An ASEM Model of cooperation in digital economy taxation: digitalisation and new technologies

Mosquera Valderrama, I.J.; Prakash, A.

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

Author

Irma Mosquera: Associate Professor of Tax Law, and Lead Researcher ERC funded project GLOBTAXGOV (Global Tax Governance in International Tax Law Making) Faculty of Law, Leiden University. E-mail i.j.mosquera.valderrama@law.leidenuniv.nl

Table of contents

Introduction

The overall aim of this paper is to address Asia-Europe challenges in digital connectivity in the field of taxation, and to facilitate the exchange of best practices in the framework of the Asia-Europe (ASEM) Connectivity and Cooperation. This paper follows the Chair's Statement in the 2018 ASEM meeting and mainly para. 15 addressing the need for digital connectivity through trust and confidence in the ICT environment and para. 26 stating the growing benefits from the digital economy and the need to find solutions to address the impact of digitalization on the international tax system. These objectives are also in line with the 2030 Sustainable Development Agenda mainly SDG 17.1 on domestic resource mobilization and 17.16 on global partnerships for sustainable development.

Digitalization and new technologies provides new opportunities for tax administrations "to better manage compliance, tackle non-compliance and protect their tax base" .[1] Through digitalization, tax administrations can benefit from the 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 allows countries to increase domestic resource mobilization (SDG 17.1).

The 2018 Asian Development Bank report on Tax and Development stressed the need for the exchange of views and experiences from other tax administrators that share similar challenges and problems.[2] Therefore, the exchange of best practices between countries in a region and among regions (Europe-Asia), can contribute to build on global partnerships for sustainable development (SDG 17.16).

This paper is structured as follows. The first section will address digitalization 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 to the ASEM Network.

1. Digitalization and the use of new technologies by tax administrations

1.1. Digitalization and the use of new technologies

Due to the new ways to collect tax information (i.e. digital sources), more data is now available to tax authorities which includes "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

[1] OECD (2019) Tax Administration: Comparative information on OECD and Other Advanced and Emerging Economies, OECD, Paris. https://read.oecd-ilibrary.org/taxation/tax-administration-2019_74d162b6-en#page23 at 22.

[2] Tax and development: challenges in Asia and the Pacific. In: Araki S, Nakabayashi S (eds). Asian Development Bank (ADB) (2018) Available at https://www.adb.org/sites/default/files/ at 128

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".[3]

This process of digitalization is "transforming the way in which governments can collect, process, and act on information"[4] and therefore, governments should formulate and implement new policies to deal with digitalization and taxation.[5] In order to analyze the data collected, tax administrations are using 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.[6]

As highlighted in a 2018 Asian Development Report on Tax and Development, for effective tax administrations in the Asia and Pacific region it is required 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".[7] Therefore, international/regional organizations, 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 in the following paragraphs.

1.2. 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 taxpayer's information. Some examples are for instance the use of bilateral/multilateral agreements to exchange tax information, exchange of data about transactions facilitated through online platforms, data from digital payments and electronic invoice, tax data from mass

[3] OECD tax and digitalisation https://www.oecd.org/going-digital/tax-and-digitalisation.pdf at 7.
[4] IMF 2017 Digital revolutions in public finance / editors: Sanjeev Gupta, Michael Keen, Alpa Shah, and Geneviève Verdier https://www.elibrary.imf.org/view/IMF071/24304-9781484315224/24304-9781484315224/Other_formats/Source_PDF/24304-9781484316719.pdf at 1.
[5] IMF 2017 Digital revolutions in public finance / editors: Sanjeev Gupta, Michael Keen, Alpa Shah, and Geneviève Verdier https://www.elibrary.imf.org/view/IMF071/24304-9781484315224/24304-9781484315224/Other_formats/Source_PDF/24304-9781484316719.pdf at 1.
[6] For instance, PwC and Microsoft provides some examples in a 2018 white paper of the way that the new information and communication technologies including advance 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 behavioral patterns differ from the norm.
• Identify sophisticated and well-disguised fraudulent behavior such as neural networks, decision trees, multiple regression, etc.
• Visualizing the nature of relationships between individual entities.
• Identify hidden patterns and inconsistencies in unstructured data such as claim forms or electronic invoices".
PwC https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf
[7] See Chapter 1 Shinichi Nakabayash. Tax Challenges in Asia and Pacific in Tax and development: challenges in Asia and the Pacific. In: Araki S, Nakabayashi S (eds). Asian Development Bank (ADB) (2018) Available at https://www.adb.org/sites/default/files/ at 13 publication/456486/adbi-tax-and-development-challenges-asia-pacific.pdf. Accessed 6 Nov 2019

media, the internet and third parties among others. These sources will be analyzed in the following paragraphs.

1.2.1. Traditional sources to collect tax information

At international level, the global standard on exchange of information, and since 2013 the standard on automatic exchange of information has facilitated the collection of information by tax administrations. Exchange of information has widespread around the world mainly due to the countries' participation in in the Global Transparency Forum[8] and countries' signature of bilateral (i.e. tax treaties and tax information exchange agreements) and multilateral instruments (i.e. 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 of the Foreign Account Tax Compliance Act ("FATCA") to exchange financial account information of US taxpayers[9] and (ii) the introduction of the BEPS Project[10] including three Actions that facilitate the collection and exchange of information among 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.[11] 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.[12]

At European level, the most important instrument to facilitate exchange of information in taxation is the Directive on Administrative Cooperation (2011/16/EU). This Directive has been amended 5 times to make possible (i) automatic exchange of financial accounting information (2014/17/EU); (ii) automatic exchange

[8] At the time of writing, the Global Transparency Forum has 161 members and 19 Observers (regional and international organizations). From the 21 Asian Partner Countries in ASEM, only 4 countries are not participating in the Forum (i.e. Bangladesh, Brunei, Lao PDR and Myanmar). All European countries are participating in the Global Transparency Forum.

[9] FATCA is applicable to the reporting by financial institutions (i.e. banks) worldwide to the Internal Revenue Service of 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

[10] 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 (Action 5,6,13 and 14) are minimum standards. Non-OECD, non G-20 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 5 countries are not participating in the Inclusive Framework (i.e. Bangladesh, Cambodia, Lao PDR, Myanmar, Philippines). All European Countries are participating in the BEPS Inclusive Framework.

[11] The adoption of these international tax rules and standards addressing Exchange of Information and the BEPS Project have been also addressed as a favorable development for developing countries in Asia and the Pacific by R. Highfield in an Asian Development Bank Governance Brief. Issue 29, 2017. Available at https://www.adb.org/sites/default/files/publication/225216/governance-brief-29.pdf

[12] At the time of writing, from the 21 Asian Partner Countries in ASEM, only 7 countries have not signed the MCAA (i.e. Bangladesh, Brunei, Cambodia, Lao PDR, Mongolia, Myanmar, Philippines, Thailand, Vietnam) and 1 European country (i.e. Bulgaria). https://www.oecd.org/tax/beps/country-by-country-exchange-relationships.htm

of tax rulings and advance pricing agreements (2015/2376/EU); (iii) 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) automatic exchange of reportable cross border arrangements by tax intermediaries(2018/822/EU). [13]

Furthermore, tax administrations are receiving data for instance following the exchange of data in joint audits between officials from two (countries) tax administrations[14], or in informal join meetings to analyze taxpayer data taking place at the location of one tax administration.[15] New forms of cooperation (e.g. cooperative compliance[16], international compliance assurance programme ICAP[17]) between tax administrations are being discussed following the rapid digitalization of the economy and the emergence of new business models.[18]

1.2.2. Digital sources to collect tax information

In addition to the traditional methods to collect information, tax administrations are making use of digital sources to access taxpayers' information. One example mentioned by the OECD is the multi-side online platforms[19]. Other digital sources mentioned by PwC and Microsoft in a 2018 white paper 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)"[20]

At domestic level, the lawmaker or tax administration can introduce rules to grant access to digital information and to ensure that the information from digital sources is shared with the tax

[13] Information EU Directive on Administrative Cooperation available at https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

[14] See OECD (2017), The Changing Tax Compliance Environment and the Role of Audit, OECD Publishing, Paris, https://doi.org/10.1787/9789264282186-en See also Burgers I. J. J. – Criclivaia D.. 2016. "Joint Tax Audits: Which Countries May Benefit Most?" In *World Tax Journal* 8, no.3: 306-355. See also . Čičin-Šain; T. Ehrke-Rabel; J. Englisch 2018 International - Joint Audits: Applicable Law and Taxpayer Rights In *World Tax Journal* 10, no. 4.

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

[16] OECD (2013), *Co-operative Compliance: A Framework: From Enhanced Relationship to Co-operative Compliance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264200852-en and more recently OECD (2016), *Co-operative Tax Compliance: Building Better Tax Control Frameworks*, OECD Publishing, Paris, https://doi.org/10.1787/9789264253384-en.

[17] OECD International Compliance Assurance Programme available https://www.oecd.org/tax/forum-on-tax-administration/international-compliance-assurance-programme.htm

[18] These new forms of cooperation were addressed in the OECD Tax Certainty day of 16th September 2019. Programme available at https://www.oecd.org/tax/forum-on-tax-administration/events/Tax-certainty-Day-2019-Agenda.pdf

[19] 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 tax and digitalization at 5.

[20] PwC https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf at 4 and 5.

administration.[21] At international level, the information can be exchanged among tax administrations provided that there is an instrument to exchange information (e.g. treaty, tax information exchange of agreement or multilateral competent authority agreement). In order to exchange this information, the OECD Forum on Tax Administration has designed a Common Transmission System[22] to facilitate automatic exchange between tax administrations of financial account information (CRS), country by country reporting and other exchanges.

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 the access to such information (e.g. Facebook, Instagram and Twitter)[23], the access by the tax administration to these digital sources of information becomes difficult.[24]

In order to address some of these problems, the OECD in a document addressing Tax and Digitalization stated the need for unilateral and multilateral initiatives to obtain tax data about transactions facilitated through online platforms. At national level, the OECD suggests to introduce "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".[25]

In case that the data is located in a jurisdiction other than the jurisdiction of the platform seller, the OECD suggests to explore the possibility of a multilateral agreement to facilitate access and exchange to such information along the lines of the Common Reporting Standard for automatic exchange of financial

[21] One example is the UK 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

[22] This system was agreed by the 44 heads of tax administrations members of the 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". https://www.oecd.org/tax/forum-on-tax-administration/meetings/fta-communique-2016.pdf

[23] In the past, the mining of social media by the IRS has been addressed by scholars. See Kimberly A. Houser and Debra Sanders. The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy as We know It? 19 Vand. J. Ent. & Tech. L. 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

In December 2018, the IRS National Office of Procurement request (2032h8 RFI MEDIA IRS)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/

[24] 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), The Changing Tax Compliance Environment and the Role of Audit, OECD Publishing, Paris, https://doi.org/10.1787/9789264282186-en pp. 75-76 In Europe, two exceptions are France and the Netherlands that 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, art. 154 2020 Budget Bill and in the Netherlands arts. 7:4 and 8:42 of the General Administrative Law. However, this has been disputed in courts see in France Constitutional Council ruling of 27 Dec. 2019 Decision No. 2019-796 DC and in the Netherlands Supreme Court decision of 4 May May 2018 (BNB 2018/164) and of 17 August 2018 (BNB 2018/182). See R. Offermans, Report on the Symposium, Tax Digitization, Help or Obstacle to Legal Protection?, 60 Eur. Taxn. 6 (2020) at 7; J. M.Calderon, J. S. Ribeiro. Fighting Tax Fraud through Artificial Intelligence Tools: Will the Fundamental Rights of Taxpayers Survive the Digital Transformation of Tax Administrations? European Taxation 2020 (Vol. 60) Issue 7 at 1.

[25] OECD tax and digitalisation https://www.oecd.org/going-digital/tax-and-digitalisation.pdf at 6.

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". [26]

1.3. Challenges tax administration

1.3.1. International level

The 2019 OECD Tax Administration report stated that "tax administrations much like tax policy makers, 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".[27]

The 2018 Summit of Regional Network of Tax Administrations (Inter-American Centre of Tax Administrations (CIAT) and Intra-European Organization of Tax Administrations (IOTA) has also addressed some of the challenges of 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 analyses to identify tax risks (for instance in country by country reporting in Germany); (ii) the development of several changes for data transmission (e.g. Switzerland referring to the use of XML upload on the FTA Portal SuisseTax, online and via webservice (M2M Communication) and (iii) the use of technology to improve tax control (e.g. development of big data tools in Spain).[28] More recently (October 2019), in the CIAT Technical conference, the experience of countries in the use of new digital technologies and big data (Chile and Mexico) and artificial intelligence (Canada) were presented. [29]

The exchange of best practices in the 2018 Summit was facilitated by CIAT and IOTA between countries in the American and European region. From the 21 Asian Partner countries in ASEM, only India and Russia presented some best practices (i.e. India: use of internal system to collect financial information and Russia: cash register reform using data analytics). [30] In the 2019 CIAT Technical Conference, from the 21 Asian

[26] OECD tax and digitalisation https://www.oecd.org/going-digital/tax-and-digitalisation.pdf at 6..
[27] OECD Tax Administration 2019. Comparative information on OECD and Other Advanced and Emerging Economies. https://read.oecd-ilibrary.org/taxation/tax-administration-2019_74d162b6-en#page23 at 22.
[28] Some of the challenges have been addressed in the CIAT-IOTA Tax Summit. See Tax Administrations and the Challenges in the Digital World. Summary Report. Lisbon Tax Summit 24-26 October 2018. https://www.iota-tax.org/sites/default/files/documents/publications/Reports/lisbontax_summit_-_summary_report_final.pdf
[29] Section 3.2. October 10, presentations available at https://www.ciat.org/ciat-2019-technical-conference/?lang=en
[30] Summary Report. Lisbon Tax Summit 24-26 October 2018. https://www.iota-tax.org/sites/default/files/documents/publications/Reports/lisbontax_summit_-_summary_report_final.pdf Russia at 11 and India at 14.

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.[31]

Therefore, it is advisable for countries in Asia to also participate actively in these types of meetings or to organize their own meetings in Asia. For instance, in the conference (BRITACOF) scheduled in May 2020 (postponed to May 2021[32]) in Kazakhstan in the framework of the Belt and Road Initiative Tax Administration Cooperation Mechanism BRITACOM[33], one of the topics to be addressed is the digitalization of tax administrations.

For this purpose, the International Chamber of Commerce (ICC) drafted a report to provide a business perspective in the digitalization of tax administrations. This report introduced some principles for digitalization 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.[34] In addition, the report addressed the prerequisites for a successful digital transformation from a business perspective (i.e. data security, system requirements, data availability, reasonable use of data, transparency, taxpayers identity and consistency). [35]

Another framework that can be used is the Annual Meeting of the Study Group on Asian Tax Administration and Research (SGATAR[36]). For instance, the 49th SGATAR (2019) Annual Meeting has addressed the challenges of digitalization for tax administrations in Asian countries.[37] One of the recommendations of this meeting is for tax administrations to enhance their modernization "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". [38]

1.3.2. European level

[31] Presentation 8 October 2019 available at https://www.ciat.org/ciat-2019-technical-conference/?lang=en
[32] This conference has been postponed due to COVID19.
http://www.chinatax.gov.cn/eng/n4260854/c5149476/content.html
[33] In order to deal with some of these challenges, and also to address the implementation of the BRI, China has launched the Belt and Road Initiative Tax Administration Cooperation Mechanism (BRITACOM). BRITACOM has 34 member countries and 11 countries as observers form different regions (e.g. Asia, Africa, Europe), plus one non-profit (academic) organization. http://www.chinatax.gov.cn/eng/n4260869/c5112279/content.html.
See on the role of BRITACOM, M. Sampson, J. Wang and I. Mosquera. Trade, Tax, and Development Finance: Understanding China's Choice of BRI Agreements and Institutions in Global Perspectives on the Belt and Road Initiative. F. Schneider (ed.) Amsterdam University Press, Amsterdan. Forthcoming.
[34] https://iccwbo.org/content/uploads/sites/3/2020/03/icc-report-britacom-tax-digitalisation-2020.pdf pp. 2 to 3.
[35] https://iccwbo.org/content/uploads/sites/3/2020/03/icc-report-britacom-tax-digitalisation-2020.pdf pp. 5 to 7.
[36] SGATAR is an organization of tax administrations in the Asia-Pacific region founded in 1970. The current members include Australia, People's Republic of China, Hong Kong SAR, Indonesia, Japan, Republic of Korea, Macao SAR, Malaysia, Mongolia, New Zealand, Papua New Guinea, the Philippines, Singapore, Chinese Taipei, Thailand and Vietnam. http://sgatar.org/category/focus/
[37] In addition, to member countries, International organizations (e.g. OECD, World Bank, IMF), and regional network of tax administrations e.g. CIAT participated in the annual meeting.
[38] Three critical issues in SGATAR Annual Meeting https://sgatar49.org/three-critical-issues-on-sgatar-annual-meeting/

At European Level, in September 2018, the EU countries created TADEUS. TADEUS is the yearly Summit of Heads of Tax Administrations of EU countries and the Commission DG TAXUD to address common challenges of digitalization and globalization. The aim is to enhance cooperation in several areas including addressing the digital economy and the digitalization of tax authorities and managing IT systems and resources.[39] 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.[40]

The first meeting of TADEUS took place on 17-18 September 2019. In this meeting, the Heads of tax Administrations acknowledge the legislative changes and the level of administrative cooperation that will require new IT developments and investment in trans-European electronic systems. Therefore, one of the outcome of the meetings was the need to align the development of the EU common or inter-operable IT systems and to set up "a coordination process based on consensus, in the form of a multi-annual plan, under the coordination of TADEUS". [41]

Finally, countries are also seeking other ways to cooperate. One example is Belgium, the Netherlands and Luxembourg (BENELUX) that decided to introduce a new system (Transaction Network Analysis) to tackle automatically VAT fraud in the BENELUX area.[42] In addition, in order to tackle tax evasion and tax fraud[43], these countries have signed in October 2019 a new agreement (memorandum of understanding)[44] that facilitates automatic exchange of information between countries including not only traditional but also digital sources. [45]

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

1.4. Data management strategies and digital infrastructure

1.4.1. Data management strategies

[39] https://ec.europa.eu/taxation_customs/news/tadeus-%E2%80%93-tax-administration-eu-summit_en
[40] Outcome Statement https://ec.europa.eu/taxation_customs/sites/taxation/files/tadeus_2019_outcomes_statement_-_1st_plenary_meeting_helsinki_finland.pdf at 2.
[41] Para..13 Outcome Statement https://ec.europa.eu/taxation_customs/sites/taxation/files/tadeus_2019_outcomes_statement_-_1st_plenary_meeting_helsinki_finland.pdf at 3.
[42] This analysis will use "data mining software with which smart algorithms can quickly uncover suspicious transactions that indicate a VAT carousel" https://www.vatupdate.com/2019/05/09/belgian-super-weapon-transactional-network-analysis-datamining-software-against-vat-fraud-to-be-rolled-out-in-eu/
[43] http://www.benelux.int/nl/nieuws/benelux-landen-versterken-hun-samenwerking-de-strijd-tegen-fiscale-fraude
[44] https://www.benelux.int/files/6015/8098/4521/MoU_fraude_fiscale_10.10.2019-NL.pdf
[45] For instance art 2 states the use of digital projects such as FCI.net. 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/

The data management strategy should be long-term strategy and focusing not only on descriptive analytics (for diagnostic) but also on predictive and prescriptive analytics.[46] Predictive analytics "provide information on likely future outcomes or resource maintenance schedules"[47] whereas prescriptive "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 optimization (e.g. pervasive, automation)".[48]

Regarding artificial intelligence, the Canadian Revenue Authority shared its experience in a 2019 presentation made in the framework of the CIAT Technical Conference. For The Canadian Revenue Authority, artificial intelligence results in (i) advance 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 mining of unstructured data. [49]

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

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

1.4.2. Infrastructure

Tax digitalization require changes to the infrastructure which can be difficult to achieve by countries with limited (personnel, budget) resources which are mainly developing countries.[50] Developing countries may have a large informal untaxed sector and therefore, it becomes difficult to obtain (and/or update) information from individuals and/or business.[51]

[46]See PwC-Microsoft White Paper PwC https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf at 9.
[47] PwC https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf at 9
[48] PwC https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf at 9
[49] Presentation available at Section 3.2. https://www.ciat.org/ciat-2019-technical-conference/?lang=en
[50] Debelva F. and Mosquera Valderrama I. J. (2017), Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues, but Few Solutions, Intertax 45(5): 362-381.
[51] As stated by Kanbur "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

One positive remark as mentioned by Krhisna et al will be 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. 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"[52].

Furthermore, some tax administrations (even though having resources) may be cautious to advance digitalization "given the potential costs of mistakes. Foremost among these are the risk to revenue, damage to reputation, and potential reduction of tax morale. The digitalization 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".[53]

To sum up data is 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) providing the access to digital sources and the exchange of digital data. The access to tax data and the use of big data[54] can help to optimize 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 the instruments to safeguard the taxpayers' rights in this new era of digitalization.

2. Instruments to safeguard the automatic processing of personal data and protecting taxpayers' rights

2.1. Collection of personal and business data

linked in to other national databases, and the use of such information is not a problem.5 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". Chapter 9 Ravi Kanbur.The Digital Revolution and Targeting Public Expenditure for Poverty Reduction Digital Revolutions in Public Finance (eds. Sanjeev Gupta, Michael Keen, Alpa Shah, and Genevieve Verdier) 2017. Available From: IMF eLibrary https://doi.org/10.5089/9781484315224.071 at 232.

[52] Chapter 7: Instilling digital trust: Blockchain and Cognitive computer for government. Arvind Krishna, Martin Fleming, and Solomon Assefa in Digital Revolutions in Public Finance (eds. Sanjeev Gupta, Michael Keen, Alpa Shah, and Genevieve Verdier) 2017. Available From: IMF eLibrary https://doi.org/10.5089/9781484315224.071 at 182.

[53] Jingnan (Cecilia) Chen, Shaun Grimshaw, and Gareth D. Myles. Chapter 5 Testing and Implementing Digital Tax Administration in Digital Revolutions in Public Finance (eds. Sanjeev Gupta, Michael Keen, Alpa Shah, and Genevieve Verdier) 2017. International Monetary Fund. https://doi.org/10.5089/9781484315224.071 at 114

[54] 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 A. 2017. "Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework. In Computer Law & Security Review 33, no. 5: 584-602. at 2.

In general, the data collected includes personal data (i.e. information relating to an identified or identifiable individual including genetic data and biometric data[55]) and business data (i.e. information relation to operation of a business including trade secrets[56]). This 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 the country.[57]

In this new digital tax administration era[58], 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 taxpayer's data? (ii) is the taxpayers' data properly collected, stored and monitored? (iii) is the processing of the taxpayer's data allowed? And (iv) who owns the taxpayer's data?[59]

As rightly mentioned in the 2018 Asian Development Bank Report on tax administrations, in order to enhance voluntary compliance, "revenue bodies must be seen to operate in a manner that instils a high level of mutual trust, respect and confidence among its taxpayer population. This can only be achieved where there is recognition and acceptance of a basic set of taxpayer's rights and obligations".[60] Therefore, countries should also take into account the instruments to safeguard the taxpayer's 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 is 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 automatic processing of data including big data[61] and (ii) taxpayer's rights including the right to confidentiality, secrecy and privacy. Some of these

[55] Example of biometric data are fingerprints, iris scan, and DNA. This data is protected as a special category of personal data in art. 9 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".

[56] See on trade secrets: D'souza, Craig, Big Data and Trade Secrets (A General Analysis) (January 15, 2019). Available at SSRN: https://ssrn.com/abstract=3316328 or http://dx.doi.org/10.2139/ssrn.3316328

[57] See Mosquera Valderrama I.J. – Mazz A. – Schoueri L.F. – Quiñones N. – Roeleveld . – Pistone P. – Zimmer F.. 2017. "The Rule of Law and the Effective Protection of Taxpayers' Rights in Developing Countries". In *WU International Taxation Research Paper Series* no.10. Available at SSRN: https://ssrn.com/abstract=3034360 See also Debelva F. - Mosquera Valderrama I. J.. 2017. "Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues, but Few Solutions". In *Intertax* 45 no.5: 362-381.

[58] 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, e-services, etc. See PwC and Microsoft 9 and 10 https://www.pwc.nl/nl/assets/documents/the-data-intelligent-tax-administration-whitepaper.pdf

[59] See Mosquera Valderrama I.J. Processing of personal and business data and the rule of law in the era of digital trade, Central European Political Science Review CEPSR Journal – 76 number

[60] Asian Development Bank 2018. A Comparative Analysis of Tax Administrations in Asia and the Pacific. At 37. https://www.adb.org/publications/comparative-analysis-tax-administration-asia-pacific

[61] See also blogpost Diana van Hout Legal Protection in the era of big data https://globtaxgov.weblog.leidenuniv.nl/2019/02/22/legal-protection-in-the-era-of-big-data/

safeguards for the protection of data in automatic processing of data have been addressed elsewhere by this author. [62]

2.2. Taxpayers' rights in Asia

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

If one example can illustrate this, is the Asian Development Bank reports published in 2018 and 2020 which presented a comparative study of Tax Administrations in Asia and the Pacific. These reports did not specify the challenges of countries to protect the taxpayers' rights in the use of digital technologies and the automatic processing of personal data. Instead reference was made to the OECD and other international organizations documents. As far as we are aware, a comparative study in taxpayers' rights in Asia in the exchange of information and digitalisation has not yet been made. [63]

In the 2018 report reference was made to the 2003 OECD document on Taxpayer Rights and Obligations. In addition, the 2018 report mainly based in international organizations surveys[64] provided a short comparison of the use of legislative or administrative rules introducing taxpayers' rights. According to this comparison, from the 28 Asia and Pacific countries analyzed in 2018,only 5 countries did not have rights set out in Law or Statute or Developed by Revenue Body (i.e. Hong Kong, Japan, Papua New Guinea, Myanmar, Singapore).

The 2020 report did not address the challenges mentioned above, nor did the report provide an update overview of 28 Asia and Pacific countries mentioned above. The 2020 report referred to common elements in Taxpayer Charters available in Asia and Pacific countries (based on the report author's own

[62] According to Debelva and Mosquera, the following safeguards should be introduced for exchange of information including automatic exchange of information. (1) similar data can be received from the receiving State reciprocity), (2) the receiving State ensures 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 of 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 F. and Mosquera Valderrama I. J. (2017), Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues, but Few Solutions, Intertax 45(5): 362-381.

[63] However, some Asian countries e.g. China, India, South Korea, 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

[64] The report cite as sources for taxpayers' rights and obligations in Asia and Pacific countries, the Asian Development Bank and IMF survey responses and Organization for Economic Cooperation and Development 2017. Report (table A124). See Asian Development Bank 2018. A Comparative Analysis of Tax Administrations in Asia and the Pacific. At 38. https://www.adb.org/publications/comparative-analysis-tax-administration-asia-pacific

compilation).[65] The 2020 report also referred to the collaborative project of Tax Consultants in ASIA, Europe and the Society of Trust and Estate Practitioners STEP to develop a Model Taxpayer Charter.[66] Finally, the 2020 report focused on access to rulings and dispute rights in Asia and Pacific.

2.3. Instruments for data protection and privacy

At international level taxpayer 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 countries member of the Council of Europe and third countries (outside the Council) which can be made applicable to taxation.[67] Some countries have also signed bilateral agreements (e.g. EU-US Privacy Shield[68]).

At regional level two EU instruments should be mentioned the 2016 Directive[69] and Regulation[70] on Data Protection (in force since May 2018). The 2016 Directive replaced the 1995 Data Protection Directive. Other regional agreements are (i) the 2005 Asia-Pacific Economic Cooperation (APEC) Framework which

[65] The elements of Charters mentioned are: statement of intent, statement of mutual obligations, taxpayer's rights, taxpayers' obligations, and details rights and obligations. These elements do not consider taxpayers' rights in digitalization.

[66] A Model Taxpayer Charter: Towards Greater Fairness in Taxation. 2015. https://www.nob.net/sites/default/files/content/article/uploads/brochure_taxpayer_0.pdf See also presetnation to the Members Platform for Good Tax Governance in February 2014. https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/cfe.pdf

[67] See on the history of the Convention. Greenleaf, G. (2014). A world data privacy treaty? 'Globalisation' and 'modernisation' of Council of Europe Convention 108. In N. Witzleb, D. Lindsay, M. Paterson, & S. Rodrick (Eds.), Emerging Challenges in Privacy Law: Comparative Perspectives (Cambridge Intellectual Property and Information Law, pp. 92-138). Cambridge: Cambridge University Press

[68] 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 is transferred to the United States for commercial purposes. Information 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

[69] 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

[70] 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).

introduced information privacy principles[71] and (ii) the 2010 Supplementary Act on Personal Data Protection within the Economic Community of West African States (ECOWAS).[72]

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 Asia and Pacific countries. [73] 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.[74] 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, Vietnam, and Japan, but they are of questionable value)"[75] among others.

Since the 2016 Directive and Regulation are new, further research should be carried out on how the provisions of the new Directive and Regulation can be also used to enhance data protection and to safeguard the right to privacy. In the past, we argue 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".[76]

Regarding the Council of Europe Convention, the influence is still limited outside non-member countries since at the time of writing, the number of non-member countries that have ratified this Convention is 8 countries. Since this is the only multilateral binding convention that can have a worldwide application.[77] In our view, more work should be carried out by the Council of Europe in promoting the adoption of this Convention by non-member countries. [78] One drawback of this Convention is that it is only applicable to

[71] 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". See Debelva and Mosquera at 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

[72] See website ECOWAS https://ccdcoe.org/organisations/ecowas/ Text of the Agreement available at http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf

[73] Some examples are Macau SAR, South Korea, Taiwan, Malaysia, Hong Kong SAR, Australia, New Zealand, India, Japan, Vietnam. See G. Greenleaf. The influence of European Data Privacy Standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, 2012, Vol 2. No. 2 at 75. See also. G. Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives, Oxford University Press, 2014, 624 pp. This book provides an analysis of 26 data privacy laws in Asia.

[74] Ibid.

[75] G. Greenleaf. The influence of European Data Privacy Standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, 2012, Vol 2. No. 2 at 80.

[76] Mosquera Valderrama I.J. – Mazz A. – Schoueri L.F. – Quiñones N. – Roeleveld . – Pistone P. – Zimmer F.. 2017. "The Rule of Law and the Effective Protection of Taxpayers' Rights in Developing Countries". In *WU International Taxation Research Paper Series* no.10. Available at SSRN: https://ssrn.com/abstract=3034360 at 47.

[77] The use of the Convention in a global level has been addressed by G. Greenleaf. The influence of European Data Privacy Standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, 2012, Vol 2. No. 2. Pp. 68-92.

[78] One reason for countries no participating in this Convention has been mentioned by Greenleaf referring to the lack of transparency on accession to the Convention. G. Greenleaf. The influence of European Data Privacy Standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, 2012, Vol 2. No. 2 at 69.

personal data. Therefore, it is recommended to the Council of Europe to extend the protection of this Convention to business data including trade secrets. The main elements of this Convention will be presented below.

2.3.1. Council of Europe Convention on the Automatic Processing of Personal Data

In 1981, the Council of Europe adopted the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This Convention protects the individual against abuses which may accompany the collection and processing of personal data and at the same time regulates the cross-border flow of personal data.[79] This Convention has been amended by two Protocols[80].

The first Protocol was approved in 2001 and extended this Convention for approval by non-member countries (countries outside the Council of Europe). This 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 opened for signature as of 25 June 2018.[81] This Protocol pursued two main objectives: to deal with challenges resulting from the use of new information and communication technologies, and to strengthen the Convention's effective implementation. This Protocol has been signed by 35 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 38 countries.

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

European countries have signed and ratified the Convention 108. As of May 2020, the 2018 Protocol has been signed by almost all EU countries (except Denmark, Malta and Romania), and it has been ratified by 3 countries (Bulgaria, Croatia and Lithuania). [82]

The Convention

The Convention is applicable to automated personal data files and automatic processing of personal data in the public and private sectors (art. 3). [83] Four articles of the Convention that can be relevant for the tax

[79] Mosquera Valderrama I.J. Processing of personal and business data and the rule of law in the era of digital trade, Central European Political Science Review CEPSR Journal – 76 number

[80] Some of the elements analysed in this section have been previously addressed by this author and others in blogpost GLOBTAXGOV I.J. Mosquera Valderrama, O. Affuso, A. Coco 2019). https://globtaxgov.weblog.leidenuniv.nl/2019/01/01/a-multidisciplinary-regulatory-approach-to-big-data-and-the-rule-of-law/

[81] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223

[82] Chart of signatures and ratifications of Treaty 223 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

[83] 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

administrations in this digital administration era refer to 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". [84]

Furthermore, art. 6 addresses the protection to 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". [85]

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". [86]

Article 8 provides for additional safeguards for the 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". [87]

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 modernize the Convention "to better address emerging privacy challenges resulting

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

[84] Convention art. 5
[85] Convention art. 6
[86] Convention art. 7
[87] Convention art. 8

from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data". [88]

For this purpose, the Council of Europe commissioned a study for new guidelines[89] on the protection of individuals with regard to the processing of a 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.[90] More recently, new guidelines have been published in 2019 on artificial intelligence and data protection.[91] These guidelines have not yet been used in the Council of Europe Convention, therefore, these guidelines are outside the scope of this analysis.[92]

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".[93] Therefore, the guidelines introduce a precautionary approach in regulating data protection and introducing risk assessment considering the legal, social, and ethical impact 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. [94]

Following to some extent the 2017 Guidelines[95], the Protocol of 2018 provides for more transparency and protection in data processing and introduce stronger accountability of data controllers, and the obligation

[88] 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

[89]Consultative Committee of the Convention for the Protection of Individuals with regard to automatic Processing of Personal Data (T-PD). Guidelines on the Protection of Individuals with regard to the processing of personal data in a world of big data. T-PD(2017)01 https://rm.coe.int/16806ebe7a

[90] 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, Germany and Ireland objected

[91] Consultative Committee of the Convention for the Protection of Individuals with regard to automatic Processing of Personal Data (T-PD). Guidelines on Artificial Intelligence and Data Protection. T-PD(2019)01 https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

[92] 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.

[93] Guidelines at 2. https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0

[94] By design refers to appropriate technical and organizational measures taken into account throughout the entire process of data management, from the earliest design stages, to implement legal principles in an effective manner and build 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". Guidelines at 2 https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0

[95] For instance regarding by design and by default solutions to mitigate risks in the processing of personal data. Cfr. Para. 2.5.(2) Guidelines https://rm.coe.int/16806ebe7a and Art. 10 2018 Protocol and para. 89 Explanatory Statement. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

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.[96]

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

Even though big data is not specific mentioned in the text of the Protocol, this Protocol introduces new rights for the 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".[98]

In addition, the Protocol includes the obligation of the controller and data processors to introduce a 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 minimizes) 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. [99]

For privacy by default, the 2018 Protocol states that controllers and processors should implement technical and organization measures which take into account the implications of the right to the protection of personal data at all states of the data processing (art. 10(3)). The explanatory statement to the Protocol further elaborates in this privacy by default principle stating that "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

[96] For instance in a word search for 'big data' in the 2017 Guidelines, the search results in the word big data mentioned 33 times whereas in the 2018 Protocol the search results are nihil. 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 to safeguard human right and fundamental freedoms. 2017 Guidelines at 3.
[97] Art. 7 2018 Protocol.
[98] See also para. 75 and 77 Explanatory Statement https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[99] Mosquera Valderrama I.J. Processing of personal and business data and the rule of law in the era of digital trade, Central European Political Science Review CEPSR Journal – 76 number

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". [100]

2.3.2. EU General Data Protection Directive and Regulation

The EU Data Protection Directive (EU) 2016/680 and the 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 to non-automatic processing.[101] 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[102], 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".[103]

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".[104]

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

[100] Para. 89 Explanatory Statement https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91a At 15.
[101] See EU data protection rules website https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en#documents
[102] The EU data protection reform and big data. Factsheet Date publication January 2016. In addition 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".Available at https://op.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1 at 1.
[103] https://op.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1 at 4.
[104] Para. 78 Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 See also. Para. 63 Directive https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

purposes of the processing". These public authorities include tax and custom authorities (para. 31 Regulation).

The automated decision making is also protected in this regulation. Accordingly, para. 71 of the Regulation states that a decision (and profiling) that affects a data subject cannot be taken only based on automated processing unless that such 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".[105] 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".[106]

3. Final Remarks and Recommendations

This paper has addressed Asia-Europe challenges regarding the use of new technologies by tax administrations and the protection of taxpayers' rights. In order to facilitate the exchange of best practices in the framework of the Asia-Europe (ASEM) Connectivity and Cooperation, this paper has addressed the Europe and Asia Pacific developments including also the work carried out by international organizations (Asian Development Bank, OECD) and regional tax administration networks (CIAT, IOTA, BRITACOM, 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 diagnostic, predictive and prescriptive analytics. Furthermore, countries should also invest in improving their digital infrastructure that includes the introduction of common transmission systems and software for analysis of big data.

For this purpose, it is important to organize regional meetings for tax administrations to present their tax digitalization challenges and to exchange best practices. These meetings could be similar to TADEUS (an EU yearly summit of Heads of Tax administration) 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 memorandum of understandings to enhance cooperation to tackle tax evasion and tax fraud based in the needs of the countries (as it is been done in the BENELUX initiatives).

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 EU 1995 Directive on data Protection. However, this Directive has been

[105] Para. 71 Regulation
[106] Para. 71 Regulation.

updated to include among 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 it has been done in the Council of Europe Convention (2018 Protocol), it is also recommended that countries include the reference to big data or data analytics including the right of persons (data subjects) in an algorithm decision-making context.

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