanation for persons subjected to a decision based on an output from an AI system; a right to lodge a complaint before national supervisory authorities and a right to an effective judicial remedy against national supervisory authorities. In addition, the AI Act should be included within the scope of the Representative Actions Directive. The S&D Group will continue to champion these measures.

In cooperation with international standardisation bodies, the EU should continue to **improve standards** on issues such as **safety, reliability, interoperability**

[17] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

and security. Moreover, it should promote and develop standards in the field of smart manufacturing, robots, autonomous cars, virtual reality, health care and data analysis, as **EU-wide standardisation for AI and robotics** will foster innovation and guarantee a high level of protection of humans.

All AI technologies developed for manufacturing or individual use should be subject to **product safety checks** by market surveillance authorities and consumer protection rules, including the possible risk of accidents resulting from interaction with humans. Europe has to avoid a patchwork of national legislations and should instead develop a single set of EU rules taking into account the interests of people, businesses and other concerned parties, while avoiding over-regulation in robotics and AI systems.

We need a "human-centric" AI in Europe. People should always be responsible for decision-making, not robots or AI, in particular in education, medical, legal, financial or accounting professions, the provision of essential services or in the law enforcement sector. People - as users and consumers - when interacting with an automated system, should always have the possibility to reach a human as well as to ensure that an automated decision can be verified and corrected.

AI will increasingly contribute to the **development of public and private services**. Such a development must be based on a **balanced approach** taking into account ethical and human-centric aspects, economic growth and jobs creation, cohesion in society and fundamental rights.

AI will also play a key role identifying and minimising the **impact of human activity on the environment**. Increased digitisation will bring new energy needs, but it will also contribute to bringing efficiency into previously energy intensive sectors providing better understanding of processes, leading to their improvement. Nevertheless, **AI also depends on a high level of energy and other natural resources consumption** and its environmental impact must therefore be mitigated.

8. Cybersecurity in a connected continent

Digitalisation brings great opportunities and solutions for societal and economic challenges. However, as critical sectors such as health, finance and energy become more dependent on digital technologies, they are progressively more exposed to **complex threats and attack methods**. Throughout 2020 and 2021, cybersecurity attacks have increased both in terms of vectors and numbers but also in terms of impact. This trend is set to grow further in the future, given that 22.3 billion devices worldwide are expected to be linked to the Internet of Things by 2024.

The shift to a hybrid office model and exponential increase of teleworking arrangements as a response to the COVID-19 pandemic have **expanded the attack surface** and increased the cyber threats that citizens, businesses and public administrations are faced with. As the threat landscape continues to expand, citizens, businesses and governments are exposed to highly sophisticated and impactful supply chain compromises, misinformation and disinformation campaigns and other attack methods with unique business models such as ransomware by both state-backed and non-state actors.

A **stronger and more coordinated cybersecurity response at Union level** is necessary to achieve the objective of building and maintaining an open and secure cyberspace. In doing so, **fundamental rights and the rule of law must be protected**, together with protecting the integrity of the single market in order to create greater trust among citizens, businesses and governments in digital tools and services.

The Network and Information Systems (NIS) Directive

In May 2022, the European Parliament and the Council reached a provisional agreement on the new measures of the revised NIS directive (NI2 Directive)[18] to ensure **stronger risk and incident management and cooperation**, while significantly widening the scope of the rules.

The new rules, which apply to both private companies and public administrations, establish swift reporting obligations to stop the spread of incidents, increase the level of coordination at Union level, create clear accountability mechanisms for senior levels of management and introduce cybersecurity capabilities and modern cybersecurity strategies fit for the future through coordinated capacity building and training. **ENISA,** the EU Agency for cybersecurity, **is at the heart of Europe's path towards a secure cyber space**, and additional safeguards have been established to integrate privacy by design for the protection of personal data, as well as targeted support towards SMEs.

The higher levels of cybersecurity achieved in the outcome of the negotiations of the NIS2 Directive for private entities and public administrations are relevant for the European public administration. **Public administrations have often been targets of cyber-attacks** and a European approach to **increasing the levels of cybersecurity** among the community of Union institutions, bodies, offices and agencies is needed **to establish a secure, resilient and effective European public administration that inspires trust**.

[18] European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

Certification and cybersecurity of products with digital elements

The development, adoption and use of digital products and services at scale requires high levels of trust by their users. To achieve these greater levels of trust, ICT products, services and processes should conform to high cybersecurity standards.

Most of the infrastructure and devices that are vulnerable to cyber-threats are privately owned. This poses a problem, as cybersecurity measures are costly and they are often sacrificed in order to offer cheaper products. This is especially problematic with the proliferation of **Internet of Things (IoT) devices**, which often lack even the most basic security features.

The upcoming discussions on the Commission's proposal for a **Cyber Resilience Act**[19] will ensure more secure hardware and software products. This is essential for their conformity with cybersecurity standards, as they are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021. Products with digital elements that are placed on the market should include fewer vulnerabilities and their manufacturers should take security seriously throughout a product's life cycle

ENISA, is central to the certification process, with the **first certification on international set of standards and guidelines** used in evaluating security products and systems taking its full shape, and the certification for cloud services maturing before a candidate scheme is proposed. The agency must therefore, be provided with the adequate resources to carry out its activities and achieve its objectives. We stress the importance of efficient, timely and close coordination between different EU institutions, bodies and agencies specialised in cybersecurity, and advocate for the establishment of a voluntary **EU-wide cybersecurity certification framework** for digital services, processes and products, including rules on safety and security by design of connected products such as Computer Emergency Response Team for the EU institutions (CERT-EU). EU competence in cybersecurity should overcome the fragmentation in this sector: technological as well as human and legal.

The EU has a unique role in ensuring cybersecurity against cyber-attacks targeting the EU institutions, national governments or other public authorities, the economy and our civil society committed and/or backed by state or non-state actors. In this context, Europe needs to **increase investment in cyber-security technology and research** and risk prevention, also when it comes to the upcoming 5G deployment, as well as improve cooperation and coordination within the EU, including in cases of large-scale cross-border cyber incidents, and with the private sector.

We therefore welcome the **Foreign Direct Investment Screening Regulation**[20] as an important tool to coordinate the actions of Member States on foreign investments, and we call for a stronger regulatory framework to **ensure that foreign investments affecting the EU's security are blocked**. 5G should also be included in the framework in order to limit its dependency on high-risk suppliers.

[19] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[20] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union.

Cybersecurity and defence

Digitalisation and AI are changing the nature of **defence and warfare** while creating both opportunities and threats. Technology has the potential to allow for greater situational awareness, enhanced cyber defence, increased surveillance possibilities, reduced risk of life losses in conflicts, and reduced costs during training and operations. Continuing to invest in defence innovation will secure our preparedness for a changing future battlefield in light of emerging and disruptive technologies.

We must pay careful attention to the development and deployment of new digital technologies in the security and defence space, such as **militarised AI and autonomous weapons**. **Europe must invest** in building its own digital capacity and improve its defence capabilities.

The development of AI and new technologies triggered discussions on the potential of developing **lethal autonomous weapon systems (LAWS)**, which would be able to operate in complex and dynamic environments and make life-and-death decisions autonomously, completely circumventing human oversight. This could have a devastating effect on life, security and international order and could be used to target specific groups of people and infrastructure. Therefore, **the EU** must reinforce its stance on the **importance of human involvement** regarding lethal use of force. **Humans must always remain accountable and responsible for decisions over life and death**.

The EU must take the lead in promoting the establishment of international norms regarding the ethical and legal parameters of the development and use of fully autonomous, semi-autonomous and remotely operated lethal weapons systems. The Member States should develop national strategies for the definition, status and use of LAWS **towards a comprehensive strategy on the EU level**.

The **civil and military use of drones** has become increasingly popular, and the EU has started regulating the civil use of drones to increase transparency regarding their registration and usage. The EU should also develop a common position on how to use armed drones in line with international humanitarian law and international human rights law. This would be a clear step towards achieving a high standard of national policies while **safeguarding EU values and fundamental rights.** All emerging technologies, including AI, that are used in weapons systems must be developed and applied according to strict ethical principles and in compliance with international law.

Cyber-attacks

New technologies challenge both private and public administrations to meet the demands of the modern age, but also to protect themselves against new forms of attacks. **Cyber-attacks and hybrid operations** can be used as **weapons of mass disruption.** The EU must be prepared for cyber-attacks, including state-sponsored malicious cyber activities and ransomware attacks on critical infrastructure and supply chains that may have potentially devastating effects on our economies and the wellbeing of citizens. EU policies need to be revised to protect a wide range of key sectors against large-scale attacks, in a coordinated manner. It is important to establish preventative measures as well as sanctions on external actors for malicious

cyber attacks on the EU and its Member States. Therefore, strengthening and further developing the **EU Cyber Diplomacy Toolbox** is of crucial importance.

Perpetrators of cyber-attacks can include foreign governments, non-state entities or private individuals. **Russia's war** of aggression against Ukraine has been multi-dimensional, and has included, before the invasion, various forms of hybrid and cyber warfare. The recently adopted **Strategic Compass**[21] clearly points at the **strengthening of EU Cyber Defence Policy**, while cyber has been identified for years as a capability gap. Increasing cyber preparedness and resilience will be key to face the long-term consequences of the conflict and **counter hybrid warfare** means used by the Kremlin to undermine EU response to the war and the EU itself.

Large-scale cyberattacks and crises must be met with an EU-coordinated response. Europe should be more resilient to cyberattacks and threats by protecting everyone, not just a few. Strengthening our cyber intelligence capacities is not only crucial for cyber resilience but also to be able to **provide effective assistance to our civilian and military CSDP missions** and operations. Cybersecurity trainings are also essential to build a highly skilled workforce.

Fight against child sexual abuse online

The EU Directive on combating sexual abuse and sexual exploitation of children and child pornography,[22] the GDPR, the ePrivacy Directive as well as its derogation interim Regulation,[23] and the European Commission's proposal for a Regulation to **prevent and combat child sexual abuse**[24] must be considered jointly to ensure children safety online. We must protect all fundamental rights equally and strive to find the right balance with the best possible result. There should be an obligation for providers of hosting or publicly available interpersonal communication services to report and remove child sexual abuse material in accordance with the DSA and in full respect of fundamental rights in particular the right to privacy, data protection and without leading to any form of mass surveillance or violate End-to-End encryption or the general monitoring prohibition. Mandatory and specific safety-by-design tools, sufficient funding and increase in staff for all relevant actors as well as mandatory human review by the respective providers and relevant law enforcement should accompany our efforts to protect children online. The S&D supports the creation of a **fully independent EU centre to help coordinate and facilitate combatting child sexual abuse and exploitation online**.

[21] A Strategic Compass for Security and Defence, available at https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

[22] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[23] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 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.

[24] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.

9. Data and the data economy

People should have control over their data

The EU is working towards developing a **strong data economy**. EU-wide non-personal data flows and secondary use of anonymized data will allow the EU to maximise the potential of digital technologies, and to sustain economic growth and increase productivity, as well as help to deliver **more efficient and smart public services** for European citizens.

The Data Act[25] and the European Digital Identity Framework[26] proposals are **essential building blocks** of a coherent approach that seeks to drive innovation, improve decision-making and enable greater all-round operational efficiency.

The Data Act

Despite the new opportunities and benefits provided by more data sharing, we have to look into the **ways in which companies collect, use and share data** and raise questions of access to data and exploitation of data, as well as of data sets audits, while fully respecting data protection laws.

Thousand-page user agreements allowing companies to share and sell data with whomever they please must be forbidden and clear legal norms for data sharing must be established. Unless clearly stated otherwise, **user data should not be shared or sold to other companies.**

The Data Act proposed by the European Commission is a first step in regulating data sharing and access between different actors within the digital single market, as well as other aspects such as cloud and data services, interoperability and international safeguards.

It is crucial to **raise awareness**, especially among the most vulnerable (children, young people or seniors) about the personal data they knowingly or unknowingly provide in exchange for access to many so-called free services. **Users and SMEs have to be in control of their data and the data they help generate!** They **should be empowered** and conscious about the benefits and risks of sharing their data to decide how and when their personal data is collected and used, and they **should benefit from the value of their data**, be it individually through more personalised services, for example, or collectively by promoting the increased efficiency of public or private services.

When privately held data are **made available** to public institutions, it can be used to **support public policies** aimed at improving **public services** or responding to **public emergencies** such as natural disasters or pandemics. By informing decision-making, providing for new scientific insights and resolving policy issues, privately held data enable more targeted intervention, better accessibility and better management of resources, bringing about significant **savings for the public budget** and delivering the benefits of the data society to European citizens as whole.

[25] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

[26] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

It is necessary that the scope of such use and its legal basis are clear and properly defined in **full respect of the GDPR, trade secrets and intellectual property rights.** Access, use, and sharing of personal data should always respect the principles of **lawfulness, fairness, proportionality and transparency** and it should aim to achieve a clear, demonstrable public interest. Under the GDPR, there is the right to data portability, so companies are under legal obligation to provide mechanisms for users to be able to take and transfer all their personal data to another platform.

Operational **model contractual clauses and secure technical systems** to enable safe and trusted data sharing should be further developed. In the same vein, interoperability is necessary in order to ensure that there are **no barriers to exit from or transfer between platforms.** The **development of interoperable standards** for the European digital market must be open, technology-neutral and inclusive.

European Digital Identity Framework

The ongoing reform of the European digital identity framework aims to achieve a harmonized approach to the use of **digital identity across the EU**. It supports the objectives that by 2030 all key public services will be available online, that all citizens will have access to their digital medical records and that 80 % of citizens will be using a digital ID for accessing public and private services. A lack of widely accessible, secure, trustworthy and interoperable digital ID remains a problem in the EU wherever the **ability to make efficient use of one's digital identity remains limited**. Therefore, this reform introduces the possibility to use digital wallets linking national digital identities with proof of other personal attributes (e.g. driving licence, diplomas, bank accounts, etc.).

Cybersecurity, privacy and protection of personal data are essential elements of the European Commission's proposal and the high level of security and control it foresees - notably through relevant certification in these areas - will offer everyone the **means to control who has access to their digital ID and to which data exactly**. As a political family, we advocate for the principle of data minimisation and full control by citizens over their data. This will strengthen the uptake and trustworthiness of the new framework - one of the key enablers of the digital transition of digital government and help **ensure seamless access to public and private services** to the benefit of our citizens and businesses.

10. Infrastructure and technology

Digital infrastructure can unleash Europe's technological potential

Europeans should be able to benefit from **safe and accessible digital infrastructure**. The development of the digital infrastructure is essential for the EU to stay competitive on the global market and to maintain its digital autonomy. Europe should exploit the full potential of future technological developments.

Innovation is key to solve global challenges and therefore it is important to support **European innovation and research, including when carried out by start-ups or companies founded by women** that currently do not find the same conditions and support in the EU as they do in other parts of the world when it comes to, for example, funding.

R&D, 5G and network security

Science, innovation and R&D will be indispensable to attain the objectives of **inclusive digital transformation**, just transition and European digital sovereignty.

5G technology is the basis for new technology and our connected communities. It will create conditions for new types of applications and business models **in areas such as transport, health, energy and media**, and it will spread the use of different types of industrial applications over mobile networks and of the Internet of Things with cost-effective and innovative applications. It is crucial that Europe is leading the 5G development. The **EU has to design a strategic approach** to roll out fifth generation mobile systems.

There should be an **EU-wide common and united policy on 5G** in order to get the best solutions and to avoid splitting into several contradictory rules. Long-term strategic interests, as well as challenges related to human health, cybersecurity risks and privacy have to be taken into account, rather than just short-term price considerations.

The EEAS has characterised **China as the EU's strategic competitor**, also due to Chinese well-known state support to its companies in the form of subsidies. Against this background, Europe should be careful about creating long-term dependencies with regard to critical communications infrastructure, especially when **cutting-edge European suppliers are available.**

Investment and EU-wide availability

Investment in basic digital infrastructure to establish a **Europe-wide availability of high performance gigabit networks** and connection (including the 5G technology) is a priority. Equal access to high-speed and quality internet everywhere has to be guaranteed, not least in rural areas. The EU must defend the **principle of net-neutrality** to promote diversity and competition in the digital sector. The S&D is committed to this principle and advocates for connectivity regulation that ensures equitable and fair end-to-end access to the whole internet for all users and online services, where content, services and applications are not unjustifiably degraded or

blocked and the access to online services remains affordable for all, particularly for those with low income.

Europe also needs to reinforce its capabilities especially in the **new frontier technologies** such as **6G and supercomputing** (for example quantum technologies).

Currently, European companies still hesitate to use the whole potential of digitisation due to the lack of a sufficient digital infrastructure. Without adequate progress, they are likely to move into countries with better digital infrastructure. **European technological sovereignty** should be made possible through innovation, technology transfer and start-ups.

If the **EU** wants to have **more digital autonomy**, it should **invest into research and innovation** capacity in strategic sectors, such as **AI, high-performance and cloud computing**, **privacy-enhancing technologies** or **clean technologies that contribute to mitigating our carbon footprint**. Europe needs a digital trust infrastructure, covering online identification, authentication, consent and security. In this way, online services, cloud providers and others will have to comply with European values.

The EU needs strong public procurement rules to ensure that only companies with trusted status are involved in the development of European digital infrastructure, driving innovation and investing into public interest technologies.

The **Chips Act**[27] and the initiatives to increase the level of EU industrial ambitions are an example of Europe taking its destiny into its own hands. **Semiconductors** are the prerequisite of most of the technologies of the future: 5G, 6G, edge computing, the Internet of Things, AI. Without these technologies, there can be no green and digital transition either: intelligent electricity distribution networks, battery management in cars or energy storage systems will be essential for future transformation. By the end of this decade, the semiconductor market will double. Europe needs to prepare the ground for its security of supply and strategic autonomy on next-generation semiconductors.

There is a growing demand for computing power, **block chain and distributed ledger technology (DLT)**. These technologies are changing the ways in which markets and businesses operate and interact, citizens and organisations collaborate, information is shared and stored, transactions are initiated, executed and settled and services are being delivered. They will continue impacting the current structure of our economies and societies, and the way we communicate and interact with digital services and with other humans, and our Group will work to ensure that neither citizens' rights nor the environment are harmed in the process. We need European standards to assess the record and trustworthiness of providers (companies) of digital infrastructure from third countries, in particular those where governments can influence or directly control these companies.

Sustainable development goals, better products and the right to repair

New technologies may allow **governments to improve the quality of interactions with citizens** by promoting transparency, efficiency, inclusiveness when designing and delivering digital public services. Furthermore, governments and policy-

[27] Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act).

makers will be able to benefit from new forms of citizens 'engagement. **Digital technologies** should also be deployed to **support the EU's climate goals, its economic growth, employment and competitiveness**.

Digitalisation and **new technologies** have both **negative and positive impacts on the environment**. On one hand, they allow better exploiting and controlling of resources; on the other, the increasing "e-waste" is a real issue that should be addressed. A first step would be to make **electronic devices more durable and recyclable**. A key tool to achieve this is by adopting binding eco-design rules for smartphones and other products, similar to already existing rules for washing machines or refrigerators. Extending the lifespan of smartphones by even a year would make a huge difference in reducing negative environmental impact.

In addition, the EU should introduce a **"right to repair" for electronic products**. Moreover, there should be a **lifespan guarantee** for products in which digital content is embedded. Consumers should always be informed about the expected lifespan of products (including connected products) and their reparability. Vital updates of digital content should be mandatory.

Europe needs **a comprehensive industrial policy** fit for the 21st century which must include digitalisation, in particular the integration of **smart technologies, platforms, big data analytics, AI and robotics** into industrial value chains.

We call for increased **investment into strategic value chains of EU industry**, such as batteries, microelectronics, high-performance computing, connected, clean and autonomous vehicles, smart health, low-carbon industry, hydrogen technologies and systems, industrial Internet of Things or cyber-security. These chains are essential to our strategic autonomy as a block, namely in order to be more resilient in the face of external decisions or factors, as exemplified by the latest health, energy and goods supply crisis.

The EU needs a clear framework on cybersecurity and it has to find ways to address open questions surrounding the issue of data ownership, identifying critical technologies, ensuring the highest levels of data protection, supporting the **competitiveness of European industry** and its digital transformation, creating digital innovation hubs or reinforcing the existing ones, for example through the European Institute of Innovation & Technology. The trends of globalisation and digitalisation represent the greatest challenges for European companies and their employees.

There is a global semiconductor-chips shortage. We use semiconductors in everything from our computers to vehicles and militaries. Europe has become dependent on foreign companies and nation-states that produce them. This is not sustainable and puts Europe at risk! The **European Chips Act** should ensure Europe's autonomy in all stages of semiconductor manufacturing, from chip-design to fabrication.

Moreover, the **digitalisation of insular economies** (small countries, islands and remote regions), among other aspects, deserves special attention due to their geographical and size limitations. Similarly, the **rural dimension** has to be taken into account in the development of all future EU policies to ensure that the 30% of Europe´s citizens who live there have equal access to services opportunities for all, particularly women.

11. Digital trade and e-commerce

Digitalisation must facilitate sustainable trade and protect citizens

We are committed **meet the challenges of an increasingly digitalised world** and to **tackle the digital trade barriers** often referred to as the “new tariffs” of our time.

Cross-border data flows and imported products

Whilst we support international trade and cherish the many benefits it brings, it is important to realise that there are risks at stake, and that **data is not a commodity**. In WTO e-commerce talks, certain trade partners are proposing rules that may undermine **EU citizens’ fundamental rights to data protection and privacy**. WTO rules should in no way undermine public authorities ’capacity to protect fundamental rights or secure other public values when it comes to data transfers. The EU already protected this prerogative at WTO level in the past, and should continue to do so, for itself and for others. Therefore, Europe must maintain its 2018 **horizontal position on cross border data flows**, and should not agree to trade rules that could limit its ability to regulate, for example on AI or cybersecurity.

The **Commission must take the lead in WTO negotiations on e-commerce**, in order to address digital trade barriers and enhance consumer and business trust.

Digital payment services and cryptocurrencies: safeguards and risks

The past decade has seen a rise of technology companies, providing alternatives and better access to many aspects of traditional finance. We should promote a competitive, trustworthy and secure payment sector as one of the driving forces behind a well-functioning European Single Market. We need more innovation in financial technology in order to create **user-friendly European payment solutions**. However, the proliferation of innovative digital payment solutions should not lead to a cashless society. **Consumers need a right to continue to use cash when paying in a shop and be able to withdraw money from ATMs and bank branches**, as cash remains an important payment instrument for many European citizens, including vulnerable groups. Consumer payment data must not be used for advertising purposes. The **accumulation of tech giants ’market power in the financial sector** must be addressed.

Europe can also set a standard through the work of the ECB on a central bank digital currency (the ‘**digital euro’**) which offers a high level of privacy, data protection, confidentiality of payment data, cyber resilience and security. **The digital euro would be a complement both to cash and to private money.**

Europe will also have to address the issue of **cryptocurrencies** and the relating challenges, such as the anonymity surrounding cryptocurrencies and risks of money laundering, terrorist financing and tax evasion, namely by using solutions offered by block chain or distributed ledger technology. Crypto-activity, however, goes beyond European borders and, therefore, international cooperation will be necessary to design and enforce a global regulatory framework on cryptocurrencies. Cryptocurrencies have enabled or facilitated **money laundering, terrorist financing, tax evasion** and offered or promoted 'get-rich-quick' schemes. Beyond this, concerns as regards the energy consumption of certain crypto-assets currently based on energy-intensive mining practices should be adequately addressed to deter them from generating large CO2 emissions that could ultimately threaten the climate transition.

The principles and regulations that apply to our traditional finance systems must also apply to cryptocurrencies adapted to the opportunities, risks and solutions provided by the underlying technology. Europe must send a clear signal that Ponzi schemes, theft, and fraud are not permitted simply because the technology has changed. The **technology itself offers the tools for real-time supervision** and enforcement and this capability should be leveraged. To achieve this, the **European Central Bank** and the European Supervisory Authorities must be given the necessary resources **to develop expertise on new financial technologies and cryptocurrencies** ensuring that they are able to continuously monitor and provide legal clarity for companies working in this space. The EU should also closely monitor the environmental impact associated with new crypto-technologies, and mandate or encourage the crypto-sector to move towards more sustainable practices.

12. Digitalisation of health and care

Increase efficiency, accessibility and sustainability of health services

The medical landscape is rapidly changing. With innovations in the fields of tele and mobile applications, as well as AI and robotics, major breakthroughs are happening that allow for easier and more accurate diagnoses, improved treatments, R&D for new medicines, customized medical devices and more. These new technologies, such as blockchain, have led to an **exponential growth of health data**.

The transformation of medical services through digitalisation **optimises and reduces costs for health service providers and public administrations,** The S&D advocates for strategic investments in this field especially relevant for certain rural and remote regions in the EU. However, we highlight the necessity of avoiding a *'robotisation'* of health services where remote medical care is privileged over in-person one.

Investment is crucial to **reduce the digital divide in health and care** between Member States and between urban and rural areas. The EU's financing instruments should ensure equal and just access to quality health care for all. In particular, it should ensure that **digital infrastructure provides smaller medical facilities in remote areas with high-speed digital services** to support top quality remote specialist diagnostics and treatment advice where such expertise would be otherwise unavailable in these locations.

Digitalisation of health care may also contribute to addressing **disinformation and misinformation on various health issues**, improve **health literacy** and help to promote **healthier and more sustainable lifestyles**.

A European Health Data Space

We support the digital transformation of health and care to maximize the **efficiency, accessibility and sustainability of health services** in the EU Member States. However, the EU needs to create a framework where **privacy, security, safety and accuracy of health data** are guaranteed and where the control of personal health data stays with European citizens. This should be a cornerstone for the creation and implementation of the **European Health Data Space**.[28]

Interoperability of Member States' electronic record systems could optimize the share of health information across Europe with the potential of increasing the quality of cross-border medical care and reducing the costs associated to it, while enhancing the efficiency and sustainability of healthcare throughout Europe.

Anonymised and, where anonymisation is not possible, pseudonymised health data can be used for **scientific health research**. This use of secured sensitive data can lead to better understanding of diseases and allow early detection of events possibly threatening public health, increase the effectiveness of current treatment methods and allow for more cures to be found more easily. Digitalisation can provide tools to implement **evidence-based health policies** thus achieving better health outcomes.

[28] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.

13. Agriculture and fisheries in the digital age

A more sustainable agriculture: producing high quality food with fewer resources

The modernisation and development of further sustainability in agriculture and fisheries can positively affect society and revitalise rural services through use of digital and social innovations. Safeguarding food production in rural areas is essential to the food security of the EU as a whole, and such programmes improve job opportunities, quality of life, and **making rural and coastal areas more attractive for young people**, young farmers, fishers and especially women, without whose work and presence rural economies and communities cannot thrive or survive.

Good governance and technologies

Digital technologies are increasingly important to farms and other agricultural businesses. They offer the opportunity to develop more data-orientated sustainable farming thanks to the rapidly increasing volume of data. This can redefine the role of farmers in the supply chain, and enable transformative agricultural business models to flourish, leading to cheaper, safer, and more sustainable quality produce. As farmers use new technologies more and more frequently, more data about their farms, their land, their animals and crops becomes accessible to the companies that have developed and operate these technologies. This raises questions about the **ownership and protection of data**, which belong to the farmers, but for which there are currently no clear safeguards in this respect. We need good governance of data-sharing and ownership, by providing regulatory coherence and avoiding information asymmetries and dependency on high-tech providers which may lead to monopolies and ultimately have an impact on food security, availability and free use of local and varied genetic resources, traditional knowledge and regional cohesion.

Digitalisation can contribute to more sustainable farming practices by providing **innovative solutions** and control methods, making it possible to work more effectively, precisely or sustainably. Aspects of digitalisation, which otherwise offers considerable benefits to farmers, may displace workers with fewer skills. In this context, training and information are essential in how big data and digitalisation can help the development of more sustainable farming.

The uptake of precision agriculture for a range of agricultural purposes can lead to an increasing **digital divide between large and small farmers**, because small farmers may lack the investment capital or knowledge to acquire precision agricultural technologies. To counter this tendency, public authorities should be proactive in organizing and guaranteeing standardisation so that farmers retain ownership of their data and can benefit from interoperability, accessibility and affordability of this technology, with incentives for cooperation between farmers as a tool to strengthen their position in the supply chain. Moreover, farmers will need to be fully informed about the cost and benefits of investments in digital technology, as well as the potential and the economic viability of precision agriculture.

Farm advisers, open data and R&D

Farm advisers (as general consultants already help farmers, including on compliance with existing legislative requirements), supported within the CAP by Rural Development policies, and the European Innovation Partnerships (EIP) on Agriculture Production and Sustainability. Developing digitalisation aspects could be important as these instruments allow Member States to develop and share appropriate knowledge and expertise.

Farming and other rural businesses must have **access to fast broadband connections** to be able to contact their customers directly and thereby compete with businesses elsewhere. Moreover, remote sensing and connectivity is a mandatory part of Common Agricultural Policy administration for farmers who need to manage their agricultural activity - whether for crops or livestock - effectively and efficiently, to be able to secure maximum benefit from the CAP. Agriculture depends on lively rural communities and rural communities depend on agriculture. Equal access to broadband is a key part of keeping those communities and economies in good shape and leads to a **fairer, more sustainable and more transparent agriculture**.

Data, and especially **open data, play a crucial role** in helping the agriculture sector. Europe has to foster open data publications and open data reuse related to agriculture. Weather data, data on seed genetics, data on environmental and growing conditions, soil and other data can help farmers to plan and optimize their planting season, and livestock management. Finally, we must ensure an efficient use of **R&D funds towards the digitalisation of agriculture**, for example under the Horizon Europe research programme to ensure the full contribution of Europe's agriculture to our future food security.

Fisheries' digital data and traceability

The digitalisation of the fisheries sector is undergoing in the framework of fisheries control reform. All **data from fishing vessels will be recorded in a digital way** and submitted electronically to Member States and the Commission. From the logbook to the sales notes, all data shall run throughout the whole food chain and be available for consumers.

In this context, and specifically as part of the Illegal, Unreported and Unregulated ('IUU') fisheries legal framework, the digital Union Catch Certification Scheme will provide for with the establishment of a database for the management of catch certificates ('CATCH') based on the Information Management System for Official Controls, allowing for **risk based controls, reducing opportunities of fraudulent imports and easing the administrative burden** of Member States.

Traceability in the fisheries sector is important not only for consumer information and food safety but also for allowing the fight against IUU fisheries. Digitalisation of all data and processes of the EU fisheries sector is the first step to allow for a **completely traceable EU food chain**. Making seafood products traceable from point-of-catch to point-of-sale is necessary to combat IUU fishing and achieve sustainable fisheries. This is especially true for the EU, as the world's leading seafood market which imports over 70% of its seafood.