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

Position Paper

Adopted on 5th February 2020

Our Inclusive Digital Europe

Leaving Nobody Behind
Offering Opportunity For Everyone

Table of content:

1. Social dimension of digital economy

In the digital revolution nobody should be left behind.

The digital revolution should neither leave anybody behind nor lead to a 'race to the bottom' with regard to labour and social standards. It must contribute to sustainable development, while balancing the economic, ethical and environmental dimensions.

The European Pillar of Social Rights applies to all actors in offline and online economy and must be vigorously implemented and enforced. **Precarious work and new forms of 'digital dumping' are not acceptable.**

We do not yet know if jobs created through new technologies will compensate (at least in the medium-term) for those lost, and this uncertainty presents **potential risk of an enormous social crisis**. The wealth created by machines and algorithms cannot remain in the hands of a few people, while workers who lose their jobs and social role become increasingly poorer.

European labour markets are evolving towards 'atypical' or 'non-standard' forms of employment, such as occasional work, work on-demand and dependent self-employment or work intermediated by digital platforms which have an excessive tendency to take advantage of economically dependent self-employed workers. This may lead, amongst other things, to imbalances in working time, occupational health and safety, workers' rights and social protection, especially affecting people with more difficulties to enter the labour market, such as women with caring and unpaid home responsibilities.

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.

The European Digital Agenda must have a social dimension! New types of employment and platform work can offer a better work-life balance, additional income and new chances for people distant from the labour market. There is a risk, however, that new working arrangements in the platform economy undermine current social and employment standards and give rise to precarious forms of employment.

New technologies and **digital trends should benefit all citizens** and contribute to the eradication of social inequalities and discrimination. They should contribute to creating new quality jobs, improving working conditions, providing new opportunities and better quality local services. Decent working conditions, professional training (as well as personalised learning pathways) and employee benefits should be universally available to all working people, including in the digital and platform economy.

We expect the new Commission to live up to the promise and deliver bold and ambitious legislative proposals on **fair working conditions for platform workers**[1]. It must be ensured that workers who use online platforms can benefit from fair and decent remuneration and working conditions, adequate social protection, occupational health and safety. Moreover, learning opportunities, upskilling and reskilling, training, collective bargaining and the rights to unionise must be available to all platform workers.

The "platformisation" of work is taking place across vast swaths of the labour market, of which platform workers form only one part. The EU should therefore take a

[1] In March 2019, the S&D Group adopted a position paper on "A Social Agenda For Digital Work: Shaping the platform economy in Europe":
http://www.socialistgroup.ep.parl.union.eu/sdorg/docviewer.htm?lg=en&docid=56390&type

more **holistic approach towards the future of work and new atypical forms of work**. Most platform workers are driven by a need for additional income (although many others are performing these jobs as their main or unique income basis), and thus there is need for policies to boost people's income from their main job. Therefore, the issue of **minimum wage and strengthening collective bargaining across Europe** is directly linked to the question of the future of work in the digital economy.

Member States and the Commission must ensure adequate social security for self-employed workers, who are key players in the digital labour market. Existing social protection schemes should be adapted and new mechanisms of protection developed, where necessary, to ensure adequate coverage of workers on these platforms as well as non-discrimination and gender equality.

The Commission must, therefore, live up to its commitment and present a proposal for a **European Social Security Number (ESSN)** without undue delay. An ESSN with real time data-access would allow the national competent authorities to verify social security coverage for workers at any given point in time and thereby also considerably facilitate labour inspections. It would ensure the rights and entitlements of workers in general, and posted workers in particular. It would also make it easier for workers to track their social security contributions and entitlements, such as pension rights. Furthermore, it would not only help Member States holding companies accountable for avoiding decent wages or social security contributions, but could also contribute to combatting undeclared work, unsafe work environments or indecent working conditions and wages.

We need a **level-playing field for the platform economy and the offline economy** based on the same rights and obligations for all actors. All platform workers must enjoy **the same social and employment rights**, the same health and safety protection as well as the same access to lifelong learning as workers in the "traditional" economy.

Flexibility and self-determination of new working models in the digital age must not become a synonym for ever-more sophisticated exploitation and **surveillance of workers' performance**, especially in the context of the development of Artificial Intelligence (AI). Therefore, the EU should look into protections against surveillance at the workplace or the use of rating mechanisms, addressing issues such as privacy, vigilance and tracking, non-discrimination and ethical aspects. Tracking apps to monitor workers or recruitment discrimination due to the use of algorithms represent dangerous trends which have to be urgently tackled. Devices like microchip implants for workers should be entirely banned. **We must stop surveillance capitalism!** It is critically important to make sure that if data is collected during an employment relationship, it must be owned by the employee and the employee must exercise full rights to their data.

For the sake of work-life balance and mental well-being the S&D Group calls for the **right to disconnect** outside established working hours. We must further examine the different risks to workers in terms of poor working conditions, lack of security, well-being and work-life balance, including issues of additional working hours. The EU should strive for a mandatory minimum level of disconnected time per day, week and month, and this should be perceived as a new battle, similar to the struggle for an 8-hour working day.

We need to **strengthen the role of social partners** within the labour market, including collective bargaining and collective agreements. It requires a high degree of membership rate. The EU should give priority to strengthening the ability of workers to organize themselves, and if possible, provide financial incentives or other stimulating measures. The role of national social protection systems needs to be examined, for example in relation to casual and on-call work.

A genuine **European Just Transition Fund** - to be established as an instrument for the transformation of energy intensive, highly polluting, carbon-based industry - should also cover the negative societal impact of digital and technological transformations. The Fund should use public and private money, including help from the European Investment Bank. The **S&D Group will stand up for all workers affected by the digital transformation**, notably with regard to job losses due to automation of tasks and processes, as well as industrial relocations.

This requires not just extra financial commitments from the EU but also giving a strong role to the workers themselves through their union representatives throughout the transition process at all levels. **A progressive just transition** must include public-led education and training strategies, instruments on the anticipation of change and restructuring, the promotion of strong and effective social protection systems, and the respect for fundamental trade union rights and human rights.

The EU must avoid the creation of new gaps resulting from 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 a high-speed internet connection, often affecting rural areas or regions suffering from depopulation.

Digital connectivity can be a key element to address, and possibly reverse, these negative trends, since it would 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 a modernised cohesion policy.

We insist on the need to **protect people and workers potentially at risk of displacement due to AI** and to develop strategies to manage digital transition by supporting reskilling programs, improving professional education and long-life trainings for the current and future workforce with particular focus on SMEs.

More than 70 million Europeans suffer from some kind of disability. New technologies must contribute to **closing the digital gap for persons with disability**, thus supporting their inclusion in the economy and ensuring their access to essential services. 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** increase **equal and easy access** for citizens while simultaneously **reducing administrative burden and bureaucracy**. This should go beyond the digitization of administrative procedures. It implies redesigning services and the way we deliver them, and using interoperability to eliminate redundant requests.

One key question remains to be answered: ‘What is the optimal political model for today’s and tomorrow’s digital age?’ **Employment needs to undergo a transformation in order to stop the explosion of inequality.**

The industry used to be at the heart of revolutionary changes. Times, however, have changed. Today, the most drastic changes of the job market are taking place in the services sector. These changes are spreading out rapidly, leaving employees all over the world to deal with consequences. As many professional categories might be replaced more and more by automated functions and skills, the **overall level of employment might decrease.**

In some European areas, workers are already affected by a tendency towards precariousness caused by a strong downward pressure on wages. In fact, many households have not seen a real income gain in the past ten years. The rise of inequality is felt by many. **New jobs will undoubtedly be created**, yet, **many jobs may disappear** worldwide. This poses a historical challenge.

We need to develop **a new social contract** by ending and reversing hyper-privatisation and, if necessary, bringing key sectors back into public ownership. This may specifically apply in cases of new digital sectors, which have major societal impacts. The supremacy of democratically elected governments must not be a subject for compromise.

2. Digital skills and literacy

Digital skills are necessary for citizens to participate in society.

All citizens need the necessary digital understanding and skills to fully embrace the opportunities of the digital revolution. To this end, education systems must be modernised across Europe, using the EU budget to support specific national initiatives on **digital education, training, upskilling and reskilling of workers.**

We need new education programmes with an approach to learning that uses **STEAM** - Science, Technology, Engineering, Arts and Mathematics, in order to support the development of adequate digital skills and tools. At the same time, **education** should not be mainly oriented towards the immediate labour market's needs, as it **should support the personal development and critical thinking of every individual**, including arts, to promote creativity and innovation. This is especially relevant for children and adolescents and in particular for girls, resulting in substantial loss of talent due to a deeply gendered education and socialisation.

A broad variety of digital means and **new learning formats** should be used, such as distance and blended learning, as an accompanying tool on all educational levels.

The EU should promote **a "digital culture", through knowledge, skills and competences** that foster understanding of digital relevance, Artificial Intelligence and robotics in everyday life, including media literacy skills that build up an **active citizenship in the digital world.**

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 digital revolution, including the impact of digitalisation on mental health, which may affect all generations, but children and young people in particular. Media and digital competence should be enshrined on all educational levels and for all generations.

Re-skilling of the adult workforce deserves special attention. Digital skills, 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 **digital literacy for adults** on a continuous basis, taking into account existing best practices across the EU.

However, providing people with a minimum set of digital skills will not help them to find sustainable jobs. It is crucial to ensure that every individual is encouraged to acquire advanced skills and competences in order to better adapt to the future. We need, therefore, to put in place **a progressive Skills Agenda**, which would guarantee learning and training opportunities for everyone.

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 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 STEAM field.

Life-long learning will become ever more important as a key factor for companies to succeed in all sectors and for workers to maintain their employability. We need a **European-wide strategy** to improve the training and upskilling of all workers, including ICT professionals, in order to **close the digital skills gap**.

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. 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.

We need more attention and **more investments to R&D, science and the scientific community**, which is the driving force of the technological revolution. EU programmes such as Future and Emerging Technologies or European Research Council should play a decisive role.

3. Tech giants' dominant market position

We need fair competition and a level-playing field.

Worldwide, voices are growing louder to challenge the market dominance of the tech giants, particularly the big US tech companies. The **continuing and ever increasing corporate concentration and commercialism of the online economy is unsustainable** and untenable.

In the United States, proposals are being floated to **break up tech giants** like Facebook, Google or Amazon, or to create public alternatives to dominant social media firms in the form of public utilities[2] exercising strict controls over commercial and government surveillance and ensuring full transparency in the construction and application of algorithms. The United States Congress started preliminary investigation into the market dominance of Silicon Valley companies, and the US regulators (the

[2] A public utility company (usually just utility) is an organization that maintains the infrastructure for a public service (often also providing a service using that infrastructure). Public utilities are subject to forms of public control and regulation ranging from local community-based groups to state-wide government monopolies. The term utilities can also refer to the set of services provided by these organizations consumed by the public: coal, electricity, natural gas, water, sewage, telephone, and transportation. Broadband internet services (both fixed-line and mobile) are increasingly being included within the definition.

Department of Justice and the Federal Trade Commission) are pursuing antitrust investigations of companies such as Facebook, Google, Apple and Amazon.

In Europe, in industries such as energy and telecommunications, there are "ex-ante" rules promoting competition benefitting consumers and allowing the sanctioning for the abuse of dominance in these sectors. In the big tech sector, however, "ex-post" measures and **fines imposed by the European Commission** in several cases[3] **neither restored fair competition nor avoided ongoing growing market dominance** by a number of large companies, not to mention the costs which will ultimately be borne by consumers.

Therefore, we call for **a review of EU competition rules**, which should take into account future competition in digital economy, including predatory pricing strategies to achieve dominance, and which should allow for preventive measures to tackle uncompetitive behaviour, thus ensuring EU global competitiveness. This review should include merger and antitrust rules as well as alert mechanisms or regulation when systematic anti-competitive behaviour is identified. The European Commission should consider ex-ante rules for dominant digital companies as well as for closed ecosystems exercising a gatekeeping activity. Furthermore, every market concentration regarding data should be subject to thorough democratic controls.

This, however, will not be enough. To secure a fair marketplace and consumer choice, to drive innovation, and to protect our democracy and fundamental rights, the EU should explore the political and legal possibilities to **tackle the tech giants' abusive market dominant power**. We need to prevent large tech companies from buying their competitors. When one company has too much market power, it should be not be permitted to merge with others. We should also think about the possibility of strengthening the European Parliament's role in competition policy, including in cases when the Commission may decide to open investigations.

For the sake of ensuring fair competition and guaranteeing **a level-playing field**, the European Commission should carefully assess whether there is a need for these big tech companies to be broken apart in order to prevent them from unfairly extending their dominance or systemic importance in the market.

Possible solutions may differ depending on the sector. When firms own an essential platform and at the same time compete on it, the best option would be **structural separation**. This would cover Amazon's e-commerce activity and Google Search. At the very least, such companies should treat users of their platforms in a fair, reasonable and non-discriminatory manner.

For powerful messaging and social networking services, such as Facebook, a **requirement of interoperability**, whilst fully complying with all personal data protection requirements, is of key importance. It would allow people to use another service, and still be able to communicate with their friends and family that remain on these platforms. We have such rules for telecoms companies (people can call each other also if they use different phone providers).

One factor that causes tech giants to grow into quasi-monopolies is the insufficient enforcement of existing privacy and data protection rules. Under the GDPR,

[3] The European Commission took action in several cases: for example on Apple's tax arrangements with the Irish authorities, Amazon tax arrangements with the Luxembourg authorities; on Google's abusive practices in online advertising and an illegal advantage-taking of its own comparison shopping service. Other antitrust investigations are ongoing, like for example on Amazon's alleged breach of EU competition rules by using sensitive data from independent retailers who sell on its marketplace.

EU Member States have a legal responsibility to provide adequate funds for their data protection supervisory authorities so that they can **efficiently enforce data protection law**. Furthermore, we should explore all possibilities to **fight data-monopolies** by means of competition law.

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

The EU must strive for a level-playing field in which smaller online operators would thrive without unnecessary burdens imposed on them. We must protect **European SMEs** and the **cultural and creative sector**, which play an essential role in sustaining social cohesion and cultural diversity in Europe as well as democratic values.

4. Digital taxation

Taxes should be paid where profits are generated.

Traditionally, taxation has been heavily reliant on labour. The **digital revolution** alongside with robotisation, automation and Artificial Intelligence have been **changing the way** in which **added value is created** in our economy and **benefits redistributed**.

In addition, the digitalisation of our economy as a whole is creating **challenges regarding our current corporate taxation policies**. 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.

This is why the **tech giants like Google, Apple, Facebook or Amazon**, as well as all large firms being digitalised, make enormous profits all around the world while using the possibility to **locate their profits in only a few low tax countries**. Such a situation is **completely unacceptable** because it distorts the functioning of the EU internal market as well as the global economy, thus creating further inequalities.

Taxation is used to finance public goods - schools, hospitals, public libraries, roads, and network infrastructure, thus advancing equal opportunities for citizens. **Tax avoidance leads to 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.

Therefore, we fight for the adoption of legislation that will **ensure that large companies pay their fair share of tax:**

- We ask for a **minimum effective level of taxation** (18%) ensuring that all companies - the tech giants included - pay their fair share of taxes. **Taxes should be paid** where services are provided, where activities and transactions take place and, most importantly, **where profits are made**!
- The Common Consolidated Corporate Tax Base (CCCTB) and the Significant Digital Presence (SDP) are still under discussion, which offers an opportunity to **stop tax competition** within the EU and ease administrative burden of companies.
- At international level, we support the OECD negotiations on reallocating taxing rights to take digitalisation into account, as well as the discussion regarding a minimum level of effective taxation. Therefore, the EU should support an ambitious international deal, or otherwise it should go ahead with **an EU solution**!
- We continue our call on EU governments to use the opportunity to significantly improve **corporate and tax transparency** by finally agreeing on a position and

giving green light to negotiations with the European Parliament on public country-by-country-reporting (CBCR).

Such **digital taxes** should be included in the basket of **EU's Own Resources** (ORs) and could constitute one of the revenues needed to complete the reform of the ORs, which aims at the reduction of the traditional GNI contributions. Therefore, such genuine own resources (CCCTB or digital tax) could generate means for promoting social justice by redistributing taxation away from ordinary people and SMEs towards the wealthiest individuals and big multinational companies.

Value creation 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. We should take the lead on this innovative issue and define how the **future of taxation in a highly digitalised 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 or the Panama and Paradise papers showed the difficulties of verifying the founder's real existence and identity. We need to strengthen the role of "gatekeepers" such as notaries, courts and competent authorities to be able to detect fraud and fake documents. The EU should create a **fully digitalised European business register** to enable exchange of information between the Member States' respective company registers.

As regards online procedures for companies, any further measures to **upgrade the 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.

5. Disinformation, fundamental rights, democracy

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 European democracy. **Disinformation**, false information or hate speech, especially when spread deliberately and adversely influence our democratic discourse and processes and have even affected the outcome of democratic elections. This phenomenon spreads fear and dangerously **diminishes the trust of our citizens in democratic processes** and institutions.

Whereas the **fundamental rights** to freedom of expression and opinion, as well as to the protection of personal data and private life, **cannot be put into question**, we need to find adequate ways to preserve those rights and at the same time limit the spread and impact of misleading or false content which otherwise could be considered as factually correct.

Much of the misinformation and disinformation 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** - in the form of a public registry - and clear **limits to behavioural advertisements** (including use of behavioural data for anticipating and guiding people's decisions) would help address

these issues. The adoption of a strong **e-Privacy Regulation** would help achieve this aim, and should be strongly supported.

The EU has been pushing to make **online platforms and social media more responsible** and accountable for the spread of disinformation on their platforms. Self-regulation represents an important element of the platforms' responsibility. However, accountability for failing to address these serious issues also needs to be established.

All **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 beyond doubt. They should also **empower users** to better detect and flag up disinformation.

We should particularly address the issue of so-called "**Deepfakes**", which create false impressions that may have a damaging impact on our democracy by misleading people and undermining their trust in democratic processes, institutions as well as individuals (candidates or elected office-holders). Deepfakes can be deployed by malign foreign or domestic actors to interfere in democratic elections. We need rules to make creators of deepfakes accountable when posting altered videos online. Moreover, all such videos should be labelled with a watermark and a disclaimer identifying them as manipulated content.

We need **media literacy programmes** which should be implemented across the EU and be included in the educational systems. Media literacy education can empower citizens to evaluate 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.

The European Commission should assess the effectiveness of the '**Code of Practice on Disinformation**', and after consulting with the European Parliament, and if deemed appropriate, make further proposals to strengthen the EU's response to disinformation.

6. Artificial intelligence (AI)

No AI without ethics, legal safeguards and fundamental rights!

The EU needs a new legal framework on AI and robotics focusing on upholding **fundamental rights, ethical aspects, legal safeguards and liability**, thus protecting our democratic societies and citizens as users and consumers. There has to be significant investments in robotics and AI, including to digital start-ups and scale-ups. Europe is lagging behind in the development of AI applications, resulting in an urgent need to develop our own **European capabilities** to re-enforce **Europe's autonomy**.

Currently, both China and the US are investing heavily in AI. So far, however, much of that investment has gone into ways to better target advertisement or to automate labour. Europe should beef up its investments (through public and private funding) in robotics and AI, to drive innovation in the public interest and in line with **European values and laws**.

To become strong in the field of AI, both in the public and private sector, Europe needs to make significant investments in the **accessibility of open high-quality non-personal data** sets. We need to create an infrastructure where non-personal data can

be shared, in order to stimulate generators of high-quality data, such as public institutions and governments, to share it easily.

The development and use of new AI technologies has the potential to transform our societies beyond recognition. The EU will need **binding ethical guidelines** covering the development, design, production, use and modification of robots and other AI technologies. It will require ambitious and **long-term research and innovation policies**, combining private and public investments.

Democratic societies must become aware that controls must also reach engineering design, imposing democratic constraints on Artificial Intelligence and promoting technologies aimed at **improving public services with collective benefits**, while developing commercial products.

AI will play a role in the education systems, in the use of interactive technologies or facilitating access to education to children in special circumstances, such as 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.

It is of paramount importance to ensure that any new legislation in this field does not undermine **fundamental rights**, especially **non-discrimination** and the **protection of privacy and personal data**. We cannot control what we do not understand, therefore, transparency and independent oversight will be crucial to get a grip on how these technologies function and are used. There will have to be strong provisions on exhaustive **ex-ante and ex-post risk assessments** and on immediate **redress mechanisms** to deal with potential and resulting breaches of fundamental rights.

The **AI in machines and robots must be free of bias** and neither discriminate nor be based on any stereotypes, for example on grounds of gender or gender identity, ethnic or social background, disability or sexual orientation (for example with regard to facial recognition and technologies using other types of sensitive personal data). The EU needs to ensure that none of its official **languages** are discriminated and made vulnerable by the use of AI, and that there are data and language sets available in all EU languages.

We need a **horizontal and technologically neutral framework on intellectual property rights** applicable to various sectors where AI technologies and robotics will be utilised. The EU has to strike the right balance between the geopolitical dimension of EU innovations 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 (most of the patents get registered in countries like China, South Korea, the United States or Japan).

The EU has to set up clear **liability rules** governing Artificial Intelligence and machine learning. **Europeans have to** be reassured that they can **trust the new technologies** whose aim is to serve people's wellbeing. We have to fight against wealth accumulation by tiny rich elites as well as against the establishment of a **surveillance capitalist system**. Questions regarding the risks posed by AI (from the development stage on, through to the moment when products and services reach the market, until when the effects brought by those products or services become evident), or when it comes to the consequences of its possible misuse - all these issues will have to be clearly addressed.

As many public and government institutions such as judicial bodies, law enforcement or military start using **predictive algorithms** for a variety of purposes, the future legislation must pass the strict test of **necessity and proportionality**, provide appropriate **safeguards and remedies** and clearly define the **responsibilities and accountability** as well as proper **public oversight**.

In addition, algorithmic bias reflecting the values of those producing these algorithms can adversely affect citizens on the basis of gender, ethnicity, language, age, disability and social/cultural background. **Transparency** is, therefore, essential in enabling equality of access and ensuring that AI products be fair, non-discriminatory and free of bias.

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

In cooperation with international standardisation bodies, the EU should continue to further **improve standards** on issues such as **safety, reliability, interoperability 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 instead it should develop a single set of EU rules taking into account the interests of users, 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 Artificial Intelligence, in particular in education, medical, legal or accounting professions or in the law enforcement sector. People - as citizens, 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.

Artificial Intelligence 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.

Artificial Intelligence will also play a key role in designing and identifying the **impact of human activity on the environment**. Increased digitisation will bring new energy needs, but it will also contribute to bring efficiency into previously energy intensive sectors providing better understanding of processes, leading to their improvement.

7. Digital privacy and protection of personal data

Digital privacy and personal data must be protected.

Gradually, digital surveillance and online intrusion threaten to dismantle our fundamental rights, such as the right to privacy, and undermine our democracies. Big corporations try to take away citizens' privacy and freedom in exchange of a vast variety of online applications and digital services. We must **protect the digital privacy of Europeans against the invasive use and abuse of their personal data**.

Trust is a fundamental requirement for a functioning digital society. In order to secure the citizens' trust when engaging in online processes, we must ensure that their **fundamental rights are safeguarded in all aspects of digital life**. Transparency and accountability in online processes, transactions and algorithms are indispensable.

Personal data always belong to the person concerned. Whoever processes them needs to comply with data protection principles such as purpose limitation, security of processing, and the general respect for fundamental rights.

The **GDPR** was an international 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 strict and guidance is abundant. Therefore, the EU Member States have a legal obligation to adequately fund and staff their supervisory authorities in order to make this fundamental right a reality on the ground. However, we also urgently need the upgrade of the EU **e-Privacy** rules, which are supposed to protect the privacy of the online communications of people, but which are hopelessly outdated.

The **EU cannot allow any form of censorship**. We must ensure that no hard-fought fundamental right is undermined in the course of the digital transformation. We need to focus on "data education" in digital literacy programmes and campaigns.

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.

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**. 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. The citizens must enjoy the same level of treatment, protections and rights of expression in the digital and physical spheres.

8. Cybersecurity, security and defence

In cyberspace, fundamental rights and rule of law must be protected.

Europe needs a **global, open, free, stable and secure cyberspace** where **human rights, fundamental freedoms and the rule of law fully apply** while

preventing the spread of hate speech and disinformation campaigns. A means to that end could be the **European cybersecurity competence centre**.

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.

ENISA, the EU Agency for cybersecurity, has an important role to play. It should establish a voluntary **EU-wide cybersecurity certification framework** for digital services, processes and products, including rules on safety and security by design of connected products. 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** against the EU institutions, national governments, other 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.

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.

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 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's values and fundamental rights.** All emerging technologies, including Artificial Intelligence, that are used in weapons systems must be

developed and applied according to strict ethical principles and in compliance with international law.

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**, and potentially, of **mass destruction**. The EU must be prepared for cyber-attacks on critical infrastructure that may have potentially devastating effects on our economies and the wellbeing of citizens. EU policies need to be revised to protect various sectors against large-scale attacks, including public administration or food processing.

Perpetrators of cyber-attacks can include foreign governments, non-state entities or private individuals. The NIS Directive should guarantee a **high-level of security in the EU**. Currently, in the event of large-scale attacks, the EU's response at the operational and political level would be rather limited. Therefore, cybersecurity should be integrated into existing EU-level crisis response coordination mechanisms.

9. Digital internal market and consumer protection

Same rules and equal consumer protection in online and offline economy!

Online platforms are shaking up highly regulated traditional business models, raising questions of **equal conditions for all market players**, responsibility, quality of the service and safety and protection of consumers. We need **a level-playing field** to ensure that there is **no unfair competition between online and offline sectors**. The EU has to guarantee that boosting digital companies does not happen to the detriment of offline companies.

Unfair commercial and trading practices on platforms, including the contractual validity of their general terms and conditions, should be tackled, as general terms are often a non-negotiable condition to use the service of a platform.

The **development of e-commerce** poses certain **challenges** regarding the **protection of health and safety of end-users** from non-compliant products. A range of non-compliant and unsafe products, which have been prohibited from sale or recalled from the market or which present inadequate product labelling and safety warnings, remain available for sale online and can cause detriment to consumers. The **EU needs a stronger and more harmonized framework** for checks on products entering the EU market.

Special attention should be given to proliferation of **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.

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 the more vulnerable consumer groups. New legislation might be the right response to all these challenges.

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

The **internet has to be a well-functioning and neutral level-playing field**. Therefore, interoperable technologies should be promoted and no region within the European Union should be left behind. The access of consumers and businesses to digital goods and services throughout Europe should be improved.

We also call for a **level-playing field between online and offline rules** for services and goods. Therefore, the laws and regulations, especially regarding employment conditions stemming from collective bargaining agreements, of countries where services are delivered to, shall be respected. No European legislation should lower the **consumer protection standards within the EU**, thus respecting national consumer protection laws.

Current e-Commerce rules date back to the year 2000 and they urgently need an update. Any **revision of the e-Commerce** directive through **a Digital Services Act** should ensure the **respect and protection of fundamental rights of consumers**, of **their privacy and autonomy** in the digital age. It should create a fair level-playing field for all digital companies, not only for the "big tech", including in the platform and collaborative economies. The **Digital Services Act** must deliver **a comprehensive coordinated approach** to address all these challenges, including the use of automated decision-making based on algorithms or robotised software which can profoundly change the functioning of markets and also influence the choices people make, including political ones.

Platforms should be **obliged to make their used algorithms transparent** as these may easily influence consumers' choices and opinions, for example by profiling in advertising or by price-personalisation. The problem of commercial surveillance needs to be addressed. In order to improve consumer confidence, an **Electronic Complaint Book**[4] should be created.

The general principles under the e-commerce directive of **limited liability of platforms** for content online and "notice and take down" should be carefully assessed, in full respect of fundamental rights. The prohibition on a general monitoring obligation should be maintained. Overall, **companies should behave ethically and in a socially responsible manner**, taking into account sustainability and the interests of society.

We should give special attention to the **European cultural and creative sector** which plays an essential role in sustaining social cohesion and cultural diversity in Europe.

With regard to the **roaming regulation** (currently in force until June 2022), the EU needs to take the necessary steps, including legislative measures, to ensure that Europeans continue to benefit from roaming without surcharges in the coming years and that wholesale markets are working well.

[4] For example, Portugal introduced such an Electronic Complaint Book on national level, as a new digital platform which allows consumers and users to submit their complaints in electronic format. See here - https://www.livroreclamacoes.pt/inicio

10. Data & data economy

People should have control over their data!

Protection of personal data, privacy and data security will likely continue to be under ever-growing pressure. Personal data has to be duly protected, as **data protection and privacy are fundamental rights under EU primary law that cannot be put into question**. The GDPR experience shows that **we can regulate** the processing of personal data **and steer innovation** in the right direction.

We need to look into the **ways in which companies collect, use and share data**, and we have to raise questions of access and ownership of data, exploitation of data, as well as of data sets audits, while fully respecting data protection laws. We must promote measures to support **transparency and accountability**.

There is a risk of algorithms and big data becoming discriminatory. In particular the algorithms, due to the way they are developed, might contain various biases (i.e. gender, ethnicity or social class based) that can lead to discriminatory results. **Transparency of algorithms** and of data collection is therefore of utmost importance. **Online platforms must** comply with the GDPR and e-Privacy Directive and **respond to users' concerns** by informing them more effectively about what kind of personal data is collected and how it is further shared and used.

It is crucial to **raise awareness**, especially among the most vulnerable (children young people or seniors) about the personal data which consumers knowingly or unknowingly provide in exchange for access to many so-called free services. **Citizens have to be in control of their data!** They **should be empowered** (for example with the help of mediators of individual data - union-like organizations that would negotiate payment on behalf of users) to decide how and when their personal data is collected and used, and they **should benefit from the value of their data**.

If **personal data is made available** to public institutions, provided it is done on a proper legal basis, it can be used to **support public policies** and to **improve public services**. Predictive analytics should prevent problems before they occur and could contribute to a more efficient design of public policies. This could be done in different areas, such as healthcare, or to address various issues and challenges, such as unemployment and long-term unemployment, online gambling addiction or allocation of EU funds. If such predictive analytics use personal data, they have to fully comply with data protection rules, including the principles of purpose limitation and data minimisation.

Under the GDPR, there is the right to data portability, so companies are under legal obligation to provide mechanisms for users to being able to take and transfer all their personal data to another platform. There should be **no barriers to exit from, or transfer between platforms.**

The EU should devise a clear strategy for developing a strong data economy. **Europe must become the world leader** in both - the **protection of privacy and personal data** and the **data economy**. EU-wide non-personal data flow and secondary usage of anonymized data will allow the EU to maximise the potential of digital technologies, and to sustain economic growth and increase productivity.

We need to **break down the business model of micro-targeted advertisements**, by constraining or even prohibiting it. A first step would be to look at

which data the users wish to keep, use or transfer, and then, in second step, prohibit the collection of specific data, such as medical data or data obtained from minors.

11. 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 self-determination. Europe should exploit the full potential of future technological developments.

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.

With regard to **network security**, individual Member States are proposing their own legislative acts in order to restrict some telecom vendors. The European Commission has published a high-level report on the coordinated risk assessment of 5G networks. 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 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.**

We need European standards to assess the trustworthiness of providers (companies) of digital infrastructure from third countries, in particular those where governments can influence or directly control these companies. The EU needs **strong public procurement rules** to ensure that only trustworthy companies are involved in the **development of European digital infrastructure**, driving innovation and investing into public interest technologies.

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. The EU must defend the **principle of net-neutrality** to promote diversity and competition in the digital sector.

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 **technologies mitigating 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.

There is a growing demand for computing power, **block-chain and distributed ledger technology (DLT)**. These technologies are changing the way citizens and organisations collaborate, share information, execute transactions and deliver services. They should be at the heart of our future strategy in Europe, as they will continue impacting the way we communicate and interact with digital services and with other humans.

New technologies may allow the **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-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**.

Digitalization and **new technologies** have both **negative and positive impacts on the environment**. On one hand they allow to better exploit and control 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. The 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.

12. Digital gender equality

No gender biases! No gender discrimination!

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 a real equality, not just employability**.

Artificial Intelligence has 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, arts and mathematics (**STEAM**) 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.

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**. 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, since rural areas are demographically male dominated due to limited labour opportunities for women, resulting in overall population decline.

13. Industrial policy in the digital age

European industry must embrace the digital revolution.

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.

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.

European industrial policy must align different policy areas, such as digitalisation, trade, environment, research, health, investment, competition, culture, energy and climate, to **combine horizontal elements** with specific approaches to **important strategic sectors.**

Innovation means capital for high productivity. Infrastructure development for industrial agglomerations and urban areas is essential for an industrial and innovative society, thus it will also contribute to **mitigation of environmental and social impacts**, and address **sustainability** issues simultaneously.

Supporting **European investments** on 5G infrastructure is crucial to preserve **European strategic interests**, while promoting innovation. Block-chain technology and its implications in various sectors (from agriculture to smart contracts, to consumer protection, to new business models for content production) must be further looked at and taken into consideration in EU industrial policy and legislation.

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 generation (virtual reality, augmented reality) by using digital tools in a positive way to encourage people embracing the European cultural diversity.

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. Moreover, **digitalization of insular economies** (small countries, islands and remote regions) deserves special attention due to their geographical and size limitations.

14. Digital trade and e-commerce

Digitalisation must facilitate sustainable trade and protect citizens.

We are committed to improving the **EU's trade policy**, our trade agreements, and the WTO, to better **correspond to the increasingly digitalised world**. We have to **tackle the digital trade barriers** often referred to as the "new tariffs" of our time.

Whilst we support 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. At the same time, we call for a **more inclusive, open and transparent negotiating process**, involving more countries.

We should modify the incentives that favour the import of cheap consumer goods that negatively affect the environment. We need to make sure that **imported goods fully comply with our product safety rules and do not harm consumers**. This will require better international cooperation between market surveillance, consumer protection and competition authorities.

Europe will have to address also the issue of **cryptocurrencies** and the relating challenges, such as the anonymity surrounding cryptocurrencies and risks of money laundering, terrorist financing and tax evasion. Crypto-activity, however, goes beyond European borders and, therefore, international cooperation will be necessary to design and enforce a global regulatory framework on cryptocurrencies.

We should promote a competitive, trustworthy and future-proof 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**. Consumers' payment data must not be used for advertising purposes. The **accumulation of tech giants' market power in the financial sector** must be prevented.

15. 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 easy and more accurate diagnoses, improved treatments, R&D for new medicines, customized medical devices and more. These **new technologies** have led to an **exponential growth of health data**.

We support the digital transformation of health and care to maximize the **efficiency, accessibility and sustainability of health services** in the EU Member States. 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 the European citizens. This should be a cornerstone for the creation and implementation of the **European Health Data Space**.

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 or pseudonymised health data can be used for **scientific health research**. This 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.

Investment is crucial to **reduce the digital divide in health and care** between Member States. EU's financing instruments should be used to ensure equal and just access to quality health care for all.

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** by all citizens.

16. Agriculture in the digital age

More sustainable agriculture: produce high quality food with fewer resources.

Modernisation of agriculture can positively affect society and revitalise rural services through digital and social innovations. Such programmes improve quality of life and **make rural areas more attractive for young people**, especially young farmers.

Digital technologies are increasingly important to farms and other agricultural businesses. As farmers increasingly use new technologies, the more data about their farms, their land, their animals and crops become accessible to the companies which have developed and operate these technologies. This raises questions about the

ownership and protection of data, which belong to the farmer, but there are currently no clear safeguards in this respect.

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, farmers need to administer their agricultural activity effectively and efficiently, to be able to fully benefit from the Common Agricultural Policy. Agriculture depends on lively rural communities. Equal access to broadband is a key part of maintaining those communities and economies in good shape and leads to a **fairer, more sustainable and more transparent agriculture**.

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. **More skilled workers** could be interested in entering into agriculture. There are, however, risks as well: **less-qualified workers** could be replaced by machines. Generally, digitisation techniques will be mostly used on capital-intensive big farms, which could lead to a further structural change in rural areas.

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 conditions or soil data can help farmers to plan and optimize their planting season.

We must ensure an efficient use of **R&D funds towards the digitalisation of agriculture**, for example under the Horizon Europe research programme.