GOING TO DIGITAL ECONOMY: AN INTEGRATED APPROACH TO POLICY MAKING

Olha Pylypenko¹

¹Ph.D., Associate professor, Associate professor of Finance and Accounting Department, V.I. Vernadsky Taurida National University, Kyiv, Ukraine, e-mail: pylypenko.olha@tnu.edu.ua, ORCID: https://orcid.org/0000-0003-3997-9108

Citation:

Pylypenko, O. (2023). Going to digital economy: an integrated approach to policy making. *Business model innovation in the digital economy:* monograph. OÜ Scientific Center of Innovative Research. 2023. 208 p. pp. 74-98, https://doi.org/10.36690/BM-ID-EU-74-98



This monograph's chapter is an open access monograph distributed under the terms and conditions of the <u>Creative</u> <u>Commons Attribution (CC BY-NC 4.0) license</u>

OPENACCESS

Abstract. The digital economy is a type of economy where the key factors and means of production are digital data (binary, information, etc.) and network transactions, as well as their use as a resource, which makes it possible to significantly increase the efficiency and productivity of activities and value for the resulting products and services. The digital economy encompasses business in all sectors of economic activity, i.e. not only in the information and telecommunications sector, but also in basic industries, agriculture, construction, etc. The analysis of digital trends makes it possible to predict the development of a specific economic, technological and even social phenomenon in the future. The development of the digital economy, depending on the assessment of criticality and the need for rapid and deep changes in the traditional economic structure, can develop according to two scenarios. The inertial (evolutionary) scenario involves the inertial continuation of the trends of the past, that is, the perception of technology and digitalization of the economy and the use of human capital as non-priority. The economy remains inefficient, labor migration and "brain drain" continue, and products lose competition on foreign markets. The target (forced) scenario envisages the transition of the economy within 5-10 years to the development and appearance of a significant share of the digital economy in its structure (up to 65% of GDP). It includes ensuring the rule of law and removing institutional (legislative, tax, etc.) barriers that hinder the development of the digital and innovative economy; systemic state stimulation of digitalization of the economy and business sectors; initiation by the state of large-scale transformational initiatives and digitization projects, in particular based on modern models of public-private partnership. According to the target scenario, the key strategy for digitization should be the focus on the domestic market, and the key initiatives should be the formation of motivations, demand and needs for digital technologies among consumers (businesses, the state, citizens). Creating a digital society means creating a society that intensively and productively uses digital technologies for their own needs (self-realization, work, recreation, education, leisure for everyone), as well as for the achievement and implementation of common economic, social and public goals. The way to an effective country and economy is through the development of the domestic market for the consumption of information, communication and digital technologies.

Keywords: digital economy, economic growth, digital growth, key policy indicators, digital society, digital security, digital transformation strategy

The technologies development evolution. The modern world has already taken the first step towards a fundamentally new technological, economic and social reality. However, the challenges ahead modern industrial society, it is difficult to overestimate. It's about change in the global socio-technological structure, the result of which is complete reformatting the systems we are accustomed to, forming new social and economic strategies. At the same time, the technological paradigm is changing, management models and social norms are changing, and large-scale ones are taking place demographic changes.

An important feature of today is the rapid increase in digital gaps, endangering the growing backwardness of developing countries. Production for any country the sector and the policy of maintaining its own technological level are strategically important national objectives for economic development, services and income growth and national welfare. Today it is complete the thesis that "any nation or group of nations that does not have the developed manufacturing sector will be at the mercy of more competent countries. Any population, rich or poor, needs a strong production base in order to prosper in the economy and defend themselves politically" (Rynn, 2000).

The potential for economic growth is determined by production capabilities of the country, which form different levels of production capacity:

1. Zero level - consumption of other people's goods and services (imports). Lack of production in the country. Proceeds from resale imports.

2. The first level is the production of goods on someone else's equipment. Import dependence on the manufacturer.

3. Second level – production of own production equipment different goods (assembly level). Import dependence on manufacturers of machines, assembly lines, other reproduction equipment required in production.

4. Third level – production of equipment for the production of equipment. Technology development.

The development of technologies is carried out by the richest countries and the most influential economies, which are called industrial states on which they depend countries consuming this equipment. Own technologies are able to provide rapid growth of industry at all levels, as well as economic independence and information security. Businesses working on technology development create modern production facilities for everyone else industries, automate, mechanize enterprises, provide continuous technical re-equipment, introduce innovations, and as a result increase their productivity, and thus affect overall growth productivity in the economy as a whole. Countries that depend on technology imports will be forced to remain on the periphery of the developed world.

Informatization and digitization of public life covers all aspects of the functioning of the economy, therefore the transition to the digital economy should be taken into account in the management system of the national economy, and information and information and communication technologies should be considered as important components of ensuring economic growth and economic security (Rumyk, & Melnichenko, 2023).

Today, we are witnessing a rapid pace of reindustrialization of technologically advanced countries on new grounds (additive technologies) (3D printing), robotics, renewable energy, etc.).

The current state of development of digitalization is quite significant (Table 1).

Tuble 1. Digital al value work							
	Indicator Value						
Indicator	Jan	Urbanisation	vs	Ion 2022	Urbanisation	vs Population	
	2021	Ulbanisation	Population	Jan 2025			
Total	7.83	56 40/	Х	8.01	57.20/	х	
population	billion	30.4%		billion	37.2%		
Unique mobile	5.22	v	66.6%	5.44	Х	68.0%	
phone users	billion	Х		billion			
Internet users	4.66	Х	59.5%	5.16	x	64.4%	
	billion			billion			
Active social	4.20	v	53.6%	4.76	х	59.4%	
media users	billion	Х		billion			

Table 1. Digital around the world

Source: Digital 2021, & Digital 2023

Essential headlines for mobile, internet, and social media use. Internet user numbers no longer include data sourced from social media platforms, so values are not comparable with previous reports.

Today, the growth of digitalization is quite impressive (Table 2).

Table 2. Global digital growth

Indicator	Indicator value				
	Jan 2021	Jan 2021 vs Jan 2020	Jan 2023	Jan 2023 vs Jan 2022	
Total population	+1.0%	+81 million	+0.8%	+67 million	
Unique mobile phone users	+1.8%	+93 million	+3.2%	+168 million	
Internet users	+7.3%	+316 million	+1.9%	+98 million	
Active social media users	+13.2%	+490 million	+3.0%	+137 million	

Source: Digital 2021, & Digital 2023

Despite these impressive figures, it's worth noting that the ongoing coronavirus pandemic has significantly impacted research into internet use around the world, so many countries have been unable to provide updates to internet user numbers in the past 12 months.

As a result, internet user numbers have likely grown more than the reported 7 percent, and we may see 'corrections' to these figures once everyday life (and research) can return to normal.

The digital economy is significantly changing traditional business processes. With the achievement of the most complex levels of digitalization in the economy is a radical transformation of industrial relations of participants, resulting in is the integration of production and services into a single digital (cyber physical) system, in which:

- all elements of the economic system are present simultaneously in the form of physical objects, products and processes, as well as their digital copies (math models);

- all physical objects, products and processes due to the availability of digital copies and elements of connectivity become part of an integrated IT system;

- due to the availability of digital copies (mathematical models) and being part of a single system, all elements of the economic system are continuous interact with each other in a mode close to real time, model real processes and predicted states, provide constant optimization of the whole system.

Developing and implementing appropriate policies for the digital age is a complex task that can bring many benefits. European countries have developed an integrated Going Digital policy that helps countries shape policies for an inclusive digital future. The framework recognizes technology, data and business models as drivers of digital transformation.

The framework includes seven interrelated policy dimensions: access, use, innovation, jobs, society, trust and market openness (OECD-1, 2020). Each of the dimensions brings together multiple policy domains that need to be considered jointly. Leveraging the benefits and addressing the challenges of digital transformation require co-ordination across all policy domains identified by the framework.

Access to communications infrastructures, services and data underpin digital transformation and become more critical as more people and devices go online.

Key policy domains and indicators of Access (Figure 1).

Communication infrastructures and services facilitate the use of digital technologies and facilitate the interaction between connected people, organizations and machines. They provide the basis for an open, interconnected and distributed Internet that provides a global free flow of information. High-quality access to competitive networks and services at competitive prices is fundamental to digital transformation.

Data is becoming an equally important resource. In many contexts, data is the driving force of economic activity and the overall contribution to production, but the benefits depend on the availability and availability of data.

Expanding access to and sharing of data is therefore important, although such decisions need to be balanced with data privacy and security considerations, in particular. Governments can improve access in four key ways.



Figure 1. Key policy domains and access indicators

Source: systematized by the author

The first key and direction is investment. Policymakers can encourage investment in communications infrastructure, especially broadband networks, by encouraging the deployment of more fiber in networks to significantly increase the speed of technology use. Among OECD countries, the private sector invests the largest share in communication infrastructures and services. However, governments sometimes support such investments when it is not economically feasible otherwise.

To stimulate further investment in the network, policymakers need to remove barriers to investment and improve competition. Some important barriers include the availability or use of key technical means, including Internet Exchange Points (IXPs), spectrum, and IPv6 addresses.

The second key and direction is communications infrastructures and services. Communications and services infrastructure policy is critical to facilitating the deployment of high-speed infrastructure. For example, simplifying licensing requirements, eliminating regulatory uncertainty, and facilitating effective access to travel rights can help stimulate investment. These regulatory issues may become increasingly important in the light of next-generation wireless networks ("5G") (OECD-284, 2019). In some countries, the lack of adequate infrastructure, such as

electricity, roads and ports, can be a significant barrier to investment. Removing illegal restrictions on foreign investment can also stimulate infrastructure investment.

The third key and direction is competition. Policymakers also need to increase competition in the communications infrastructure and services markets to stimulate private investment and help further deploy fiber in fixed networks. This can support the increase in speed and bandwidth of all next-generation technologies, including 5G networks (OECD-284, 2019). Competition between infrastructure and service providers influences investment and pricing decisions. This can improve the quality and speed of broadband access, including for underserved populations. Competition policy should ensure that users benefit from a wider choice of services from networks and service providers, or through bundled or simple voice, data and video offerings.

The fourth and last key and direction is regional development. Regional development policies are important to bridge the digital divide, namely the differences in access to broadband access in urban, semi-urban, rural and remote areas. Governments may decide to address the critical bottlenecks of needed private investment in rural areas by investing in high-speed highways or transport infrastructure (OECD, 2017). Public investment is often driven by open access policies to avoid encouraging monopolies in underserved areas (OECD-264, 2017).

Along with communication infrastructures and services, access to data flowing through such infrastructures is becoming increasingly important as data is a key source of value and its efficient and innovative use and reuse can stimulate economic and social benefits. However, these benefits, from innovative applications to increased transparency and accountability, depend on the availability of data. As a result, expanding access to and sharing of data is an important policy issue in the digital age (OECD-1, 2019).

Key areas for access policy:

1. Promote competition to stimulate investment in communication infrastructure and services. Depending on local market conditions, having more mobile network operators (for example, four instead of three) can lead to more competitive and innovative services. Passive infrastructure sharing and co-investment can also help expand coverage.

2. Ensure the availability of technical facilities such as Internet exchange points, efficient spectrum allocation and next-generation Internet protocol addresses. Reduce administrative barriers to investment, such as burdensome licensing requirements and difficult travel rights.

3. Increase connectivity in rural and remote areas, for example by investing directly in high-speed fixed networks or encouraging private investment. This may include competitive tenders, tax exemptions, low-interest loans, government support or lower spectrum fees.

4. Expand access to and exchange of data, balancing the benefits and risks, taking into account legitimate national, commercial, private and security interests through, for example, contractual agreements, limited data sharing arrangements, data portability and open government data (OECD-2, 2019).

The use of the capabilities and potential of digital technologies depends on how they are used. Effective use enables people to participate in society, firms to increase productivity, and governments to move to digital technologies and use a user-centered approach. The widespread and effective use of digital technologies and data requires an awareness of the opportunities they bring, business dynamism, investment in information and communication technologies (ICTs) and additional assets, especially skills.

At the same time, policies need to build trust in the digital environment, for example by empowering people and organizations to better manage digital risks.

Key policy domains and indicators of Use (Figure 2).



Figure 2. Key policy domains and use indicators

Source: systematized by the author

The first key and direction is digital government. Digital government strategies help to provide a more integrated approach to the digital transformation of government and the public sector (OECD, 2014). Most OECD countries have digitized some aspects of public service delivery (eg public procurement and tax collection). However,

large differences between countries persist. There is still great potential for more integrated approaches to digital government.

This includes the use of digital technologies to digitize analog processes and services; reorganization of administrative procedures to make them digital for the project; make user needs change drivers; and the discovery of government data. In addition, countries are increasingly using a "mobile first" approach to digital government.

The second key and direction is investment. Unlocking the potential of digital tools for firms to increase productivity requires successful dissemination, which depends heavily on firms' investment in ICT as well as public investment in infrastructure and equipment. Countries encourage investment in ICT through financial support or incentives for the purchase of ICT equipment or services, as well as non-financial support (e.g. targeted training), including (OECD-280, 2019). Effective use of technology also requires firms to invest in additional assets, including knowledge-based capital (KBC). KBC's assets include research and development (R&D), data, organizational capital and skills.

The third key and direction is business dynamism. The spread of technology is due to the dynamism of the business, which depends on the efficient allocation of resources. The digital transformation of firms involves experimentation and learning. Some firms are successfully implementing digital tools and expanding rapidly, while others are downsizing or exiting the market (Andrews, & Criscuolo, 2013). Business dynamism can benefit from structural reforms. Some policies may affect competitive pressure and business dynamism, and in turn, the spread of technology and better allocation of resources. These include labor market regulation, employment protection legislation and the development of insolvency regimes. For example, governments could impose lower penalties for bankruptcy and reduce barriers to corporate restructuring of insolvent companies (Sorbe, Gal, Nicoletti, & Timiliotis, 2019).

The fourth key and direction is small and medium-sized enterprises. Effective use of digital tools is becoming increasingly important for small and medium-sized enterprises (SMEs) to improve business processes, innovation, expansion and internationalization. However, SMEs lag behind large companies in implementing digital tools and, most importantly, in using advanced ones. The main obstacles are lack of awareness; limited collateral for risk and access to finance for investment in ICT and additional assets; and lack of human resources and capabilities (e.g., ICT professionals). To help overcome these barriers, governments need to better target policy on SMEs (OECD-2, 2019).

The fifth key and direction is skills. The dissemination and effective use of technology depends crucially on skills (Andrews, Nicoletti, & Timiliotis, 2018). The success of firms in the digital age depends on employees who are well versed in

literacy, numeracy, problem solving and general ICT skills used in the workplace. Increasingly, this also requires ICT specialists and data specialists. In addition, firms need additional skills and competencies for new organizational forms and in intensive digital sectors. Ensuring the right skills for the digital age requires investment in education and training. Primary education should provide strong literacy and numeracy skills. Over time, students need options for developing ICT and additional skills, including social, communication and management skills. In addition, many forms of learning can benefit from the use of digital technologies (OECD-3, 2019).

The sixth and last key and direction is digital security and privacy. Mistrust of digital technologies can be an important barrier to dissemination and efficient use. In particular, concerns about digital security and privacy can seriously hamper people's propensity to engage online. For business, trust is also a key factor influencing the adoption and use of digital tools. Governments may also face privacy concerns, such as linking datasets or disclosing government data to the public. Removing these barriers requires better digital risk management for all participants. This involves building capacity to assess digital risk and reduce it to an acceptable level, including by mitigating and/or transferring risk.

Key areas for increasing effective use policy:

1. Bridge the gap between high- and low-educated people and give everyone a combination of skills to thrive and trust in the digital world. To do this, review education and training systems to make better use of digital learning opportunities.

2. Accelerate the proliferation of digital tools to stimulate productivity growth for companies, including small and medium-sized enterprises. To this end, encourage investment in digital technologies and intangible assets (such as patents, software) and promote business dynamism and structural change that stimulates implementation.

3. Transition from e-government to a holistic and user-driven approach to digital government. At the same time, continue to improve public services on the Internet and ensure the consistent use of digital technologies and data at all levels and levels of government.

4. Address distrust to increase online engagement by raising awareness and enabling people and businesses to better manage digital risks (OECD-2, 2019).

To fully embrace and benefit from the digital transformation, individuals, companies and governments need to be confident that the digital environment will outweigh the negative outcomes of their social and economic performance. The digital environment can exacerbate digital security incidents, information asymmetries, power imbalances, or jurisdictional issues. This can lead to violations of laws and regulations, such as privacy, consumer protection or product safety, that aim to reduce this imbalance and problem. This uncertainty needs to be mitigated as much as possible to ensure trust.

Key policy domains and indicators of Trust (Figure 3.3).



Figure 3. Key policy domains and trust indicators

Source: systematized by the author

The first key and direction is digital risk management. Digital risk management applies to both individuals and organizations - from small and large businesses to government agencies. All entities share some responsibility for managing the digital risks of their activities. This will vary depending on their roles, ability to act, context and the need to have appropriate risk management skills. Risk is a cross-border, cross-sectoral and multilateral problem. Thus, digital risk management provides a common reference structure for different political communities to discuss trust policies in an integrated way. It also allows different actors to view risks in a more holistic way, based on the fundamental components of the risk management cycle.

The second key and direction is privacy. As the digital transformation progresses, confidentiality is becoming a critical factor affecting trust, especially the protection of personal data. Confidentiality is recognized as a fundamental value that deserves protection, as well as a condition for the free flow of personal data across organizations and borders (OECD, 2016). Technological advances can help build trust through "design confidentiality," which takes into account the implications of confidentiality at the initial stage of product or service design.

While technology can help, it cannot replace a strategic approach to protecting privacy and personal data. One example is the national data strategy, which is supported at the highest level of government, which includes the perspective of the whole society and balances individual and collective interests. The compatibility of confidentiality and data protection at the national and international levels must be maintained at the international level. The third key and direction is small and medium enterprises. SMEs, and startups in particular, are crucial for economic growth, fostering competition, innovation and job creation. However, they also face various challenges in digital risk management. As a rule, SMEs do not have the awareness, resources or experience to effectively assess and manage risks. To help SMEs realize the potential of digital transformation, they need to be more aware of best practices in digital risk management.

The fourth key and direction is consumer protection. For digital transformation to thrive, it is important to effectively protect consumers when they engage in e-commerce and other online activities. Transactions involving digital content and services (including zero-cost actions that include user data) as well as blurred boundaries between consumers and businesses can also complicate traditional notions of ownership, responsibility, rights and responsibilities.

The main problems are information disclosure, fraudulent and unfair commercial practices, confirmation and payment, fraud and theft of personal data, product security, as well as dispute resolution and redress. New forms of asset and content use, including leasing, asset sharing and subscription sharing, create problems for consumers to understand their rights and responsibilities. In financial markets, people (especially those with low digital literacy) need new skills and knowledge to use new digital products and services effectively, and to understand the potential implications of data exchange.

The fifth and last key and direction is digital security. Because it is not possible to create a completely secure and secure digital environment, businesses, other organizations and individuals are always at some risk of digital security when working online. Safety standards (such as ISO 27000 series) can increase resilience and maintain business continuity by mitigating the potential consequences of security incidents. All stakeholders are interdependent in the digital environment, including abroad. Thus, fostering partnerships, including with small and medium-sized enterprises, can help reduce risks and promote effective risk management. Cyber insurance can be an important element of digital security risk management.

Key areas for strengthening trust:

1. Use risk management as a basis for developing trust policies, including assessing and managing risks related to digital technologies, data and cross-border flows. Ensure that digital security risk goes beyond technical issues to be a strategic priority for individuals, companies, including small and medium-sized enterprises, and governments, and for everyone to take responsibility for managing digital risks.

2. Develop and implement a national society-wide privacy strategy supported by the highest levels of government. Encourage the compatibility of confidentiality systems in different jurisdictions to ensure the free flow of personal data; increase transparency regarding the purpose and use of personal data collections; and expand users' access and control over their data, including through "design privacy".

3. Support digital consumers who face problems with online disclosure, deceptive and unfair commercial practices, verification and payment, fraud and identity theft, product security, and dispute resolution and redress, including in the context of connected devices where offline and online worlds coincide (OECD-2, 2019).

Digital technologies are changing the environment in which firms compete, trade and invest. The openness of the market allows digital transformation to flourish, creating a business-friendly environment. This allows foreign and domestic firms to compete on equal terms and without undue restrictions or rules. In this regard, market openness policies related to trade, investment, financial markets, competition and taxation play an important role.

Key policy domains and indicators of Market openness (Figure 4).



Figure 4. Key policy domains and Market openness indicators *Source: systematized by the author*

The first key and direction is trade. Digital technologies and data have a profound effect on international trade, reducing trade costs; promoting the coordination of global value chains; dissemination of ideas and technologies across borders; and connecting more companies and consumers around the world. In particular, goods are increasingly being combined with services, and new and previously non-traded services are now being traded across borders. To reap the benefits of trade in the digital age, a dialogue with many stakeholders on regulatory approaches is needed. These approaches should ensure the compatibility of different regulatory regimes, especially for international issues such as cross-border data flows. To support this dialogue, it is

necessary to better understand the nature and composition of disparate data flows, as well as to clarify the scope of public policy objectives.

The second key and direction is investment. Investment regimes that mobilize private investment, in particular in communications infrastructure, technology and KBC (e.g. business models, software and data), combined with open financial markets, attract foreign direct investment (FDI). Multinational cross-border businesses can make extensive use of digital technologies and data to organize their business operations and improve processes and procedures (see Use). The use of such technologies also facilitates international market transfer (Lesher, & Miroudot, 2008).

The third key and direction is financial markets. Effective, stable and open financial markets based on transparency, confidence and honesty help allocate financial resources to companies investing in digital transformation. Open financial markets also ensure that domestic financial services firms can compete with foreign competitors. Increased competition should make domestic firms more efficient and transparent. Cash flows can reduce the cost of capital for firms in countries where capital is scarce. This, in turn, can increase investment in digital transformation. Digital technologies are also at the heart of new forms of external financing (e.g. crowdfunding).

The fourth key and direction is competition. Increased competition in the digital age, including by opening access to markets, benefits consumers by lowering prices and diversifying goods and services. This, in turn, supports trade and investment. Competitive markets also contribute to digital transformation by stimulating innovation, new business models, dynamism and business productivity, stimulating structural change in the economy. However, as digital technologies and data increase competition in many markets, they have also shown the potential to lead others to greater concentration, market power, and even dominance. The OECD Competitive Assessment Toolkit helps governments remove barriers to competition by identifying unnecessary restrictions on market activity and developing alternative, less restrictive measures (OECD-2, 2020).

The fifth and last key and direction is taxation. Digital transformation has a wide range of implications for taxation. This affects tax policy and tax administration at both domestic and international levels, introducing new tools and challenges for politicians. Work under the OECD / G20 project "Base Blurring and Profit Movement" (BEPS) and the BEPS Inclusive Platform have recognized that digitalization – and some related business models – are important challenges for international taxation (OECD, 2018).

Members of the BEPS Inclusive Platform agreed to conduct a coherent and simultaneous review of two key aspects of the existing tax system - income distribution rules and interconnection rules. This review will look at the impact of digitalization on

the economy, related to the principle of matching profits with core economic activities and value creation.

Key areas for fostering market openness:

1. Monitor changes in competitive dynamics, especially trends in market concentration and dominance in digital-intensive sectors, and ensure that competition authorities use flexible tools and cooperate across borders to address transnational competition.

2. Reducing trade barriers, especially for digital services, such as inefficient interconnection management. Ensure a holistic market openness policy through dialogue with many stakeholders to ensure interoperability between regulatory regimes, including for cross-border data flows and relevant privacy and security considerations.

3. Reduce barriers to international investment, including in communication infrastructures, digital technologies and knowledge-based capital (eg business models, software, data), and promote the opening of financial markets.

4. Make sure tax systems meet the goals of the digital age through ongoing international cooperation to reach a global consensus solution (OECD-2, 2019).

The digital transformation has already begun to change organizations and markets, raising important questions.

What works may disappear?

Where will the new ones come from?

What will they look like?

What skills will be needed?

At the same time, other questions arose.

Who can suffer the most?

What can be done to help create jobs and match skills development to the changing needs of new jobs?

The social partners can play an important role in answering such questions.

Key policy domains and indicators of Jobs (Figure 5).

The first key and direction is labour markets. Maintaining and improving the efficiency of the labor market in the digital world of labor requires a new look at the labor market rules. These include employment protection legislation, minimum wage laws, working hours and health and safety regulations, in particular (OECD-4, 2019). The digital transformation can continue to contribute to non-standard forms of work, which will lead to job security and income for some such workers. Countries need to decide whether to update the legal framework or update it to meet the objectives. Such a framework should ensure that all workers, regardless of the type of contract, receive appropriate rights, including freedom of association and negotiation, equal pay for equal work, benefits and protection.



Figure 5. Key policy domains and jobs indicators

Source: systematized by the author

The second key and direction is skills. People need the right combination of skills to prepare for future work. The evolution of skills needed to thrive in a highly digital economy and society remains uncertain. However, a set of important skills includes literacy, computing and problem solving, general ICT skills, and complementarity skills and competencies (e.g., creative thinking and teamwork). Effectively responding to these skills needs requires a holistic approach to skills development, from early education to lifelong learning. Investments in training needed to meet future needs are beyond the reach of the public sector, which also involves firms and individuals. Training should be targeted at those who need it most, who are often low-skilled workers. Online courses, such as mass open online courses (MOOCs), also offer flexible and affordable distance learning options in several areas, however (OECD-3, 2019).

The third key and direction is tax and benefit systems. Governments also need to expand and / or adapt tax and benefit systems to ensure that all workers have minimum protection and wages, and that their various sources of income are included in the tax system. Tax and benefit systems should facilitate the transfer of rights to social insurance to prevent the loss of entitlements when workers move out of work. Governments may also need to expand the role of contributory schemes so that no one is left without social protection due to their contractual status.

The fourth key and direction is social protection. Social protection is crucial to ensure a successful and equitable transition for all, including displaced workers. Some workers will want to move to new professions. Others will try to enter the labor market

for the first time or after a period of unemployment. In both cases, they may not immediately find a new job. Assistance to these workers includes a system of welldesigned and adequately resourced active and passive labor market programs. These approaches provide employees with timely access to basic job search services and target those who need more assistance. Many people work informally and are not protected by current rules. All this adds to the problems faced by social security systems, which still largely involve the conclusion of a permanent, permanent contract with one employer.

The fifth and last key and direction is regional development. Regional development policy is needed to overcome the geographical differences that arise from the creation and automation of jobs created by digital means (Sorbe, Gal, & Millot, 2018). Reducing the cost of relocation, for example through subsidies, is one way to increase labor mobility and help relocated workers return to work. In addition, well-designed housing policies can encourage people to relocate to regions with more and better jobs (Andrews, Caldera Sánchez, & Johansson, 2011).

Key areas for ensuring good jobs:

1. Promote a successful and equitable transition from job cuts to job expansion, balancing flexibility and mobility (including by stimulating wages for workers to move from low-productivity to high-performance firms) and job stability, including through dialogue with the social partners).

2. Review labor market policies and institutions to facilitate the adaptation of firms' workforces and facilitate the transition from work to work for workers. Ensure adequate protection through better skills transfer, transferability of benefits and effective employment services.

3. Make sure people have the right combination of skills to succeed in technologyrich work environments, including strong cognitive skills, ICT skills, advanced skills, special skills, and the ability to cope with change and continue learning, including without work. Coordinate between educational and training institutions, employers and social partners.

4. Prepare for a serious learning task and review education systems. Improve the accessibility, quality and equity of youth education and adult learning throughout their working lives, including by removing barriers to adult learning, promoting learning for those most in need, and making better use of digital technologies for learning.

5. Solve the problems of new forms of work and ensure good results for all workers by applying and, if necessary, reviewing and expanding labor market regulation and strengthening the voice of workers. Reduce the risk of arbitrage between different forms of employment and work by ensuring neutrality of regulation, tax systems and benefit schemes.

6. Improve social protection so that no one is left behind. Strengthen active labor market programs to support displaced workers and develop effective income support schemes to ensure income security without undermining incentives to work (OECD-2, 2019).

Digital transformation affects society and culture in a complex way.

First, digital technologies are dramatically changing the way individuals, firms, and governments interact. In addition, the overall impact is often unclear and may vary from country to country. For example, digital technologies improve access to information (free and interconnected Internet), improve health care (e.g. telemedicine) and enrich education (e.g. MOOCs).

On the other hand, there are problems related to the imbalance between work and life; division of people into relatively isolated groups of like-minded people; Adverse effects on mental health, such as screen addiction, depression and cyberbullying, including among children; and the emergence of digital divide (e.g., gender, skills).

Key policy domains and indicators of Society (Figure 6).



Figure 6. Key policy domains and society indicators

Source: systematized by the author

The first key and direction is social policies. Social policy can help bridge a number of digital gaps. For example, when knowledge-intensive firms come together in places with highly skilled workers, locally based social policies can help bridge geographical gaps (Moretti, 2012). Digital instruments can also help governments make better social policy choices and improve welfare. For example, a combination of

long-term and multi-domain data on individuals, families, and the environment can give an idea of the impact of policy on communities.

The second key and direction is skills. Developing skills throughout the life cycle, especially through education and training policies, can ensure that digital transformation benefits all and avoids the escalation of existing differences. Skills development includes a number of core competencies, including literacy, numeracy and problem-solving skills (see "Use"). It also covers social and emotional skills that are increasingly valued by employers and society at large. Approaches to developing such "soft skills" include working with students 'feelings and attitudes through role-playing games, collaborative pedagogy, games, case studies, problem-solving pedagogy, sport and the arts (Le Donné, Fraser, & Bousquet, 2016).

The third key and direction is tax and benefit systems. As the economy and societies change and adapt, redistribution policies, such as tax and benefit systems, ensure that no one is left behind. Redistribution due to income support has declined in OECD countries along with a decline in the share of personal income tax. However, higher aggregate spending on policies such as health care has partially offset this change (Causa, & Hermansen, 2017). Governments may also need to review redistribution models in light of changes in the organization and nature of work (Causa, Vindics, & Akgun, 2018).

The fourth key and direction is digital government. The digital government can provide users with access to digital public services in a way that is convenient for them and in a new way. For example, citizens can enjoy enhanced interaction with public administrations within and between levels of government. If the provision of services differs between different government agencies, governments can apply the "once only" principle. This would reduce the burden on citizens and businesses, which would have to provide the same information several times. In addition, digital "single windows" can facilitate access to information and assistance, for example, for job seekers. Governments can also gather more information by interacting with citizens online to personalize public services and better target public policy.

The fifth key and direction is environment. Digital technologies also create challenges and opportunities to address some of the major collective challenges, such as the environment and health. In terms of the environment, digital technologies can support green growth. For example, they can ensure efficiency and monitoring in "smart" infrastructures and cities. However, expanding the range and rapidly spreading digital technologies can also increase the need for resources and energy in production and use. This offsets some environmental benefits, which will lead to a greater need for recycling and disposal of old equipment.

The sixth and last key and direction is health care. With regard to health care, the digitization of medical records, the expansion of remote care and teleconsultation,

91

and the introduction of mobile health technologies can improve health care and potentially reduce costs. However, data-based health services also pose new challenges. These relate primarily to the protection and confidentiality of personal data, security, control and ownership, transparency and accountability, and quality and security. Proper management of sensitive health data can solve many of these problems.

A number of social problems have arisen or exacerbated as digital transformation progresses, including ethics and morality. For example, AI, machine learning and autonomous decision-making raise new questions about transparency (possible prejudice and discrimination), accountability and accountability. Misinformation has also attracted attention, as it has a negative impact on people and society.

Key areas for promoting an inclusive digital society:

1. Reduce the digital divide and integrate everyone into the digital society, including women, the elderly and low-income people, including through social policies that support mobility and redistribution.

2. Promote the development of basic skills for all, including by providing incentives and facilitating access to adult learning, as well as improving the recognition of skills acquired after primary education.

3. Use the potential of digital technology and data to solve common problems, such as the environment and health, by increasing energy efficiency and reducing health care costs through mobile health technologies.

4. Increase citizen activism through digital government strategies and engage all stakeholders, including the technical community, business community, trade unions and civil society, to help understand and address societal issues such as risks such as cyberbullying and misinformation (OECD-2, 2019).

It is important to understand that digital security is a process. You can't install something today, buy some magic button that would protect all your data, information of your friends, colleagues, etc. You are constantly learning about new threats and new tools that appear - you use something and you don't.

It is important to understand what threats you may encounter. If you are a journalist and work in Europe, these are some threats, if you work in Ukraine, they may be completely different.

At the present stage of transformational change, there are certain rules of digital security (Kvantaliani, 2018).

1. Use the licensed software everywhere, including on phones and tablets, work and home computers.

2. Update all software regularly.

Recently, Windows is being updated and restarted without your desire: you want to work, but he does not care that you have a conference.

3. Install antivirus programs and firewall.

Antivirus solves the problem of virus infection, and the firewall monitors the interconnections of our computer and the Internet and, accordingly, helps us protect ourselves from external threats.

Mac OS users also need to install anti-virus programs and firewalls, as the number of viruses created for Macs in 2017 increased significantly more than in the last 10 years. These are mostly viruses that encrypt your computer and demand money. If you have Windows, you can use the built-in security programs Windows Defender or some other - it all depends on who you trust.

4. Set a password to log in to the device (phone, tablet, computer).

You need a complex unique password.

A complex unique password is one that contains uppercase, lowercase, special characters, and a total size of at least 14 characters is the minimum standard, preferably 20 or 30. Uniqueness means that each account must have its own password. That is, on Facebook we must have one password, and on the Gmail mailbox - a completely different one.

5. Use the password manager.

If we create unique passwords for each account, there are difficulties with their number. You can use a manager that is convenient for you and that you trust. Mac OS users, for example, have a built-in Keychain manager that automatically saves passwords. LastPass is an online password manager for the accounts you create online. KeePass is an offline manager where you provide password security yourself.

6. Do not use unreliable e-mail services, social networks, messengers.

Unreliable services are those that provide information about their users, or they are of poor quality, do not use encryption, or have been compromised. In this case, it turns out that our data is protected by a user agreement with any corporation.

7. Separate accounts.

For example, we have mailboxes separately for work and for home. If they broke our home box, they did not get access to the office, and vice versa. Even if we share communication between different messengers: for example, part of the correspondence in WhatsApp, and part in Viber - it already protects information, because those who attack, you need to access another channel of communication.

8. Lock the devices.

For example, if you go to drink coffee, it is important to lock your device so that people walking past your desktop do not have access. It is better to set the shutdown on the mobile phone after 60 seconds, so that it locks itself if you leave it on the table. For Windows, it's a Win + L lock, on Macs you just lock the cover, and it goes to sleep and asks for a password.

9. Use full-disk device encryption.

If you use the latest iPhone models or premium Android phones, this encryption is the default.

10. Delete the history from the browser and cache.

When you go online, the sites you visit send small files to your computer to let you know who they are and index all your actions accordingly. For example, CCleaner is a program that can be used to delete such temporary files. This is so that the person who will be working on the computer after you cannot see what you are looking for, that is, to be more anonymous.

11. Do not provide obvious answers to regain access to your account.

If the secret question for password recovery is your mother's maiden name, this information is publicly available, can be found on social networks and is easy to access in your inbox.

12. Do not use unsecured mailboxes to restore access.

If you have a well-protected Gmail mailbox and another mailbox, and they are linked by a recovery feature, then you are potentially vulnerable.

13. Use secret messengers if you decide to keep secret correspondence.

For example, Viber, Signal, secret chats in Telegram.

One of the important components is not only the transmission of encrypted communication, but also its storage. If you passed secret information to someone, you and your colleague have it. Accordingly, if you do not want this to be detected later, it is best to delete the information immediately. Some messengers have a certain time to delete a message: for example, you set it for 1 minute, after which the message is automatically deleted.

14. Use messengers with encryption from device to device – Signal, WhatsApp, Viber, and in Telegram - secret chat.

In this case, the service provider does not have the opportunity to read your correspondence.

15. Do not click on suspicious links.

16. Do not catch phishing.

Phishing is a type of fraud, the purpose of which is to extract from gullible or inattentive users of the network personal data of customers of online auctions, money transfer or currency exchange services, online stores.

17. Back up important files in cloud storage.

Cloud storage is Google Drive, Dropbox. It is statistically very likely that a hard drive or flash drive can be damaged without the possibility of recovery.

If you use Gmail, you can use Google Drive. If you have secret files, you can preencrypt them and then upload them to the cloud storage.

17. Back up important files in cloud storage.

Cloud storage is Google Drive, Dropbox. It is statistically very likely that a hard drive or flash drive can be damaged without the possibility of recovery.

If you use Gmail, you can use Google Drive. If you have secret files, you can preencrypt them and then upload them to the cloud storage.

19. Use VPN (Virtual Private Network) technology when connecting to public Wi-Fi.

A VPN is a tunnel from your PC to another computer and then to the Internet. In essence, this is a reliable tunnel that protects your data on an unreliable network. For example, there is a VPN service TunnelBear - a socially responsible business, so if you write that you are an activist or journalist from Ukraine, they will give you a discount. You can create a VPN service yourself (buy a server, connect Open VPN). If we can't do it ourselves, we buy a VPN subscription. Opera has a VPN that forwards your web traffic through Opera servers. The difference is that a standard VPN passes all traffic. For example, you connect to public Wi-Fi, go to a mailbox, a news site, etc. People who work here see that the user №1 entered the social network, then read the news - all traffic is open through the access point. If you want to hide this information, buy a VPN and use it in such cases.

20. Use the Tor network if you want to be anonymous.

If you are a regular user and you do not need to hide almost anything, a VPN will suffice. Tor (The Onion Router) is an anonymity tool and VPN is a security tool.

21. Change the default password on the home Wi-Fi router.

Default passwords are the default passwords. Your router is connected to the Internet. If it has standard passwords, such as "admin" or your phone number, then an attacker can connect to it. For example, 5 years ago, the Moldovan telecommunications network of routers switched to a small botnet - this is when you have access to devices, and you can remotely tell them what to do. In this way, you can force everyone to visit one site at a time, and it will no longer be available. If I can connect to your router, I can send something to someone on your behalf. So think about your safety in advance.

Putting the framework into practice in digital economy. A whole-ofgovernment approach to digital transformation requires a digital transformation strategy (DTS). Many countries have a national digital strategy or equivalent policy, but most are still narrow. The DTS needs to be comprehensive in addressing a number of interrelated policy issues discussed above. It should ensure policy coherence and coordination in all areas and sectors that shape digital transformation. Finally, it should involve all relevant stakeholders in its development and implementation. There are five key steps to developing a DTS (Table 3).

Conclusions. Government policy-makers and policymakers can never have a full understanding of all the possibilities, challenges, and challenges of DTS. Thus, one of the keys to success is the involvement of stakeholders in the early stages of strategy

and policy development. The cooperation of many stakeholders brings tangible benefits that lead to better policies and results. This improves the quality of rulemaking thanks to the ideas, experience and evidence of stakeholders. In addition, it creates a sense of ownership of policies and rules and increases legitimacy. In turn, involving stakeholders can increase trust in government and compliance.

Table	3. Five	steps to	develop a	digital	transformation	strategy

Steps	Strategy		
1. Establish a governance	1.1. Establish a governance approach that supports effective steering		
approach that supports	and co-ordination of digital transformation policies in light of the		
effective co-ordination	country's culture and institutions.		
	1.2. Assign clear responsibilities for strategic co-ordination (e.g. the		
	head of government or a lead minister) and operational co-ordination		
	(e.g. chief digital officers in implementing bodies) for development		
	and implementation of a national digital transformation strategy		
	(DTS).		
2. Articulate a strategic vision	2.1. Articulate a strategic vision that provides direction on identifying		
and ensure coherence	the main priorities and scoping the main objectives of a DTS.		
	2.2. Ensure coherence between a DTS and other related domestic and		
	international digital strategies and/or policy objectives.		
3. Assess key digital trends,	3.1. Monitor key digital trends, including by international		
related policies and regulations	benchmarking, to identify opportunities and challenges and related		
	priorities to be addressed by a DTS.		
	3.2. Evaluate the effectiveness of current strategies and/or policies,		
	identify gaps and/or incoherence, and scope objectives for a DTS.		
4. Develop a comprehensive	4.1. Leverage the governance approach, the strategic vision, and		
and coherent strategy	insights from monitoring and evaluation to develop a comprehensive		
	and coherent DTS.		
	4.2. Engage all relevant actors in developing a DTS, including		
	different parts and levels of government, non-governmental		
	stakeholders and international partners.		
5. Implement the strategy	5.1. Anticipate and address implementation challenges related to		
successfully	institutions and policy frameworks, social preferences and (lack of)		
	administrative capacity.		
	5.2. Issue an action plan with specific measures, clear responsibilities,		
	budget, timeframes and measurable targets to successfully implement		
	the DTS.		

Source: OECD-2, 2019

References:

1. Rynn, J. (2000). Why Manufacturing Matters: A production-centered path to economic growth. Available at:

https://economicreconstruction.org/sites/economicreconstruction.com/static/SeymourMelman/archive/de_re/ ProductionCenteredEconomics.pdf.

Rumyk, I., & Melnichenko, I. (2023). Development of innovative business companies and Fintech industry in the digital economy. *The development of innovations and financial technology in the digital economy*: monograph. OÜ Scientific Center of Innovative Research. <u>https://doi.org/10.36690/DIFTDE-2023-170-188</u>

2. Digital 2021: global overview report. Available at: <u>https://datareportal.com/reports/digital-2021-global-overview-report</u>

4. Digital 2023: global overview report. Available at: <u>https://datareportal.com/reports/digital-2023-global-overview-report</u>

3. OECD-1 (2020). Going Digital integrated policy framework. *OECD Digital Economy Papers*, 292, OECD Publishing, Paris. Available at: <u>https://read.oecd-ilibrary.org/science-and-technology/going-digital-integrated-policy-framework_dc930adc-en#page1</u>

4. OECD-284 (2019). The road to 5G networks: Experience to date and future developments. *OECD Digital Economy Papers*, 284, OECD Publishing, Paris. Available at: <u>https://read.oecd-ilibrary.org/science-and-technology/the-road-to-5g-networks_2f880843-en#page1</u>

5. OECD (2017). Key Issues for Digital Transformation in the G20. *Report prepared for a joint G20 German Presidency/ OECD conference, OECD,* Berlin. Available at: <u>https://www.de.digital/DIGITAL/Redaktion/EN/Publikation/key-issues-for-digital-transformation-</u> g20.pdf?__blob=publicationFile&v=1

6. OECD-264 (2017). The evolving role of satellite networks in rural and remote broadband access. *OECD Digital Economy Papers*, 264, OECD Publishing, Paris. Available at: <u>https://read.oecd-ilibrary.org/science-and-technology/the-evolving-role-of-satellite-networks-in-rural-and-remote-broadband-access_7610090d-en#page1</u>

7. OECD-1 (2019). Enhancing Access to and Sharing of Data. *Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris. Available at: <u>https://read.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en#page1</u>

8. OECD-2 (2019). Going Digital: Shaping Policies, Improving Lifes. OECD Publishing, Paris. Available at: https://read.oecd-ilibrary.org/science-and-technology/going-digital-shaping-policies-improving-lives 9789264312012-en#page4

9. OECD (2014). Recommendation of the Council on Digital Government Strategies. *OECD Legal Instruments*, OECD, Paris. Available at: <u>https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406</u>.

10. OECD-280 (2019). ICT investments in OECD countries and partner economies: Trends, policies and evaluation. *OECD Digital Economy Papers, 280,* OECD Publishing, Paris. Available at: <u>https://read.oecd-ilibrary.org/science-and-technology/ict-investments-in-oecd-countries-and-partner-economies_bcb82cff-en#page1</u>

11. Andrews, D., & Criscuolo, C. (2013). Knowledge-Based Capital, Innovation and Resource Allocation. *OECD Economics Department Working Papers*, 1046, OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/5k46bj546kzs-en</u>.

12. Sorbe, S., Gal, P, Nicoletti, G., & Timiliotis, C. (2019). Digital Dividend: Policies to Harness the Productivity Potential of Digital Technologies. *OECD Economic Policy Papers, 26*, OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/273176bc-en</u>.

13. Andrews, D., Nicoletti, G., & Timiliotis, C. (2018). Digital technology diffusion: A matter of capabilities, incentives or both? *OECD Economics Department Working Papers*, *1476*, OECD Publishing, Paris. Available at: http://dx.doi.org/10.1787/7c542c16-en.

14. OECD-3 (2019). OECD Skills Outlook 2019: Thriving in a Digital World. OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/df80bc12-en</u>.

15. OECD (2016). OECD Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity ("Cancún Declaration"). *OECD Legal Instruments*, OECD, Paris. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426

16. Lesher, M., & Miroudot, S. (2008). FDI Spillovers and their Interrelationships with Trade, *OECD Trade Policy Papers*, *80*, OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/235843308250</u>.

17. OECD-2 (2020). Competition Assessment Toolkit, OECD. Available at: https://www.oecd.org/competition/assessment-toolkit.htm. 18. OECD (2018). Tax Challenges Arising from Digitalisation – Interim Report 2018: Inclusive Framework on BEPS. *OECD/G20 Base Erosion and Profit Shifting Project*, OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/9789264293083-en</u>.

19. OECD-4 (2019). OECD Employment Outlook 2019: The Future of Work, OECD Publishing, Paris. Available at: <u>https://dx.doi.org/10.1787/9ee00155-en</u>.

20. Sorbe, S., Gal, P., & Millot, V. (2018). Can productivity still grow in service-based economies? Literature overview and preliminary evidence from OECD countries. *OECD Economics Department Working Papers*, *1531*, OECD Publishing, Paris. <u>https://doi.org/10.1787/4458ec7b-en</u>.

21. Andrews, D., Caldera Sánchez, A., & Johansson, A. (2011). Housing Markets and Structural Policies in OECD Countries. *OECD Economics Department Working Papers*, 836, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kgk8t2k9vf3-en.

22. Moretti, E. (2012). The New Geography of Jobs, Houghton Mifflin Harcourt, Boston.

23. Le Donné, N., Fraser, P., & Bousquet, G. (2016). Teaching Strategies for Instructional Quality: Insights from the TALIS-PISA Link Data. *OECD Education Working Papers*, *148*, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jln1hlsr0lr-en.

24. Causa, O., & Hermansen, M. (2017). Income redistribution through taxes and transfers across OECD countries. *OECD Economics Department Working Papers*, 1453, OECD Publishing, Paris. http://dx.doi.org/10.1787/bc7569c6-en.

25. Causa, O., Vindics A. & Akgun O. (2018). An empirical investigation on the drivers of income redistribution across OECD countries. *OECD Economics Department Working Papers*, 1488, OECD Publishing, Paris. <u>http://dx.doi.org/10.1787/5cb47f33-en</u>.

26. Kvantaliani, N. (2018). 21 rules of digital security. Digital Forum for Civil Society. Available at: <u>https://euprostir.org.ua/practices/133410</u>