Chapter 6

An ASEM Model of Cooperation in Digital Economy Taxation: Digitalisation and New Technologies

Irma Mosquera Valderrama

November 2021

This chapter should be cited as
Valderrama, Irma Mosquera (2021), 'An ASEM Model of Cooperation in DIgital Economy Taxation: Digitalisation and New Technologies', in Prakash, A. (eds.), *13th Asia-Europe Meeting (ASEM) Summit: Multilateral Cooperation for a Resilient, Sustainable and Rules-Based Future for ASEM*, Jakarta: ERIA, Phnom Penh: ASEM13 and The Royal Government of Cambodia, pp.86-111.

6

An ASEM Model of Cooperation in Digital Economy Taxation

DIGITALISATION AND NEW TECHNOLOGIES

IRMA MOSQUERA VALDERRAMA

Introduction

The overall aim of this chapter is to address the challenges that Asia and Europe face in digital connectivity in the field of taxation and to facilitate the exchange of best practices in the framework of Asia–Europe Meeting (ASEM) connectivity and cooperation. This chapter follows the Chair's Statement at the 2018 ASEM meeting and mainly para. 15 for addressing the need for digital connectivity through trust and confidence in the information and communications technology (ICT) environment. It also follows para. 26, which states the growing benefits from the digital economy and the need to find solutions to address the impact of digitalisation on the international tax system. These objectives are also in line with the 2030 Sustainable Development Agenda, mainly Sustainable Development Goal (SDG) 17.1 on domestic resource mobilisation and SDG 17.16 on global partnerships for sustainable development.

Digitalisation and new technologies provide new opportunities for tax administrations 'to better manage compliance, tackle non-compliance and protect their tax base' (OECD, 2019a:22). Through digitalisation, tax administrations can benefit from new information and communication technologies (e.g. artificial intelligence and data analytics methods) to process personal and business data. These technologies can increase transparency and enhance the fight against tax evasion and tax fraud. This increase in transparency can allow countries to increase domestic resource mobilisation (SDG 17.1).

An Asian Development Bank Institute report on tax and development (Araki and Nakabayashi, 2018:128) stressed the need for the exchange of views and experiences from other tax administrators that share similar challenges and problems. Therefore, the exchange of best practices between countries in a region and amongst regions (Europe and Asia), can contribute to building global partnerships for sustainable development (SDG 17.16).

This chapter is structured as follows. The first section will address digitalisation and the use of new technologies by tax administrations, including the collection of tax information by means of traditional and digital sources. The second section will address the instruments used by tax administrations to safeguard the automatic processing of personal data and protecting taxpayers' rights. The third section will conclude with some final remarks and recommendations for the ASEM Network.

Digitalisation and the Use of New Technologies by Tax Administrations

Digitalisation and the Use of New Technologies

Due to the new ways of collecting tax information (i.e. digital sources), more data are now available to tax authorities, including 'transaction and income data, behavioural data generated from taxpayers' interactions with the tax administration, operational data on ownership, identity and location, and open-source data such as social media and advertising. This data can be used as individual sources or in combination to enable partial or full reporting of taxable income and to uncover under-reporting, evasion or fraud. It can also be used to better understand taxpayer behaviour, to measure the impact of activities and to identify the most effective interventions, both proactive and reactive' (OECD, 2019b:7).

This process of digitalisation is 'transforming the way in which governments can collect, process, and act on information' (Gupta et al., 2017:1) and therefore, governments should formulate and implement new policies to deal with digitalisation and taxation. To analyse the data collected, tax administrations are using new information and communications technologies (e.g. artificial intelligence and data analytics methods) to process personal and business data. These technologies can increase transparency and enhance the fight against tax evasion and tax fraud.[1]

[1] For instance, Microsoft and PwC (2018) give the following examples of the way new information and communications technologies, including advanced analytics, can be used in order to:

- 'set up rules to identify and filter fraudulent transactions;
- search databases of known or suspected fraudsters using data matching algorithms;
- use statistical analysis to detect cases where behavioural patterns differ from the norm;
- identify sophisticated and well-disguised fraudulent behaviour such as neural networks, decision trees, multiple regression, etc.;
- visualise the nature of relationships between individual entities; and
- identify hidden patterns and inconsistencies in unstructured data, such as claim forms or electronic invoices'. (Microsoft and PwC, 2018: 25)

As highlighted by the Asian Development Bank Institute (Araki and Nakabayashi, 2018:13), effective tax administrations in the Asia and Pacific region require the 'extensive use of information technology to gather and process taxpayer information, undertake selective checks based on risk analysis, automatically exchange information between government agencies, and provide timely information to support management decision making and tax policy formulation'. Therefore, international and regional organisations and countries in the ASEM network should be aware of the challenges that tax administrations face in order to facilitate the collection of tax information through traditional and digital sources, as well as the need for tax administrations to enhance their data management strategies and improve their digital infrastructure. These two elements will be addressed below.

Collection of Tax Information: Traditional and Digital Sources

Tax administrations aim to increase transparency and to tackle tax fraud and tax evasion by making use of traditional and digital sources to access taxpayers' information. Some examples are the use of bilateral and multilateral agreements to exchange tax information, facilitating the exchange of transactions data through online platforms, data from digital payments and electronic invoices, and tax data from the mass media, the internet, and third parties, amongst others.

Traditional sources to collect tax information

At the international level, the standard on exchange of information, and since 2013 the standard on automatic exchange of information has facilitated the collection of information by tax administrations. The exchange of information has been widespread around the world, mainly due to countries' participation in the Global Transparency Forum[2] and them signing bilateral agreements (e.g. tax treaties and tax information exchange agreements) and multilateral instruments (e.g. the Multilateral Convention on Mutual Administrative Assistance in Tax Matters and the Multilateral Competent Authority Agreement for the Global Standard on Automatic Exchange of Information).

Two international developments that have also increased the amount of information exchanged are: (i) the introduction by the United States (US) of the Foreign Account Tax Compliance Act (FATCA) to exchange financial account information on US taxpayers[3] and

[2] At the time of writing (7 July 2020), the Global Transparency Forum has 161 members and 19 observers (regional and international organisations). Of the 21 Asian Partner Countries in ASEM, only four countries are not participating in the Forum (i.e. Bangladesh, Brunei Darussalam, the Lao PDR, and Myanmar). All European countries are participating in the Global Transparency Forum.

[3] FATCA is applicable for the reporting by financial institutions (i.e. banks) worldwide to the Internal Revenue Service for foreign accounts held by US taxpayers. FATCA aims to tackle offshore tax evasion and non-compliance by US taxpayers with foreign accounts. See https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca (accessed 7 July 2020).

(ii) the introduction of the Base Erosion Profit Shifting BEPS Project,[4] including three Actions that facilitate the collection and exchange of information amongst countries: Action 5 addressing harmful tax practices and exchange of rulings; Action 12 addressing mandatory disclosure for aggressive tax planning schemes; and Action 13 addressing transfer pricing documentation and country-by-country reporting.[5] The exchange of country-by-country reporting is now possible for countries that have activated the exchange relationship by signing a Multilateral Competent Authority Agreement (MCAA).[6]

At the European level, the most important instrument for facilitating the exchange of information on taxation is the Directive on Administrative Cooperation (2011/16/EU). This Directive has been amended five times to make possible (i) the automatic exchange of financial accounting information (2014/17/EU); (ii) the automatic exchange of tax rulings and advance pricing agreements (2015/2376/EU); (iii) the automatic exchange of country-by-country reports (2016/881/EU); (iv) to ensure that tax authorities have access to beneficial ownership information collected pursuant to the anti-money laundering legislation (2016/2258/EU); and (v) the automatic exchange of reportable cross border arrangements by tax intermediaries(2018/822/EU).

Furthermore, tax administrations are receiving data, for instance, following the exchange of data in joint audits between officials from two (countries) tax administrations[7] or in informal joint meetings to analyse taxpayer data taking place at the location of one tax administration.[8]

[4] The BEPS Project was initiated by the OECD with the political mandate of the G20 with the aim to tackle base erosion and profit shifting by multinationals. The BEPS Project contains 15 Actions, and 4 of those Actions (Actions 5, 6, 13, and 14) are minimum standards. Non-OECD, non-G-20 countries can participate as members of the BEPS Inclusive Framework and commit to the implementation of the BEPS Minimum Standards. At the time of writing, the BEPS Inclusive Framework has 137 tax jurisdictions. From the 21 Asian Partner Countries in ASEM, only five countries are not participating in the Inclusive Framework (i.e. Bangladesh, Cambodia, the Lao PDR, Myanmar, and the Philippines). All European countries are participating in the BEPS Inclusive Framework.

[5] The adoption of these international tax rules and standards addressing the exchange of information and the BEPS Project have been also addressed as a favourable development for developing countries in Asia and the Pacific by Highfield (2017) in an Asian Development Bank Governance Brief.

[6] At the time of writing, from the 21 Asian Partner Countries in ASEM, only seven countries have not signed an MCAA (i.e. Bangladesh, Brunei Darussalam, Cambodia, the Lao PDR, Mongolia, Myanmar, the Philippines, Thailand, and Viet Nam) and European country (i.e. Bulgaria). https://www.oecd.org/tax/beps/country-by-country-exchange-relationships.htm (accessed 7 July 2020).

[7] See OECD (2017), Burgers and Criclivaia (2016), and Čičin-Šain, Ehrke-Rabel, and Englisch (2018).

[8] This is, for instance, the case in the Netherlands, where tax administrations of several countries gather in one room to analyse data collected or received from the Panama Papers, Paradise Papers, or LuxLeaks, amongst others.

New forms of cooperation (e.g. cooperative compliance [OECD, 2013, 2016a] and the International Compliance Assurance Programme ICAP[9]) between tax administrations are being discussed following the rapid digitalisation of the economy and the emergence of new business models.[10]

Digital sources to collect tax information

In addition to the traditional methods of collecting information, tax administrations are making use of digital sources to access taxpayers' information. One example mentioned by the OECD (2019b:5) is the use of multi-side online platforms.[11] Other digital sources mentioned by Microsoft and PwC (2018) are: '(i) digital payments, electronic invoicing and connected devices (e.g. online cash-registers and point-of-sale solutions)'; (ii) 'tax data from mass media, the internet and third-party sources (e.g. banks, chambers of commerce, and stock exchange committees); (iii) digital channel and new business models (e.g. mobile platforms, messaging apps, IoT, social media and bitcoins)'. (Microsoft and PwC 2018:4–5)

At the domestic level, lawmakers or the tax administration can introduce rules to grant access to digital information and ensure that the information from digital sources is shared with the tax administration.[12] At the international level, the information can be exchanged amongst tax administrations provided that there is an instrument to exchange information (e.g. a treaty, tax information exchange agreement, or MCAA). In order to exchange this information, the OECD Forum on Tax Administration has designed a Common Transmission System[13] to facilitate automatic exchange between the tax administrations for financial account information (Common Reporting Standard CRS), country-by-country reporting, and other exchanges.

[9] See OECD International Compliance Assurance Programme (ICAP). https://www.oecd.org/tax/forum-on-tax-administration/international-compliance-assurance-programme.htm (accessed 7 July 2020).

[10] These new forms of cooperation were addressed at the OECD Tax Certainty Day, held on 16 September 2019. Programme available at https://www.oecd.org/tax/forum-on-tax-administration/events/Tax-certainty-Day-2019-Agenda.pdf (accessed 7 July 2020).

[11] These platforms 'often facilitate transactions between individual sellers of goods and services to individual consumers, which occur outside the traditional business structures (e.g. in the case of marketplaces)' (OECD, 2019b).

[12] One example is the United Kingdom's initiative Making Tax Digital for VAT and Income Tax, introduced in the Finance (No. 2) Act of 2017. https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital (accessed 7 July 2020).

[13] This system was agreed on by the 44 heads of tax administration members of the OECD Forum on Tax Administration in Beijing, 13 May 2016. As stated in the Communique: 'The cornerstone of the CTS is data security, with leading industry standards of encryption applied to each transmission' (OECD, 2016b).

However, when the information is outside the limits of the jurisdiction (e.g. information held by a third party in online platforms) or there are no rules to facilitate access to such information (e.g. Facebook, Instagram, and Twitter),[14] access by the tax administration to these digital sources of information becomes difficult.[15]

To address some of these problems, the OECD (2019), in a document addressing tax and digitalisation, stated the need for unilateral and multilateral initiatives to obtain tax data on transactions facilitated through online platforms. At the national level, the OECD suggests introducing 'legislative measures which require platforms or other third parties to report payment and identification data of users and/or which allow information requests on group information, could provide tax administrations with information needed to improve compliance or to enhance selection of cases for audit' (OECD, 2019b:6).

In cases where the data are located in a jurisdiction other than the jurisdiction of the platform seller, the OECD suggests exploring the possibility of a multilateral agreement to facilitate access and exchange to such information along the lines of the Common Reporting Standard for the automatic exchange of financial accounting information. Such an agreement 'might require all platforms carrying out particular types of activity to provide information in a standardised format on platform users, transactions and income to the tax authority in their jurisdiction of residence for exchange, through appropriate legal gateways, to the jurisdiction of tax residency of the user' (OECD, 2019b:6).

Challenges for Tax Administration

International level

The 2019 OECD Tax Administration report stated that 'tax administrations much like tax policymakers, are exposed to rapid change through the digitalisation of the economy and the emergence of new business models and ways of working. At the same time, the availability of new technologies, new data sources, analytical tools and increasing international co-operation and exchange of information are also providing new opportunities for tax administrations to better manage compliance, tackle non-compliance and protect their tax base' (OECD, 2019a:22).

[14] In the past, the mining of social media by the IRS has been addressed by scholars. See Houser and Sanders (2017). In December 2018, the IRS National Office of Procurement made a request to Facebook, Instagram, and Twitter to access their social media to identify tax cheaters. https://qz.com/1507962/the-irs-wants-to-use-facebook-and-instagram-to-catch-tax-evaders/ (accessed 7 July 2020).

[15] In Asia, one exception is Singapore, since the tax administration (Inland Revenue Authority) uses social network analysis to identify risks and to select cases for audit. See OECD (2017:75–76). In Europe, two exceptions are France and the Netherlands, which have introduced rules that give the power to tax authorities to gather taxpayer data through artificial intelligence tools that operate in an automated manner: in France, article (art.) 154 2020 Budget Bill and in the Netherlands arts. 7:4 and 8:42 of the General Administrative Law. However, these have been disputed in courts: see in France, the Constitutional Council ruling of 27 December 2019 Decision No. 2019-796 DC, and in the Netherlands, Supreme Court decision of 4 May 2018 (BNB 2018/164) and of 17 August 2018 (BNB 2018/182). See Offermans (2020) and Calderon and Ribeiro (2020).

The 2018 Summit of the Regional Network of Tax Administrations (the Inter-American Centre of Tax Administrations [‘CIAT’] and the Intra-European Organization of Tax Administrations [‘IOTA’]) has also addressed some of the challenges faced by tax administrations, mainly the need to enhance tax transparency in the digital era, the need to use new technologies to enhance tax compliance and tax collection, and the need to exchange best practices.

Examples of best practices are (i) the use digital tools to simplify the exchange of information and the use of new analytical methods, such as statistical analysis to identify tax risks (for instance in country-by-country reporting in Germany); (ii) the development of several changes to data transmission (e.g. Switzerland referring to the use of XML uploads on the Federal Tax Administration [FTA] Portal Suisse Tax) online and via web services (M2M Communication); and (iii) the use of technology to improve tax control (e.g. the development of big data tools in Spain).[16] More recently, in October 2019, the experience of countries in the use of new digital technologies and big data (Chile and Mexico) and artificial intelligence (Canada) were presented at the CIAT Technical Conference.[17]

The exchange of best practices at the 2018 Summit was facilitated by CIAT and IOTA between countries in the North American, Central America, South America, Asian and European regions. From the 21 Asian Partner countries in ASEM, only India and Russia presented some best practices (i.e. India on the use of an internal system to collect financial information, and Russia on cash register reforms using data analytics) (CIAT and IOTA, 2018). At the 2019 CIAT Technical Conference, from the 21 Asian Partner countries in ASEM, only India presented, mainly addressing the use of data analysis and business intelligence to target the lack of reporting in the informal economy.[18]

Therefore, it is recommended for countries in Asia to also participate actively in these types of meetings or to organise their own meetings in Asia. For instance, in the Belt and Road Initiative Tax Administration Cooperation Forum (BRITACOF) conference scheduled for May 2020 (postponed to May 2021[19]) in Kazakhstan, in the framework of the Belt and Road Initiative Tax Administration Cooperation Mechanism (BRITACOM),[20] one of the topics to be addressed is the digitalisation of tax administrations.

[16] Some of the challenges have been addressed by the CIAT–IOTA Tax Summit (CIAT and IOTA, 2018).

[17] Section 3.2, presentation on 10 October 2019, available at https://www.ciat.org/ciat-2019-technical-conference/?lang=en (accessed 7 July 2020).

[18] Presentation on 8 October 2019, available at https://www.ciat.org/ciat-2019-technical-conference/?lang=en.

[19] This conference has been postponed due to COVID-19. http://www.chinatax.gov.cn/eng/n4260854/c5149476/content.html (accessed 7 July 2020).

[20] China launched BRITACOM in order to deal with some of these challenges and also to address the implementation of the Belt and Road Initiative. BRITACOM has 34 member countries and 11 countries as observers from different regions (e.g. Asia, Africa, Europe), plus one non-profit (academic) organisation. http://www.chinatax.gov.cn/eng/n4260869/c5112279/content.html (accessed 7 July 2020).
On the role of BRITACOM, see Sampson, Wang, and Mosquera Valderrama (forthcoming).

For this purpose, the International Chamber of Commerce (ICC, 2020) drafted a report to provide a business perspective on the digitalisation of tax administrations. The report introduces some principles for digitalisation to ensure that digital systems are designed and operated in a way that considers the need for balance between the legitimate interests of governments and businesses (ICC, 2020:2–3). In addition, the report addresses the prerequisites for a successful digital transformation from a business perspective (i.e. data security, system requirements, data availability, the reasonable use of data, transparency, taxpayers' identity, and consistency) (ICC, 2020: 5–7).

Another framework that can be used is that of the Annual Meeting of the Study Group on Asian Tax Administration and Research (SGATAR).[21] For instance, the 49th SGATAR (2019) Annual Meeting addressed the challenges of digitalisation for tax administrations in Asian countries.[22] One of the recommendations of the meeting was for tax administrations to enhance their modernisation, 'including cultural and change management, managing and handling big data, focusing on identity management, working with partners to provide software to taxpayers, preparing for workforce transformation which is in line with the technology development' (SGATAR, 2019).

European level

At the European level, in September 2018, the countries of the European Union (EU) created the Tax Administration European Union Summit (TADEUS). TADEUS is the yearly summit by the heads of tax the administrations of the EU countries and the EU Commission Directorate General Taxation and Customs Union (DG TAXUD) to address the common challenges of digitalisation and globalisation. The aim is to enhance cooperation in several areas, including addressing the digital economy and the digitalisation of tax authorities and managing IT systems and resources (Statement TADEUS Plenary Meeting 17–18 September 2019). For this purpose, several projects have been initiated. For instance, regarding new technologies, one project is the digital and data project led by Finland on reporting requirements for the sharing and gig economy (Statement TADEUS Plenary Meeting 17–18 September 2019:2,3).

In the 17–18 September 2019 meeting, the heads of the tax administrations acknowledged the legislative changes and the level of administrative cooperation that will require new IT developments and investment in trans-European electronic systems.

[21] SGATAR is an organisation of tax administrations in the Asia–Pacific region founded in 1970. The current members include Australia, China, Hong Kong, Indonesia, Japan, the Republic of Korea, Macao, Malaysia, Mongolia, New Zealand, Papua New Guinea, the Philippines, Singapore, Taiwan, Thailand, and Viet Nam (http://sgatar.org/category/focus/).

[22] In addition to member countries, international organisations (e.g. the OECD, World Bank, and the IMF), and regional tax administration networks (e.g. CIAT) also participated in the annual meeting.

Therefore, one of the outcomes of the meetings was the need to align the development of the EU common or interoperable information technology systems and to set up 'a coordination process based on consensus, in the form of a multi-annual plan, under the coordination of TADEUS'. (Statement TADEUS Plenary Meeting 17–18 September 2019:3).

Finally, countries are also seeking other ways to cooperate. One example is Belgium, the Netherlands, and Luxembourg (BENELUX), which decided in 2001 to introduce a new system, Transaction Network Analysis, to tackle value-added tax fraud automatically in the Benelux area.[23] This Transaction Network Analysis has been recently adopted by the EU Commission as the new system to tackle VAT fraud in the EU. (Press release 15 May 2019)

More recently, and in order to tackle tax evasion and tax fraud BENELUX countries signed a new agreement (memorandum of understanding MOU) on 10 October 2019[24] that facilitates the automatic exchange of information between countries including not only traditional but also digital sources and digital projects such as FIC.net[25] (MOU Benelux, 10 October 2019:3).

In this process of digitalisation, tax administrations need to have data management strategies and proper digital infrastructure. These two elements will be explained below.

Data Management Strategies and Digital Infrastructure

Data management strategies

The data management strategy should be a long-term strategy that focuses not only on descriptive analytics (for diagnostics) but also on predictive and prescriptive analytics (Microsoft and PwC, 2018). Predictive analytics 'provide information on likely future outcomes or resource maintenance schedules' whereas prescriptive analytics 'calculate expected outcomes and help recommend the best course of action for decisions such as changing a tax regulation. This form of insight often includes the use of artificial intelligence (e.g. cognitive, context aware) and augmented analytics and optimisation (e.g. pervasive, automation)'. (Microsoft and PwC, 2018:9)

Regarding artificial intelligence, the Canadian Revenue Authority shared its experience in a 2019 presentation made in the framework of the CIAT Technical Conference.

[23] This analysis will use 'data mining software with which smart algorithms can quickly uncover suspicious transactions that indicate a VAT carousel' (Vat Update, 2019).

[24] https://www.benelux.int/files/6015/8098/4521/MoU_fraude_fiscale_10.10.2019-NL.pdf (accessed 7 July 2020).

[25] FCInet is a non-commercial (government developed) decentralised computer system that enables FCISs (Financial and/or Criminal Investigation Services) from different jurisdictions to work together while respecting each other's local autonomy. https://www.fcinet.org/index.php/what-is-fcinet/ (accessed 7 July 2020).

For the Canadian Revenue Authority, artificial intelligence results in (i) advanced insights from big data for network analysis, association analysis, and clustering analysis; (ii) prediction systems including tree-based algorithms, neural networks, and regression algorithms; (iii) anomaly detection including outlier detection algorithms, and (iv) natural language understanding for text-voice understanding and the mining of unstructured data.[26]

The Canadian Revenue Agency addressed some of the ways that artificial intelligence has been used by them: chatbots to improve service, neural networks to generate risk scores for small and medium-sized enterprises, predictive systems to detect offshore non-compliance, predictive models to optimise debt resolution, unsupervised clustering to measure the potential of corporate income tax non-compliance, and data engineering to achieve 360-degree views of taxpayers (network analysis).

In light of the above, it can be argued that access to digital sources and the use of new technologies including a data management strategy can provide tools for tax administration to increase transparency and fight tax evasion and tax fraud by detecting risks, predicting behaviours, and carrying out intelligent audits. However, one of the challenges for countries to benefit from these data management strategies is to introduce changes to the infrastructure of the tax administration as explained below.

Infrastructure

Tax digitalisation requires changes to the infrastructure, which can be difficult to achieve by countries with limited (personnel or budget) resources, mainly developing countries (Debelva and Mosquera Valderrama, 2017). Developing countries may have a large informal untaxed sector and, therefore, it becomes difficult to obtain (and/or update) information from individuals and/or businesses.[27]

One positive remark, as mentioned by Krishna, Fleming, and Assefa (2017) is that in this new era of technology, developing countries can build their digital infrastructure from scratch and are not constrained by 'older 'legacy' systems in the developed world.

[26] Presentation available at Section 3.2. https://www.ciat.org/ciat-2019-technical-conference/?lang=en (accessed 7 July 2020).

[27] As stated by Kanbur (2017): 'Clearly, the most obvious entry point is the potential of the digital revolution to reduce information costs in targeting. Biometrics and identification of individuals is often put forward as the solution to the information problem in targeting. However, what fine targeting needs is not just unique identification of individuals, but detailed information allowing computation of income or consumption and, thus, identification as poor. Further, this computation needs to be updated annually if the program is to continue to be finely targeted. In small, developed, and highly formalized economies, such as Finland's, such income information is already digitized and linked in to other national databases, and the use of such information is not a problem. But in a developing country with a large informal untaxed sector it is not clear how exactly digitalization can help, at least not for many years to come. And it does not seem that informality is declining sharply or at all in many developing countries'.

Therefore, they can 'choose to build out a modern infrastructure, underpinned by blockchain and cognitive computing, rather than retrofit equipment that may be several decades old' (Krishna, Fleming, and Assefa, 2017:182).

Furthermore, some tax administrations, even though having resources, may be cautious to advance digitalisation 'given the potential costs of mistakes. Foremost amongst these is the risk to revenue, damage to reputation, and potential reduction of tax morale. The digitalisation of tax administration is technically complex given the volume of activity the system will have to accommodate and the importance of security and absence of errors. The required quality standards will be achieved only through extensive technical and functional testing. Any system inadequately tested will quickly fall into disrepute, with potentially significant financial and reputational costs' (Chen, Grimshaw, and Myles, 2017:114).

To sum up, data are collected from traditional and digital sources, and this data can be used by tax administrations to increase transparency and to tackle tax evasion and tax fraud. However, countries should introduce new instruments (domestic rules and international agreements) for providing access to digital sources and the exchange of digital data. Access to tax data and the use of big data[28] can help to optimise risk detection and to carry out intelligent audits with the use of data analytics. In order to achieve these objectives, tax administrations should have a long-term strategy for the analysis of the data and to make use of diagnostic, predictive, and prescriptive analytics. The following section will address instruments to safeguard taxpayers' rights in this new era of digitalisation.

Instruments to Safeguard the Automatic Processing of Personal Data and Protect Taxpayers' Rights

Collection of Personal and Business Data

In general, data collected include personal data (i.e. information relating to an identified or identifiable individual including genetic data and biometric data[29]) and business data (i.e. information related to the operation of a business, including trade secrets[30]). These data can be regarded as taxpayer data, and therefore, protected under the rules of secrecy and confidentiality available in the constitution and/or tax laws of a country.[31]

[28] The term big data 'usually identifies extremely large data sets that may be analysed computationally to extract inferences about data, patterns, trends and correlations' (Mantelero, 2017).

[29] Example of biometric data are fingerprints, iris scans, and DNA. These data are protected as a special category of personal data in art. 9 General Data Protection Regulation (GDPR) Art. 9 states that 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited'.

[30] On trade secrets, see D'souza (2019).

[31] See Mosquera Valderrama et al. (2017). See also Debelva and Mosquera Valderrama (2017).

In this new digital tax administration era,[32] countries should guarantee the rule of law in the processing of personal and business data. Hence, the following questions should be addressed by tax administrations collecting and processing data: (i) Who has the taxpayers' data? (ii) Are the taxpayers' data properly collected, stored, and monitored? (iii) Is the processing of the taxpayers' data allowed? (iv) Who owns the taxpayers' data? (Mosquera Valderrama, 2019).

As rightly mentioned in the Asian Development Bank Institute's report on tax administrations, in order to enhance voluntary compliance, 'revenue bodies must be seen to operate in a manner that instills a high level of mutual trust, respect and confidence amongst its taxpayer population. This can only be achieved where there are recognition and acceptance of a basic set of taxpayer's rights and obligations' (ADB, 2018:26). Therefore, countries should also take into account instruments to safeguard taxpayers' rights in the collection, exchange, and processing of information by tax administrations.

To enhance voluntary tax compliance, taxpayers need to know that tax is being paid by all, including wealthy tax individuals and multinationals, and that the data collected are being used for legitimate (tax purposes) and in accordance with the rule of law. Therefore, the increase in transparency and the use of new technologies need to take into account (i) safeguards for the automatic processing of data, including big data (Van Hout, 2019), and (ii) taxpayers' rights, including the right to confidentiality, secrecy, and privacy. Some of these safeguards for the protection of data in the automatic processing of data have already been addressed.[33]

Taxpayers' Rights in Asia

Taxpayers' rights in Asia (e.g. the right to privacy, confidentiality, and secrecy) have been addressed in a very succinct way by international and regional organisations. These rights have been left to the rules of the country, which may decide to introduce or not introduce privacy laws or specific taxpayer rights either in the law or in administrative regulations.

[32] Another element in this digital tax administration era is the incorporation of digital technology in the interaction between tax administration and taxpayers e.g. pre-populated tax returns, e-filing, and e-services, etc. See Microsoft and PwC (2018).

[33] According to Debelva and Mosquera Valderrama (2017), the following safeguards should be introduced for the exchange of information, including the automatic exchange of information: (1) similar data can be received from the receiving state reciprocity, (2) the receiving state ensures the adequate protection of confidentiality and data privacy that is guaranteed by a follow up by the supplying state to guarantee the respect of such confidentiality in the receiving state, (3) the exchange is adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed, (4) the sending of data does not constitute an excessive burden for the tax administration that lacks the administrative capacity or technical knowledge to develop a secure electronic system to exchange data, and (5) the principle of accuracy, stipulating that the data controller has the duty to carry out regular checks of the quality of personal data (Debelva and Mosquera Valderrama, 2017).

Some examples that can illustrate this are the Asian Development Bank Institute reports (ADB, 2018 and ADB, 2020), which present a comparative study of the tax administrations in Asia and the Pacific. These reports do not specify the challenges faced by countries in protecting taxpayers' rights for the use of digital technologies and the automatic processing of personal data. Instead, reference is made to documents by the OECD and other international organisations. As far as we are aware, a comparative study on taxpayers' rights in Asia on the exchange of information and digitalisation has not yet been made.[34]

In the 2018 report, reference is made to the 2003 OECD document on Taxpayer Rights and Obligations (OECD, 2003). In addition, the 2018 report, mainly based on international organisation surveys (International Monetary Fund IMF, 2007; OECD, 2017), provides a short comparison of the use of legislative or administrative rules introducing taxpayers' rights (ADB, 2018:38–39). According to this comparison, from the 28 Asia and Pacific countries analysed in 2018, only five countries did not have rights set out in laws or statutes or developed by a revenue body (i.e. Hong Kong, Japan, Papua New Guinea, Myanmar, and Singapore) (ADB, 2018:39).

The 2020 report does not address the challenges mentioned above, nor does the report provide an updated overview of the 28 Asia and Pacific countries mentioned above. The 2020 report refers to common elements in taxpayer charters available in Asia and Pacific countries (based on the report author's own compilation [Highfield and Chooi]) (ADB, 2020:105).[35] The 2020 report also refers to the collaborative project of Tax Consultants in Asia, Europe[36] and the Society of Trust and Estate Practitioners to develop a Model Taxpayer Charter (Cadesky, Hayes, and Russell, 2015). Finally, the 2020 report focuses on access to rulings and dispute rights in Asia and the Pacific (ADB, 2020:103).

[34] However, some Asian countries, e.g. China, India, the Republic of Korea, and Taiwan, have been addressed in the IBFD Observatory on the Protection of Taxpayers' rights. This observatory monitors developments concerning the effective protection of taxpayers' fundamental rights. Information observatory available at https://www.ibfd.org/Academic/Observatory-Protection-Taxpayers-Rights (accessed 7 July 2020).

[35] The elements of charters mentioned are statement of intent, statement of mutual obligations, taxpayers' rights, taxpayers' obligations, and details of rights and obligations. These elements do not consider taxpayers' rights in digitalisation.

[36] In Europe, Confédération Fiscale Européenne (CFE); in Asia, Asia Oceania Tax Consultants' Association (AOTCA). Text Charter available at http://www.taxpayercharter.com/index.asp (accessed 7 July 2020).

Instruments for Data Protection and Privacy

At the international level, taxpayers' data may be protected by the 1981 (and its Protocol 2001 and 2018) Council of Europe Convention on the Automatic Processing of Personal Data, open for ratification to member countries of the Council of Europe and third countries (outside the Council) that can be made applicable for taxation.[37] Some countries have also signed bilateral agreements (e.g. the EU–US Privacy Shield[38]).

At the regional level, two EU instruments should be mentioned: the 2016 Directive (EU, 2016a) and the Regulation on Data Protection (in force since May 2018) (EU, 2016b). The 2016 Directive replaced the 1995 Data Protection Directive. Other regional agreements are (i) the 2005 Asia–Pacific Economic Cooperation (APEC) Framework, which introduced information privacy principles[39] and (ii) the 2010 Supplementary Act on Personal Data Protection within the Economic Community of West African States (ECOWAS).[40]

From the above-mentioned instruments, research carried out by Greenleaf shows that the 1995 Data Protection Directive has been used extensively by countries outside Europe, including by countries in Asia and the Pacific.[41] According to Greenleaf, the APEC framework has not been extensively used even though it was presented as an alternative to EU standards by non-EU countries, such as the United States, Australia, Canada and Mexico (Greenleaf, 2012:75). Some of the reasons argued by Greenleaf are, for instance, 'almost no evidence of adoption of its principles in legislation in the region; little increase in self-regulatory initiatives (there are privacy seals in Mexico, Viet Nam, and Japan, but they are of questionable value)' (Greenleaf, 2012:75) amongst others.

[37] On the history of the convention, see Greenleaf (2014a).

[38] The EU–US Privacy Shield decision was adopted on 12 July 2016 (European Commission 2016) and the Privacy Shield framework became operational on 1 August 2016. This framework protects the fundamental rights of anyone in the EU whose personal data are transferred to the United States for commercial purposes. Information is available at the website of the EU Commission. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (accessed 7 July 2020).

[39] This framework also provides for 'information privacy principles being (1) preventing harm, (2) providing notice, (3) collection limitations, (4) use of personal information,(5) mechanisms to exercise choice, (6) integrity of personal information, (7) security safeguards, (8) access and correction, (9) accountability' (Debelva and Mosquera Valderrama (2017:369). The content of the APEC Privacy Framework is available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (accessed 7 July 2020).

[40] See ECOWAS website: https://ccdcoe.org/organisations/ecowas/ (accessed 7 July 2020). Text of the agreement is available at http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf (accessed 7 July 2020).

[41] Some examples are Macau, the Republic of Korea, Taiwan, Malaysia, Hong Kong, Australia, New Zealand, India, Japan, and Viet Nam. See Greenleaf (2012). See also Greenleaf (2014b:624) for an analysis of 26 data privacy laws in Asia.

Since the 2016 Directive and Regulation are new, further research should be carried out on how their provisions can also be used to enhance data protection and to safeguard the right to privacy. Previously, Mosquera Valderrama et al. (2017) argued in a comparative study that 'in respect of the new EU Data Protection Directive the specific definitions of personal data, genetic data and biometric data (art. 3) and the protection of the processing of these data as special categories of personal (sensitive) data (art. 10) may represent an enhancement since the 1995 Directive'.

Regarding the Council of Europe Convention, the influence outside member countries is still limited since at the time of writing, only eight non-member countries had ratified the convention. Since this is the only multilateral binding convention that can have a worldwide application,[42] in our view, more work should be carried out by the Council of Europe in promoting the adoption of the convention by non-member countries.[43] One drawback of the convention is that it is only applicable for personal data. Therefore, it is recommended that the Council of Europe extend the protection of this convention to business data, including trade secrets. The main elements of the convention are presented below.

Council of Europe Convention on the Automatic Processing of Personal Data

In 1981, the Council of Europe adopted Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This convention protects the individual against abuse that may accompany the collection and processing of personal data and at the same time regulates the cross-border flow of personal data (Mosquera Valderrama, 2019). This convention has been amended by two protocols.[44]

The first protocol was approved in 2001 and extended the convention for approval by non-member countries (countries outside the Council of Europe). The convention has been ratified by the 47 members of the Council of Europe and 8 non-member countries, i.e. Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay.

The second protocol was approved in May 2018 and was opened for signature as of 25 June 2018.[45] The protocol pursued two main objectives: to deal with the challenges resulting from the use of new information and communication technologies, and to strengthen

[42] The use of the convention at a global level has been addressed by Greenleaf (2012:68–92).

[43] A reason for countries not participating in the convention has been mentioned by Greenleaf (2012), who referred to the lack of transparency on accession to the convention.

[44] Some of the elements analysed in this section have been previously addressed by Mosquera Valderrama, Affuso, and Coco (2019).

[45] Details of Treaty No. 223, 10 October 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 (accessed 7 July 2020).

the convention's effective implementation. This protocol has been signed by 38 of the 47 members of the Council of Europe and by 3 of 8 non-member countries (Argentina, Tunisia, and Uruguay) for a total of 41 countries.

From the Asian Partner Countries in ASEM, only Russia has signed and ratified Convention 108 and signed the 2018 Protocol (pending ratification). Some ASEM countries have an observer status to Convention 108 (New Zealand, Australia, Indonesia, the Philippines, Japan, and the Republic of Korea).

European countries have signed and ratified Convention 108. As of July 2020, the 2018 Protocol has been signed by almost all EU countries (except Denmark) and it has been ratified by four countries (Bulgaria, Croatia, Poland, and Lithuania).[46]

The convention

The convention is applicable to automated personal data files and the automatic processing of personal data in the public and private sectors (art. 3).[47] Four articles of the convention that can be relevant for the tax administrations in this digital administration era are art. 5, 6, 7 and 8. Art. 5 addresses the quality of data stating that 'personal data undergoing automatic processing shall be obtained and processed fairly and lawfully, stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored'.[48]

Furthermore, art. 6 addresses protection for special categories of data, stating that 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions'.[49]

[46] Chart of Signatures and Ratifications of Treaty 223 as of 6 July 2020. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (accessed 7 July 2020).

[47] According to art. 2, 'personal data' means any information relating to an identified or identifiable individual ('data subject'); 'automated data file' means any set of data undergoing automatic processing; 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval, or dissemination; and 'controller of the file' means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored, and which operations should be applied to them (https://rm.coe.int/1680078b37, accessed 7 July 2020).

[48] Convention art. 5.

[49] Convention art. 6.

Article 7 introduces the data security requirement, stating that 'appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination'.[50]

Article 8 provides additional safeguards for the identified or identifiable natural person (data subject). Accordingly, 'any person shall be enabled:

- to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
- to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
- to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
- to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with'.[51]

2017 Guidelines and the 2018 Protocol

The convention has been in place since 1981 (more than 30 years). Therefore, the Council of Europe decided in 2012 to modernise the convention 'to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data' (Council of Europe, 2018a).

For this purpose, the Council of Europe commissioned a study for new guidelines (Council of Europe, 2017) on the protection of individuals with regard to the processing of personal data in a world of big data. These guidelines (published in 2017) were discussed in the consultative committee of the convention for the Protection of Individuals with regard to Automatic Process of Personal Data.[52] More recently, new guidelines have been published in 2019 on artificial intelligence (AI) and data protection (Council of Europe, 2019).

[50] Convention art. 7.

[51] Convention art. 8.

[52] These guidelines were not accepted by all Council of Europe members. Out of the 50 voting members consulted by written procedure, Denmark, Liechtenstein, and Luxembourg abstained and Germany and Ireland objected.

These guidelines have not yet been used in the Council of Europe Convention and are therefore outside the scope of this analysis.[53]

The 2017 guidelines on the protection of individuals for the processing of personal data are applicable to big data and big data analytics. In this context the guidelines state that 'in terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract new and predictive knowledge for decision-making purposes regarding individuals and groups' (Council of Europe, 2017:2). Therefore, the guidelines introduce a precautionary approach in regulating data protection and introducing risk assessment considering the legal, social, and ethical impacts of the use of big data. In addition, controllers should adopt preventive policies to ensure the protection of persons with regard to the processing of personal data, and introduce appropriate measures to identify and mitigate the risks of data processing by introducing measures such as 'by design' and 'by-default' solutions.[54]

Following to some extent the 2017 Guidelines,[55] the Protocol of 2018 provides for more transparency and protection in data processing and introduces stronger accountability for data controllers and the obligation to declare data breaches. However, one important distinction is that unlike the 2017 Guidelines, no specific reference was made to big data in the 2018 Protocol.[56]

The 2018 Protocol also introduces the legitimacy of data processing (art. 5 of the convention), stating that such 'processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake'.[57]

[53] According to the Preliminary Introduction, these guidelines provide a set of baseline measures that governments, AI developers, manufacturers, and service providers should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection.

[54] 'By design' refers to appropriate technical and organisational measures taken into account throughout the entire process of data management, from the earliest design stages to implementing legal principles in an effective manner and building data protection safeguards into products and services. According to the 'by default' approach to data protection, the measures that safeguard the rights to data protection are the default setting, and they notably ensure that only personal information necessary for a given processing is processed' (Council of Europe, 2017: 2).

[55] For instance, regarding 'by design' and 'by default' solutions for mitigating risks in the processing of personal data, see Para. 2.5.(2) of Council of Europe (2017) and art. 10 of the 2018 Protocol and para. 89 of the Explanatory Statement (Council of Europe, 2018b).

[56] For instance, in a word search for 'big data' in the 2017 Guidelines, 'big data' is mentioned 33 times, whereas in the 2018 Protocol there are no matches. Clearly, the guidelines wanted to give specific provisions to regulate big data and to address the impact of big data processing and its broader ethical and social implications for safeguarding human rights and fundamental freedoms.

[57] See art. 7 of the 2018 Protocol.

Furthermore, art. 6 states that the safeguards for the processing of data should include genetic data, personal data (including sensitive data), and biometric data. The controller also has the requirement to notify data breaches.

Even though big data is not specifically mentioned in the text of the Protocol, it introduces new rights for persons in an algorithmic decision-making context. These rights are particularly relevant in connection with the development of data analytics and artificial intelligence. Accordingly, art. 9 (1[a] and [c]) of the 2018 Protocol, respectively, state that the data subjects have the right (i) 'not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration' and (ii) 'to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her'.[58]

In addition, the 2018 Protocol includes the obligation of the controller and data processors to introduce privacy by design principle and privacy by default (art. 10, 2018 Protocol). For privacy by design (art. 10[1]), these obligations include: '(i) the implementation by controllers/processors of technical and organizational measures, which take into account the implications of the right to the protection of personal data at all stages of the data processing; (ii) the examination, prior to the commencing of such processing, of the likely impact of intended data processing on data subjects' rights and fundamental freedoms; and (iii) the design of the data processing in such a way that it prevents (or minimises) the risks of interference with those rights and fundamental freedoms. These changes aim to make data controllers/processors aware of the data protection risks of processing big data, and to take them into account when designing their data processing systems' (Mosquera Valderrama, 2019).

For privacy by default, the 2018 Protocol states that controllers and processors should implement technical and organisational measures that take into account the implications of the right to the protection of personal data at all stages of the data processing process (art. 10[3]). The explanatory statement to the Protocol further elaborates on this privacy by default principle: 'When setting up the technical requirements for default settings, controllers and processors should choose privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), notably to avoid processing more data than necessary to achieve the legitimate purpose. For example, social networks should be configured by default so as to share posts or pictures only with restricted and chosen circles and not with the whole internet'.[59]

[58] See also para. 75 and 77 of the Explanatory Statement (Council of Europe, 2018b).

[59] See para. 89 of the Explanatory Statement (Council of Europe, 2018a).

EU General Data Protection Directive and Regulation

The EU Data Protection Directive (EU) 2016/680 and Regulation (EU) 2016/679 (in force since 25 May 2018) apply to the processing of personal data wholly or partially by automated means as well as for non-automatic processing.[60] The 2016 Directive and Regulation do not specifically refer to big data. However, in a document from the European Commission on data protection and big data,[61] the EU Commission stated that 'Big Data analytics does not always involve personal data. But, when it does, it should comply with the rules and principles of data protection: the EU's Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet. Big Data is no different' (European Commission, 2018).

Like the 2018 Protocol to the Council of Europe Convention, the regulation introduces the obligation of data controllers to introduce 'privacy by design', or 'by default' mechanisms. The regulation states that 'the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations'.[62]

Regarding the processing of personal data, the regulation also states that 'the processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing'. These public authorities include tax and customs authorities (para. 31 of the regulation [EU, 2016b]).

[60] See EU data protection rules website. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en#documents (accessed 7 July 2020).

[61] See European Commission (2018). A definition of big data is also given, stating that 'the term 'Big Data' refers to large amounts of different types of data produced from various types of sources, such as people, machines or sensors. This data could be climate information, satellite imagery, digital pictures and videos, transition records or GPS signals. Big Data may involve personal data: that is, any information relating to an individual, and can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address'.

[62] See para. 78 of the regulation (EU, 2016b). See also para. 63 of the Directive (EU, 2016a).

Automated decision making is also protected in the regulation. Para. 71 states that a decision (and profiling) that affects a data subject cannot be taken only based on automated processing unless that decision making is 'expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent'.[63] However, this decision making should be subject to 'suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision'.[64]

Final Remarks and Recommendations

This chapter has addressed the challenges faced by Asia and Europe regarding the use of new technologies by tax administrations and the protection of taxpayers' rights. To facilitate the exchange of best practices in the framework of ASEM connectivity and cooperation, this chapter has addressed developments in Europe and Asia and the Pacific, including also the work carried out by international organisations (the Asian Development Bank and the OECD) and regional tax administration networks (CIAT, IOTA, BRITACOM, and SGATAR).

The first recommendation is for countries in the ASEM network to be aware of the challenges that tax administrations face in the collection of tax information (traditional and digital sources) and invest in their data management strategies. These strategies should be (i) long term strategies and (ii) take into account the use of diagnostic, predictive, and prescriptive analytics. Furthermore, countries should also invest in improving their digital infrastructure, which includes the introduction of common transmission systems and software for the analysis of big data.

For this purpose, it is important to organise regional meetings for tax administrations to present their tax digitalisation challenges and to exchange best practices. These meetings could be similar to TADEUS (an EU yearly summit of the heads of tax administrations) but with countries participating in the ASEM network. Furthermore, since there are 27 countries participating as Asian Partner countries in ASEM, some countries may conclude memorandums of understanding to enhance cooperation to tackle tax evasion and tax fraud based on the needs of the countries (as has been done in the BENELUX initiatives).

[63] See para. 71 of the regulation (EU, 2016b).

[64] See para. 71 of the regulation (EU, 2016b).

The second recommendation addresses the instruments to safeguard the protection of taxpayers' rights. Countries in the Asia and Pacific region have introduced rules to protect personal data and the right to privacy, mainly following the 1995 EU Data Protection Directive. However, this directive has been updated to include, amongst others, the use of personal data, genetic data, and biometric data. Therefore, we recommend to countries to introduce changes to the data protection laws following the EU 2016 Directive on Data Protection and the Regulation. As has been done in the Council of Europe Convention (2018 Protocol), it is also recommended that countries include references to big data or data analytics, including the rights of persons (data subjects), in an algorithmic decision-making context.

Finally, regarding the automatic processing of personal data, we argue that the Council of Europe Convention and its 2018 Protocol is an instrument that countries need to ratify. Therefore, further research should be carried out on the application of the convention for the collection and exchange of taxpayers' information.

The ASEM cooperation in digital connectivity is well placed to take these recommendations forward. When Asia and Europe are moving towards a digital economy – albeit at a different pace – an early convergence and cooperation programme for capacities and digitalisation should be a highlight of the Leaders statement of the 13th ASEM Summit (ASEM13) in Cambodia in 2021.

Note: The author acknowledges the Lead Research GLOBTAXGOV Project European Research Council funded project (Grant Agreement 758671).

REFERENCES

Araki, S. and S. Nakabayashi (eds.) (2018), *Tax and Development: Challenges in Asia and the Pacific*. Tokyo: Asian Development Bank Institute. https://www.adb.org/publications/tax-and-development-challenges-in-asia-pacific (accessed 7 July 2020).

Asian Development Bank (ADB) (2018), *A Comparative Analysis of Tax Administration in Asia and the Pacific: 2018 Edition*. Manila: ADB. https://www.adb.org/sites/default/files/publication/441166/tax-administration-asia-pacific-2018.pdf (accessed 7 July 2020).

ADB (2020), *A Comparative Analysis of Tax Administration in Asia and the Pacific: 2020 Edition*. Manila: ADB. https://www.adb.org/publications/comparative-analysis-tax-administration-asia-pacific-2020 (accessed 7 July 2020).

Benelux (2019), *Benelux-landen versterken hun samenwerking in de strijd tegen fiscale fraude*. 10 October. https://www.benelux.int/nl/nieuws/benelux-landen-versterken-hun-samenwerking-de-strijd-tegen-fiscale-fraude (accessed 7 July 2020).

Burgers, I.J.J. and D. Criclivaia (2016), 'Joint Tax Audits: Which Countries May Benefit Most?' *World Tax Journal*, 8(3), Amsterdam, International Bureau of Fiscal Documentation IBFD, pp. 306–355.

Cadesky, M., I. Hayes, and D. Russell (2015), *Towards Greater Fairness in Taxation: A Model Taxpayer Charter*. AOTCA, CFE, and STEP. https://www.nob.net/sites/default/files/content/article/uploads/brochure_taxpayer_0.pdf (accessed 7 July 2020).

Calderon, J.M. and J.S. Ribeiro (2020), 'Fighting Tax Fraud through Artificial Intelligence Tools: Will the Fundamental Rights of Taxpayers Survive the Digital Transformation of Tax Administrations?', *European Taxation*, 60(7), International Bureau of Fiscal Documentation IBFD. Online Publications.

Chen, J., S. Grimshaw, and G.D. Myles (2017), 'Chapter 5: Testing and Implementing Digital Tax Administration in Digital Revolutions in Public Finance', in S. Gupta, M. Keen, A. Shah, and G. Verdier (eds.) (2017), The United States. Washington, DC: International Monetary Fund. https://doi.org/10.5089/9781484315224.071 (accessed 7 July 2020).

CIAT and IOTA (2018), *Tax Administrations and the Challenges of the Digital World: Summary Report*. CIAT and IOTA. https://www.iota-tax.org/sites/default/files/documents/publications/Reports/lisbontax_summit_-_summary_report_final.pdf (accessed 7 July 2020).

Čičin-Šain, N., T. Ehrke-Rabel, and J. Englisch (2018), 'International – Joint Audits: Applicable Law and Taxpayer Rights', *World Tax Journal,* 10(4), Amsterdam, International Bureau of Fiscal Documentation IBFD, pp. 585–631.

Council of Europe (2017), *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*. https://rm.coe.int/16806ebe7a (accessed 7 July 2020).

Council of Europe (2018a), *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91a (accessed 7 July 2020).

Council of Europe (2018b), *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data.* https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (accessed 7 July 2020).

Council of Europe (2019), *Guidelines on Artificial Intelligence and Data Protection*. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (accessed 7 July 2020).

D'souza, C. (2019), *Big Data and Trade Secrets (A General Analysis)*. http://dx.doi.org/10.2139/ssrn.3316328 (accessed 7 July 2020).

Debelva, F. and I.J.M. Mosquera Valderrama (2017), 'Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues, but Few Solutions', *Intertax*, 45(5), pp. 362–381.

European Commission (2016), *EU–US Privacy Shield.* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (accessed 7 July 2020).

European Commission (2018), *The EU Data Protection Reform and Big Data*. https://op.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1 (accessed 7 July 2020).

European Union (EU) (2016a), *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN (accessed 7 July 2020).

EU (2016b), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 7 July 2020).

Greenleaf, G. (2012), 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108', *International Data Privacy Law*, 2(2), p. 75.

Greenleaf, G. (2014a), 'A World Data Privacy Treaty? 'Globalisation' and 'Modernisation' of Council of Europe Convention 108', in N. Witzleb, D. Lindsay, M. Paterson, and S. Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives*. Cambridge: Cambridge University Press, pp. 92–138.

Greenleaf, G. (2014b), *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford University Press, p. 624.

Gupta, S., M. Keen, A. Shah, and G. Verdier (2017), *Digital Revolutions in Public Finance*. Washington, DC. International Monetary Fund. https://www.elibrary.imf.org/view/IMF071/24304-9781484315224/24304-9781484315224/Other_formats/Source_PDF/24304-9781484316719.pdf (accessed 7 July 2020).

Highfield, R. (2017), 'Adopting the New International Tax Rules and Standards', *The Governance Brief*. Manila: Asian Development Bank, p. 29.

Houser, K.A. and D. Sanders (2017), 'The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy as We Know It?' *Vanderbilt Journal of Entertainment & Technology Law*, 19(4). p. 817. https://www.law.columbia.edu/sites/default/files/microsites/public-integrity/article_the_use_of_big_data_analytics_by_the_irs_efficient_solutions_or_the_end_of_privacy_as_we_1.pdf (accessed 7 July 2020).

International Chamber of Commerce (ICC) (2020), *ICC BRITACOM Report: Digitalisation of Tax Administration: A Business Perspective*. https://iccwbo.org/content/uploads/sites/3/2020/03/icc-report-britacom-tax-digitalisation-2020.pdf (accessed 7 July 2020).

International Monetary Fund (IMF). 2007. *Manual on Fiscal Transparency*. Washington, DC.

Kanbur, R. (2017), 'The Digital Revolution and Targeting Public Expenditure for Poverty Reduction', in S. Gupta, M. Keen, A. Shah, and G. Verdier (eds.), *Digital Revolutions in Public Finance*. International Monetary Fund. https://doi.org/10.5089/9781484315224.071 (accessed 7 July 2020).

Krishna, A., M. Fleming, and S. Assefa (2017), 'Instilling Digital Trust: Blockchain and Cognitive Computer for Government', in S. Gupta, M. Keen, A. Shah, and G. Verdier (eds.), *Digital Revolutions in Public Finance*. Washington, DC: International Monetary Fund. https://doi.org/10.5089/9781484315224.071 (accessed 7 July 2020).

Mantelero, A. (2017), 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework', *Computer Law & Security Review*, 33(5), pp. 584–602.

Microsoft and PwC (2018), *The Data Intelligent Tax Administration: Meeting the Challenges of Big Data and Analytics.* PwC. https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf (accessed 7 July 2020).

Mosquera Valderrama, I.J. (2019), 'Processing Personal and Business Data and the Rule of Law in the Era of Digital Trade', *Central European Political Science Review,* 76(20), pp. 111–128.

Mosquera Valderrama, I.J., O. Affuso, and A. Coco (2019), 'A Multidisciplinary Regulatory Approach to Big Data and the Rule of Law', *Glob Tax Gov*, 1 January. https://globtaxgov.weblog.leidenuniv.nl/2019/01/01/a-multidisciplinary-regulatory-approach-to-big-data-and-the-rule-of-law/ (accessed 7 July 2020).

Mosquera Valderrama, I.J.M., A. Mazz, L.F. Schoueri, N. Quiñones, J. Roeleveld, P. Pistone, and F. Zimmer (2017), 'The Rule of Law and the Effective Protection of Taxpayers' Rights in Developing Countries', *WU International Taxation Research Paper Series* No. 10. https://ssrn.com/abstract=3034360 (accessed 7 July 2020).

Organisation for Economic Co-operation and Development (OECD) (2003), *Taxpayers Rights and Obligations*. Centre for Tax Policy and Administration. Paris. ww.oecd.org/tax/administration/Taxpayers'_Rights_and_Obligations-Practice_Note.pdf (accessed 7 July 2020).

OECD (2013), *Co-operative Compliance: A Framework: From Enhanced Relationship to Co-operative Compliance*. Paris: OECD Publishing. https://doi.org/10.1787/97892642 00852-en (accessed 7 July 2020).

OECD (2016a), *Co-operative Tax Compliance: Building Better Tax Control Frameworks*. Paris: OECD Publishing. https://doi.org/10.1787/9789264253384-en (accessed 7 July 2020).

OECD (2016b), *Communiqué of the 10th Meeting of the OECD Forum on Tax Administration (FTA), Forum on Tax Administration, Beijing, 13 May*. http://www.oecd.org/tax/administration/fta-communique-2016.pdf (accessed 7 July 2020).

OECD (2017a), *The Changing Tax Compliance Environment and the Role of Audit*. Paris: OECD Publishing. https://doi.org/10.1787/9789264282186-en (accessed 7 July 2020).

OECD (2017b), Tax Administration 2017: Comparative Information on OECD and Other Advanced and Emerging Economies, OECD Publishing, Paris. https://doi.org/10.1787/tax_admin-2017-en (accessed 7 July 2020).

OECD (2019a), Tax Administration: Comparative Information on OECD and Other Advanced and Emerging Economies. Paris: OECD Publishing. http://www.oecd.org/ctp/administration/tax-administration-23077727.htm (accessed 7 July 2020).

OECD (2019b), *Tax and Digitalisation*. Paris: OECD Publishing. https://www.oecd.org/going-digital/tax-and-digitalisation.pdf (accessed 7 July 2020).

Offermans, R. (2020), *Report on the Symposium, Tax Digitization, Help or Obstacle to Legal Protection?*, European Taxation, 60(6), International Bureau of Fiscal Documentation IBFD. Online Publications.

Sampson, M., J. Wang, and I.J. Mosquera Valderrama (forthcoming), 'Trade, Tax, and Development Finance: Understanding China's Choice of BRI Agreements and Institutions', in F. Schneider (ed.), *Global Perspectives on the Belt and Road Initiative*. Amsterdam: Amsterdam University Press.

Study Group on Asian Tax Administration and Research (SGATAR) (2019), *Three Critical Issues on SGATAR Annual Meeting*, 25 October. SGATAR. https://sgatar49.org/three-critical-issues-on-sgatar-annual-meeting/ (accessed 7 July 2020).

van Hout, D. (2019), 'Legal Protection in the Era of Big Data', *GLOBTAXGOV*, 22 February. https://globtaxgov.weblog.leidenuniv.nl/2019/02/22/legal-protection-in-the-era-of-big-data/ (accessed 7 July 2020).

Vat Update (2019), *Belgian Super-Weapon against VAT Fraud to Be Rolled Out in EU: Transactional Network Analysis*, 9 May. https://www.vatupdate.com/2019/05/09/belgian-super-weapon-transactional-network-analysis-datamining-software-against-vat-fraud-to-be-rolled-out-in-eu/ (accessed 7 July 2020).