# Processing personal and business data and the rule of law in the era of digital trade

Mosquera Valderrama, I.J.

*PRE-PRINT VERSION Mosquera Valderrama, I.J. Processing Personal and Business Data and the rule of law in the era of digital trade. Central European Political Science Review. Vol. 20, No. 76, Summer 2019. ISSN: 1586-4197. pp. 111-128*

# Processing personal and business data and the rule of law in the era of digital trade

**Irma Johanna Mosquera Valderrama** [1]

**Abstract:** This article addresses data protection including the automatic processing of personal and business data as a result of the flows of information and the digital trade. Nowadays, data is being collected, exchanged and used in small or large amounts by governments, international organizations and companies for medical, educational, social, industrial and tax purposes amongst others. The increasingly collection, exchange and use of data by companies and governments, calls for attention to the legal protection in the collection, exchange, use, monitoring and processing of this data. Furthermore, the use of big data also raises questions regarding the protection of privacy and also the safeguards in place for the data controllers among others. The main question of this article is *are the instruments in the era of digital trade, internet governance and taxation sufficient to guarantee the privacy and data protection of individuals and business?* In order to answer this question, this article will address the challenges and the instruments for the protection of the use of data and big data in three areas: trade and internet governance and taxation.

**Keywords**: Big Data, Data Protection and Privacy, Exchange of Information, Taxation, Digital Trade

## 1. Introduction

Due to the liberalization of trade and to the use of digital services, data flows have increased in the last decade. Data is used for instance for medical, educational, social, industrial and tax purposes. Companies such as Facebook, Google, Netflix, Amazon have used digital platforms to collect and exchange social data and at the same time to facilitate digital services. Governments are also seeking to collect data to access taxpayer information to prevent tax evasion, tax avoidance including aggressive tax planning and money laundering.

Further to the collection of data, there is an increase flow in the exchange of data among governments and companies and in the analysis of large data sets by using software to identify possible patterns to enhance productivity, public sector performance, and facilitate enforcement

[1] Initial version of this article was presented at the *2018 Conference of the World Complexity Science Academy (WCSA), organized by Prof. Andrea Pitasi, that took place in Rome between 12 and 15 November 2018.* The author is grateful for the feedback provided by the discussants and participants at this conference. The writing and research carried out for this article is the result of the ERC research in the framework of the GLOBTAXGOV Project (2018-2023). The GLOBTAXGOV Project investigates international tax law making including the adoption of OECD and EU standards by 12 countries. The GLOBTAXGOV Project has received funding from the European Research Council (ERC) under the European Union's Seven Framework Programme (FP/2007-2013) (ERC Grant agreement n. 758671). Information available at https://globtaxgov.weblog.leidenuniv.nl/a-new-model-of-global-governance-in-international-tax-law-making-globtaxgov/

of the law. This use of large data sets is called big data. 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 2017:2).

Despite the increasingly collection, exchange and use of data by companies and governments, this article argues that there is no enough legal protection in the collection, exchange, use, monitoring and processing of this data. Furthermore, the use of big data also raises questions regarding the protection of privacy[2], and also the safeguards in place for the data controllers among others.

Accordingly, even though the use of data and big data has increased, and it is justified in the era of digital trade, recent developments such as Facebook Cambridge analytic scandal[3] and the Panama Papers, Paradise Papers and Luxleaks[4] raise questions regarding the processing of personal and business data in this new environment. Some of the most important questions that need to be raised in the processing of personal and business data are (i) who has my data? (ii) is my data properly collected, stored and monitored? (iii) is the processing of my data allowed? And (iv) who owns my data?

Against this background, the main question of this article is *are the instruments in the era of digital trade, internet governance and taxation sufficient to guarantee the privacy and data protection of individuals and business?* In order to answer this question, this article will address the challenges and the instruments for the protection of the use of data and big data in three areas: trade and internet governance (Section 2) and taxation (Section 3). Thereafter, this article will provide some conclusions and recommendations.

## 2. Challenges: Data and Big Data in Trade and Internet Governance

### 2.1. Digital trade and Internet Governance

In digital trade, the use of digital (internet) platforms, the increase of digital economy and the introduction of digital services market create challenges for the regulation of these services and for the protection of privacy, and personal and business data of individuals and companies.

Nowadays, individuals and companies use digital platforms (e.g. Facebook) to exchange data and to disseminate their work in social and professional networks. Furthermore, by means of digital economy there is "a worldwide network of economic activities, commercial transactions and professional interactions that are enabled by information and communications technologies".[5]

---

[2] Privacy defined as the right to keep one's affair secret whereas data protection addresses the person's right to control his or her personal data and the processing of such data. This data protection can also be applicable to companies when referring to business data (e.g. trade secrets, business strategies, list of clients)

[3] In the Cambridge analytical data, the data of 87 million Facebook users was improperly obtained, and misused for political purposes (UK Brexit Referendum and the US 2016 Presidential Election) (European Parliament, 2018).

[4] Panama papers, Paradise papers and Luxleaks revealed by the International Consortium of Investigative Journalists (ICIJ) disclosed the exploitation of offshore tax regimes to hide funds and income, which reduce tax revenue in countries. See website ICIJ https://www.icij.org/investigations/ (Accessed 9 February 2019)

[5] Definition of digital economy https://searchcio.techtarget.com/definition/digital-economy (Accessed 9 February 2019)

The digital services market makes possible that multinational companies (e.g. Netflix) can provide services worldwide but also small companies (SMEs) are able to access consumers outside its own territory. As rightly stated by Mishra "the digitals service market is the fastest growing sector in the world today and is a key driver of the global economy. The entry barriers in the industry are low, and consumers have access to a range of competitive and high-quality services from across the world. Further, digital platforms have also increased access of SMEs to consumers outside their local or domestic markets" (Mishra 2019:29).

Another area that is closely related to digital trade is internet governance that promotes data flows among countries and the use of commercial digital platforms so that "customers can access and use different digital services". (Mishra 2019: 15) In addition to openness, internet governance aims to ensure security of the internet network to protect personal data and confidentiality of the information that is stored, and privacy to ensure consumer trust (Mishra 2019: 16, 20, 21).

Therefore, in digital trade and internet governance, the protection of privacy, personal and business data is important to ensure the user and consumer trust. However, the instruments used to protect this data are limited since it is mostly left to the domestic laws of the country. Even in cases such as the Facebook Cambridge analytic scandal that affected 87 million Facebook users, there were no international instruments to enforce the privacy and protection of the Facebook users' data. If one example can illustrate this, is the lack of sanctions to Facebook at the United States Congress' hearings (Kozlowska 2018) and at the EU Parliament hearings (European Parliament 2018a).

### 2.2. Instruments and challenges for data protection and privacy

The promotion of data flows in the area of digital trade and internet governance bring challenges to the balance between the use (and exchange) of data for digital services, and the protection of data and privacy including also the protection against cybersecurity.

Countries have regulated these areas in several instruments such as the Constitution addressing the right to privacy and confidentiality and domestic data protection laws. In addition, countries have also implemented EU laws (e.g. General Data Protection Regulation[6]) and/or signed bilateral agreements (e.g. EU-US Privacy Shield[7]) and/or multilateral agreements, for instance Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe 1981)[8].

---

[6] According to the EU website, regulation (EU) 2016/6791 (European Parliament – Council 2016) regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU. It doesn't apply to the processing of personal data of legal entities. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (Accessed 9 February 2019)

[7] 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 (Accessed 9 February 2019)

[8] See section 3.2.2. bellow.

For cybersecurity examples of these instruments are found in domestic criminal laws and at EU level also in the use of an 'Information and Communication Technology cybersecurity certification'[9].

Finally, in some cases, due to reasons of national security, countries have also restricted the access to data flows that contain a political or cultural banned content. For instance, "Russia and China have repeatedly asserted sovereign control over free flow of information to block or filter information that could be harmful to the cultural or moral ethos of the country, or for purposes of national security. This idea of 'national sovereignty' in cyberspace (or 'cyber sovereignty') entails governments 'governing' the internet and the multi-stakeholder community playing only a secondary role" (Mishra 2019:14). These restrictions may influence the rule of law mainly on the right to be informed and the freedom of press. Therefore, it can be argued that it is not always clear how these restrictions enhance the protection of personal and business data since in some countries the free flow of data will be restricted but mainly for political reasons (Mishra 2019:10-11).[10]

## 3. Challenges: Data and Big Data in Taxation

### 3.1.1. Exchange of Information and Collection of Personal and Business Data

At international level, governments have agreed to exchange information first on request and since 2013 (as introduced by the Organization for Economic Cooperation and Development (OECD) with the political support of the G20) also automatic exchange of financial accounting information.[11] For this purpose, different bilateral and multilateral instruments[12] have been used

[9] This certificate has been proposed in the framework of the EU Cybersecurity Act approved on 10 December 2018 http://europa.eu/rapid/press-release_IP-18-6759_en.htm (Accessed 9 February 2019). This is an "EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. The certification will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements. The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.". Information available at https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (Accessed 9 February 2019)

[10] Mishra rightly argues that "Measures restricting data flows can also be examined in light of the nature of the measure and its underlying objective. Certain measures restrict data flows based on the nature or content of the digital service and underlying data flows, for example, preventing supply of digital services that contain politically or culturally sensitive or banned content. For example, the restriction on the supply of Virtual Private Network ('VPN') services in China is intended mainly to ensure a clean internet environment within the country in line with its public morals and order interests. Similarly, Korea bans cross-border transfer of mapping data, and thereby, significantly reduces business opportunities for location-based applications such as Google Maps".

[11] The standard of transparency including exchange of information on request was endorsed in the G20 Summits in Washington, London and Pittsburgh, and G8 Summits in L'Aquila and Lecce (Italy); Hokkaido (Japan). The G20 meeting of Sept. 2013 in Saint Petersburg endorsed the development of a new global tax standard i.e. automatic exchange of information. Tax Annex to the St. Petersburg G20 Leader's Declaration, para.3 (G20 2013).

[12] For an overview of the developments in exchange of information see http://www.oecd.org/ctp/exchange-of-tax-information/ (Accessed 9 February 2019)

including art. 26 of the OECD Model (DTC) used in Bilateral Tax Treaties (OECD 2017); Bilateral Tax Information Exchange Agreements (TIEAs); and the Multilateral Convention on Administrative Assistance in Tax Matters (MAC) which at the time of writing (February 2019) has been signed by more than 120 jurisdictions.[13]

In addition, under art. 6 of the MAC, two Multilateral Competent Authority Agreements have been agreed the first one to introduce the standard on automatic exchange of financial accounting information (signed by 140 jurisdictions[14]) and the second one to facilitate the exchange of country by country reporting (signed by 76 jurisdictions).[15] The aim of these instruments is to tackle tax evasion and tax avoidance including aggressive tax planning. [16]

At European level, the most important instrument to facilitate exchange of information in taxation is the Directive on Administrative Cooperation (2011/16/EU).[17] This Directive has been amended 5 times to make possible (i) automatic exchange of financial accounting information (2014/17/EU); (ii) automatic exchange 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[18] (2018/822/EU) (Council 2011, 2014, 2015, 2016, 2016a, 2018).

These amendments increase the amount of information exchanged within the EU. For the EU, "Administrative cooperation in direct taxation between the Competent Authorities of the EU Member States helps to ensure that all taxpayers pay their fair share of the tax burden, irrespective of where they work, retire, hold a bank account and invest or do business".

---

[13] List of jurisdictions participating in the Convention available at http://www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf (Accessed 9 February 2019)

[14]Information available at http://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/MCAA-Signatories.pdf (Accessed 9 February 2019)

[15] Information available at http://www.oecd.org/tax/automatic-exchange/about-automatic-exchange/CbC-MCAA-Signatories.pdf (Accessed 9 February 2019)

[16] The need for more instruments for exchange of information increased since 2013 when news media around the world highlighted a steady decrease in contributions to public finances by many high-profile multinational companies and high net worth individuals. Concerning individuals, the decrease was associated to the use of offshore tax havens. Concerning multinationals, this decrease was associated with sophisticated (aggressive) tax planning techniques to shift otherwise taxable income and transactions out of the tax base. One example is the Canadian Revenue Agency on International Tax Gap and Compliance report (June 2018), where it was estimated that in 2013, the stock of hidden offshore wealth held by Canadians was between $75.9 billion and $240.5 billion. Canadian individuals were hiding this money in offshore tax havens, and not paying tax on it. See Section 4.1. International Tax Gap and Compliance Results for the Federal Personal Income Tax System https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/tax-canada-a-conceptual-study/tax-compliance.html (Accessed 9 February 2019)

[17] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en#heading_2
(Accessed 9 February 2019)

[18] An intermediary can be either an individual or a company (i.e. accountants, advisers, lawyers, banks, etc.). https://ec.europa.eu/taxation_customs/sites/taxation/files/dac-6-council-directive-2018_en.pdf (Accessed 9 February 2019)

At national (domestic) level, information is also being disclosed to the public. For instance, politicians may voluntarily disclose their tax return, or the tax administration can disclose the information prior request of any person exercising the right to access to public information (Nguyên-Duy 2016).[19] Furthermore, tax administrations are exchanging data for instance in joint audits between officials from two (countries) tax administrations (Burgers – Criclivaia 2016), or in informal join meetings to analyze taxpayer data taking place at the location of one tax administration.[20]

Another development that it is important to mention is the introduction by the United States of the Foreign Account Tax Compliance Act ("FATCA") to exchange financial account information of US taxpayers. 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. [21]

The introduction of automatic exchange of information as the global standard in 2013 and the use of multilateral instruments to exchange information result on information (personal and business data) being exchanged at a fast pace around the world. In the past, exchange of information will only take place if there was a bilateral agreement/instrument making possible the exchange of information (e.g. art. 26 OECD Model in bilateral tax agreements or Tax Information Exchange Agreements) and for specific purposes (to tackle tax evasion).

These instruments allowed the disclosure of information (on request) between authorities of two countries (including courts and administrative bodies) dealing with the assessment, collection, enforcement, and/or prosecution in respect of taxes. The information exchanged could only be disclosed to a third country with the authorization of the Supplying State (country providing the information).

Nowadays, information is not only provided by the taxpayer but also information is provided by intermediaries (e.g. tax advisors, accountants, lawyers, bank). This information is not only provided to one country in a bilateral relationship, but it can also be sent (automatically) to other countries due to the two Multilateral Competent Authority Agreements for automatic exchange of financial accounting and for country by country reporting.

In light of these developments, it can be safely argued that the multilateral instruments and the flows of information exchanged makes more difficult to prevent leaks to third parties and to prevent the misuse of the information by the countries or government officials for other purposes than the ones for which the information has been exchanged (Debelva - Mosquera Valderrama 2017).

### 3.2. Instruments and challenges for data protection and privacy

[19] This is for instance the case of Norway due to the Freedom of Information act enacted in 2006. This Act gives the right to access (certain) public documents, as well as records of public administration, at the national and local level. This means also that taxpayer income tax returns and registration of property can be accessed by any person.

[20] 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.

[21] The 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 9 February 2019)

### 3.2.1. Data Protection Laws

Notwithstanding the use of multilateral instruments to exchange information, the safeguards to protect personal/business data and privacy are left to the individual country. These safeguards are mainly in the Constitution (right to privacy) or in data protection laws. Furthermore, even if the data protection law exists, this may be obsolete to regulate the current developments of data processing, automatic exchange of information and use of big data. For instance in a study carried out by this author of 4 countries, Uruguay, Brazil, Colombia and South Africa it was concluded that the data protection laws were mainly based on the 1995 Data Protection Directive which makes these laws nowadays obsolete in accordance to the current developments on digital trade, internet governance and tax information exchange.

Therefore, countries around the world should revisit their data protection laws to provide more protection for taxpayers. One way is to use the new EU Data Protection Regulation provisions by introducing in the domestic law, provisions containing specific definitions of personal data, genetic data and biometric data (art. 3) and regulating the protection of the processing of these data as special categories of personal (sensitive) data (art. 10).[22] Another way is by signing on a multilateral instrument for data protection for instance the Council of Europe Convention No. 108 that will be addressed in the following section.

Finally, following this Convention 108 and some other instruments (OECD 1980, 2012, 2013) [23], this author and Debelva (2017) proposed to introduce the following safeguards to guarantee privacy, data protection and confidentiality in taxation:

"(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" (Develba – Mosquera Valderrama 2017:381). However, in order to introduce these safeguards, political will and compromise from countries around the world is needed.

### 3.2.2. The Council of Europe Convention No. 108 for the protection of individuals with regard to Data Protection Laws[24]

[22]" If one example may illustrate this is for instance the conditions for lawful processing of data and the transfer of personal data to third countries (Mosquera Valderrama – Mazz – Schoueri – Quiñones – Roeleveld – Pistone – Zimmer 2017:20).

[23] The 1980 (updated in 2013) OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data and the 2013 OECD report on the protection of confidentiality of information exchanged for tax purposes.

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

One of the most important challenges in the era of digital trade, internet governance and tax information exchange is the protection of the processing of personal and business data. Until now, the efforts have been mainly directed towards domestic or EU regulations to regulate data protection, but since data flows all around the world, there is a need for multilateral instruments.

The Convention No. 108 (Council of Europe 1981)[25] is the only binding multilateral instrument that can potentially have a worldwide application, since the 2001 Protocol opened this Convention to countries non-members of the Council of Europe (third countries). However, in practice the scope of application is limited since it applies only to personal data (thus no business data) and at the time of writing only few third countries have ratified this Convention. As of December 2018, 6 countries i.e. Cabo Verde, Mauritius, Mexico, Senegal, Tunisia, Uruguay have ratified this Convention.[26] Therefore, from the 193 countries around the world 53 countries (47 countries members of the Council of Europe and 6 third countries) have ratified this Convention.

The Convention No. 108 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. Furthermore, in order to modernize this Convention and address the challenges of big data, the 2018 Protocol amending the Convention No. 108 was approved in May 2018 and open for signature as of 25 June 2018. [27] The modernization of Convention 108 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.[28]

In respect of big data, art. 11 of the 2018 Protocol introduces new rights for the persons in an algorithmic decision-making context, which are particularly relevant in connection with the development of artificial intelligence. For instance: (i) in order to obtain confirmation of the processing of personal data on request, at reasonable intervals, and without excessive delay or expense, the communication of the processed data must take place in an intelligible form in order to ensure the transparency of processing and (ii) the data subjects have the right 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.

In addition, art. 12 of the 2018 Protocol introduce additional obligations for signatory countries, mainly regarding big data. These obligations include: (i) the implementation by controllers/processors of technical and organizational measures, which take into account the

---

[25] "The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data" (Council of Europe 1981).

[26] However, 3 countries have also asked for access to the Convention which at the time of writing (February 2019) is pending of approval i.e. Argentina, Burkina Faso and Morocco. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa (Accessed 9 February 2019)

[27] At the time of writing (February 2019), this new Protocol has been signed by 24 countries of the Council of Europe and 1 third country (Uruguay) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (Accessed 9 February 2019)

[28] See website modernisation of the Convention available at https://www.coe.int/en/web/data-protection/convention108/modernised (Accessed 9 February 2019)

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.

However, one drawback is that this convention is only applicable to personal data by individuals, and therefore, the protection of business data or any other data by companies is left to the domestic laws of the countries. However, since the focus of the domestic law is also personal data, the protection of business data should be also addressed at a multilateral level. One way could be to introduce a protocol to this Convention 108 (Council of Europe 1981) for the protection of business data.

## 4. Conclusions and Recommendations

Nowadays, data is being collected, exchanged and used in small or large amounts by governments, international organizations and companies for medical, educational, social, industrial and tax purposes amongst others.

This article concludes that in this era of digital trade, internet governance and tax information exchange, the current instruments used to guarantee the privacy and the data protection of individuals and business are not sufficient and are limited in their application and enforcement. For instance, domestic data protection rules can be obsolete if the rules do not follow the new technological developments in data such as the use of biometric data, or genetic data. In other cases, even though the rules exist and are up to date, there is a lack of enforcement of these rules as shown in the Facebook Cambridge analytic scandal where neither the US-EU Privacy Shield nor the EU General Data Protection Regulation were able to introduce sanctions to Facebook. In some countries, these rules are used to ban the use of data flows that contain a political or cultural content and therefore, restricting the freedom of information.

The protection of personal data and privacy and the use of big data calls for a new multilateral instrument that takes into account the processing of data in a world of big data such as the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data which was opened to third (non-EU countries) in 2001 Protocol. Up till the time of writing only 6 non-EU countries have signed this Convention and therefore, non-EU countries are losing an opportunity to participate in this Convention and to provide more safeguards and protection for the automatic processing of personal data. The 2018 Protocol has amended this Convention 108 to address the challenges of big data. One of the drawbacks of this Convention 108 and its 2018 Protocol is that it only protects automatic processing of personal data (individuals). Therefore, in order to guarantee the protection of companies, it is recommended to introduce a Protocol to this Convention 108 to address the protection of business data.

More data means more responsibilities for all actors involved in the collection, processing, and analysis of this data. If the use of big data is relevant to enhance the countries' democratic

processes and compliance with rules, the protection of the processing of this data (including personal and business data) is also relevant in order to enhance the rule of law. Therefore, the challenge for governments is to adopt the Convention 108 while, at the same time introducing safeguards to guarantee the safe and adequate use of personal and business data.

**References**

**Council of Europe**. 1981. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol (Accessed 9 February 2019)

**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.

**Burgers I. J. J. – Criclivaia D.**. 2016. "Joint Tax Audits: Which Countries May Benefit Most?" In *World Tax Journal* 8, no.3: 306-355.

**European Commission**. 2016. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Available at: https://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj. (Accessed 9 February 2019)

**European Parliament – Council**. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Regulatio). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Accessed 9 February 2019)

**European Parliament.** 2018. *Facebook-Cambridge Analytica: MEPs demand action to protect citizens' privacy.* Press Release. Available at: http://www.europarl.europa.eu/news/en/press-room/20181018IPR16525/facebook-cambridge-analytica-meps-demand-action-to-protect-citizens-privacy (Accessed 9 February 2019)

**European Parliament.** 2018a. Resolution 2018/2855(RSP) of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection. Available at: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2018/2855(RSP) (Accessed 9 February 2019)

**European Union Council**. 2011. Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC. Available at: http://data.europa.eu/eli/dir/2011/16/oj (Accessed 9 February 2019)

**European Union Council**. 2014. Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation. Available at: http://data.europa.eu/eli/dir/2014/107/oj (Accessed 9 February 2019)

**European Union Council**. 2015. Council Directive (EU) 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation. Available at: http://data.europa.eu/eli/dir/2015/2376/oj (Accessed 9 February 2019)

**European Union Council**. 2016. Council Directive (EU) 2016/881 of 25 May 2016 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation. Available at: http://data.europa.eu/eli/dir/2016/881/oj (Accessed 9 February 2019)

**European Union Council**. 2016a. Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities. Available at: http://data.europa.eu/eli/dir/2016/2258/oj (Accessed 9 February 2019)

**European Union Council**. 2018. Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements. Available at: http://data.europa.eu/eli/dir/2018/822/oj (Accessed 9 February 2019)

**G20**. 2013. "G20 Leader's Declaration St. Petersburg on September 6, 2013". Available at: http://www.g20.utoronto.ca/2013/2013-0906-declaration.html (Accessed 9 February 2019)

**Kozlowska I.**. 2018. "Facebook and Data Privacy in the Age of Cambridge Analytica", Blogpost. Available at https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/ (Accessed 9 February 2019)

**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.* DOI 10.1016/j.clsr.2017.05.011.

**Mishra N.**. 2019. "Building Bridges: International Trade Law, Internet Governance and the Regulation of Data Flows". In *Vanderbilt Journal of Transnational Law*. Forthcoming 2019.

**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. (Accessed 9 February 2019)

**Mosquera Valderrama I.J. – Affuso O. – Coco A..** 2019. "A Multidisciplinary regulatory approach to big data and the rule of law". Blogspot. Available at: https://globtaxgov.weblog.leidenuniv.nl/2019/01/01/a-multidisciplinary-regulatory-approach-to-big-data-and-the-rule-of-law/ (Accessed 9 February 2019)

**Nguyên-Duy I.**. 2016. "The Norwegian Freedom of Information Act – A not so Transparent Act?. *In Revue Internationale des Gouvernements Ouverts [S.l.]* 2:77-100. Available at: http://ojs.imodev.org/index.php/RIGO/article/view/10/71 (Accessed 9 February 2019)

**OECD**. 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Accessed 9 February 2019)

**OECD.** 2012. Keeping It Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes. Available at: http://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe.htm (Accessed 9 February 2019)

**OECD.** 2013. The OECD Privacy Framework. Available at: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (Accessed 9 February 2019)

**OECD.** 2017. Text art. 26 OECD Model and 2017 Commentary on article 26. Available at: https://www.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017/commentary-on-article-26_mtc_cond-2017-29-en (Accessed 9 February 2019)