# Chapter 2
# POLICY TRENDS

**KEY FINDINGS**

- OECD countries are strengthening their strategic approach to policy for the digital transformation.
- National digital strategies are increasingly co-ordinated at the highest levels of government. In 2019, four more countries reported co-ordination at the prime minister/chancellery level and several more indicated a ministry dedicated to digital affairs than in 2016.
- In the last three years, many countries, including Australia, Austria, Colombia, France, Germany, Korea, Spain, the United Kingdom and the United States, have issued national 5G strategies.
- All OECD countries and several partner economies enhance access to and sharing of public sector data. Only a few (Australia, Germany, Japan, Singapore, United States) also have initiatives to facilitate data sharing within the private sector.
- Digital security innovation is an emerging trend in the OECD. Several OECD countries, including Australia, France, Germany, Israel and the United Kingdom, have established open innovation centres to promote its development.
- By mid-2020, over 60 countries had a national artificial intelligence (AI) strategy. Priority areas include AI-related research and development (R&D) (Canada, United States, European Commission), AI adoption (Finland, Germany, Korea), and AI skills (Australia, Finland, United Kingdom, United States).
- Blockchain and quantum computing are attracting increasing policy attention worldwide. Several countries have issued a blockchain strategy (Australia, People's Republic of China [hereafter "China"], Germany, India, Switzerland). Others (France, Italy) are developing one. The United States, China and the European Union are leading on quantum computing R&D expenditure.
- Dealing with the socio-economic effects of the COVID-19 pandemic has become a policy priority in the digital area. Governments, academia and businesses in OECD countries (United Kingdom, United States) have rapidly developed AI systems to predict and monitor the spread of the disease and advance medical research.
- OECD national privacy enforcement authorities, as well as the European Data Protection Board and the Council of Europe, have issued guidance on the collection, processing and sharing of personal data in relation to COVID-19.
- Digital security agencies in countries such as Canada, the Czech Republic and the United States have responded to the COVID-19 crisis by raising awareness, monitoring threats and providing assistance.
- All OECD countries have policies to support digital uptake by firms, particularly start-ups, and the creation of new businesses.
- Some countries have extended collective bargaining (Canada, Denmark, France). Others are considering minimum wages (Netherlands, United Kingdom) to platform-mediated workers, who have been most severely hit by the economic crisis.

## Introduction

National digital strategies (NDSs) help governments shape the way digital transformation takes place in a country. Such strategies define policy priorities, set objectives and outline actions for implementation. As such, their development should involve representatives from a wide range of stakeholder groups[1] and different parts of the government, including at the subnational level. Today, almost all OECD countries and many partner economies have developed NDSs.

Based on responses to the 2019 OECD Digital Economy Policy Questionnaire on national digital strategies and policies from 32 OECD countries[2] and 5 partner economies,[3] the first section of this chapter analyses recent developments in NDSs across countries. It identifies the main policy objectives, exploring key developments and progress, as well as challenges faced in developing such strategies. It then outlines different governance approaches to NDSs. The second section presents key developments of the domain-specific policies that are described in more detail in the thematic chapters. These policies

focus on connectivity, usage, data governance, security, privacy, innovation, work and key technologies such as artificial intelligence (AI), blockchain and quantum computing.

## National digital strategies

### *More countries are developing national digital strategies*

Most OECD countries and partner economies have established an NDS. Of the 37 countries that responded to the 2019 OECD Digital Economy Policy Questionnaire on national digital strategies and policies, 34 countries have an overarching NDS, many of which were established in 2018. The exceptions include Poland, which does not have a strategy; Mexico, which is developing an NDS; and the United States, which takes a decentralised, market-driven approach to its overall digital policy.[4]

In all, 27 countries used an earlier strategy as a foundation to build the current one. Countries with a specified time frame for their strategies develop them every four to six years.

Most countries with available data reported having a budget associated with the NDS. Some indicated the NDS was part of a broader framework (e.g. United Kingdom), while in others it is decentralised (e.g. Austria, Costa Rica).

Half of the countries have stand-alone strategies, while the other half have ones that form part of a broader national strategy, such as a national innovation strategy. In addition, 19 countries have aligned their NDS with a supra-national agenda. For example, most European OECD countries have based their strategies on the principles and objectives of the Digital Agenda for Europe (European Commission, 2010[1]), the Digital Single Market Strategy for Europe (European Commission, 2015[2]), the Europe 2020 Strategy (European Commission, 2010[3]), the European Union eGovernment Action Plan (European Commission, 2016[4]) or a combination thereof.

### *Countries follow a common set of digital economy policy priorities*

As in 2016, countries were asked to rank policy objectives by priority in the 2019 OECD Digital Economy Policy Questionnaire. In the 2019 questionnaire, however, countries could allocate a unique value to each priority. Countries such as Japan, Sweden and the United Kingdom reported their NDS does not allow them to make such distinctions.

The following results are based on countries that could allocate priorities. While priority objectives in NDSs have evolved in recent years, some have remained highly important to most countries (Table 2.1). For example, "enhance digital government" was the highest ranked policy objective in both 2016 and 2019. "Develop telecommunications infrastructure" was the second-highest ranked policy objective over the same period. "Develop skills for the digital transformation" likewise remains important for many countries. In 2019, however, "foster innovation in digital technologies" emerged as an important policy objective.

Mid-ranked policy objectives (in order of priority in both 2016 and 2019) include improving digital security, enhancing data governance and promoting digital uptake by businesses. Promotion of digital uptake by individuals, enhancement of consumer protection on line and enhancement of Internet governance rank the lowest, with the latter falling the most during the period. Respondents indicated that most policy objectives in 2019 were foreseen to remain the same over the next three to five years. The two exceptions – developing skills for the digital transformation and enhancing data governance – were expected to become more important.

The 2019 priority ranking of policy objectives, from highest to lowest, corresponds approximately with the number of countries whose NDSs feature matching policy objectives (Table 2.1, column 3). For example, the top three ranked policy objectives – enhancing digital government, developing telecommunications infrastructure and fostering innovation in digital technologies – are mentioned the most frequently of all policy objectives (26, 26 and 25 times, respectively). In parallel, the two lowest ranked policy objectives – enhancing consumer protection on line and enhancing Internet governance – are mentioned the least frequently of all policy objectives (twice and thrice, respectively).

**Table 2.1. The evolution of digital policy objectives, 2016 and 2019**

| Policy objective | Priority in 2016 (Ranking) | Priority in 2019 (Ranking) | Number of national digital strategies featuring the objective |
|---|---|---|---|
| Enhance digital government | 1 | **1** | 26 |
| Develop telecommunication infrastructure | 2 | **2** | 26 |
| Foster innovation in digital technologies | - | **3** | 25 |
| Develop skills for the digital transformation | 3 | **4** | 25 |
| Improve digital security | 4 | **5** | 21 |
| Enhance data governance | 5 | **6** | 10 |
| Promote digital uptake by businesses | 6 | **7** | 19 |
| Promote digital uptake by individuals | - | **8** | 22 |
| Enhance consumer protection on line | 8 | **9** | 2 |
| Enhance Internet governance | 7 | **10** | 3 |

*Notes*: The rankings are based on self-reported priorities from 35 countries for 2016 and 31 countries for 2019. The 2016 questionnaire included eight objectives, and importantly did not include the policy priorities "foster innovation in digital technologies" and "promote digital uptake by individuals".

*Sources*: OECD, 2017 and 2019 OECD Digital Economy Policy Questionnaires.

In addition to those listed in the OECD Digital Economy Policy Questionnaire, other policy priorities figure as important in some NDSs. For example, Brazil's E-Digital Strategy (MCTIC, 2018[5]) includes gender as an explicit policy objective by highlighting the need to include and promote women and girls in information and communication technology (ICT)-related fields. Moreover, Turkey's National e-Government Strategy and Action Plan (Informatics and Information Security Research Center, 2016[6]) refers to the United Nations Sustainable Development Goals when transitioning to an information society.

### *Challenges to advancing policy objectives for national digital strategies*

OECD countries and partner economies indicated they face several challenges to achieve their digital policy objectives. The following list reflects the most prominent challenges reported by 22 countries in 2019:

- geographical dispersion of the population, including in remote and rural areas
- budget and financing constraints
- appropriate co-ordination and interaction of different actors across sectors, ministries and bodies
- development of effective regulatory instruments and frameworks
- adaptation to the rapid pace and development of digital technologies
- achievement of balance between the need to foster innovation and address consumer safety and privacy concerns related to use of data and uptake of new digital technologies.

Some challenges, such as balancing innovation with consumer safety and privacy concerns, can be minimised by ensuring coherence and co-ordination of policies across all domains and sectors that shape digital transformation (OECD, 2020[7]). Others, such as adapting to the rapid pace and development of digital technologies, can be addressed by using digital technologies in the policy process (e.g. design, implementation and monitoring) (OECD, 2019[8]).

### *Governance approaches to national digital strategies*

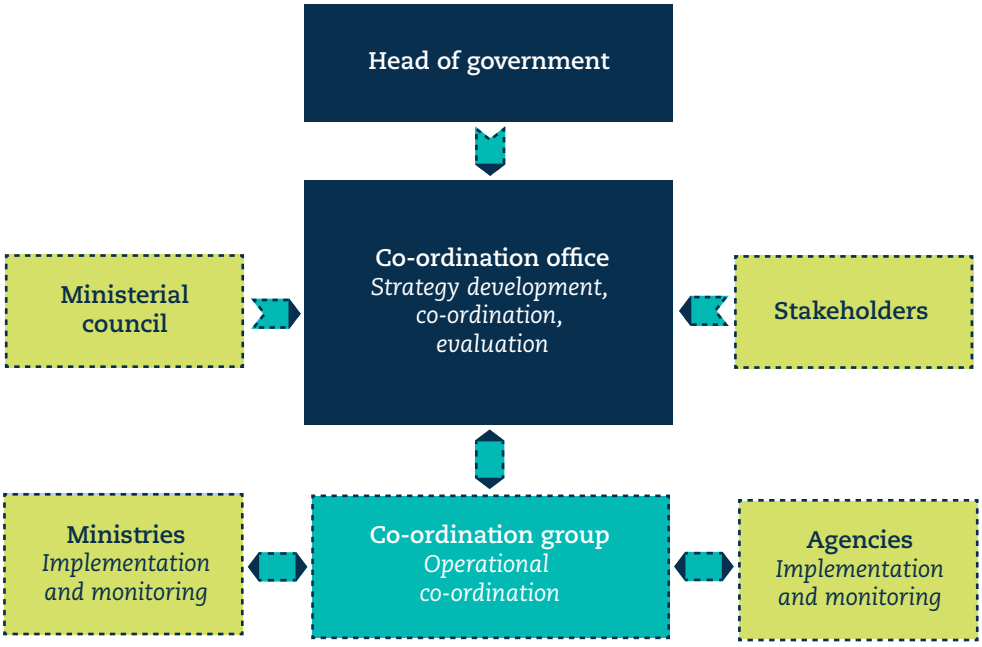
This section highlights the most common approaches to the governance of NDSs across the OECD and partner economies. Such governance concerns the development, implementation, monitoring and evaluation of an NDS, responsibilities among the bodies and actors involved in these activities, and arrangements for effective co-ordination.

While all OECD member countries and partner economies with an established NDS have a governance approach to support their strategy, specific arrangements vary. Different approaches can reflect, for

example, variations in countries' domestic institutions, government organisation, or administrative culture and capacity. In addition, governance arrangements can evolve over time, underpinned, for example by changes in government, technological progress and the evolution in the constellation of key actors due to digital transformation (OECD, 2019[9]). This can affect the allocation of key responsibilities, such as for strategy development, co-ordination, implementation, monitoring and evaluation.

Two main types of approaches can be identified. In the first approach, countries assign high-level leadership and centralised responsibility for strategic co-ordination above ministerial level (Figure 2.1). In these countries, a co-ordination office under the president, prime minister or chancellor usually holds the pen in drafting the strategy and involves key ministries and stakeholders in the process. This office tends to be led by a state secretary or a similar function. In about half of the countries with this approach, this office also leads strategic co-ordination. In some countries, co-ordination can instead be part of a centre of government.[5] Focal points within each implementing ministry and agency, such as chief digital officers, tend to ensure operational co-ordination for the strategy. These ministries and agencies usually also monitor implementation and report to the co-ordinating office. In most cases, this office ensures strategy evaluation, with oversight by the head of government (OECD, 2019[9]).

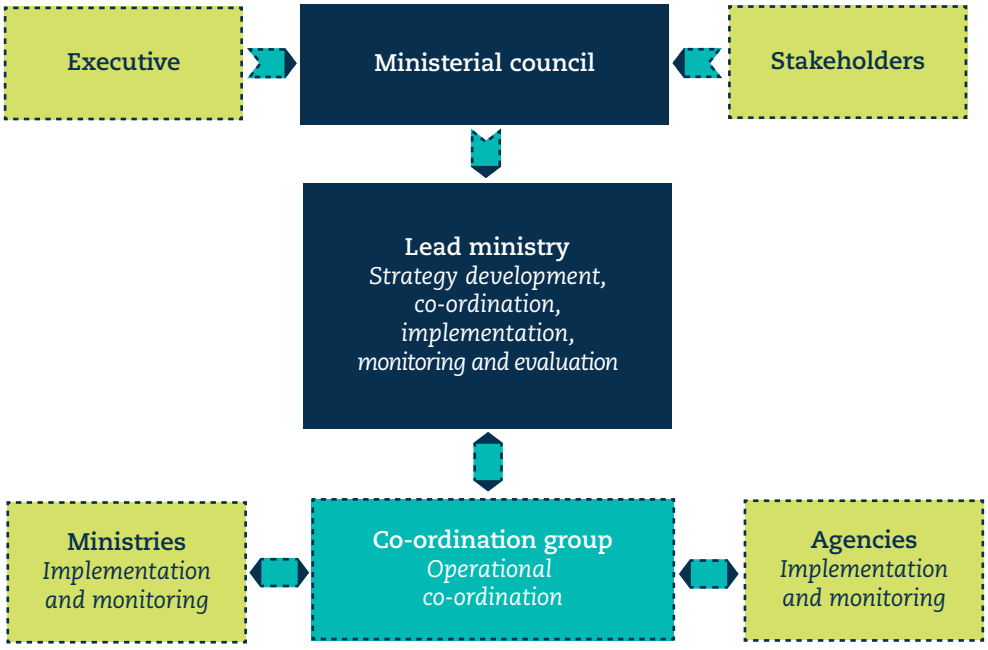
**Figure 2.1. High-level strategic co-ordination of national digital strategies**




*Source*: OECD (2019[9]), *Going Digital: Shaping Policies, Improving Lives*, *https://dx.doi.org/10.1787/9789264312012-en*.

In the second approach, a lead ministry is typically in charge of strategy development and strategic co-ordination (Figure 2.2). This approach is likely to be most effective if the lead ministry is exclusively dedicated to digital affairs instead of having a range of portfolios. Strategy development tends to involve stakeholders, e.g. under the auspices of a ministerial council, which is usually hosted by the lead ministry and sometimes chaired by the head of government. Similar to the first approach, a dedicated group of focal points from the implementing ministries and agencies usually ensures operational co-ordination. The same bodies also tend to monitor implementation, reporting to the lead ministry and/or the ministerial council, which often ensures strategy evaluation. In most cases where the lead ministry is dedicated to digital affairs, the latter also ensures monitoring and evaluation (OECD, 2019[9]).

**Figure 2.2. Ministry-level strategic co-ordination of national digital strategies**




*Source*: OECD (2019[9]), *Going Digital: Shaping Policies, Improving Lives*, *https://dx.doi.org/10.1787/9789264312012-en*.

Information collected via the 2019 OECD Digital Economy Policy Questionnaire confirms the persistence of these two main types of governance approaches, but also reveals some evolution in recent years (OECD, 2017[10]). Table 2.2 provides an overview of the responsibilities allocated for the development, co-ordination, implementation, monitoring and evaluation of NDSs in 2016 and 2019.

**Table 2.2. National digital strategy governance**

*Number of countries that have allocated respective responsibilities*

| Entity responsible | Lead strategy development | | Contribution | | Co-ordination | | Implementation | | Monitoring | | Evaluation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2016 | 2019 | 2016 | 2019 | 2016 | 2019 | 2016 | 2019 | 2016 | 2019 | 2019 |
| Office of the Prime Minister, Presidency, Chancellery | 4 | **8** | 0 | **0** | 5 | **5** | 1 | **0** | 6 | **3** | **4** |
| Ministry or body dedicated to digital affairs | 8 | **10** | 1 | **0** | 10 | **14** | 3 | **5** | 8 | **14** | **13** |
| Ministry or body not dedicated to digital affairs | 15 | **12** | 2 | **0** | 13 | **10** | 1 | **2** | 11 | **9** | **9** |
| Several ministries or bodies | 6 | **3** | 14 | **9** | 5 | **4** | 26 | **15** | 7 | **7** | **4** |
| Multiple public and private stakeholders | 1 | **0** | 17 | **24** | 0 | **0** | 3 | **11** | 0 | **0** | **0** |

*Notes*: The data for 2016 are based on survey responses from 35 countries. The data for 2019 are based on survey responses from 33 countries. Italy, Hungary and Turkey provided no information on Evaluation. Multiple public and private stakeholders include government actors, as well as civil society and the private sector.

*Sources*: OECD, 2017 and 2019 OECD Digital Economy Policy Questionnaires.

The number of countries that allocate strategic responsibilities to a high-level government body has doubled from four to eight between 2016 and 2019. However, only in Chile, Colombia and Turkey is the high-level body leading both strategy development and strategic co-ordination. In Japan, Luxembourg, the Russian Federation and Switzerland, the responsibility for leading the development of the strategy also lies with a high-level government body, while the task of strategic co-ordination is entrusted to

a ministry or body dedicated to digital affairs. Individual approaches exist across these countries on handling the monitoring and evaluation of the strategy.

The largest group of countries still has a single ministry or body in charge of strategy development and strategic co-ordination. In most countries, this entity has a portfolio that extends beyond digital areas to include others such as the economy, science, innovation or industrial affairs. Countries with a dedicated digital affairs ministry or body include Austria, Belgium, Greece, Israel, Slovenia, Sweden and the United Kingdom. In these countries, the lead ministry or body has a strong mandate for both strategy development and strategic co-ordination. Concurrently, they are also in charge of monitoring and evaluation. This is also the case in Spain, with the exception of strategic co-ordination being managed across several ministries.

The contribution of several ministries or bodies to strategy development has decreased between 2016 and 2019 – from 14 to 9. This may be explained, at least in part, by the increase in the contribution of multiple public and private stakeholders, including government actors, civil society and the private sector. The latter is a positive development, given that stakeholder input is essential for the inclusiveness and subsequently the quality and successful implementation of the strategy (OECD, 2019[9]).

### *Monitoring and evaluation of national digital strategies*

Monitoring and evaluation are essential to know how well an NDS is implemented and how effective it is. Countries do this in different ways, including through benchmarking surveys, annual or bi-annual status and progress reports, and dashboards with forecasts.

According to the results of the 2019 OECD Digital Economy Policy Questionnaire, all countries with available data monitor progress in the implementation of their NDS, and 24 countries reported having set specific targets against which they measure progress. Japan, for example, has targets to reduce the operating costs of information systems, while Estonia, Finland, Norway and Sweden have ambitious targets for faster Internet. Other countries have targets on improving e-commerce development (Latvia) or fostering start-up creation (Belgium).

Most countries also use international metrics and scoreboards to measure national progress towards policy objectives set in NDSs. Such metrics can be found in the *OECD Digital Economy Outlook*, the OECD Going Digital Toolkit, the European Commission's Digital Economy and Society Index, the UN e-Government Survey and the World Economic Forum's Global Competitiveness Index, among others. In the Czech Republic, for example, the Government Council for Information Society periodically carries out a benchmark survey with a set of performance indicators that focus on assessing the maturity and performance of each entity involved in the NDS.

Beyond monitoring and evaluating progress against an NDS' own targets and objectives, it can be informative for countries to also measure the effects of achieving objectives of their NDSs on higher-level national goals, such as growth, productivity and innovation. For example, in Iceland, initiatives that form part of their Digital Iceland strategy also relate to its financial strategy (Ministry of Finance and Economic Affairs, 2019[11]). In Japan, spurred by the Internet of Things (IoT), big data and AI, the Fourth Industrial Revolution, as envisaged in its New IT Strategy, is expected to contribute to nominal gross domestic product (GDP) growth over the next few years. Similarly, in the Russian Federation, more than half of GDP growth by 2030 is expected to come from increased efficiency and competitiveness resulting from higher uptake of digital technologies.

## Key policy developments

This section reviews the main policy trends across different fields of the digital economy: connectivity, usage, data governance, security, privacy, innovation, work and key technologies (AI, blockchain and quantum computing). Further information on each field is provided in the thematic chapters.

### *Access and connectivity*

Over the past few years, policy makers and regulators have been adapting regulatory frameworks to spur competition, innovation and investment in communication markets (Chapter 3).

As countries weather the COVID-19 crisis, connectivity, more than ever, is essential to ensure that economic activities can continue remotely. Disparities in access to communication services among and within countries may accentuate the consequences of the COVID-19 crisis. Therefore, policies aiming to reduce digital divides are of paramount importance. In addition, regulation and policies that foster competition and investment in communication infrastructure become even more crucial. In the medium and long term, upgrading networks to the next evolution of fixed and wireless broadband will help ensure reliable and resilient connectivity for all.

Communication markets are changing, including a trend towards convergence. This had led countries such as Colombia, Finland and Germany to modify the mandates and responsibilities of communication regulators. Other countries, such as Italy and the United Kingdom, have adapted regulatory frameworks as part of the transition of legacy networks and services, such as copper fixed networks.

OECD countries, including Austria, France, Germany and Korea, increasingly use data-driven regulation to complement traditional regulatory tools. Data on network quality, for example, provide incentives for operators to "self-regulate" and improve their networks.

OECD countries are further focusing on how to extend and improve access through policies to reduce broadband deployment costs. This includes work on infrastructure sharing and co-investment provisions, as well as "dig-once" policies.

Passive infrastructure sharing has been common in OECD countries, including Australia, France, Korea and Switzerland. There are also more examples of active infrastructure sharing. These range from radio access network sharing agreements (Czech Republic, France, Germany, Spain, Sweden, Switzerland) to national roaming agreements (Colombia, France).

Several OECD countries have focused on "dig-once" policies. These aim to leverage non-broadband infrastructure projects (e.g. utilities, street light providers, and highway/road construction) and reduce the costs of broadband network deployment. For example, countries belonging to the European Union (EU) transposed the EU Broadband Cost Reduction Directive (2014/61/EU) into legislation by January 2016. This includes provisions that allow communication network operators to access other utility networks. Switzerland has also taken initiatives in the same sense.

In mobile markets, OECD countries continue to focus on efficient spectrum management to boost deployment of the next generation of wireless networks. Spectrum assignments for wireless networks have been prominent in the OECD since 2016. The 15 countries that have embraced such spectrum assignments are Austria, Canada, Chile, Denmark, Finland, France, Germany, Ireland, Italy, Latvia, Spain, Sweden, Switzerland, the United Kingdom and the United States.

The "network densification" required for 5G deployment will have important technical, regulatory and policy implications for all levels of government, including municipalities, industry and the public. Several OECD countries, including the United Kingdom and the United States, are streamlining rights of way to facilitate network densification. Others, such as Korea, Ireland and Sweden, have adopted policies to enhance backhaul and backbone connectivity.

In the last three years, many countries, including Australia, Austria, Colombia, France, Germany, Spain and the United Kingdom, have issued national 5G strategies. The European Union has several 5G initiatives, such as the "5G Action Plan" and the 5G Infrastructure Public Private Partnership. Korea has rolled out a comprehensive strategy named "5G+" to promote a "5G ecosystem", where 5G is the underlying infrastructure connecting advanced devices and innovative services. In the United States, the Federal Communications Commission (FCC) released a comprehensive strategy to "Facilitate America's Superiority in 5G Technology" coined as the "5G FAST Plan".

Almost all OECD countries have established broadband access targets, and in some cases, usage targets. Korea, for example, has the highest target for download speeds: 10 Gigabits per second (Gbps) to 50% of urban households by 2022. Luxembourg aims to offer 1 Gbps to all households by 2020. Sweden follows with the goal of connecting 98% of both households and businesses with 1 Gbps broadband by 2025. Austria is targeting nationwide coverage of 1 Gbps broadband connections, both fixed and mobile, by 2030. Canada aims for 90% of Canadians to have access to 50 Megabits per second (Mbps) download

speeds by 2021. By 2020, the United States aims to have broadband of 100 Mbps or more for 80% of households, while Norway has a similar goal for 90% of households.

A growing number of OECD countries have changed their legal frameworks to include broadband as part of their universal service framework. Switzerland was the first to do so, followed by Australia, Belgium, Canada, Finland, Spain and Sweden, among many others. In Korea, fixed broadband was designated as universal service in 2020.

Several policies have been introduced to ease market entry and reduce switching costs for the IoT. For example, Italy has allowed the use of extraterritorial numbering resources for the IoT, thus creating a clear regulatory framework for SIMs used in connected vehicles. EU member states may allow the use of certain national numbering resources, in particular certain non-geographic numbers, in an extraterritorial manner. This could create a new range for machine-to-machine (M2M) communication.

Some countries have reviewed their legislative frameworks around network neutrality in recent years. The European Union reviewed its legislation on Open Internet Access (2015/2120) and published a report on its implementation in April 2019. The Body of European Regulators for Electronic Communications began reviewing its Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Japan initiated discussions on network neutrality; the Study Group on Network Neutrality organised by the Ministry of Internal Affairs and Communications issued a report in 2019. In the United States, the FCC enacted its 2017 "Restoring Internet Freedom Order" to pursue a lighter-touch regulatory approach. Among other changes, the order classified broadband Internet access service as an information service, eliminated certain reporting requirements and authorised the Federal Trade Commission to oversee the privacy practices of Internet service providers.

Governments are seeking ways to foster IPv6 adoption. To that end, they are establishing promotion programmes to upgrade Internet services, adapting government purchasing and/or by promoting multi-stakeholder task forces to foster IPv6 deployment. For example, in 2019 Sweden implemented the recommendation by the OECD Review on Digital Transformation and provided the communication regulator with funds to promote IPv6 deployment.

## *Digital uptake and use*

### *Households and individuals*

Of the 30 countries responding to the 2019 OECD Digital Economy Policy Questionnaire on the uptake and usage of digital technologies, all but 4 – Italy, Germany, the Netherlands and Spain – reported explicit policies to promote the use of digital technologies in households and by individuals (Chapter 4).

Policy objectives across countries vary greatly. They include addressing the digital divide; raising digital skills and literacy; improving connectivity; enhancing cybersecurity and trust; and increasing e-government efficiency.

Often these policies target specific population groups. Common target groups include children (Czech Republic, Japan, Portugal), students (Colombia, Singapore), seniors (Australia, Austria, Japan), low-income households (Costa Rica, Singapore) or people with disabilities (Costa Rica, Israel, Japan).

Non-financial support is the most widespread instrument to promote use of digital technologies by households and individuals. In particular, official portals or hubs provide a virtual space for sharing experiences (Japan, Korea), running awareness campaigns (Colombia, Denmark, Mexico, Portugal) and undertaking training activities (Singapore). Cybersecurity, trust and consumer protection are a common focus.

Direct financial support may go through lead agencies managing programme implementation or take the form of loans, grants, vouchers or specific training. Programmes benefiting from this kind of support aim to reduce the digital divide in its many dimensions. This includes increasing network speed and availability (Australia, Colombia, Estonia, Finland, Singapore, Sweden, United States) and increasing digital skills (Portugal, the Russian Federation). In some countries (Costa Rica, Estonia, United States), such programmes also benefit from indirect financial support.

Indirect financial support is often provided in the field of education. This includes improving the educational system (Czech Republic, Portugal), promoting technological development (Russian Federation) and improving digital skills of students and teachers (Denmark). In Austria, fees for government services at the federal level are reduced when the application for such services is submitted by electronic means.

Regulations and statutory guidelines are employed to lay legal foundations in a wide range of areas, mainly in relation to consumer protection (Mexico, Turkey); personal data (Portugal, Singapore); digital security (Austria, Denmark); e-government (Australia, Japan) and e-health (Latvia).

### *Businesses*

Of the 30 countries responding to the Digital Economy Policy Questionnaire, all but 3 – Italy, the United Kingdom and the United States – reported having policies to promote the use of digital technologies by businesses.

Policy objectives vary greatly. They range from fostering uptake of productivity-enhancing digital technologies in firms and fostering access to knowledge and skills to supporting development of innovative products and social services (e.g. e-Health).

Small and medium-sized enterprises (SMEs) are the most common target for policies aiming to increase digital skills, technology awareness and adoption, as well as for awareness campaigns about digital security and privacy.

Direct financial support measures are the most widely used. These include grants for firms' uptake of digital technologies, such as cloud services (Korea) and big data (Portugal), digital consultancy services and digital skills (Denmark, Slovenia). While not directly aimed at digital technologies, many countries report grants or vouchers to support research and development (R&D). Germany, for example, targets big data, autonomous systems, information technology security and service platforms for this kind of direct support.

Indirect financial support takes several forms. Brazil and Japan, for example, offer tax credits or other relief for ICT investment. Other countries offer broader tax support for R&D; the Russian Federation has an explicit focus on digital technologies.

Non-financial support also takes several forms. Australia, Lithuania, Singapore and Sweden provide tailored business advice and counselling services. Turkey provides tailored advice on regulations relevant to new business models. Latvia and Norway provide training, while Portugal and Slovenia support the sharing of experience and mentorship.

Regulations and statutory guidelines lay legal foundations in a wide range of areas. These range from cybersecurity (Czech Republic) and FinTech (Mexico) to electronic signatures (Chile) and e-invoicing for public procurement (Austria, Norway). Actions in this area also include establishing guiding principles for regulation of new business models enabled by digital technologies (Denmark).

### *Digital government*

Over the past decades, large-scale public sector reforms have enabled greater efficiency and effectiveness of public services through digital transformation. As part of these efforts, governments invested heavily in new practices and modernised services to better respond to citizens' needs. Online service platforms common to several public sector organisations have been established to simplify administrative processes and improve interaction with citizens.

Most OECD countries have given responsibility for digital government strategies to the central or federal levels, according to the 2019 OECD Survey on Digital Government. Many have also established bodies dedicated to digital government, with varying degrees of advisory and decision-making responsibilities. The mandate of these bodies is the broadest in Canada, the Czech Republic, Iceland, Israel, Korea and Luxembourg, while its scope is narrower in Belgium and Sweden.

According to the same survey, 22 OECD countries, as well as Brazil, use a standard model for ICT project management. Further, 22 have adopted a business-case approach, such as cost-benefit

and/or cost-effectiveness analysis. In addition, 24 have a specific ICT procurement strategy for the public sector, while another 10 have a whole-of-government procurement strategy that covers ICT. Only 12 of 31 OECD countries with available data have adopted all three policy levers (ICT project management, business-case approach and ICT procurement strategy) as part of their digital government strategy.

### *Skills*

In recent years, several countries have adapted school curricula to changing skills requirements driven by the digital transformation. In Australia, the "ICT capability development" framework aims to develop digital skills in stand-alone ICT classes, as well as across other learning areas. In Canada, several provincial governments have adopted a comprehensive approach to digital competence. In the Czech Republic, the Digital Education Strategy for 2020 aims to open education to new ways of learning through digital technologies and to improve pupils' competences in ICTs and computational thinking. France has recently introduced a mandatory course on computational sciences and technology in secondary schools. Sweden has made changes in the curricula for the school system, aiming to strengthening digital competence, media and information literacy, as well as abilities to be source-critical.

For over a decade, countries across the OECD have been tackling the need for teachers to develop ICT skills through diverse policies. These range from developing national plans promoting this goal to introducing compulsory training, national accreditation standards or national certification for teachers. Denmark, for instance, has developed a voluntary licence that combines pedagogical knowledge of ICTs and basic ICT skills training. In Portugal, the Train the Trainers programme aims to improve teachers' competencies, including digital skills.

Many OECD countries have established digital literacy programmes to increase digital inclusion, especially for the most vulnerable groups (Chapter 4). The Pact for Digital Competence in Austria, for example, targets young career starters; off-liners; professionals aged 45 or more; and seniors. Other examples include Colombia's Digital Citizenship; Israel's Senior Citizens Digital Skills Course; and Latvia's Father's Third Son, where libraries provide counselling on how to use e-services and navigate safely on the Internet. In Norway, the Digital Inclusion for All programme targets the elderly, women and immigrants. Portugal's National Digital Competences Initiative e.2030 helps citizens and workers improve their digital competences. Finally, the Future Digital Inclusion Programme in the United Kingdom supports adult learning.

Programmes to upskill or reskill workers have also become common among OECD countries. These include vouchers for raising digital competences (Slovenia), Competence Centres (Germany), ICT training for SMEs (Israel), training support for employees in the ICT industry (Latvia), business counselling for SMEs (Lithuania), programmes to reskill and upskill workers (Portugal) and free online courses (United Kingdom).

### *Data access, sharing and re-use*

All OECD countries and most partner economies have one or more initiatives around data access, sharing and re-use (Chapter 5). Most focus on access to and sharing of public sector data. For example, France, Japan, the United Kingdom and the United States aim to enable open access to government data. Many countries have public sector information initiatives, while others have open data initiatives or both. The latter is the case for EU member states, following Directive (EU) 2019/1024 of 20 June 2019 on Open Data and the Re-Use of Public Sector Information. A general trend towards the establishment of open data portals can be observed across the OECD.

Governments' commitment to become more data-driven and to leverage technological developments, e.g. big data and AI, have led them to facilitate data sharing within the public sector. Australia's data sharing and release legislation is a prominent example. Other examples include Estonia's Information Sharing Data Sheet (X-Road) and the United Kingdom's Government Data Ethics Framework.

Opening geospatial data and transportation data ranked high on the agenda of public sector data initiatives. Examples include the Geocoded National Address File in Australia. In Switzerland, the Federal Office of Transport wants to facilitate the exchange of data between public and private actors active in the Swiss public transport system.

Few countries facilitate data sharing within the private sector, although they recognise this as an emerging challenge. Most initiatives are voluntary, the most common being contract guidelines and data partnerships, including public-private partnerships. Examples of government initiatives based on contract guidelines include the Contract Guidance on Utilisation of AI and Data in Japan and the Privacy and Security Principles for Farm Data in the United States. The Industrial Data Space in Germany, the Data Integration Partnership for Australia, Japan's Certification System for data-sharing platforms, Singapore's Trusted Data Sharing Framework and Digital Hub Denmark are examples of data partnerships.

Where data sharing is mandated, regimes are commonly restricted to trusted users. Australia, for instance, is considering a framework to identify "national interest datasets" or "designated datasets". In France, the Law for a Digital Republic (*Loi pour une République numérique*) defines criteria for "data of general interest" (Government of France, 2016[12]). The European Commission is examining data sharing between the private and public sector under the notion of "private-sector data for public interest purposes". In some cases, access to data is based on competition and (system) efficiency considerations. This mainly touches network industries such as telecommunications, energy and transport. Finland's Act on Transport Services is an example.

Data portability is often regarded as a promising means for promoting cross-sectoral re-use of data. At the same time, it could strengthen the control rights of individuals over their personal data and of businesses, particularly SMEs, over their business data. Prominent data portability initiatives include My Data in the United States, Midata in the United Kingdom, the European Union's Right to Data Portability set by the General Data Protection Regulation (GDPR) and Australia's recent proposal for a Consumer Data Right.

Some governments established dedicated initiatives to support the development of data-related skills and infrastructures in the public sector. Examples include the Digital Skills Partnership in the United Kingdom, Estonia's Digital Solutions seminars, the data analytic competitions in China and Slovenia's education and training programmes for civil servants.

Some governments have established data analytic and innovation centres to support their government agencies in the sharing and re-use of data. Others have created and strengthened partnerships with such centres. Ireland established the Insight Centre for Data Analytics, considered one of Europe's largest data analytics research organisations. Australia's data innovation centre, Data61, has partnered with government agencies to build new technologies that make high-value government data available to more people, while preserving privacy. The European Commission is developing a support centre for data sharing under the Connecting Europe Facility Programme.

Several countries have also supported innovation and R&D in data analytics and related technologies. The European Commission, for example, has a number of funding mechanisms for data-related innovation. These are in relation to data innovation incubators, pan-European aggregators of public sector information (European Data Portal) and privacy-enhancing technologies.

Governments have turned to a wide array of digital technologies and advanced analytics to collect, analyse and share data for frontline response to the COVID-19 crisis. For example, Deutsche Telekom has provided anonymised "movement flows" data of its users to the Robert Koch Institute, a research centre and government agency responsible for disease control and prevention in Germany. Vodafone Group's Five Point Plan to address COVID-19 includes providing large anonymised data sets to help authorities better understand population movements. The European Commission has liaised with eight European telecommunications operators to obtain anonymised aggregate mobile location data in order to co-ordinate measures tracking the spread of COVID-19.

COVID-19 response applications (apps) for location tracking have also emerged. Singapore, for example, initiated contact tracing for all confirmed and suspected cases since the early days of the outbreak. In addition, the app can share people's health information between hospitals, the government and third parties. Such apps may raise considerable privacy issues, particularly if users do not give informed, explicit consent for this data sharing but even when they do.

### *Privacy*

Privacy frameworks are particularly important during crisis periods such as the COVID-19 pandemic. Such frameworks facilitate data sharing when in the interests of national security and public security, including public health and welfare. Recent OECD work suggests that despite these frameworks, few countries have policies to facilitate data sharing within the private sector. Even fewer have governance frameworks to support extraordinary data collection and sharing in ways that are fast, secure, trustworthy, scalable and in compliance with relevant privacy and data protection regulations.

As a result, many countries have recently sought advice from privacy enforcement authorities (PEAs), private-sector law firms, civil society, academics and other actors. They wish for assurance that their actions are necessary and proportionate, and that they fully understand their potential implications. Many governments passed or have pending legislation that restricts data collection based on population, time period and purpose. PEAs across many OECD countries have generally endorsed a pragmatic and contextual approach. To that end, they have enforced laws with discretion to ensure that respect for fundamental data protection and privacy principles do not stand in the way of necessary and proportionate frontline responses to COVID-19. Additionally, PEAs in many jurisdictions are issuing guidance on the collection, processing and sharing of personal data for COVID-19 contact tracing and other measures. Much of this guidance relates to how privacy-by-design features can be incorporated into "track and trace" applications so as to ensure the protection of personal data collected.

The past two years have seen a number of significant regulatory developments worldwide (Chapter 6). In particular, the European Union's GDPR on 25 May 2018 introduced new rules governing the global free flow of personal data regarding data subjects in the European Union.

Further, the Council of Europe has recently extensively revised its 1985 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). These revisions aim to ensure its applicability to new ICTs and to strengthen implementation. The modernised instrument, Convention 108+, was to enter into force in October 2023.

The OECD is also monitoring the implementation of the 2013 revisions to the 1980 OECD Privacy Guidelines (OECD, 2013[15]). This exercise planned to identify gaps and suggest possible next steps to ensure the guidelines remain relevant.

There has been an increase in various trade agreements and other frameworks that seek to promote trust in transborder flows of personal data. These instruments sit alongside others that continue to shape privacy and global data transfers, e.g. EU-US Privacy Shield Framework or the Asia-Pacific Economic Co-operation (APEC) Privacy Framework.

At a national level, an increasing number of countries around the world, including OECD countries, are putting in place modern data protection frameworks and policies. These combine openness for international data flows with the highest level of privacy and data protection for individuals. Many governments have been introducing and modifying data-related policies to adapt them to the digital age. Such policies also place conditions on the transfer of data across borders or require that data be stored locally.

Understanding how privacy laws apply to emerging technologies, such as AI, and their impact on consumers, remains a challenge. Countries are developing dedicated regulation and guidance to deal with the privacy challenges from emerging technologies, such as AI. Countries are also employing, developing or considering measures for regulatory innovation in the context of emerging technologies, most commonly regulatory sandboxes and experimentation. Other measures reported include development of international standards for specific technologies (such as blockchain), a Digital Charter, a privacy research grants programme and an AI auditing framework.

Some privacy developments are particularly notable. The California Consumer Privacy Act, enacted in 2018, creates new consumer rights regarding the collection, processing, retention and sharing of personal data. Brazil also enacted a General Data Protection Law in 2018. In India, long-awaited national data protection legislation was before parliament.

The 2013 revision of the OECD Privacy Guidelines (OECD, 2013[15]) calls on governments to "develop national privacy strategies that reflect a co-ordinated approach across governmental bodies." However, just under half of the 29 respondents to the 2019 OECD Privacy Guidelines Questionnaire have a national privacy strategy or whole-of-government approach to privacy.

In addition to regulatory reforms and innovation, countries are addressing challenges posed by emerging technologies through policy responses. Primarily they develop new data governance frameworks but they also create new bodies or institutions and guidance on specific technologies. For example, the United Kingdom recently established a Centre for Data Ethics and Innovation to identify ethical issues raised by emerging technologies, agree on best practices around data use and develop potential new regulations to "build trust and enable innovation in data-driven technologies".

Countries today are striving to provide additional and complementary policy responses to enhance the protection of children's privacy. At the domestic level, almost all respondents to a 2017 OECD survey reported their privacy laws include specific provisions regarding the protection of children. The GDPR recognises that children merit special protection in regard to their personal data, particularly in relation to their marketing and collection. However, OECD countries differ in approaches to notice and consent for the collection, processing and sharing of children's personal data.

As more privacy and data protection frameworks are enacted, attention has shifted increasingly towards how to enhance compliance with those frameworks, including by greater enforcement. In particular, governments are investing in policy measures to enhance awareness of requirements in privacy and data protection frameworks. Governments also emphasise promoting data controllers' accountability, along with engaging in international enforcement co-operation. Some key mechanisms at the multilateral level include the Global Privacy Enforcement Network, the International Conference of Data Protection and Privacy Commissioners (now the Global Privacy Assembly) Enforcement Cooperation Arrangement and the APEC Privacy Cross-border Privacy Enforcement Arrangement.

### *Digital security*

Several OECD countries have national digital security strategies to support economic and social prosperity and/or foster trust and confidence in the digital environment (Chapter 7). Capacity building, protection of critical infrastructures, information sharing and international co-operation are the main pillars of these strategies.

Government agencies in charge of digital security across the OECD have responded to the COVID-19 crisis in several key ways. They have raised awareness, monitored the threat landscape, provided assistance where appropriate, and co-operated with all relevant stakeholders, including at the international level. For example, the United States' Cyber and Infrastructure Security Agency set up a section on its website dedicated to security risks related to COVID-19 (*www.cisa.gov/coronavirus*). The European Commission, the European Union Agency for Cybersecurity, the Computer Emergency Response Team for the EU Institutions and Europol co-operated to track malicious activities related to COVID-19 and alert their respective communities. The Canadian Centre for Cybersecurity recommended that Canadian health organisations involved in the national response to the pandemic remain vigilant and ensure use of digital security best practices. The Czech National Office for Cyber and Information Security ordered selected health care entities to enhance the security of key ICT systems; it offered consultations and support to these entities.

Co-ordination mechanisms tend to differ among countries. In Denmark, for instance, the Agency for Digitisation (Ministry of Finance) and the Centre for Cyber Security (Ministry of Defence) share responsibility. In the Netherlands, the Ministry of Justice is in charge of overall co-ordination. In some countries, such as Latvia, Spain or the United States, a national council gathers representatives of all ministries and agencies involved.

The nature and the scope of multi-stakeholder co-operation also varies greatly. Some governments co-operate on an ad-hoc basis with specific trade associations, while others involve stakeholders more broadly from the design phase. As an example of the latter, Brazil set up three working groups on, respectively, digital governance, prevention and mitigation of threats, and protection of government and critical infrastructures.

Beyond national strategies and policies, governments across the OECD are facilitating new forms of multi-stakeholder and international partnerships to enhance digital security. Examples include the Paris Call for Trust and Security in Cyberspace, the Charter of Trust and the Cybersecurity Tech Accord.

Digital security innovation is an emerging trend in OECD countries, which have established open innovation centres to encourage its development. Examples include Israel's CyberSpark campus, the Australian Cyber Security Growth Network, the London Office for Rapid Cybersecurity Advancement in the United Kingdom, Singapore's Innovation Cybersecurity Ecosystem, the Agency for Innovation in Cyber Security in Germany, the Cyber Campus France and the European Cyber Security Organisation.

Governments support educational programmes to overcome the shortage of digital security professionals. In the United States, for example, the National Institute of Standards and Technology, within the Department of Commerce, has launched the National Initiative for Cybersecurity Education. Canada promotes talent development by teaching programming and digital skills to children from a young age. Governments can also promote sustainable interlinkages between academia, industry, government itself, entrepreneurs and financial actors. For instance, the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity co-ordinates co-operation between digital security ecosystems across the world.

Some OECD countries have launched voluntary labelling schemes to improve product transparency and reduce vulnerability. For instance, the Finnish government is partnering with industry to launch an IoT security label. The governments of Japan and Germany plan their own labelling schemes for IoT products and routers, respectively.

Facilitating multi-stakeholder partnerships is an additional tool for governments. For instance, the Dutch government is working with stakeholders to monitor and enhance the digital security of connected devices. In the United States, the National Telecommunications and Information Agency is encouraging developers to provide a "software bill of materials". Other governments in the OECD have funded and/or facilitated joint work on botnets, including "botfrei" in Germany and the National Operation Towards IoT Clean Environment in Japan.

Some governments are also mandating basic security features for all IoT products through regulations. In the United Kingdom, for instance, the government plans to mandate manufacturers to implement the key principles of its guidelines for IoT security. In Japan, the regulator has also imposed requirements on IoT products.

Several industry players have established coalitions to enhance digital security of their products. The Charter of Trust, for example, gathers companies along the value chain to create a reliable foundation for trust in the digital environment. Through the Cybersecurity Tech Accord, 120 ICT sector companies partner on initiatives that improve the security, stability and resilience of cyberspace. Meanwhile, France launched the Paris Call for Trust and Security in Cyberspace to strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.

### *Consumer policy*

Governments need to consider how to adapt, change and implement consumer policy in this age of rapid technological progress (Chapter 8). While consumer policy is generally broad enough to cover new technologies and business models, governments should ensure there are no gaps that leave consumers exposed. Governments have a key role in ensuring that new technologies are used in a human-centric, ethical and sustainable way to maintain consumer trust.

As another key challenge, governments must have the technical expertise to understand these emerging issues to engage in effective policy making and enforcement. Many risks span several areas, including data protection, privacy, consumer protection, competition and security. Therefore, consumer authorities need to co-operate and co-ordinate with counterparts in other relevant disciplines. Furthermore, the global nature of the digital transformation implies that governments increasingly need to co-operate across borders. They should enhance their authority to do so, including by implementing the co-operation provisions of the 2016 OECD *Recommendation of the Council on Consumer Protection in E-commerce* (OECD, 2016[13]) and the 2003 *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (OECD, 2003[16]).

Consumer policy should consider the vulnerabilities of different groups of consumers to target protections and awareness accordingly. In this way, they can ensure the benefits of new technologies are shared across society. For example, some consumer groups, such as the elderly, may be more prone to online scams. Moreover, data protection and privacy concerns may be more sensitive when it comes to IoT products used by, and aimed at, children who may be less aware of the risks. In addition, the COVID-19 crisis shows that policy makers should also consider whether large-scale events, such as pandemics or natural disasters, might render wider groups of consumers vulnerable to online commercial exploitation. For example, the pandemic has made many mainstream groups of consumers more vulnerable to exploitative practices on line due to job and financial losses, as well as to fear and anxiety regarding the virus. Such practices include price gouging of essential or in-demand products.

It is important to encourage businesses and industry associations, as well as consumer and other civil society organisations, to provide input into policies regarding the incorporation of new technologies in consumer products. This will help ensure that new products benefit consumers without harming them economically, compromising the privacy or security of their personal information, or otherwise putting them at risk.

### *The digitalisation of science and innovation policy*

As well as profoundly affecting science, research and innovation, digitalisation is also beginning to impact how policy is made in these areas (Chapter 9).

Digital Science and Innovation Policy (DSIP) initiatives are underway in several countries. They experiment with semantic technologies to link datasets; with AI to support big data analytics; and with interactive visualisation and dashboards to promote data use in the policy process.

Data linking and synchronisation across digital systems can help optimise administrative workflows to reduce reporting burdens. They can also support performance monitoring and management. Finally, they can provide anticipatory intelligence to identify the need for innovation policy.

Realising the potential of DSIP involves overcoming several possible barriers, including data quality, interoperability, sustainable funding and data protection regulations. Policy makers wishing to promote DSIP face further systemic challenges. These include overseeing fragmented DSIP efforts and multiple, often weakly co-ordinated, initiatives; ensuring responsible use of data generated for other purposes; and balancing the benefits and risks of private-sector involvement in providing DSIP data, components and services.

Digital tools may help provide solutions for data interoperability. Harvesting datasets from all the public and private actors involved in research and innovation activities requires common data formats and other interoperability enablers. These include application programming interfaces (APIs), ontologies, protocols and unique persistent and pervasive identifiers (UPPIs) for research, development and innovation (R&DI) actors.

Some UPPIs exist as an integral part of, or support for, commercial products such as publication/citation databases, research information systems and supply-chain-management services. Others exist solely to provide a system of identifiers for wide adoption and use. Open Researcher and Contributor ID, for example, aims to resolve name ambiguity in scientific research. It develops a digital register of unique identifiers and basic associated identity information for individual researchers.

As a UPPI system gains traction there may be a "network effect", whereby each additional registrant increases the value of the system to all users. Eventually the UPPI system may become a generally expected way for entities to unambiguously identify each other. This results in strong incentives for those not yet registered to join.

Besides UPPIs, APIs have become a standard for enabling M2M interactions and data exchanges. Within a framework of digital government initiatives, several countries have started to proliferate APIs across the landscape of government websites and databases, improving data re-use. Improvements in access to administrative datasets have positive impacts on the functionality and reliability of the results of analyses delivered by DSIP systems.

Aside from government agencies and other public funders, R&DI-performing organisations store a significant share of research and innovation data. However, these often have different formats and structures, even for the same type of information. The Common European Research Information Format and metadata formats by Consortia Advancing Standards in Research Administration Information were originally designed to serve the needs of higher education institutions in data management. Some DSIP systems use them to harvest curated data from research institutes and directly apply them in analysis.

Interoperability remains a major hurdle despite the recent proliferation of identifiers, standards and protocols. Policy makers may be able to influence the development of international UPPI systems. They could focus on target populations, information captured, compatibility with statistical systems, governance systems and especially adoption both by entities and potential users. International efforts related to data documentation and the development of metadata standards could be consolidated to improve data interoperability.

### *Work in the digital era*

In recent years, many countries have experienced an increase in non-standard forms of work, an umbrella definition for arrangements such as temporary jobs, part-time contracts and self-employment. Although some of these forms are not new, digitalisation, together with globalisation and changes in regulations/policies, have contributed to their diffusion. Digital technologies have also enabled new forms of work, such as jobs mediated by platforms. The COVID-19 pandemic has most severely hit non-standard workers, as they are more exposed to health risks and often receive less government support than employees (Chapter 10).

Several countries, including the United Kingdom, the Netherlands and Poland, are discussing the introduction of minimum rates for some groups of self-employed workers. Subnational governments have also set minimum wages for platform workers. New York City, for example, has set a minimum wage for Uber and Lyft drivers. Platforms have also voluntarily set minimum wages (e.g. Topdesigner in the Czech Republic; Adtriboo in Spain; Upwork and Prolific in the United Kingdom; and Favor in the United States).

As an alternative or complement to minimum wage, countries like Canada, Denmark, France, Germany and Sweden have extended collective bargaining rights to certain groups of self-employed workers. In addition to worker-led initiatives, some platforms have also started addressing platform workers' limited access to representation and social dialogue. These actions are mostly in response to government threats to reclassify their activities.

Governments have taken steps to regulate atypical contracts, such as "zero-hours" contracts, to reduce unpredictability in working hours and income. Finland, for example, restricts use of this type of contract to situations where employers truly have a variable need for labour. Along with Norway and Ireland, Finland also requires employers to provide information (such as the minimum number of hours) up-front or in the employment contract. Those three countries, alongside the Netherlands and the state of Oregon in the United States, require advance notice of work schedules. Meanwhile, Australia and the United Kingdom give employees the right to request a more predictable contract after a certain period.

Countries have also taken steps to extend occupational and safety health protection to non-employees. Australia, Ireland, Lithuania, Turkey and the United Kingdom have decoupled such protections from the employment relationship. Australia, Bulgaria, Canada and Poland are connecting related regulation to the workplace rather than to any specific contract type. Korea had plans to extend the Occupational Safety and Health Act to "all working people". Meanwhile, France's new labour law foresees that platforms must reimburse workers who voluntarily insure themselves against occupational risks or illness.

Denmark and France have also introduced significant reforms to their social protection system to establish portability of entitlements for individuals moving between or combining employee status and self-employment. In November 2019, the European Union adopted a *Council Recommendation on Access to Social Protection for Workers and the Self-Employed* (European Commission, 2019[17]). This encouraged member states to allow non-standard workers and self-employed to adhere to social security schemes, while increasing adequacy of these schemes to non-standard work.

Some OECD countries, including France and Ireland, have extended available financial incentives for training to self-employed, including own-account workers. Incentives include both tax deductions and subsidies. Other approaches, such as in Korea, Austria and Belgium, make financial support for training conditional on the payment of social security contributions or enrolment in an employment insurance plan. Some countries, including Austria, Finland and Luxembourg, provide wage replacements to self-employed enrolled in training. France's labour law requires platforms to pay employers' contributions for training, cover expenses for the recognition of prior learning and provide a training indemnity for all gig workers above a set income threshold.

To deal with increasingly non-linear career paths, several OECD countries have established some individual learning schemes. In these cases, the rights to training are attached to individuals rather than to a specific employer or employment status. Some countries, including Belgium (Flanders), Germany and Latvia, have also extended skills advice and guidance services provided by public employment services to own-account workers.

### *Artificial intelligence*

Canada was the first country to launch a national AI strategy in 2017. By April 2020, over 60 countries had devised a national AI strategy and policies, while others were developing policies. Priority areas include AI R&D and financing, industry, societal challenges, education and employment, regulation and international co-operation. At the same time, countries are addressing AI-related risks and ethical challenges. Some have created oversight bodies and issued ethical guidance. Several are reviewing and adapting the applicable policy and regulatory frameworks (Chapter 11).

During the COVID-19 pandemic, governments, academia and companies have rapidly developed AI systems. These aimed to predict and monitor the spread of the disease, provide medical diagnosis, fight misinformation and undertake research on vaccines and treatments. Many countries have also deployed virtual assistants and chatbots to support health care organisations. For example, the US Center for Disease Control and Prevention and Microsoft provide a Coronavirus Self-Checker service to help users self-assess COVID-19 and suggest a course of action.

Several countries have established dedicated bodies to co-ordinate implementation of their AI strategy (Canada, Egypt, United Kingdom, United States); conduct technology foresight and impact assessment (Austria, Canada, United Kingdom, United States); or address ethical issues (Singapore, New Zealand, United Kingdom). In addition, AI observatories have been established at the regional (Quebec), national (Italy, France, Germany) and international levels (European Commission's AI Watch, AI4EU Observatory, OECD.AI).

Building on digital government approaches, many national AI strategies and policies explicitly encourage adoption of AI in the public sector. Denmark, for example, aims for the public sector to use AI to offer world-class services for the benefits of citizens and society. Finland's AuroraAI project aims to use AI to provide personalised, one-stop-shop and human-centric AI-driven public services. Korea's AI service – The Work – helped 2 666 job seekers find relevant job offers that led to a job in the second quarter of 2019. The EU Coordinated Plan on AI aims to "make public administrations in Europe frontrunners in the use of AI".

Most countries have introduced guidelines for trustworthy AI, largely aligned with the OECD *Recommendation of the Council on Artificial Intelligence* (OECD AI Principles) (OECD, 2019[14]). Examples include Australia's AI Ethics Framework, Hungary's AI Ethical Guidelines, Japan's AI R&D Guidelines and AI Utilisation Guidelines, Singapore's Model AI Governance Framework and the European Commission's Ethical Guidelines on AI.

Several governments and intergovernmental bodies are considering or have adopted binding legislation for areas of AI applications deemed high risk. For example, Belgium has prohibited the use of lethal autonomous weapons by local armed forces. New regulations have been issued on driverless cars (Belgium, Denmark) or unmanned aircraft systems (United States). In February 2020, the European Commission issued a White Paper on Artificial Intelligence – A European approach to excellence and trust. It proposed a voluntary "quality label" for AI applications considered not to be high risk.

The International Organization for Standardization, the Institute of Electrical and Electronics Engineers and similar bodies are developing cross-sector and sector-specific AI standards. Several countries, including Australia, Canada, China, Germany, the Russian Federation and the United States, emphasise the need for common standards, including to address security issues. Others, including Denmark and Malta, plan to establish AI certification programmes.

Most countries seek to enhance national AI R&D capabilities. The United States plans to invest an additional USD 950 million in non-defence AI R&D in 2021 and the creation of national AI research institutes. Canada's federal and provincial governments have dedicated over CAD 300 million (USD 227 million) to AI research over 2017-22, anchored in the three AI institutes of the Pan-Canadian AI Strategy. The EU Horizon 2020 programme has committed EUR 1.5 billion to AI research over two years and expects an additional EUR 20 billion in 2020 from the private sector and member states.

As part of their AI strategy, several countries have developed or are developing centralised and accessible repositories of open public data in relation to AI (Norway, Portugal, Spain, United States). Others seek to incentivise data sharing in the private sector (United Kingdom, European Union).

Countries also boost development of innovative AI research ecosystems by establishing networking and collaborative platforms. Examples include Canada's Innovation Superclusters Initiative, Denmark's Digital Hub for AI public-private partnerships, Finland's AI Business programme, Hungary's AI in practice self-service online platform and Portugal's Digital Innovation Hubs.

Countries are introducing a wide range of policy initiatives to spur innovation and AI adoption by SMEs. Examples include the European Commission's AI4EU project, Finland's AI Accelerator, the SME 4.0 Excellence Centres in Germany and Korea's AI Open Innovation Hub. Governments are also experimenting with controlled environments for the testing of AI systems, including by SMEs (Lithuania, New Zealand, United Arab Emirates, United Kingdom, United States).

Education and skills are a priority for all national AI strategies. Some initiatives pertain to formal education and training programmes on AI, including science, technology, engineering and mathematics education (Australia, Finland, United Kingdom, United States). Others provide incentives to retain and attract foreign skills and top talent in AI (Belgium, United Kingdom).

Countries are also devising vocational training and lifelong learning programmes to help citizens keep up with technological and societal changes. As an example, Finland's Elements of AI programme seeks to increase AI literacy across the Finnish population through a ten-hour Massive Open Online Course.

In parallel, national AI strategies are collaborating among government and business, as well as educational and non-profit communities, to develop educational programmes, tools and technologies. Examples include Korea's Smart Training Education Platform and Germany's Learning Systems Platform (Plattform Lernende Systeme).

Some countries, including, France, the Czech Republic, Germany and Poland, have established dedicated labour market observatories to better understand the impact of AI on jobs.

International co-operation for AI is taking place in fora including the OECD, the Group of Seven, the Group of Twenty, the European Union, Council of Europe and the United Nations Educational, Scientific and Cultural Organization. Cross-border research on AI is also a priority. For example, the French National Research Agency together with the German Research Foundation and the Japan Science and Technology Agency have called for trilateral French-Japanese-German collaborative research projects on AI.

Some countries (Canada, Italy, France, Germany, United Kingdom, United States) have begun policy intelligence activities to evaluate implementation of their national AI strategies. At the European level, AI Watch is collecting indicators to monitor investments in AI. In February 2020, the OECD launched the AI Policy Observatory (OECD.AI),[6] a platform for policy makers to monitor developments in the AI policy landscape. The OECD also hosts the new Global Partnership on AI (GPAI), a coalition launched in June 2020 to ensure AI is used responsibly, respecting human rights and democratic values. Its founding members are Australia, Canada, the European Union, France, Germany, India, Italy, Japan, Korea, Mexico, New Zealand, Singapore, Slovenia, the United Kingdom and the United States.

The GPAI will bring together experts from industry, government, civil society and academia to conduct research and pilot projects on AI. It aims to bridge the gap between theory and practice on AI policy. For example, it could look at how AI could help societies respond to and recover from the COVID-19 crisis.

### *Distributed ledger technologies*

Governments are increasingly interested about the effects of blockchain and other distributed ledger technologies (DLTs) on economies and societies, as well as on their use as a policy tool. Several countries have already issued overarching blockchain strategies, including Australia, China, Germany and India. Others, including France and Italy, are developing them (Chapter 11).

Blockchain and other distributed technologies pose important challenges to traditional policy and regulatory frameworks and governments' ability to control risks for end-users and provide certainty. These challenges relate particularly to their potential for highly distributed and completely decentralised governance, as well as ease of operation across borders. At the same time, evidence from several OECD projects shows that over-regulation could suffocate innovation and result in a loss of competitiveness.

In 2018, OECD countries agreed to establish the Global Blockchain Policy Centre. This move responded to growing international interest in blockchain, as well as the OECD's own research and analysis. The Centre supports governments to better understand blockchain technology, address the challenges raised by DLTs and their applications, seize opportunities to achieve policy objectives and deliver more effective government services.

### *Quantum computing*

Several countries have formulated a national agenda for the development of quantum computing (Chapter 11).

The United States is a world leader in quantum computing research. It has billions of dollars in funding and around 50 companies and start-ups engaged in quantum technology and services. Funding is aimed at practical and commercial purposes, as well as fundamental scientific research. Europe has a long academic tradition of quantum mechanics research. It has received funding from the European Commission since 1998. In 2018, the European Union established the Quantum Technology Flagship Research Initiative to develop a solid industrial base to exploit its scientific leadership. The initiative has an expected budget of EUR 1 billion over ten years. This complements the spending of individual countries and stimulates international collaboration. It focuses on applications, as well as the basic science behind the technologies.

While China is lagging behind on the development of universal quantum computers, its Quantum Experiments at Space Scale project is on the forefront of space-based quantum communication and cryptography. In 2016, the Chinese Academy of Sciences (CAS) launched the first "quantum satellite". This satellite emits signals to different receiving stations in the world to establish a shared random secret key. Initial experiments within China were soon followed by intercontinental quantum cryptography between China and five ground stations in Europe. The latter were supervised by a team from the University of Vienna and the Austrian Academy of Sciences.

China is also trying to catch up on universal quantum computing. In 2015, CAS and Alibaba Cloud established the Alibaba Quantum Laboratory, the first quantum computing laboratory in Asia. In 2018, they launched the first free public quantum computing service, accessible through the cloud. However, their processor has only a fraction of the computational power of rival services by Google and IBM. Alibaba's competitor Baidu reportedly invested USD 15 billion in 2018 in its own institute for quantum computing.

In addition to the European Union, China and the United States, other countries are pursuing quantum technology. Japan, Korea, Israel, the Russian Federation and India have formulated a national agenda for the development of quantum computing. Furthermore, India has announced investment in quantum computing to maintain its technological edge and attract further investments. Israel plans to invest in applications of quantum technology and peripheral hardware.

On top of collaborations within the scientific community, quantum computing strategies often involve close ties with industrial partners. In Canada, through the Quantum Alliance, the University of Waterloo and industry partners exchange research ideas and collectively develop quantum technology via focused workshops. In the United Kingdom, the Quantum Technology Innovation Centre at the University of Bristol is a dedicated open-access innovation facility. Businesses can access "pay-as-you-go" incubator labs, office space and state-of-the-art equipment, while being supported by experts in a range of business, technology and manufacturing areas.

Besides national initiatives, international collaborations are sought as well. Various governments worldwide have entered a partnership with IBM, which installed their machine on university campuses. Through this initiative, governments hope to foster quantum computing talent worldwide by providing access to the newest quantum technology.

Cryptographic algorithms are essential in e-commerce, mobile and online communication, online banking and cloud computing. Many methods for cryptography that are effective today may be easy to break once large quantum computers are developed. In response, the European Union started PQCRYPTO, a project that develops post-quantum cryptographic techniques. The US National Security Agency created the National Institute of Standards and Technology in 2016 to develop encryption schemes that could withstand a quantum assault.

# *References*

European Commission (2019), *Council Recommendation on Access to Social Protection for Workers and the Self-Employed*, 2019/C 387/01, ST/12753/2019/INIT, Brussels, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.387.01.0001.01.ENG&toc=OJ:C:2019:387:TOC*. [17]

European Commission (2016), "European Union eGovernment Action Plan", webpage, *https://ec.europa.eu/digital-single-market/en/egovernment-action-plan-digitising-european-industry* (accessed on 24 March 2020). [4]

European Commission (2015), "A digital single market strategy for Europe", *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2015), 232, Final, European Commission, Brussels, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN*. [2]

European Commission (2010), "A digital agenda for Europe", *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2010), 245, Final, European Commission, Brussels, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245&from=en*. [1]

European Commission (2010), *Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth*, European Commission, Brussels, *https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf*. [3]

Government of France (2016), *Loi pour une République numérique*, Paris, *http://www.senat.fr/leg/pjl15-744.html*. [12]

Informatics and Information Security Research Center (2016), "2016-2019 National e-government strategy and action plan (Turkey)", webpage, *https://bilgem.tubitak.gov.tr/en/urunler/2016-2019-national-e-government-strategy-and-action-plan* (accessed on 2020 March 24). [6]

MCTIC (2018), *Digital Transformation Strategy*, Ministry of Science, Technology, Innovation and Communications, Brasilia, *http://www.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/digitalstrategy.pdf*. [5]

Ministry of Finance and Economic Affairs (2019), *Icelandic Financial Plan for the Years 2019-2023*, Ministry of Finance and Economic Affairs, Reykjavík. [11]

OECD (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, *https://dx.doi.org/10.1787/dc930adc-en*. [7]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264312012-en*. [9]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, OECD, Paris, *https://legalinstruments.oecd.org/api/print?ids=648&lang=en*. [14]

OECD (2019), "Using digital technologies to improve the design and enforcement of public policies", *OECD Digital Economy Papers*, No. 274, OECD Publishing, Paris, *https://dx.doi.org/10.1787/99b9ba70-en*. [8]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264276284-en*. [10]

OECD (2016), *Recommendation of the Council on Consumer Protection in E-Commerce*, OECD, Paris, *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422*. [13]

OECD (2013), *OECD Privacy Framework*, OECD Publishing, Paris, *https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm*. [15]

OECD (2003), *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*, OECD Publishing, Paris, *https://doi.org/10.1787/9789264103573-en-fr*. [16]

# *Notes*

1. Stakeholder groups include business, civil society, the Internet technical community and trade unions, among others.
2. OECD countries that responded to the 2019 OECD Digital Economy Policy Questionnaire on national digital strategies and policies are Australia, Austria, Belgium, Chile, Colombia, the Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.

3. The OECD's partner economies that responded to the 2019 OECD Digital Economy Policy Questionnaire on national digital strategies and policies are Brazil, Costa Rica, the Russian Federation, Singapore and Thailand.
4. The United States approaches digital policy through a portfolio strategy: it has a collection of policies, regulations and laws associated with specific issues and/or sectors that together support the evolution and progression of digital transformation. Elements include, in no particular order, policies relating to telecommunications and the Internet, digital privacy, cybersecurity, big data, smart information technology (IT) delivery, open data, IT research and development, educational technology, online education and environmental information systems. The portfolio strategy is reflected in policies at the national (federal) and subnational (state and local) levels. The United States nurtures the continued development and improvement of the technologies that underlie digital transformation economy and that contribute to advancing its priority areas.
5. The centre of government usually supports the highest level of the executive branch of government.
6. *https://www.oecd.ai/*.