FIRE Conference
Proceedings from
the First Annual International
FIRE CONFERENCE
10th–11th of November 2022
Örebro University
Sweden

EDITOR
MAGNUS KRISTOFFERSSON
# Table of Contents

Preface 7

The Authors 11

*Magnus Kristoffersson*
Chapter 1
An Overview of the FIRE Research Project 15

*Rigmor Argren*
Chapter 2
Using the European Convention on Human Rights to Shield Citizens from Harmful Datafication 43

*Giovanni Botto*
Chapter 3
Blockchain and European Administrative Integration: a Reflection on Public Governance and Technology, Starting from the European Competition Field 61

*Clémence Garcia and Takeo Itabashi*
Chapter 4
An Experiment on Double Entry Bookkeeping and Financial Reporting Using Blockchain 75

*Hanna Grylin*
Chapter 5
Income taxation of forestry, forest deduction and digitalization 93

*David Hadwick*
Chapter 6
Breaking the Fiscal Omerta: The Roadmap to Transparency in EU Tax Algorithmic Governance 107
Table of Contents

Jan Kellgren
Chapter 7
The Current Corporate Income Tax Rule Architecture & Automated, Real-Time Taxation – Would the Necessary Prerequisites of Today’s Tax Rules Have to Be Changed? 127

Eleonor Kristoffersson
Chapter 8
ViDA – VAT in the Digital Age 143

Yurii Orzikh
Chapter 9
Accounting Regulation and Financial Reporting under Ukrainian Legislation 153

Mais Qandeel
Chapter 10
Blockchain Application in Information Ecosystems: The Right to Privacy in Cyberspace 177

Francesco Paolo Schiavone
Chapter 11
The Free Movement of Capital within The EU and Digitalisation: The Role of Cryptocurrencies 193

Vadym Tsymbal
Chapter 12
The Digitalization of Governance and Tax Administration in Ukraine 209

Sam van der Vlugt
Chapter 13
Ensuring an Inclusive Shift Towards a Technology-Driven Dialogue Between Taxpayer and Administration: How the Law Can Benefit from a Different Methodology 229

Anna Husman
Chapter 14
Automation in the Public Sector and the Principle of Non-Discrimination 249
Preface

In the autumn of 2021, the decision was made to begin work on the research project known as FIRE, which stands for the Financial Information Retrieval Ecosystem. The concept was developed through collaboration with a young, innovative FinTech start up. From a legal perspective, I was asked to evaluate a business model that involved a system that was developed to make more effective use of transportation that was either empty or only partially loaded. The project’s goal was to create a mobile application that would improve efficiency in the use of vehicles that were already on the road. In addition, one of the primary goals of the project was to develop a system that would enable the ordering, billing, and payment processes to be carried out within the logistics system. During this process, I came to the realization that many different kinds of financial information have already been digitalized to a significant extent, and that the trend of digitalization is rapidly expanding.

Moreover, the Organization for Economic Cooperation and Development (OECD) released a report in the year 2020 titled “Tax Administration 3.0.” Within this report, the OECD’s Forum on Tax Administration presents their perspective on what the future of tax administration will look like (OECD TA 3.0, 2020). Tax Administration 3.0 involves digitizing and automating the flow of data, which makes it possible to determine and pay taxes in real time. The OECD’s vision goes beyond financial data and includes for example the use of GPS coordinates as an example of information that could be used for tax assessments. This is just one example of how the OECD’s vision could be realized. The phrase “Tax Just Happens” refers to the end goal of Tax Administration 3.0, which is to achieve a state in which taxation is so seamlessly integrated into individual transactions that taxpayers may not even be aware that they are being taxed. This is the “Tax Just Happens” state (OECD TA 3.0, 2020).

The Nordic Smart Government & Business (NSG&B) initiative is yet another significant endeavour that connects to the FIRE project. The goal
of the NSG&B program, which is a collaboration between 14 Nordic organizations, is to make the region of the Nordic countries the most digitally advanced business region in the entire world by the year 2030. The central concept is that all corporate related information in regard to SME's in the Nordic Region should for real become digitalized. The FIRE project has a significant amount of interest in the NSG&B approach.

In 2022, Örebro University was the site of three international events—two international workshops, one international and interdisciplinary conference—all of which were funded by the Riksbankens Jubileumsfond. A large number of researchers, hailing from ten different countries, presented their findings at the conference. Their fields of study included business and administration, law, psychology, computer science, and social work. By working together, we have successfully established a global research consortium centered on the FIRE project. This anthology includes some of the proceedings from the conference.

The first chapter of the book, penned by me, serves as an overview of the FIRE project idea, outlining the research project. In the second chapter, Rigmor Argren, a PhD and Senior Lecturer, guides readers through aspects of human rights and harmful digitalization. The third chapter features a contribution from Doctoral Candidate Giovanno Botto who presents an article about blockchain.

The fourth contribution emanates from Professor Clemence Garcia and her husband, Associate Professor Takeo Itabashi. Their report covers an experiment that uses Distributed Ledger Technology as a tool for double-entry bookkeeping and financial reporting.

The fifth chapter sees Doctor of Laws and Senior Lecturer Hanna Grylin share insights on forest taxation and some associated technological perspectives. In his article titled “Breaking the Fiscal Omerta: Roadmap to Transparency in EU Tax Algorithmic Governance,” Doctoral Candidate David Hadwick divulges how artificial intelligence tools are employed within tax administration.

Chapter seven features a contribution from Professor Jan Kellgren, who shares thoughts on how current corporate income tax rules relate to real-time taxation. In the subsequent chapter, Professor Eleonor Kristoffersson introduces the ViDA proposal, elucidating how it will digitalize Value Added Tax.
Chapter nine, penned by Guest Researcher and Associate Professor, Yurii Orzikh, offers an introduction to the digitalization of Ukrainian accounting regulation. The tenth chapter, written by PhD and Senior Lecturer, Mais Qandeel, navigates us through blockchain use for information ecosystems and the right to privacy in cyberspace.

In chapter eleven, Doctoral Candidate Francesco Paolo Schiavone discusses the free movement of capital within the EU and cryptocurrencies. We return to Ukraine in chapter twelve, where Guest Researcher, Vadym Tsymbal, contributes an article on Ukrainian tax administration and digitalization.

In the penultimate chapter, Doctoral Candidate Sam van der Vlugt offers a philosophical perspective on technology, digitalization, and tax administration. The final contribution to the anthology is a student paper by Anna Husman, supervised by Mais Qandeel. Anna, who won the student speech contest at the conference, delves into automated decision-making and the principle of non-discrimination.

I hope you will enjoy reading this!

Örebro 26 of June 2023

*Magnus Kristofferson, editor*
The Authors

Rigmor Argren is a Senior Lecturer of Public International Law, Örebro University, Sweden. She holds a Ph.D. in International Human Rights Law (2012) and a LL.M. in International Human Rights Law (2003) both from Essex University, as well as a Master of Communications from Örebro University (2004). Her main areas of research are international human rights law (IHRL), international humanitarian law (IHL), and the intersection of IHRL and IHL.

Giovanni Botto is a doctoral student (PON) in Security, Risk and vulnerability (curriculum Security and law) – University of Genoa.

Professor Clemence Garcia, with a Ph.D. in Business Administration from Paris Dauphine University, is a tenured faculty member at Gakushuin University, Japan. Her main research areas are accounting for intangibles and tax law.

Dr. Hanna Grylin is a senior lecturer at University of Gävle, Sweden. Her main areas of research are tax law and tax procedural law.

David Hadwick is a doctoral researcher at the Centre of Excellence DigitaTax of the University of Antwerp and a Fellow at the Research Foundation for Flanders (Grant n° 11J1524N). His main areas of research are tax law, digital constitutionalism, and public algorithmic governance.

Anna Husman is a Bachelor graduate in Legal Science from Örebro University with a specialisation in digitalisation, with a background in different technology areas such as programming software, Artificial Intelligence, Kali Linux and more. She is currently working on achieving her Advanced LL.M. in Law and Technology from Leiden University.
The Authors

Associate Professor Takeo Itabashi, with a Ph.D. in Economics from Kyoto University and an MBA from Paris Dauphine University, is a tenured faculty member at Tokyo Keizai University, Japan. His main research interests are tax accounting and digitalization, in particular blockchain-based accounting databases.

Professor Jan Kellgren, who holds an LL.M. and an LL.D. from Uppsala University, is professor of tax law at Linköping University, Sweden, and also affiliated professor at Örebro University, Sweden. His main area of research is corporate taxation.

Professor Eleonor Kristoffersson, who holds an LL.M. from Gothenburg University and an LL.D. from the Jönköping Business School, is the research leader of the law subject at Örebro University.

Associate Professor Magnus Kristoffersson (editor), who holds an LL.M. and LL.D. from Uppsala University, is a senior lecturer at Örebro University, Sweden. In addition to being the project leader for the FIRE project, his main areas of research are tax law, digitalization, and public law.

Associate Professor Yurii Orzikh, Ph.D. from National University “Odessa law academy”, is a researcher at Örebro University, Sweden. In addition to being the project participant for the FIRE project, his main areas of research are private law, application of law and tax law.

Dr. Mais Qandeel is a Senior Lecturer of Law and Technologies at Örebro University, Sweden. She is also an affiliated Guest Researcher at iHub: Interdisciplinary research hub on digitalization and society at Radboud University, The Netherlands. Qandeel’s main research focuses on the contemporary challenges of human rights in cyberspace and on environmental issues within international law. She holds a Ph.D. from University of Fribourg, Switzerland.

Francesco Paolo Schiavone, Ph.D. Candidate in Tax Law at Department of Law – University of Naples “Federico II”. His main areas of research are Tax law, financial law and digitalization.
Dr. Vadym Tsymbal, who holds an LL.M. and LL.D. from the National Tax Service University of Ukraine, is a researcher at Örebro University, Sweden. With extensive practical experience in the implementation of participatory practices in local governance, his research encompasses legal, political, and societal aspects of transitional processes. He specifically focuses on studying digitization and tax policy of modern-day Ukraine.

Sam van der Vlugt holds an LL.M. in Tax Law from the Erasmus University of Rotterdam, and an LL.M. in European Union Law from the University of Amsterdam. He is a joint-PhD student at the university of Salerno and the university of Antwerp. At the former he is connected to the Laboratorio Giuridico and at the latter he is part of the DigiTax Centre of Excellence.
Chapter 1
An Overview of the FIRE Research Project

Abstract: This article presents a concise overview of the Financial Information Retrieval Ecosystem (FIRE) project. In the article an overview of the technological cornerstones of FIRE, its potential legal implications, stakeholder perspectives, and its influence on various professions, with a particular emphasis on the underlying technologies propelling this initiative. The FIRE project also suggests that both mandatory book-keeping and annual reporting might be possible to abolish in the future.

1.1 Introduction

The Financial Information Retrieval Ecosystem (FIRE) model advocates for the utilization of contemporary technology to transition from traditional book-keeping and annual reporting practices. This model encourages the provision of real-time access to unprocessed financial data of significant relevance to stakeholders. The aim is to allow each stakeholder to process and interpret this data according to their unique needs and objectives.

FIRE introduces a reversed approach in informing stakeholders about company affairs. Instead of receiving curated, periodic financial reports, stakeholders get direct access to the “raw data”, empowering them to draw their own insights and make timely decisions.

In my perspective, the FIRE model carries an array of advantages, leveraging the power of modern technology to enhance transparency, immediacy, and autonomy in financial data management. Furthermore, it appears that the evolution of various technologies has reached a critical point, enabling the possibility of a paradigm shift in financial data
Magnus Kristoffersson

handling. This paradigm shift would mark a significant departure from conventional methods, opening up new possibilities for stakeholder engagement and data-driven decision making.

In this article, I will share my thoughts on the FIRE project. It is important to note that the following opinions are solely my own. I recognize that the researchers associated with the FIRE consortium have their own unique perspectives, which may differ to some extent. Among us, there are those who hold a critical view of the project’s development, with a focus on the risks associated with digital information flow and technology based on Artificial Intelligence (AI). Conversely, there are others who maintain an optimistic outlook and believe that the opportunities outweigh the risks. Despite our differing viewpoints, our common ground lies in the study of the same phenomenon: the increasing digitalization of information of financial significance and the continuous evolution of technology.

The article is structured as follows: Section 1.2 provides an overview of the design of the FIRE project. Section 1.3 focuses on defining information of financial significance. In Section 1.4, a discussion is presented from the perspective of stakeholders. Section 1.5 briefly describes the developments in business intelligence. Section 1.6 explores the implications of the FIRE model. Section 1.7 delves into the role of technology. Section 1.8 addresses certain legal aspects. Finally, Section 1.9 concludes the article with closing remarks.

1.2 The Design of the FIRE project

The FIRE project consists of two main research tracks. Firstly, it examines the impact of digitalization and technological advancements on existing systems, such as external financial reporting and taxation. Additionally, the project explores the broader societal implications of technology. In the context of the FIRE project, external financial reporting encompasses all types of reports that companies are required to prepare and submit, including annual reports and tax returns.

Secondly, the project also involves the development of a hypothetical model called the “FIRE model.” This model aims to shift the responsibility of refining financial information from the auditees (companies) to
the stakeholders who utilize the information. The overall research strategy is comprehensive and addresses various complex concerns. It could be argued that the FIRE initiative focuses more on forming a research consortium rather than solely conducting one large research project.

As a starting point, audited entities produce most external financial reporting of various types today. The audited entities may be individuals or legal entities. However, the FIRE project is mainly concentrated on company-related information. Questions about personal data regarding natural persons are included in the FIRE framework to the degree that they may be included in the company-related data. For example, personal information about a natural person can be included in invoicing details, which covers the interest in FIRE-related research.

Annual reports play a crucial role in external financial reporting, as corporations are required to produce and make them public (Trites, P., 2021). In Sweden, the Swedish Companies Registration Office is responsible for receiving, storing, and publicizing these reports, as stated in Chapter 8, Paragraph 1 of the Annual Reports Act (ARA) (Årsredovisningslagen (1995:1554)).

Furthermore, companies listed on a stock exchange market are also obligated to prepare and submit interim reports in accordance with Chapter 16 of the Securities Act (SA) (lagen (2007:528) om värdepappersmarknaden). These reports typically rely heavily on numerical data to evaluate the company’s operational position, performance, and management.

Over time, a relatively complex regulatory system has evolved for annual reports, with a primary focus on establishing a rational foundation for economic decision-making (Trites, P., 2021).

Declarations, which can be considered a type of financial report, are also submitted for tax purposes. These include annual income tax returns, monthly/quarterly/yearly VAT returns, and social security tax returns. The relationship between accounting and taxation varies across jurisdictions (Nobes, C., & Parker, R., 2020). In some countries, like Sweden, there is a close connection between accounting principles and taxation (Knutsson, M., et al., 2013). For example, the income taxation of corporations in Sweden is partly influenced by accounting rules (Income Tax Act, Chapter 14, Paragraphs 2 and 4). In contrast, in other countries
like Germany, the income taxation of corporations is not directly linked to accounting practices (Nobes, C., & Parker, R., 2020).

Today, many of these reports are compiled by companies themselves, often involving complex and subjective evaluation components (Berg, P., 2020). As a result, businesses often rely on external experts such as accountants, auditors, tax consultants, and other specialists for assistance. Larger companies frequently utilize sophisticated data systems to facilitate their reporting processes (Trites, P., 2021).

The self-reporting system described should be viewed in the context of the growing interest and need for business intelligence and analysis (Sheng, J., et al., 2019). Many companies, both small and large, recognize the importance of retrieving, producing, and utilizing digital data for decision-making (Wiener, M., 2020). Credit ranking reports have become more sophisticated and comprehensive over time (Chen, Y.-J., & Chen, Y.-M., 2022). Stakeholders have come to appreciate the value of more extensive information beyond what is available in traditional external financial statements. External reports can also be verified or cross-checked against more impartial sources.

In several domains, the FIRE model is already being utilized to some extent. One notable example is the taxation of individuals’ employment income. In Sweden, individuals are required to file a tax return, but the Swedish Tax Agency has simplified the process by providing prefilled income tax returns based on information obtained from employers and other third parties, such as banks. In most cases, taxpayers only need to review and accept the prefilled tax return.

Another instance where stakeholders refine information is the availability and development of various business analysis tools. These tools, supported by diverse AI-based technologies and access to vast amounts of relevant information, assist in making informed financial decisions.

In summary, it is important to further investigate the impact of digitized financial information from a different perspective. This includes examining how this technological shift affects the current standard model for external financial reporting and exploring alternative models such as the FIRE model.
1.3 Defining “information of financial significance”

In section 1.1, I intentionally used the term “information of financial significance” as a crucial aspect of the FIRE project’s focus. This deliberate choice is because the project goes beyond the study of purely digitized financial information. As highlighted in the introduction, the OECD’s report on Tax Administration 3.0 emphasizes that information beyond purely financial data can also have implications for taxation (OECD TA 3.0, 2020). For instance, the collection of Value Added Tax (VAT) can be influenced by factors such as whether a product crosses national borders. In such cases, GPS positioning data from a truck transporting goods could directly impact taxation decisions.

Non-financial data, often referred to as side data, also play a crucial role in economic decision-making (Chen, Y.-J., & Chen, Y.-M., 2022), such as assessing a company’s future performance or considering an investment opportunity. Various factors, including a company’s management, are assumed to have financial significance and influence decision-making.

Defining the specific information relevant to economic decision-making is challenging today (Spektor, M. S., & Seidler, H., 2022). It largely depends on the tools available to stakeholders. With manageable amounts of data, stakeholders can produce more refined decision-making foundations when they have access to extensive information. However, it is essential to consider fundamental principles such as data integrity and careful handling, even as automated systems capable of handling vast amounts of data emerge. The General Data Protection Regulation (GDPR) already sets clear requirements for the lawful and minimal processing of personal data. Similar objectives could be pursued for corporate-related data, as companies are ultimately associations/cooperations between individuals, and data about companies indirectly reflects the individuals connected to them.

Within the FIRE project, the assumption is that stakeholders are interested in accessing as much information as possible. From this perspective, virtually all information could be considered of financial significance in some way. However, considering privacy perspectives, an important objective of the project is to explore what information is sufficient for
rational financial decision-making for different stakeholders. Defining the boundaries of “information of financial significance” will be a significant task for the research consortium. These boundaries may be based on legal considerations, expediency, or the necessity for stakeholders to be adequately informed. This work is facilitated by the project’s interdisciplinary nature and the participation of researchers from various scientific disciplines.

The starting point of the FIRE project is that the concept of “information of financial significance” is still in a conceptual stage. The core focus of the project can be described as the information required to generate current financial statements. Many research activities within the project are based on this type of information. However, it is evident that “information of financial significance” encompasses a broader range of data than what has been mentioned thus far. In this regard, the FIRE project represents a forward-looking effort to identify and establish the scope of information that should be considered as falling within the definition of “information of financial significance.

1.4 The Stakeholders’ Perspective

1.4.1 General

The FIRE project primarily concentrates on digitalized corporate information of financial significance and investigates the influence of technological advancements on financial reporting, with a particular focus on the stakeholder perspective. The main objective of external financial reporting is to meet the information requirements of stakeholders. Therefore, a key aspect of the FIRE project is to conduct a detailed examination of the stakeholders and their specific information needs. In this section, I will explore stakeholder models and provide two examples of discussions regarding information needs.

1.4.2 Different Stakeholders Groups

Traditionally, stakeholders are divided into different groups. Following is an example of different stakeholder groups:
• Authorities (including Tax Authority)
• Banks
• Competitors
• Customers
• Employees
• Other lenders
• Shareholders
• Stock Exchange Market
• Suppliers

It can be presumed that different stakeholder groups have distinct information interests. Additionally, within a specific stakeholder group, there may be variations among its members. Despite being categorized under the same stakeholder group, the information interests of different stakeholders can vary (Trites, P., 2021). This highlights the challenge with the current central paradigm, where a single financial report is expected to fulfil the information needs of diverse stakeholders. What may be considered relevant information for one stakeholder could be irrelevant or less significant for another.

Another perspective to consider in the stakeholder discussion is the advantage that businesses gain from accessing and utilizing data (Fast, V., et al., 2023). The benefit tends to increase when a particular stakeholder has exclusive access to certain data. Furthermore, data collection itself has become a standalone business model (Wiener, M., et al., 2020). Established sectors have recognized the value of collecting data on both existing and new client groups to enhance corporate value (Chen, H.-M., et al., 2016). Consequently, stakeholders already have a tendency to collect information independently of what is provided by the auditees (companies).

Certain stakeholder groups are interested in more than just financial information. In recent years, there has been an increased focus on various sustainability issues related to corporate activities (Remlein, M., 2021). For example, some stakeholders may place a premium on a company’s climate-friendly practices. It can be challenging to assess the environmental impact of a company’s operations and to what extent they contribute to sustainability goals using only financial data. Access to additional information is necessary to improve the decision-making process.
Currently, only relatively large enterprises are required to file sustainability reports. The administrative burden is the primary reason why only larger firms are mandated to submit such reports. However, it is difficult to argue that access to this type of information would be less valuable for some stakeholders of smaller enterprises. If such information were readily accessible, it would undoubtedly be of great importance to a considerably broader audience.

A fundamental concept of the FIRE project is the alignment of financial information reporting with stakeholders’ information requirements. Therefore, there is significant value in analyzing different stakeholder groups and individual stakeholders. When applying stakeholder models to current accounting and reporting regulations, a critical question arises: do these regulations contribute to the creation of reports that provide stakeholders with the necessary information?

For instance, accounting and reporting standards only partially fulfill the needs of taxation due to an inherent conflict between the information requirements of various stakeholder groups. Additionally, there may be a disparity in information needs between existing shareholders and potential shareholders. In many cases, accounting standards should be designed for the group of potential owners to ensure that the results and financial position are not inflated. Existing shareholders are concerned that the financial statements do not present an overly negative portrayal of the company and its operations. Striking a balance between these competing interests is crucial.

By examining these dynamics, the FIRE project aims to address the challenge of meeting diverse stakeholder information needs while ensuring the accuracy and reliability of financial reports.

1.4.3 Examples of Stakeholders’ informational requirements

1.4.3.1 Introduction

Different stakeholder groups are presumed to have distinct information needs. In today’s digitally driven and technologically advanced society, there is a widespread interest in information of financial significance. While some groups may have clearly defined information requirements, others may vary in their specific needs. An excellent example is the Tax Authorities, whose demand for information is primarily focused on
obtaining the necessary data to determine accurate tax assessments. However, the extent of this requirement can vary depending on factors such as the form of taxation, the tax base, and the method of data submission to the tax authorities.

In the following section, I will provide two examples illustrating the probable information needs of two well-known stakeholder groups: tax administration and creditors. These examples have been chosen due to the familiarity and importance of these stakeholder groups.

1.4.3.2 Tax Administration

Taxation methods can vary in complexity, with income taxes being one of the most intricate forms of taxation employed today. In systems like the one in Sweden, there is a significant divergence between Corporate Income Taxation (CIT) and labour income taxation. The regulations specifically addressing labour income taxation cover only three relatively short Chapters in the Income Tax Act (IL) (Chapters 10–12), whereas the rules governing business income taxation span 36 chapters (Chapters 13–40). VAT serves as an example of a complex indirect tax. The primary challenge with this tax lies in the right to deduct input VAT paid against output VAT, especially given that the Swedish legislation is based on EU directives (Kleerup et al., 2020; Doesum et al., 2020). Transaction taxes, which rely primarily on gross payment flow, tend to be more straightforward compared to other forms of taxation. The amount of information required by the examining authority, such as the Tax Authority, to make accurate taxation determinations can be assumed to be directly related to the complexity of the tax type.

The design of the tax base also significantly affects the information requirements of the tax authority. A tax base can encompass nearly all taxable income and transactions or be substantially narrower. In the case of CIT in Sweden and many other countries, the starting point is generally that all business income is subject to taxation, as stated in Chapter 13, Section 1 of the Income Tax Act. However, various exclusions are often introduced to narrow the tax base for CIT by excluding specific revenues or transactions from taxation. For example, the favourable tax regulations in Chapter 23 regarding tax-exempt under-priced transactions and the participation exemption regime in Chapters 24 and 25a, which exempts
inter-corporate dividends and disposal of business-related shareholdings from tax, are common ways to narrow the tax base (Prop. 1998/99:15, 1998; Prop. 2002/03:96, 2003). Additionally, rules governing tax-favourable restructurings, such as mergers (Chapter 37) and tax-exempt business line transfers (Chapter 38), further narrow the tax base for CIT (Prop. 1998/99:15, 1998). These sets of rules are often extensive and complex, and they can be exploited for undue tax advantages, leading to tax avoidance. As a result, legislators frequently introduce rules to prevent abuse, which in turn increases the need for information to ensure fair and accurate taxation.

The method of transmitting information from taxpayers to the examining authority is the third significant component to consider. Companies, as taxpayers, collect, store, and process information before submitting comprehensive reports (declarations) to the relevant governing body. This is typically supported by control data received by the authority from third parties, such as customers, suppliers, and banks. Since most tax information is collected, stored, and processed by the taxpayer, the authority must rely on the accuracy of this data. There is a non-negligible risk of errors in the information, both unintentional and deliberate. Inadvertent discrepancies may arise due to the complexity of the law, while other errors may stem from taxpayers seeking to avoid taxation. Therefore, a substantial amount of information is likely required to ensure accurate taxation.

1.4.3.3 Lenders

Lenders, such as banks, have additional considerations. Credit risk assessments are generally complex processes for lenders (Tsai, S., et al., 2016). Before granting a loan, there are multiple factors to consider. While the financial performance of a company, as reflected in historical data such as annual reports, provides one perspective, lenders also require information about the company’s management and owners. Additionally, assessing market risk is of great importance.

It is therefore reasonable to assume that lenders need access to a substantial amount of information, not only about the borrower but also, in the case of corporate borrowers, about the company’s management and owners. Credit risks extend beyond the borrower’s ability to make
interest and instalment payments; this is just one aspect of credit risk. Another crucial aspect is evaluating the borrower’s willingness to make timely repayments.

By having comprehensive information about the borrower, its management, and its market risks, lenders can make informed credit risk assessments to ensure responsible lending practices.

1.5 The tendency in development — a backwards approach

The current model in which the auditee (companies) collects, stores, and refines data for reporting purposes has significant limitations. One of the most notable drawbacks is that a single set of external reports must primarily cater to the needs of multiple stakeholder groups, often with competing objectives. As a result, auditees may be required to file supplementary reports, such as tax returns, or stakeholders may have to settle for information that only partially serves their needs. It has become evident to many stakeholders that additional data is necessary to make informed decisions.

As mentioned previously, data collection and utilization of Big Data have emerged as both a standalone business model and an integral part of traditional businesses. Providers of administrative systems, such as bookkeeping software, leverage user data to develop business analysis tools. AI-based technologies, driven by Machine (ML) Learning processes, often rely on access to large amounts of relevant data (Big Data) to train their algorithms and achieve optimal results.

From the stakeholders' perspective, there are compelling reasons to explore a new approach that enables access to information of financial significance. The working hypothesis of the FIRE model is built upon the foundation of today’s more advanced business assessments. However, the FIRE model aims to go a step further. It proposes removing accounting and reporting obligations and replacing them with a requirement for multiple actors to make certain raw data available. The goal is to provide stakeholders with access to the data, allowing them to refine it in a manner that best suits their individual needs.
The proposed model has several apparent strengths that can be identified:

- The output can be tailored to individual stakeholders and their specific needs.
- Some administrative burdens are shifted from the auditee (companies) to those who will utilize the information.
- The risk of errors in final reports due to auditee judgments is reduced.
- Comparing information from different data providers can facilitate the identification and correction of errors in the data.
- Access to information may be granted in real-time.

It is important to note that these are initial assumptions and further investigation is required to verify their validity. However, the model also faces various challenges, including:

- Technical aspects: determining the appropriate technology to make the information available.
- Data security: ensuring the maintenance of data security.
- Personal privacy protection: safeguarding individuals’ privacy.
- Protection of companies’ trade secrets.
- Resilience to external stresses, such as war or other crises.

Undoubtedly, there are both advantages and disadvantages to the FIRE model. From my perspective, a compelling argument in favour of exploring the model is that it builds upon an approach that is already being partially implemented. Extensive data collection and processing of information on both companies and individuals are already taking place. Therefore, the research findings from the study of the FIRE model can independently contribute to the field of data-driven business analysis and business intelligence.

Overall, it is crucial to further investigate the FIRE model to evaluate its feasibility and address the challenges it presents.
1.6 Potential Repercussions of the FIRE model

1.6.1 General

In this section, I will provide a high-level overview of how the FIRE model may impact various viewpoints and different types of stakeholder groups. Within the framework of the FIRE project, the aim is to produce an initial mapping of research fields. The review will not delve into excessive detail, as the reasons for doing so are self-explanatory. Nonetheless, the primary objective is to draw attention to some intriguing research areas. It should be emphasized that in addition to the issues I will address below, there are likely many others that can be discussed.

1.6.2 Internal Control of Businesses

Accounting and reporting goals extend beyond providing information to external stakeholders (Berg, P., 2020). Current accounting practices and various interim reports are sometimes crucial for managing a business. It is worth noting, however, that there may be a distinction between small and large businesses. Closely held companies and sole traders may be less concerned with profit and loss accounts, except for minimizing tax burdens. On the other hand, large publicly traded corporations are often highly results-oriented to meet market demands.

Eliminating the current mandatory bookkeeping and external financial reporting obligations does not imply that accounting and reporting standards would become unnecessary. However, the methods and presentation of information could be adapted to better meet the actual internal control requirements of a business. If we disregard creditor protection, taxes, and similar third-party interests, the following questions are likely of importance to small businesses:

- Do they have sufficient liquid assets to cover current expenses?
- Is there enough cash available for planned owner profit distributions?
- How will future investments be financed?

It is plausible that this would lead small businesses to focus more on cash flow control, making profit and loss accounts less significant.
Larger organizations, whose management is more removed from day-to-day operations, may have diverse information requirements. Performance measurement could be a crucial piece of data. The FIRE model would allow corporations to conduct internal performance evaluations without the need for a standardized and comparable set of reporting standards. As a result, internal reporting could be customized to specific information needs, optimizing control over particular activities.

It would be interesting to investigate whether accounting, especially for internal purposes, should remain in its current form if a model like FIRE were implemented. One conceivable scenario is that the focus would shift to circumstances that also benefit the company’s primary external stakeholders. The key aspect to measure would be activities that positively impact stakeholder relationships. It is plausible that internal reporting would aim to support an optimized process for a specific company’s most important stakeholder group(s).

1.6.3 Creditor Security

Accounting plays a crucial role in limited liability companies to comply with specific creditor protection requirements under Swedish Corporate Law. One such requirement is the preparation of a Balance Sheet for Liquidation Purposes (BSLP) (Lindroos-Moll, S., 2020). If the management of a limited liability company suspects that more than half of its share capital has been depleted, a BSLP must be prepared. Failure to do so and comply with statutory requirements may result in the management being personally liable for obligations incurred by the company after the deadline for the BSLP’s preparation and public disclosure (Lindroos-Moll, 2020). It is worth noting that the BSLP is prepared similarly to an ordinary annual report, except that there is no requirement for additional prudence when evaluating the assets (Lindroos-Moll, S., 2020).

Another creditor protection measure is value transfer restrictions outlined in Chapter 17 of the Companies Law Act (Andersson, S., et al., 2022). According to the primary rule governing permissible value transfers, only unconstrained equity may be transferred, and there is a precautionary liquidity rule to reinforce this requirement.

However, it is important to highlight that capital protection measures related to a specific amount of share capital have limited effectiveness. Currently, a Swedish limited liability corporation can be founded with a
share capital of 25,000 Swedish Krona (SEK), and an “assured” capital of 12,501 SEK is often insufficient (Blad, K., 2023). This is particularly significant considering that the asset side of a BSLP can be evaluated without prudence. In contrast, other jurisdictions, such as the British, do not require paid-up share capital when establishing a corporation similar to Swedish limited corporations. Additionally, in Sweden, there are forms of associations with limited liability for owners/members that do not require any capital contribution.

Moreover, these regulations do not provide protection against purely criminal conduct. Preventing a corporate raid by someone knowledgeable about Swedish law and unscrupulous is virtually impossible for the authorities in Sweden. The process of requiring an annual report to be submitted by the end of the seventh month following the income year and subsequent reminders can delay effective action by the authorities for up to two years.

Essentially, continuous oversight and transparency of a company’s activities, particularly its financial aspects, are likely to be more effective creditor protections. This is especially important for potential creditors considering lending money or providing products and services to a potentially delinquent debtor. Granting the stakeholder group of possible creditors direct access to a company’s financial information, particularly through access to raw data, can enhance creditor protection. It allows creditors to create practical decision-making tools or at least make better judgments compared to the current system.

1.6.4 Investors

Investors are another important stakeholder group, and it is necessary to distinguish between private individuals purchasing market shares and institutional investors. Private individuals may require assistance in creating tools for market analysis, making them a distinct subgroup of stakeholders.¹

When considering institutional investors such as venture capitalists, activist funds, pension funds, and others, the response of the stock market to the FIRE model becomes uncertain. The reporting requirements for

¹ It is likely that some kind of public information services must be provided for this stakeholder group.
publicly traded corporations are more stringent, and they are obligated to file both annual and interim reports. This demonstrates that the market needs more frequent information than just once a year. The question arises: how would the market react to a constant flow of real-time information? (Harasim, J., 2021).

Accurately assessing the market and the company’s performance provides investors with a competitive advantage. Insider trading laws are comprehensive to prevent unfair advantages (Fox, M., et al., 2019). If all stock market participants had continuous and unlimited access to raw data for listed companies, the speculative aspect of trading in stocks and derivatives could potentially lose much of its significance. There would be fewer surprises, as trading in stocks relies on unknown variables that introduce risk (Pham, H. V., et al., 2014).

The role of the stock market in providing external capital to listed companies may be influenced by the availability of excessive real-time information to market participants. If information access is democratic, with all actors having access to the same data and reaching similar conclusions, it may become more challenging for reliable businesses to obtain risk funding. However, companies with stability may have greater access to borrowed capital.

One possible scenario is that venture capital may shift towards unlisted companies, where forecasting the future is more challenging. Whether this scenario is likely to occur and whether it is desirable are important research questions for the FIRE consortium.

1.6.5 The Professions

A particularly intriguing topic is the impact of digitalization and technological advancement on various professions, particularly those involved in managing and refining external financial reporting, such as accountants and auditors.

Accounting consultants are professionals who are engaged in a wide range of tasks. Their core competence lies in assisting companies with day-to-day bookkeeping. Additionally, they provide support for tasks such as annual accounts, tax returns, and annual income tax returns. In the FIRE model, some of these tasks will be eliminated. However, the need for internal control is likely to remain, and there may even be greater business opportunities if accountants can demonstrate the value of their
services in assisting with internal control. This could potentially lead to an expansion of their services to include advanced business analysis and legal advice.

Another group directly affected by the FIRE model is auditors. The traditional role of auditors is likely to diminish in the FIRE model, as data from companies can be validated by third-party sources, reducing the need for traditional audits. However, auditors are well-suited to assist stakeholders in assessing counterparties and building analytical models and tools. They may shift towards becoming more business advisors, including providing legal advice.

One consequence of the FIRE model is the potential convergence of the accounting and auditing professions, blurring the boundaries between their roles. The legal profession will also be impacted by technological developments. It is possible that most legal advice will not require human intervention, and legal advisors may move towards providing business and financial services (Susskind, R., 2017).

Overall, the FIRE model has the potential to reshape the roles and responsibilities of accounting, auditing, and legal professionals in response to technological advancements.

1.6.6 Methods and Tools

Due to the implementation of the FIRE model, stakeholders will have access to a substantial amount of information about the businesses they are interested in. The volume of data is likely to be overwhelming for a human being to effectively utilize. As a result, there will be a significant need to develop strategies and tools to successfully leverage the FIRE model.

Research in the field of business intelligence already exists, with a focus on the conventional model that relies on external financial reporting as its primary foundation (Jourdan, J., et al., 2008). However, it is important to note that business analysis and intelligence already incorporate artificial intelligence technologies and the use of secondary data in addition to financial data (Hu, Y., et al., 2019). The adoption of the FIRE model will likely require the exploration of new perspectives and approaches to business intelligence.
1.7 Technology
1.7.1 General
The management of digitized information of significant financial importance faces a significant challenge in ensuring storage and access. This challenge depends largely on the available technologies. Key considerations from a technical standpoint include finding the right balance between providing sufficient data access to relevant stakeholders while safeguarding personal information and trade secrets. Data security itself is another critical aspect that needs thorough examination.

The functionality of systems should be assessed from both legal and technical perspectives. On one hand, it involves understanding the current legal requirements for information management and determining the future legal requirements in this context. On the other hand, it is essential to assess whether the necessary technologies already exist or need to be developed to effectively utilize the information, as well as how the system’s security can be ensured in compliance with the applicable regulatory framework.

In the following sections, I will discuss the challenges and technical opportunities that our research group working on the FIRE project has identified thus far.

1.7.2 Centralized vs decentralized storage of information
Centralized data storage is a traditional model where data is stored and managed in a single location, such as a data center or cloud storage provider. It offers simplified management, easier access control, and can be more cost-effective. However, centralized storage presents a single point of failure, which can lead to data loss or inaccessibility during downtime, and it may face scalability challenges as data volume increases (Wang, S., et al., 2018).

Decentralized data storage, on the other hand, is a newer model that distributes data across multiple nodes or devices, often leveraging blockchain technology (Wang, S., et al., 2018). This approach provides enhanced security and greater resilience, as it eliminates the single point of failure and allows for continued operation even if some nodes experience downtime (Peng, X., & Hu, J., 2021). However, decentralized storage systems can be more complex to implement and manage and may
sometimes result in slower data retrieval times due to the need to access

Overall, there is much to suggest that the FIRE model should use a
decentralized storage system as a whole. However, how companies choose
to store their data is of less interest. So far, the research conducted within
the framework of FIRE on the technical side has mainly concentrated on
distributed ledger technology (DLT) (Wang, S., et al., 2018). There are
also other models that can complement or even replace DLT within the
framework of FIRE, mainly Edge Computing (EC), and combining this
with Federated Learning (FL) models to process the financial information

1.7.3 Distributed Ledger Technology

DLT, or distributed ledger technology, is a cutting-edge technology that
has the potential to be used in the FIRE concept. It is a digital system
that records transactions in a manner that is decentralized as well as
transparent (Hughes, A., et al., 2019). Blockchain technology serves as
the foundation for distributed DLT, functioning as a distributed database
that enables the creation of a shared and immutable ledger of transactions
(Hughes, A., et al., 2019). DLT offers several advantages over conven-
tional storage systems, including increased efficiencies, transparency, and
safety (Hughes, A., et al., 2019).

One significant advantage of DLT in the context of financial matters
is the increase in operational efficiency (Hughes, A., et al., 2019). The
transparency provided by DLT is also a valuable feature. With DLT,
all transactions are logged into a public and immutable ledger that can
be accessed by authorized participants, facilitating easy auditing and
verification of transactions, reducing the risk of fraud, and fostering
trust (Hughes, A., et al., 2019). Moreover, DLT can provide an accurate
and transparent view of an organization’s financial position, which is
beneficial for investors and other stakeholders.

DLT offers enhanced security for accounting procedures (Hughes, A.,
et al., 2019). Unlike conventional storage systems, which are vulnerable
to hacking and cyberattacks, DLT employs advanced cryptography to
secure transactions and prevent unauthorized access, ensuring the relia-
bility and safety of the storage system.
By recording transactions on multiple nodes within a decentralized network, DLT enables scalability and the handling of large transaction volumes (Hughes, A., et al., 2019). The system can easily adapt to the requirements of stakeholders, allowing for efficient processing of financial information.

Overall, DLT has the potential to revolutionize financial information management and reporting within the FIRE model, offering increased efficiencies, transparency, security, and scalability (Hughes, A., et al., 2019). However, further research and exploration are needed to fully understand the implications and potential applications of DLT in the FIRE project.

1.7.4 Edge Computing

The term “edge computing” (EC) refers to a paradigm in distributed computing that moves data processing and storage closer to the data's origination point (Chen, J., et al., 2021). EC enables data processing to take place at or close to the source, eliminating the need to rely on a centralized data center or cloud service for processing (Chen, J., et al., 2021). This change in the location of data processing has significant implications for the speed, efficiency, and overall functionality of various technologies and applications.

Implementing EC brings several notable benefits, including reduced latency, improved security, and increased scalability (Chen, J., et al., 2021). By processing data closer to its source, EC can significantly reduce the time it takes for data to travel between the source and the processing location, thereby reducing latency (Chen, J., et al., 2021).

One crucial advantage of EC is the ability to keep sensitive information on the device or within the local network, thus reducing the risk of data breaches and exposure to cyberattacks (Chen, J., et al., 2021). Local processing of data ensures that sensitive information remains within the controlled environment, enhancing security measures.

When applied to financial information, EC offers the benefit of processing companies’ data within their own systems, ensuring better control and protection of sensitive information (Chen, J., et al., 2021). The desired output or result can then be transferred to the stakeholders, maintaining the security and confidentiality of the financial data.
In summary, the implementation of EC in processing financial information provides advantages such as reduced latency, improved security, and enhanced control over sensitive data (Chen, J., et al., 2021). By leveraging EC, companies can enhance their information processing capabilities while safeguarding sensitive financial information.

1.7.5 Federated Learning

FL, or Federated Learning, is an approach to training machine learning models that emphasizes collaboration and brings the model to the data instead of transmitting data to a centralized server for training (Pandey, M., et al., 2022). In the context of the FIRE model, FL can be utilized in the business intelligence/analysis system, allowing the auditees’ ERP systems to train a local model. The results can then be transmitted to the stakeholders, who compile the new information and improve the global model. This iterative process continues until the global model converges, resulting in a more accurate and efficient machine learning model.

One significant advantage of FL is its ability to protect sensitive data within companies (Pandey, M., et al., 2022). By keeping the data within the auditees’ own systems, the underlying data is not exposed to external parties. Additionally, FL reduces the amount of data that needs to be transferred from companies to stakeholders (Pandey, M., et al., 2022). Compared to transferring all data from companies to stakeholders, an FL-based system minimizes the need for high bandwidth requirements.

Overall, FL offers the benefits of enhanced data privacy and reduced data transfer requirements, making it a valuable tool for the FIRE model. By leveraging FL, companies can maintain control over their sensitive data while still benefiting from collaborative machine learning and improved business intelligence.

1.8 Some Legal Aspects of the FIRE Model

The legal implications of the FIRE model and the increasing digitalization of financial information are significant and require careful consideration. One important aspect to address is the interaction between the existing regulatory framework for accounting and taxation and the changing landscape of digitalization. The introduction of the FIRE model or similar
approaches would likely have an impact on these regulations, and it is crucial to explore how they can be adapted to accommodate the evolving needs and technologies.

Personal data protection is a critical area of concern when handling financial information. As more data is collected and processed in the digital realm, ensuring compliance with data protection regulations becomes paramount. Safeguarding individuals’ privacy and implementing appropriate security measures to protect sensitive financial data are essential considerations within the FIRE model.

The General Data Protection Regulation (GDPR) has been in effect since 2018. It aims to protect living people’s privacy and ensure the right to freely move data between Member States’ systems. It applies to the processing of personal data that is carried out by automated means and forms part of a filing system. It also applies to personal monitoring and may apply to a controller outside the EU if international public law applies EU law there. It is only legal to process personal data if at least one of the following conditions is met: the individual has given consent, the processing is necessary for a contract, the processing is required for legal compliance, the processing protects the vital interests of the person or another individual, or the processing serves the legitimate interests of the organization or a third party (Kuner, C., et al., 2020).

The Union’s or a member state’s law must provide a legal and fair basis for processing data for a different purpose. Sensitive personal data, such as race, ethnicity, political or religious beliefs, trade union membership, genetic or biometric data, health information, or sexual life and orientation, is generally prohibited. Non-profit organizations are exempt from this rule if an individual has made their personal information public or if it is needed for legal claims or the public good. The GDPR requires controllers to present data processing information in a clear, concise, and unambiguous manner and make it easy for data subjects to exercise their rights. Individuals have more rights under the GDPR, such as the right to correct, erasure, restrict certain processing activities, portability of data, and object to automated processing-based decisions (Kuner, C., et al., 2020).

All of the mentioned aspects of GDPR are important to investigate as part of the FIRE project.
Increased access to a substantial quantity of digitized company information, particularly in the context of FIRE, poses a threat to the confidentiality of businesses and the trade secrets they maintain. The legislation that exists today, which in the EU is mainly based on DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure, is not particularly effective in relation to the increased digitalization. The question also concerns the operation of other intellectual property protection rules in an environment that is becoming increasingly digitalized.

Regarding this matter, people view it from a variety of angles. One option is to consent to a less stringent level of protection for commercial secrets. The second strategy entails employing a mixture of technological innovation and legislative action. It would appear that technologies like EC and FL are the ones that could be used to keep a reasonable level of protection even if it were compromised.

Furthermore, the regulation of AI becomes increasingly relevant in the context of the FIRE model. AI technologies play a crucial role in processing and analysing vast amounts of financial data. It is essential to examine the legal frameworks governing AI and ensure that the use of AI in financial reporting adheres to ethical and legal standards. At the moment, there is also an ongoing discussion and proposal from the EU commission on a legal framework in respect of the use of AI (Brumen et al., 2023).

As the FIRE model moves towards implementation, it will be necessary to assess and address the legal challenges that arise. This includes navigating the complex landscape of personal data protection and adapting regulatory frameworks to accommodate advancements in AI. By proactively addressing these legal issues, the FIRE model can be developed and implemented in a manner that ensures compliance, protects stakeholders’ rights, and fosters trust in the digitalized financial reporting ecosystem.
1.9 Concluding Remarks

In summary, the rapid advancement of technology and the increasing digitalization of information have resulted in significant transformations in economic life. While these changes bring certain risks, they also present numerous opportunities. The objective of the FIRE project is to explore the impact of digitalization on various aspects of business, such as companies, stakeholders, legislation, privacy, trade secrets, and business models, from diverse disciplinary perspectives.

The FIRE project, with its proposal to take advantage of technology and advanced data management solutions, has the potential to revolutionize traditional financial reporting practices. A pivotal consideration arising from this transformation is the possible abolition of mandatory book-keeping and annual reporting obligations, which have been a cornerstone of financial transparency and accountability for decades.

The underlying premise of this perspective is rooted in the real-time, continuous, and automated nature of financial data retrieval and dissemination that FIRE promotes. By harnessing advanced technologies such as AI, ML, EC, FL and DLT, the FIRE model might result in more effective accurate use of information of financial significance.

In a traditional system, businesses are obligated to maintain regular book-keeping records and provide annual financial statements, a process that is often manual, time-consuming, and prone to human error. This necessitates a considerable allocation of resources, both in terms of finances and personnel, while also contributing to the risk of data inconsistencies and inaccuracies.

With FIRE, however, the financial data landscape could be transformed. The real-time tracking and recording of financial transactions facilitated by AI and ML, coupled with the security and immutability offered by blockchain technology and/or EC and FL, could render traditional book-keeping redundant. All financial transactions could be instantly and accurately logged in real-time, reducing the need for additional record-keeping efforts.

Similarly, the requirement for annual reporting could be revisited. Given FIRE’s capacity for real-time data analysis and generation of “financial reports”, stakeholders could potentially access up-to-date financial statements at any given time. This not only expedites the decision-making
Chapter 1 An Overview of the FIRE Research Project

process but also offers a more accurate and timely depiction of an entity’s financial health, as opposed to the static, time-bound insights provided by annual reports.

However, it’s crucial to remember that the transition towards this model would involve overcoming significant challenges. Changes in legislation, stakeholder acceptance, technological infrastructure, and cybersecurity measures are all crucial factors that would need to be considered. Additionally, the complete abolition of traditional book-keeping and annual reporting practices may not be feasible or desirable in all contexts and industries.

Overall, while the implementation of FIRE does present the potential for a paradigm shift in financial data management, further research, experimentation, and dialogue are necessary to fully understand the implications and navigate the challenges of this transformative shift.

The project also investigates the potential impact of these developments on different professional communities involved in financial matters. Additionally, it focuses on whether the technology employed for information transfer and management should prioritize preserving the confidentiality of business information and personal privacy.

The project is expected to span an extended period, and immediate implementation of a FIRE model is not anticipated. However, it is believed that ongoing developments align with the project’s focal areas of interest. Despite the preservation of the current system of mandatory accounting and annual report requirements, the issues examined in the project remain highly relevant.

References


Chapter 1 An Overview of the FIRE Research Project

Peng, X., & Hu, J. (2021). Research on Decentralized Storage Technology in Internet of Things. In 2021 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 986–989). IEEE.


Prop. 2002/03:96 (2003), Skattefri kapitalvinst och utdelning på näringsbetingade andelar.


**Abstract:** Encoding and (re-)using data about or created by citizens to generate new value is a process referred to as datafication. Extracting data from and about citizens raises numerous human rights questions, particularly in the area of the right to private life. The European Court of Human Rights (ECtHR) has over the years developed and shaped the right to digital private life by outlining what type of collection, processing and retention of data about individuals is considered permissive – and what is not. Although the datafication process entails elements that currently lie outside the core ambit of the ECtHR, it has a longstanding and indeed heightened interest in defining and protecting what constitutes genuine human private life. In this regard, digital private life falls into a domain of matters which the ECtHR finds worthy of protection. By pointing out specific requirements in order to prevent the abuse of State power, the ECtHR is a mechanism that can be reckoned with when it comes to shielding European citizens from datafication.

### 2.1 Introduction

The ongoing digitalisation and automation of human existence means that human life is currently experiencing wide-reaching datafication. The encoding of data from and about citizens, the data subjects, can generate new value. This raises a number of human rights questions. It has been
pointed out that the mere knowledge about processes of datafication and encoding of human life can tacitly or explicitly influence human behaviour. What are, if any, the human rights implications when data snippets ‘produced’ by citizens in their daily lives, many online but also offline, are separated from the data subject and gathered by authorities and companies for (possible) value-generating purposes? What are citizens’ reasonable expectations concerning the protection of their data? Is there a human right to digital private life?

This chapter begins by delineating the notion of datafication. Next, the right to private life is outlined thus unveiling the central original features of this classic right within the framework of the European Convention on Human Rights (ECHR), and the nature of State obligations it gives rise to. This is followed by an examination of how Article 8, which safeguards the right to private life, is used when datafication comes before the European Court of Human Rights (ECtHR). Although the right to private life is not the only right invoked in relation to datafication, Article 8 remains the most frequently used provision. The chapter ends by highlighting the key findings concerning how the ECtHR approaches datafication. Before we further explore the right to private life/privacy, an introduction to the concept of datafication is required.

2.2 The Notion of Datafication

Datafication now enables the “processing of personal information on an industrial scale” (Cohen, 2017:224). Commenting on these technological developments, Land & Aronson concluded that from a human rights perspective “the very same characteristics of technology that present the greatest opportunities also create the greatest risks.” (Land & Aronson, 2018:126). Two decades have passed since the global community affirmed that the Universal Declaration of Human Rights (UDHR) should equally apply to cyberspace (Andrew & Bernard, 2021:1). The impact of new technology and digitalisation on human life and behaviour has been perceived to be fundamental enough to even potentially infringe on the freedom of thought (Alegre, 2022:132). Despite such alarmistic views, it is here submitted that human rights law is well-versed when it comes to 1) finding the balance between the interests of individuals on the one
hand and the State on the other, and 2) assessing whether the State has reached a fair balance between the competing interests of individuals.

The ECtHR relies on Article 2 of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) when defining data processing as “... any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data” (Convention 108, Art 2). The net to capture what data processing entails is cast wide intentionally. Nevertheless, there is at times a presumption that data handling, in particular computerised analysis, data capturing and registration is done passively, while people do what they normally do anyway; this presumption may be false (Rothschild-Elyassi, 2022:56). In fact, datafication entails turning citizens’ day-to-day actions, such as having a chat with a friend or waving down a cab into digital platforms and apps. In other words, common human habits that were previously done elsewhere have been turned into activities performed via digital media (Mejias & Couldry, 2019:5). It is this process of gathering, collecting and the storing of data that has led commentators to suggest that what has been taken away should not actually be called data (Latin: that which is given), but rather capta (that which is taken). (Mejias & Couldry, 2019:2). One may even argue that the taking of data can be understood as a colonial process, due to the same historical function of dispossession (Mejias & Couldry, 2019:6).

When datafication amounts to surveillance, the ECtHR has held that it has a chilling effect, meaning that a person restrains him or herself from otherwise lawful speech or other acts, fearing legal consequences or privacy harm. (Penney 2022:1454). This impacts citizens in general, as well as the behaviour of those working in public authorities, be it with legal or non-legal tasks. Therefore, the term datafication “signals a historically new method of quantifying elements of life that until now were not quantified to this extent” (Mai, 2019:3).

Datafication is said to be a process that consists of the following three segments: First comes a transformative stage where something is encoded into data (Rothschild-Elyassi, 2022:56). Second, such data becomes the smallest building block from which knowledge and information is drawn (Kitchin, 2014:1). Third, this information constitutes a new value of
some sorts. The first segment, the encoding of human behaviour which also includes sentiments and attitudes (Mayer-Schönberger & Cukier, 2013:93), is a transformation that entails making what is encoded quantifiable (Mejias & Couldry, 2019:1). The sheer volume as well as the wide aspects of human life that are transferred into data in this manner, is unprecedented. The transformation is subtle and entails both cognitive and evaluative abstractions (Mejias & Couldry, 2019:3).

It is noteworthy that the encoding is not neutral to ideology. It is based on decisions regarding the selection of reality and how such quantification is done (Rothschild-Elyassi, 2022:61). As Mai has pointed out, “data has to be cleaned or conditioned to be usable, which involves deciding which attributes and variables to keep and which to ignore” (Mai, 2019:111). Other authors present the view that the values and views of those responsible for coding influence the datasets. (Goldkind et al., 2018:175). Either way, there are indications that marginalised people remain the most vulnerable groups, also when it comes to having their data exploited (Goldkind et al., 2018:176).

As for the second segment, it is important to remember that the tracking and analysing of data is increasingly done in real-time (Rothschild-Elyassi, 2022:61). Lastly, generating new value should not solely be understood in monetary terms, although profit can be generated through “data’s sale as a commodity or data’s incorporation as a factor of production” (Mejias & Couldry, 2019:5). New value could also be a “means of state control, cultural production, civic empowerment” (Mejias & Couldry, 2019:3); or aspects of social and healthcare benefits or, for example, improved customer experiences (Stănescu & Onufreiciuc, 2020:101).1 Such value creation has been described as “a pattern of appropriation by some, with economic and political consequences for others” (Cohen, 2017:230). The infrastructure required for datafication is “owned or controlled mostly by corporations and states” (Mejias & Couldry, 2019:3). Thus, corporations are the main actors and beneficiaries of datafication, but many States also have strong stakes in this process (Mejias & Couldry, 2019:7). The next section begins with a brief look at the general features of the right to private life as protected by Article 8 of the ECHR. This is followed by

---

1 For criticism regarding equating data with resources, see, e.g., van Dijck, 2014 and Boyd & Crawford, 2012.
a short outline of how the right to digital private life has evolved in the light of contemporary technological developments.

2.3 The Expansion of the Protection of Private Life in the Age of Datafication

The ECHR is said to be “a living instrument anchored to the reality of the Member States in which it applies” (Andrew, 2021:2). Article 8 of the ECHR has been called “one of the most open-ended provisions of the Convention” (Ovey, C., & White, R., 2006:241). This provision has over the years become “one of the richest areas of legal development” (Schabas, 2015:366) in ECtHR case-law. Therefore, it is not surprising that this provision is at the forefront when it comes to tackling the “quantum leap in surveillance, interception of communications and data retention” (Data protection guide, 2022:7), faced by citizens.

2.3.1 Citizens’ Right to Private Life

Article 8 belongs to those provisions in the ECHR which have inherent limitations.² It is important to point out that permissive limitations do not allow the authorities or companies to reduce the right to zero (Barbulescu v Romania, § 80). The right to private life is originally of the classical negative kind and the ECtHR holds that the essential object of the provision is to “protect the individual against arbitrary action by the public authorities” (Kroon and Others v the Netherlands, § 31), once referred to as “a right to be left alone” (Brandeis, cited in Schabas, 2015:358). This view has the underlying assumption “that we have a property right to our personal information” which immediately leads to the question: Who owns the information? (Mai 2019:96). However, this, Mai argues, misses the point, namely that what in fact is essential is what happens with personal data. What is foreseeably done with it?

² The other ECHR-rights with such limitations are Article 9, thought, conscience and religion, Article 10, freedom of expression, and Article 11, freedom of assembly and association. The inherent limitations are similar, but not identical. (Ovey & White, 2006:218).
Foreseeability is a special feature in the protection from arbitrariness: “Foreseeability is primarily dependent on the provision of an adequate indication as to the circumstances and conditions under which monitoring may be lawfully employed”.

The four interests for which Article 8(1) ensures respect are private life, family life, home and correspondence. Interestingly, respect does not appear in any other substantive provision in the ECHR (Schabas, 2015:367). Although they are distinct interests, they occasionally overlap (Schabas, 2015:367). One may safely assume that the drafters had human beings in mind when seeking to protect private and family life (Emberland, 2006:115). This can be concluded from the reasoning in, for example (X v Iceland, 87), where the European Commission argued that private life should be understood in a broad sense, to include “the right to establish and develop relationships with other human beings, especially in the emotional field, for the development and fulfilment of one’s own personality”.

Furthermore, the notion of ‘private life’ is so broad, that it neither can nor should be given an exhaustive definition (Niemietz v Germany, § 29). For instance, the ECtHR has held that private life includes someone’s physical and psychological integrity, including at times aspects of an individual’s physical and social identity (Mikulić v Croatia, § 53). In fact, the concept of private life is considered heterogenous and more far-reaching than an end in itself: “The specific contours of privacy can be clearly distinguished and perceived only when it is being defended against different kinds of encroachments. Moreover, privacy is an aspect of the person’s general well-being, and not necessarily only an end in itself” (Hatton and others v the United Kingdom, 43: § 11) as the dissenting judges in this case argued. Furthermore, the ECtHR has elaborated on the protection of our consciousness, seeking to emphasise and appreciate less tangible aspects of human life by protecting every citizen’s right to “freely pursue the development and fulfilment of his personality” (Smirnova

3 'Respect' does appear in the title of Article 1. The ECtHR has stated that the concept is not clear-cut, but emphasised that the ‘rule of law’ is one of its elements (Schabas, 2015:367).

4 The Commission further held that such a right did not extend to relationships with dogs, and subsequently deemed the case inadmissible.
v Russia, § 95). This integrity of the self can be seen as the foundation for autonomy and human agency (Mejias & Couldry, 2019:6). But an autonomous personality does not exist in a vacuum. Rather, according to the ECtHR, it distinctively encompasses a social dimension, which extends beyond the family (Biriuk v Lithuania, § 38).

The social dimension directs attention towards professional activities, given that “professional life is often intricately linked to private life” (Fernández Martínez v Spain, § 110). Professional or business activities may under certain circumstances be given protection under Article 8. (Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland, § 130).5

Most notably is this when the interference concerns “correspondence” or “home” and legal entities are seen to have the status of victim in the meaning of the ECHR.6

Although the right to private life originates from a desire to restrain State interference, it also clearly raises positive State obligations, in that a State must actively provide horizontal protection of the right to private life between private individuals themselves, or individuals and legal persons. The bulk of Article 8 case-law is in fact concerned with positive obligations that require an activity from the State (Schabas, 2015:366). In this case, the State has a wide margin of appreciation. If the principles laid out in ECtHR’s case-law are followed by the domestic court, no violation is likely to occur (Von Hannover v Germany, §§ 125–126). As will be shown in the following section, the ECHR provides the State several legitimate purposes of interference with Article 8.

2.3.2 The Legitimate Interests of the State

The right to private life has to be respected both vertically and horizontally – giving rise to negative as well as positive State obligations. In practice, the positive and negative State obligations are similar. As for the former type of obligation, the ECtHR will assess whether a fair balance has been struck between the competing interests of an individual and the community as a whole. The requirements of Article 8(2) mean that the ECtHR will conduct a three-pronged test to establish whether the

5 A comment to the case is available by McCully, J. (2018).
6 See, e.g., Bernh Larsen Holding AS and Others v Norway, Liberty and Others v the United Kingdom.
interference was a) in accordance with the law, 2) pursued any of the permissible aims listed, and 3) was necessary in a democratic society. The listed permissible aims for limitations are a) national security, public safety b) the economic wellbeing of the country, c) the prevention of disorder or crime, d) the protection of health or morals, e) for the protection of the rights and freedoms of others. The ECtHR has explicitly held that the formulation of permissible limitations under Article 8(2) “leaves no room for the concept of implied limitations” (*Golder v United Kingdom*, § 44), a position that has been upheld.

The margin of appreciation enjoyed by the State will be wider, if the matter concerns balancing someone’s right to private life against another fundamental right (Schabas, 2015:368) such as, for example, the freedom of expression. In contrast, a narrower margin of appreciation will be applied where “a particularly important facet of an individual’s existence or identity is at stake” (*E.S. v Sweden*, § 58). This includes the most intimate aspects of private life (*ibid*).

One may, as Deeks has done, argue that the existing international human rights framework is no longer fit for what is now technically possible in relation to human surveillance across national borders (Deeks, 2015:294). Nevertheless, the right to private life has been considerably extended by the ECtHR since the matter of (analogue) data protection first came before it in *Leander v Sweden*7 almost 35 years ago. By now the right to private life also includes the right to digital private life. Mai has pointed out that the focus of the debate has “shifted from concerns about revealing information about oneself to others to concerns about the new insights that others can generate based on the already available data” (Mai 2016:199). The following section examines how the ECHR operates in view of this shift. Focus remains primarily on matters of legitimate State interests, such as national security, the well-being of the country and the prevention of disorder or crime.

---

7 The claimant sought access to classified data about himself. The ECtHR found no violation, arguing that knowing what the secret service had on file on the applicant (which prevented him from getting a civil job in the marine base), did not constitute an interference with his private life.
Chapter 2 Using the European Convention on Human Rights to Shield …

2.4 Applying Article 8 of the ECHR to Shield Citizens from Datafication

The protection of citizens as data subjects is in human rights terms concerned with at least three aspects of data handling. The ECtHR pays attention to the collection, retention and disclosure actions of data, by State bodies as well as by private bodies. At the outset of this discussion, it is perhaps important to mention that scholars have already identified that international human rights law could make a useful contribution in relation to datafication and digitalisation, given its well versed system for approaching bias and discrimination (McGregor, Murray & Ng, 2019:326). This legal regime not only identifies and defines unlawful harm, it also provides a “means to determine harm through its interpretation of how rights may be interfered with, it also provides established tests to assess when and how rights may have been violated” (ibid.). The three-pronged test mentioned earlier will ensure that interferences with the right to digital private life is done for explicit purposes. In this discussion, the legitimate purposes of the State are national security, public safety, the prevention of disorder or crime, and the economic well-being of the country.

2.4.1 The Collection of Personal Data

The ECHR does not provide any autonomous right to personal data (digital or otherwise) (Data protection guide, 2022:7). Therefore, despite the increasing scope of what falls within the notion of ‘private life’, all contemporary automatic processing and handling of personal data will not categorically fall within the ambit of Article 8 or otherwise avail itself of protection by the ECHR (ibid.). Rather, it has to be anchored in the right to private life, as expressed in Article 8 of the ECHR. That being said, the ECtHR remains bound by numerous aspects of balancing the State’s interests with the citizens right to digital private life. This includes data collected through covert surveillance by the authorities, the collection of data by employers at workplaces, data collection as evidence in courts, data in medical contexts, and citizens’ compulsory communication of personal data. The ECtHR has consistently held that personal data is defined as “any information relating to an identified
or identifiable individual” (*S and Marper v UK*, § 41). Therefore, even “public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities” (*Rotaru v Romania*, § 43).

At the heart of the ECtHR’s attention is the protection of the data subject – the citizen. In line with Article 6 of Convention 108, such data is termed as ‘sensitive’ by the ECtHR and merits a heightened degree of protection. Sensitive data pertains to data revealing racial or ethnic origin; political opinions, and religious or other beliefs, including philosophical beliefs; trade union membership; genetic and biometric data; health, sex life or sexual orientation and criminal offences and convictions (Convention 108, Article 6). Biometric data consists not only of biological characteristics such as fingerprints, the topography of face and fingers, or DNA, but also behavioural aspects such as voice and gait (Zwanenburg, 2021:1406).

The ECtHR assesses to what extent an individual is reasonably entitled to expect the protection of his/her private life as regards the processing of data by public authorities (*Perry v the United Kingdom*, § 37). This means that the ECtHR is concerned with the handling of personal data whether or not it has merely been collected or has been subjected to more sophisticated processing. ECtHR has referenced Article 3(2) of the Directive (EU) 2016/680 which states that processing is: “… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (Directive 2016/680).

The ECtHR is not only concerned with sensitive data, it also assesses the protection of ‘other’ data linked to citizens. This includes employment data, financial data, traffic data, voice samples, GPS location data and photography and the like. Although the assessment concerning these forms of data is carried out with the same three-pronged test set out in Article 8(2), the ECtHR is likely to provide a wider margin of appreciation to the State in these cases. For instance, in tax matters, where the State generally speaking has a wider margin of appreciation, the citizens will have their data protected should it be published in a manner or to
Chapter 2 Using the European Convention on Human Rights to Shield …

a degree beyond what the data subject could reasonably have foreseen (M.N. and Others v San Marino, § 72).

In its work with finding a fair balance between matters of security and the survival of the State, the ECtHR has carved out and follows clear lines. The ECtHR examines a) the proportionality of the measures taken b) if measures were subject to independent authorisation at the outset and c) the existance and nature of supervision and ex post facto review.

2.4.2 The Retention of the Smallest Data Block

Data collection may well increasingly be done in real-time, but the ECtHR is focussed on how any data (sensitive or otherwise) is retained. The ECtHR scrutinises what safeguarding measures a State has in place against abuse. If a State that resorts to using cutting-edge technology for mass surveillance for the legitimate aim of pre-empting incidences of serious crimes, then the ECtHR expects that the introduction of the use of new technology “…has been accompanied by a simultaneous development of legal safeguards securing respect for citizens’ Convention rights” (Szabó and Vissy v Hungary, § 68). The safeguarding against abuse does not only require the State to have separate rules concerning sensitive and other data retention. Additionally, explicit rules concerning the destruction of both types of data are required.

2.4.3 The Duration of Data Retention

The ECtHR acknowledges that personal data may have to be retained for the purpose of crime prevention. This can be seen in the case of B.B. v France, where the applicant, a convicted sex offender, complained about the inclusion of his address in a sex offender database, with the obligation to update his address once a year. The ECtHR found that the aim sought, to prevent criminal activities, was a legitimate one. On assessing the safeguarding measures against abuse, the ECtHR held that they were satisfactory. First, such gathered data can only be consulted by the courts, police or administrative authorities subject to a duty of confidentiality. Second, the duration of the data retention was pre-determined, albeit amounting to the maximum of 30 years (§ 68). Thus, the ECtHR was satisfied that independent reviews were available to the applicant (ibid.) and found no violation of Article 8.
Furthermore, a State seeking to retain the data of convicts must distinguish between serious offences (such as terrorism, sexual offences and crimes against humanity) and non-serious offences such as striking a gendarme with an umbrella in connection with turmoil at a political rally (*Aycaguer v France*, § 44).8

As mentioned above, data retention if determined precisely, even for a maximum of 30 years, may be deemed not to violate the right to private life of a convicted sex offender. Although the ECtHR requires the precise determination of the duration of data retention, there is an outer limit: the ECtHR has held that a definite period of forty years may be equal to an indefinite period in practice, as it is likely to extend beyond the reasonable life expectancy of the applicant (*ibid.*, § 42).

But the length of retention can also be lawfully organised without an explicit duration period. Such was the case where sensitive data such as blood samples had been taken for the purpose of an exhumation programme to identify deceased relatives. ECtHR held that no violation was found, because the destruction of the samples was determined to take place when the consent form expired (*Cakisisoy and Others v Cyprus*, § 52).

The ECtHR has found violations of the right to digital private life when: 1) the data retention was indefinite; 2) the seriousness of the offence had not been taken into consideration, and 3) no real possibility of review was provided (*Gaughran v the United Kingdom*, § 94). These criteria are not cumulative since every one of them has to be satisfied independently of the other. In the view of the ECtHR, measures against abuse can be achieved through end-to-end protection.

### 2.4.4 End-to-End Protection

The practice of bulk surveillance although not automatically prohibited requires specific safeguarding measures. Notably, fundamental safeguards against abuse in the form of end-to-end safeguards are required. First,

---

8 Similarly, pertaining to private companies, the ECtHR has held that the tax authorities did not overstep their margin of appreciation when a backup file was taken from a mixed server jointly used by three companies for the purpose of tax auditing (*Bernh Larsen Holding AS and Others v Norway*, § 173). The majority of five votes to two argued that the situation was less serious than a search and seizure under criminal law.
an assessment of the necessity and proportionality has to be made at the domestic level, at each stage of the measures taken. Second, from the outset, any bulk interception should be subject to independent authorisation. Third, the operation should be subject to supervision and *ex post facto* review (*Big Brother Watch and Others v the United Kingdom*, § 350). Additionally, should journalistic material and the professional protection of sources’ anonymity be at risk due to bulk interception, Article 10 will also be used (*ibid.*, § 448). The end-to-end requirement of safeguarding bulk inceptions can also be invoked by a non-governmental organisation. The requirement includes clear rules on the destruction of incepted data even if it does not include personal data (*Centrum för rättvisa v Sweden*, § 369).9 The ECtHR has also held that when incepted data is transmitted to foreign partners, the privacy interests of citizens should be given consideration by the law (*ibid.*).

### 2.4.5 Disclosure Actions

The ECtHR has distinguished between the disclosure of personal data by one authority to another and public disclosure by media. The disclosure of personal data is safeguarded by clear requirements: 1) domestic law must regulate the measures taken by the data processor; 2) their responsibility in the case of non-compliance must be in place; and 3) the data receiving authority must have corresponding rules and guarantees, notably, the duty of confidentiality should be in place (*M.S. v Sweden*, § 43). When it comes to sensitive personal data, the prior consent of the data subject is one element to consider, albeit not a decisive one (*ibid.*, § 35). Furthermore, even when citizens do not actively hide data that make them identifiable, there is a reasonable expectation of privacy that should be protected (*Benedik v Slovenia*, § 116). Should, however, a person actively seek publicity, such a legitimate expectation of privacy becomes limited (*Axel Springer AG v Germany*, § 101).

The ECtHR has held that, in principle, the public’s interest to know, as protected under Article 10, should be given equal weight with the

---

9 A separate discussion exists concerning to what extent examining cases pertaining to general matters of mass surveillance, rather than the handling of petitions of individual victims of violations, can be said to alter the ECtHR’s nature, turning it into a constitutional court. See, *e.g.*, van der Sloot, (2020).
individual’s right to privacy (Satakunnan v Finland, § 163). In that case, the ECtHR held that no violation of Article 10 had occurred when the news outlet was held liable for making extracted data pertaining to taxation publicly available. In passing, the ECtHR notes that even if regulating the manner in which data is disclosed by a media outlet may render the business less profitable, this is not a sanction in the eyes of the ECtHR. (ibid., § 197).

2.5 Concluding Discussion

The first segment of datafication which concerns the encoding of human life does not currently draw much direct attention from the ECtHR, if it is considered primarily from a technological perspective. However, if considered from the inverted perspective, that is seeking to establish what genuine private life is and what truly human aspects of being or existence are, an emerging stance from the ECtHR can be discerned. First, the ECtHR recognises that humans do not and cannot thrive and develop in isolation or on their own, being requires and happens in context: the ECtHR seeks to capture nuances of humanness, with aspects of social life and the fulfilment of one’s personality. Second, arguably, the ECtHR protects the humanness of digital private life by distinguishing between sensitive data and other data, clearly providing the first category more attention and scrutiny. Third, the ECtHR explicitly requires the State to develop separate sets of rules for both data categories.

The second segment of datafication, dealing with when and how data is gathered and processed, gives rise to an abundant amount of case-law. The ECtHR has a strong focus on what is done with personal data in terms of its capturing, collection, retention and disclosure. The actual type or kind of data is not that much on the ECtHR’s radar. What matters, and rightly so, is what is done with it.

Finally, the third segment of datafication leading to the creation of new value which is not limited to monetary aspects, but that also could consist of public values such as security gains, or improvements in health care systems, occasionally draws attention from the ECtHR. This will be the case when the appropriation of new value has consequences for the human rights of citizens. The ECtHR clearly is of the view that States
that strive to be at the forefront and aim to lead technical developments and the quest for datafication, through such a commitment have an automatic obligation to develop satisfactory safeguards against abuse. One such mechanism against abuse that the ECtHR has repeatedly asked for, is so called end-to-end protection, with legal rules pertaining to the duration of retention, and the explicit regulation of data destruction. This end-to-end requirement also applies to sensitive and other data.

Although legal persons such as associations and companies may avail themselves of Article 8 protection from time to time, it is clear that what the ECtHR provides human rights protection for are aspects of human private life and the enterprises, function in relation thereto. The ECtHR’s approach to business interests such as profit making, may at best be described as indifferent.

In conclusion, it can be argued that the ECtHR is capable of shielding citizens from several aspects of datafication. This is done primarily by requiring regulation against abuse in matters pertaining to digital private life and what is considered sensitive data. Given the ECtHR’s capacity to define and identify harm, it is possible to conclude that the human rights framework is a mechanism to be reckoned with when it comes to shielding citizens from harmful datafication.

References

ECtHR, Axel Springer AG v Germany (Application no. 39954/08) Judgment [GC] 7 February 2012.
ECtHR, Benedik v Slovenia (Application no. 62357/14) Judgment Final 24 July 2018.
ECtHR, Bernh Larsen Holding AS and Others v Norway (Application no. 24117/08) Judgment 27 November 2009.
ECtHR, Biriuk v Lithuania (Application no. 23373/03) Judgment Final 25 February 2009.
ECtHR, Cakicisoy and Others v Cyprus (Application no. 6523/12) Judgment 23 September 2014.
ECtHR, Centrum för rättvisa v Sweden (Application no. 35252/08) Judgment 25 May 2021.
ECtHR, E.S. v Sweden (Application no. 5786/08) Judgment 21 June 2012.
ECtHR, Gaughran v the United Kingdom (Application no. 45245/15) Judgment Final 13 June 2020.
ECtHR, Hatton and others v the United Kingdom (Application no. 36022/97) Judgment [GC] 8 July 2003.
Chapter 2  Using the European Convention on Human Rights to Shield …


ECtHR, Liberty and Others v the United Kingdom (Application no. 58243/00) Judgment Final 1 October 2008.


ECtHR, M.N. and Others v San Marino (Application no. 28005/12) Judgment Final 7 October 2015.


ECtHR, Perry v the United Kingdom (Application no. 63737/00) Judgment Final 17 October 2003.

ECtHR, Rotaru v Romania (Application no. 28341/95) Judgment 4 May 2000.


ECtHR, Szabó and Vissy v Hungary (Application no. 37138/14) Judgment Final 6 June 2016.

ECtHR, von Hannover v Germany (No. 2) (Applications nos. 40660/08 and 60641/08) Judgment [GC] 7 February 2012.


European Commission, X v Iceland (Application no. 6825/74). Decision of 18 May 1976. 5 DR 86.


Rigmor Argren


Abstract: After its invention in 2008 by the unknown computer scientist known under the pseudonym Satoshi Nakamoto, and after its diffusion, the blockchain system, later also referred to as the “God Protocol”, gained immediate success, sparking the interest of both private entities – its first fervent supporters – and public authorities, which saw its potential in terms of reorganizing the administrative machine.

The characteristics of the said technology – particularly that of interoperability – prove to be interesting in relation to the slow process of European administrative integration that has seen the relations between European and national administrations change radically.

This process of integration has led to forms of co-ownership – between supranational and national levels – of important administrative functions and, consequently, co-management of the resulting administrative activities.

This research, therefore, analyzes the application and regulatory profiles related to the use of blockchain technology in the process of European administrative integration.
3.1 Premise: Public Administration and New Technologies: Towards Administration 4.0

The aim of this paper is to provide some general reflections – which have arisen within the Italian legal landscape and beyond – on the use of new information technologies for administrative causes and to emphasize the fundamentally important role played by information and its exchange for the purposes of good administration.

This is not an easy task, given that the discourse on the so-called “digital simplification” (Orofino A.G., 2019) and its complex significance has been enriched in recent years by many valuable contributions that have highlighted its most important nodes. For a long time, the dialogue between doctrine and jurisprudence on these issues has been focused predominantly on the role of the so-called “administration 2.0” (and 3.0). Recently, the debate has shifted to the possibility of using, for administrative purposes, means such as Artificial Intelligence and distributed ledger technologies, placing the problem of the role of information and of the modalities of its use at the center of the legal debate on the phenomenon known as “administration 4.0” (Galetta D.U., 2019).

This latter form of administration represents the final stage (currently) of a long evolutionary process that has seen the public administration as a protagonist.

If the use of the computer in carrying out administrative activities has already developed starting from the so-called “administration 2.0” – mostly in the form of an alternative to printed paper and the typewriter – and during “administration 3.0” led to a wider digitization through portals, applications and social networks, we are nowadays facing an even more radical change.

The advent of this new operating model has its origins in what is called the “Fourth Industrial Revolution” whose main pillars are basically two in number: automation and interconnection (Viola L., 2018).

Indeed, you cannot help but notice how – especially because of the massive financial plans put in place in order to overcome the effects of the crisis triggered (or exacerbated) by the pandemic that began in 2020 – the topic of the innovation of public administrations has become absolutely fundamental. Suffice it to say that within the framework of the Italian
National Recovery and Resilience Plan, the reform of the public administration, especially with reference to its digitization and the training of its staff, represents a so-called “horizontal reform” functional, from a general point of view, to the pursuit of all the other planned systemic changes.

As already mentioned, the digital transition of public administration is based, on the one hand, on the gradual introduction of technologies that ensure a greater degree of automation of the more mechanical and repetitive administrative activities, as well as the so-called “constrained” administrative activity. Already, notable experiments have been carried out, for example, in the field of education, with the use of algorithms in charge of identifying teacher tenure locations. Although the reported example was unsuccessful, considering that the algorithm used came to unreasonable decisions, causing extensive administrative litigation, it was nevertheless of great importance, as it represented an opportunity for the Italian Council of State to decide on the possibility for public administrations to use such technological tools (Pesce G., 2021). While upholding the appeals, the highest administrative judge admitted, within certain terms, such a possibility not only with reference to the administration’s constrained activity, but also to the discretionary one. Therefore, it should not be ruled out that in the near future and with the evolution of the available technological means (and the decrease in their cost), public administration will be affected by a wide phenomenon of automation.

As, however, the case I have just reported teaches us, a key role in this process will certainly be played by information and its quality. It is no coincidence that, recently, it is precisely blockchain technology that has been placed in the spotlight as a possible enabling technology for a greater degree of accuracy, order and “cleanliness” of public administration data (D’Onofrio, 2020).

What emerges, then, is that before we can discuss the automation of public administrations, it is essential to reflect on the evolutionary lines of its organizational structure and the role that new technologies can play in this regard.

The present paper would, indeed, like to highlight how the evolution of relations between national and European administrations, in the context of the process that is defined as “integration”, gives rise to the idea that a first need to be met is a greater degree of interconnection between those who are involved in the administrative proceedings.
Indeed, from an analysis of the main doctrine that has dealt with the subject of European administrative integration, it is clear that some of the features immanent to what today must be called “good governance”, such as clarity and accountability, can be achieved precisely with the help of new technologies.

In particular, blockchain would appear to be in tune with these needs and functional to them, being able to also act, in the future, as a basis for the implementation of more penetrating automation tools.

3.2 The European Administrative Integration Process and Competition Law Enforcement

Given the vastness of the theme pointed out above, I consider it appropriate, first of all, to delimit the field of investigation to a more precise research context: and in particular that of the relationship between blockchain technologies and the process of European administrative integration, referring to the specific case of the European Competition Network. I will try to explain the peculiarities of this type of technology that make it so interesting in the eyes of the administrative jurist.

First of all, it is necessary to establish what is meant by the “European integration process”.

From the perspective of the founders of the Community, the European administrative sector was supposed to be very small, leaving it to the national administrations to implement Community policies internally.

This can easily be deduced from the third paragraph of Article 5 of the Treaty of Paris: «The institutions of the Community shall carry out these activities with a reduced administrative apparatus, in close cooperation with the parties concerned». This was, on closer inspection, the normative definition of that principle, expressed by Jean Monnet, according to which, the Community «does not do, but makes do» (Chiti E., Franchini C., 2003).

However, with the proliferation of the European Community’s powers and attributions, its administrative organization, inspired by the principle of the so-called “indirect administration”, began to show its weaknesses,
initiating an evolutionary process that, starting with the Maastricht Treaty (1992), saw the Union’s administrative apparatus greatly strengthened.

The integration process is thus, first and foremost, a process of expansion of the organizational sphere of the European institutions, followed by the identification of new models of integration, communication and interaction between European administrations, in particular the Commission, and national administrations, as well as between the administrations of different Member States (Della Cananea G., Franchini C., 2017).

This process is based on the two fundamental principles of loyal cooperation and of subsidiarity, and it lays on new forms of co-ownership of the administrative function, which sees the framework of relations between administrations, national and supranational, becoming more and more intertwined.

Indeed, the administrative integration required the creation of operational models that made it possible to effectively carry out joint administrative activities, and to this regard, we can point out the “co-administration”, the “decentralized administration” and the “networks of bodies”, which have been joined more recently by the so-called “common systems of independent powers” (Massera A., Spagnuolo F., Simoncini M., 2009).

With particular regard to the competition field, the process of integration leads us to that particular model of administrative collaboration which goes under the name of “European Competition Network” (Expression first used in the Commission Notice on cooperation within the Network of Competition Authorities 2004, C 101/43). The examination of the “ECN” is particularly interesting in this context, as the evolution of the discipline of the protection of competition reflects the parable of the European administrative integration process.

The protection of competition is, in fact, a function originally centralized to the community institutions: not only has the discipline, primary and secondary, been of Community origin, but also its implementation has been left to the direct intervention (ed exclusive) of the Commission. The reasons for this “centralization” can easily be placed at the door of the protection of competition which was immediately attributed a fundamental role in view of the achievement of the objectives of the EU legal system.
However, a lot of problems arose from this centralization, for many reasons, first of all the difficulty for the Commission to manage the workload and, of course, the increased capacity of national authorities to manage disputes rooted in their areas of expertise. These are, in fact, the main reasons for the creation of the Network by Regulation n. 1/2003.

Such a system requires adequate coordination and the control of coordination mechanisms, in order to ensure the unity of the network and the consistent application of antitrust legislation. National authorities and the Commission are therefore integrated in a unitary system both from a functional and an organizational point of view. In accordance with the peculiar criterion of the division of competences chosen by the Community legislator, this organization does not have a vertical structure, but instead a reticular one in which, while not lacking superordinate relationships necessary to ensure consistency in the implementation of the discipline, the principle that dominates is the one of collaboration. The authorities are, in fact, all called to collaborate in the same way, not only in view of the uniform application of Community law, but also to ensure a correct and adequate “division of labor”.

The Network is based on two main pillars, which leads us directly to the problem of information exchange: “The first pillar is an informal case allocation regime which is set forth in detail in the Commission’s Network Notice. The primary objective of this mechanism is to attribute each individual investigation, to the possible extent, to a single ‘well placed authority’ based on the link between the geographical market in question and the territory of the competition authority involved; The second pillar contains extensive information exchange mechanisms between the competition authorities.” (Kegeleers S., 2017)

For the correct functioning of the network, it is therefore essential that the cooperation is effective. In addition, it is important to underline that this effectiveness is strictly related to the quality of the information exchange going on between the authorities.

So far, this complex activity has been carried out through a very articulated set of meetings and relations internal to the network, whose organizational chart is particularly complex. This kind of functioning has some core problems which, to be perfectly honest, are very common in every complex administrative proceeding.
First of all, the system put in place by Regulation n. 1/2003 should be strongly based on equality between all the members of the Network. However, it must be said that this is more an aim of the Regulation than the starting point. This is very clear from the reading of the Regulation, which maintains many specific rights and attributions concerning the Commission with the risk of an unwanted verticalization of the relationships between it and the national authorities (D’alberti M., 2005).

Some scholars pointed out that the ultimate and desirable goal of the equality might be achieved with just a stronger and wider homogeneity among the national authorities, making the necessity of a centralized intervention far less needed (D’alberti M., 2005; Cassese S., 2003; Gauer C., 2002; Jenny F., 2002). Here, it is important to incidentally underline that this is actually the core concept behind the Blockchain technology: providing a decentralization of power by making the participants actually peers. This is probably the number one reason why this technology is now under the lens of public lawyers.

Another very important issue, strongly related to the first one, is that for the functioning of the network, it is of capital importance that every member has and works on the same information. So the transparency among the authorities has to be complete in order to guarantee the accountability of the authorities and, as a consequence, full trust inside and outside the Network.

The trust issue is of central importance, and many studies have been carried out in the past with particular regard to this issue in the European integration process (Brito Bastos F., 2019; Volpato A., 2019; Dzino N., Rusu S., 2019). The fact is that a lack of trust inside a network of public administrations or authorities may inevitably lead to an increment of the use of the callback powers (of the Commission in the case of the ECN) and to wide phenomena of overlapping between the different authorities, with a negative effect on the efficacy of the network itself.

So, generally speaking, for integration modules to function, some qualities are needed: at least we need transparency and accountability – in order to create trust – and procedural standardization. Trust and procedural standardization help the system become a healthy functioning system because they create the right assumptions for real cooperation between peers, a real equality. If something in this valuable circuit does
not function properly, there is the rule of law, providing callback systems which permit the network to function anyway.

Thus, in order to arrive at the second topic – the use of blockchain – let us draw some early conclusions on this first part of the discussion.

Firstly, the administrative integration process follows the one on normative integration, and, at a very basic and conceptual level, it consists of the creation of an organizational administrative framework coherent with the co-ownership of the administrative function that is to be exerted. Since this administrative function is co-owned, the organizational framework should be designed to guarantee full information exchange, procedural standardization and, consequently, accountability and trust.

Those characteristics are indeed the only ones which are able to lead the integration towards an equality-based system, avoiding the verticalization of power that leads to inefficiency of the exercise of the administrative function. So, we can clearly see that it is in the relationship between the organizational and functional level that the integration process lies.

3.3 Blockchain, e-Governance and the European Competition Network

Thus, the question is: can we use ICT as a tool to achieve this coherence between the organizational and the functional level?

It has been said that “E-government is undoubtedly one of the most effective tools for establishing common administrative standards, by defining the computer code and other technology options” (Amoretti F., Musella F., 2011). The main difference between the rule of law and the rule of technology is that the former may lead to a certain result by imposing regulations from the outside, while the latter is instead able to implement the solution to a certain problem directly in its functioning.

This is the main reason for the level of interest that all the branches of law – including the administrative one – have recently been showing in the technologies that are able to lead us towards this kind of automation, both with regard to the internal and external activity of the public authorities.
Recently, blockchain in particular has been at the center of the discussions between legislators and public lawyers.

Firstly, the European Union is clearly interested in this means. It is sufficient to recall the establishment of the European Blockchain Observatory and Forum, of the European Blockchain Partnership and of the European Blockchain Services Infrastructure (EBSI), a joint initiative between the European Commission and the European Blockchain Partnership that aims at providing cross-border public services at the EU level using Blockchain technology. Moreover, it is of particular interest that the “European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation”, “Underlines the profound impact that DLT-based applications could have on the structure of public governance and the role of institutions” (paragraph 2), “Notes that ensuring efficiency requires interoperability: (i) between DLTs; (ii) between applications built on the same DLT; and (iii) between DLTs and legacy systems” (paragraph 40), and, finally, “Underlines the efficiency potential of DLT for public sector services and management as regards reducing bureaucracy, especially with a view to enforcement of the eGovernment Action Plan, with particular reference to the EU-wide adoption of the digital Once-Only Principle (TOOP) and thus further reducing administrative burdens for citizens, businesses and public administrations” (paragraph 47).

At the Italian level, I would recall the “Proposals for the Italian strategy on the subject of technologies based on shared registers and Blockchain” instead, and, most importantly, the Law Decree, n. 76/2020 (so-called “simplification decree”) which has arranged many innovations in the field of new technologies. Among those innovations, one is particularly interesting as regards public governance: the modification of Article 3 bis of law 241/1990 (the general law on administrative proceedings), which now establishes that “To achieve greater efficiency in their activities, public administrations act through IT and telematic tools, in internal relations, between the various administrations and between these and private individuals”. An application of this principle is Article 14c 5 bis, of the same law: “By agreement between the administrations involved, the conference of services is convened and carried out using the IT tools available”. I incidentally underline that the conference of services is an organizational tool used in cases in which some different administrations need to collaborate; as in the case of European integration.
On the side of doctrine, the discussion has instead initially been focused on the particular type of blockchain – private or public – that might be used in the public administration sector (with a strong preference for the private one). In this regard, it is important to underline an aspect which is strictly linked to what was said previously: in one way or the other, a rigid application of the blockchain model for administrative activities leads, hypothetically, to the dissolution of the role of public administration (Caldarelli S., 2020). This demonstrates what was said in relation to the ability of this means to make the functional and organizational layers coexist.

Afterwards, the attention shifted to the specific applications of the technology at issue, leading to all sorts of new ideas and concerns.

For sure, the first reason why blockchain might be a useful tool in integrated administrative proceedings is the one related to the interoperability of information. Networks of authorities such as the ECN are mainly based on a vast process of information exchange which largely happens on an informal basis. Luckily, the national authorities have shown a great capacity to collaborate, but the lack of a clear system of communication – going beyond the periodical meetings and the informal updates – may create trust issues inside the Network and, also, outside of it, with consequent drawbacks on the market. So, a tool that may guarantee a perfect state of equal information – kept constantly up to date – and the interoperability between that information – as blockchain maybe – would protect the Network from the risk of a lack of transparency and thus from the verticalization process that would follow from it.

Moreover, once the Network is fully connected, and all the operators are in a condition to work in a state of perfect reciprocal information, guaranteeing transparency and traceability of the activities of each and every authority, blockchain may be then used as a rule of code.

First of all, as discussed above, in the ECN, every time a particular case emerges, it must be firstly decided which authority is going to intervene. This decision is made on the basis of the information at hand, but in a network linked by a blockchain system, in which all the operators share the same information, the process may be far easier and also far more efficient. Moreover, especially for the cases that are of supranational relevance, once the decision has been made, the authority in question will be able to count on the unstoppable flow of interoperable information
collected by the other authorities or by the Commission. They will just have to carry out their activities as usual, knowing that the state of the information is constantly being updated. Such a system might make the need for joint interventions less important, with a direct effect on the overall efficiency of the Network, leaving the national authorities free to take care of their specific cases. From this point of view, blockchain can help us in coding the cooperation paradigm of the Network, reducing the necessity of imposing it through rules and guidelines.

This might actually be disruptive for all the administrative procedures, which are evolving towards a less linear and more multi-structured way instead. The complete interoperability of information and the other features of a blockchain system – such as traceability and transparency – may release public administration from the burden of the reciprocal active exchange of information made necessary by the otherwise inevitable trust issues.

From a second point of view, blockchain – under the form of smart contracts – may help in the standardization of the leniency programs of the different national authorities, the inhomogeneity of which may be the cause of their failure to achieve their goal: making the emergence of complex economical cartels easier. Indeed, for the regulators, blockchain may also become a way to intervene in the market. A smart leniency program may be used in the contexts which are suspicious in the eyes of the authorities in order to ensure, if one of the companies agrees to it, a constant flow of information regarding the transactions made in the cartel, eliminating the issue of proof (Schrepel T., 2019). The advantages of this system would probably lead to a standardization of the leniency programs, guaranteeing far more efficient ways to investigate cartels (Favaro T., 2020). So, we can say that blockchain may be used for the internal process of integration between different administrative authorities, but also for intervention purposes in the market.

Finally, let us draw some conclusions. One of the European competition networks is just an example of why blockchain is at the center of the administrative law discussion and of what the so-called “rule of code” means.

From the first point of view, blockchain is both an organizational and a procedural tool, the most important characteristic of which – from the side of public administration – is the interoperability of information.
From the second point of view, blockchain – in all its forms – is able to embed the goal in the process itself, going beyond that distinction between the organizational and procedural level that has always been the main concern of administrative theory. In many ways, it is a completely different perspective on the administrative function.

Finally, if the ECN is a clear example of the direction of the European integration process – in which, as some scholars have highlighted (Della Cananea G., Franchini C., 2017; Cassese S., 2004), the functions and the procedures are prevalent in the organizations and the structures, and moreover, the administrative paradigm is shifting from a hierarchical one to a more reticular one – it seems quite evident that blockchain, by virtue of its ability to guarantee the interoperability of information and disintermediation in proceedings, will be a fundamental tool for the evolution of the European Governance. In this perspective, blockchain should not necessarily be the end of the administration, but a way to build an organization coherent with the administrative function: which is the key to efficiency. As one scholar has put it: “the blockchain does not appear so much as a further innovative tool for governing public and private policies, as a new vision which identifies in the interaction and mutual control a guarantee of efficiency and modernity” (D’Onofrio, 2022).

References


Chapter 3  Blockchain and European Administrative Integration: a Reflection …


Matassa M., Blockchain e pubblica amministrazione: stato dell’arte e prospettive, in Istituzioni del federalismo, 2021, 3.

Orofino A.G., La semplificazione digitale, in Il diritto dell’economia, 2019, 3.

Paco D’Onofrio, La blockchain nell’azione pubblica e privata di governo, in Il lavoro nelle pubbliche amministrazioni, 2022, 2.


Pesce G., Funzione amministrativa, intelligenza artificiale e blockchain, Napoli, 2021, 253 ss.


Viola L., L’intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell’arte, in Federalismi.it, 2018, 21.

Chapter 4
An Experiment on Double Entry Bookkeeping and Financial Reporting Using Blockchain

Abstract: Within the framework of the Financial Information Retrieval Ecosystem (FIRE) project, we conducted an accounting experiment on Hyperledger Fabric, which is a freely available permissioned blockchain platform. The experiment consisted of journalizing several types of transactions including some equity and profit accounts (e.g., double-entry bookkeeping). Thereafter, financial statements were generated automatically off-chain by retrieving data from the journal entries.

This experiment adds to the literature on the use of distributed ledger technology in accounting. The outcome confirms the feasibility of using this infrastructure at a reasonable cost and with an acceptable administrative burden. We conclude by discussing some remaining concerns regarding the scalability of the system and some possible alternatives.

4.1 Introduction
If corporate blockchain is still limited to certain niches like IoT or smart contracts, there is a strong consensus that distributed ledger technology (DLT) will spread to numerous management areas in the near future (Deloitte, 2018, 2019, 2020, 2021). In the field of financial information, few companies actually keep their accounts using distributed ledger technology (Itabashi and Garcia, 2021, Pedreno et al., 2021). Most of them are businesses that record only cryptocurrencies and token transactions
From a technical point of view, these transactions are cash-based, and not sufficient to fulfil financial and tax declaration requirements. However, the accounting profession has repeatedly acknowledged the importance of digitalization and big data in the future of accountancy (Ernst and Young, 2019, Ghandar, 2022) and academic research in this area is growing rapidly (Kokina, 2017, Schmitz and Leoni, 2019).

Our paper, as part of the Financial Information Retrieval Ecosystem (FIRE) project, experiments with corporate bookkeeping techniques using Hyperledger Fabric, a permissioned blockchain platform. The FIRE project is investigating several options for the sharing, storing and retrieval of raw financial information using joint databases. One of these options is to have companies record journal entries on distributed ledgers, which would then be shared with tax administrations and other entitled third parties.

The purpose of our research is to experiment with the feasibility of 1) recording complex transactions using a wide range of accounts 2) generating financial statements from these entries. It is limited in scope, since we did the accounting procedures for one single company, while the FIRE ecosystem is intended to be used by a large number of firms.

The remainder of this paper is organized as follows. In Section 1, we review prior literature and professional reports of DLT corporate state of the art. In Section 2, we explain the research design and technical choices of the experiment while in Section 3, we provide a summary of tasks and processes necessary to achieve the preparation of accounts. Finally, in Section 4, we conclude and discuss the results of the experiment.

### 4.2 Prior Research and the State of Affairs Regarding the Use of Blockchain for Accounting Purposes

#### 4.2.1 Distributed Ledgers and Business Accounting

Can blockchain become the new ledger for businesses? There is room for innovation in information systems, and recent years have shown
that accounting techniques are changing rapidly in order to adapt to technological change (Coyne and Mc Mickle, 2017, Tysiak, 2017).

Modern accounting records consist mostly of databases and digital records from management software or open-source solutions. Blockchain is also a kind of database – with some particularities – that could become the next mainstream technique in this field if different infrastructure will allow it (Carlin, 2018, Tan and Low, 2019, Cai, 2019).

Distributed accounting ledgers using cryptography such as blockchain are qualified as “triple entry bookkeeping”, after the pioneering work of I. Grigg (2005). Basically, triple entry bookkeeping consists of a set of two journal entries using a shared ledger between the parties (Tyra, 2014). In other words, if a transaction between A and B is recorded based on this technique, A will record an entry using an account from his or her own private ledger for one side, and a shared ledger with B for the counterpart account. B does the same, and the entry on the shared ledger is common to A and B, which makes it unfalsifiable (Grigg, 2005).

A shared ledger is immutable once a transaction has been recorded. This is the most important difference between DLT and traditional information systems (Itabashi and Garcia, 2021). This is an interesting way of avoiding fraud. In this regard, using some ledgers that are embedded in a blockchain could improve the reliability of accounting data for users such as investors, tax authorities or even for internal controls. Its benefits for auditing have also been emphasized in the literature (Simoyama et al., 2017, Dai and Vasarhelyi, 2017, Schmitz and Leoni, 2019).
Besides, information can be shared selectively using public or private codes for blocks. Transparency can be adjusted depending on the target of the information: if companies want information to be readable by others, they can set public codes for the blocks, while private information can remain protected by private codes. In so doing, businesses would be able to share part of their ledgers with some users, while keeping other transactions secret (Itabashi and Garcia, 2021).

Enterprise blockchain is particularly interesting for companies that operate through several business units and production sites (Faccia and Petratos, 2021). Since they can decide the level of transparency and which parties are to be allowed to participate in their blockchain, they can control who creates and accesses information (Karadakis, 2018). For example, some intra-organizational information systems could allow the sharing of sales data between several distribution sites (Japan Blockchain Association, 2020).

“Smart contracts” are a particular example of a transaction being shared and automatized between parties. In this case, transaction terms and payment information are written automatically in a block and shared between the vendor and the seller, sometimes even with VAT embedded (Coyn and McMickle, 2017).

However, transparency should not be overemphasized in business accounting, since it implies certain risks for companies. For example, why would they share their transactions with competitors? Information asymmetry is part of negotiations with business partners, and it also protects their strategic decisions. In addition, transparency regarding tax and various declarations may not be a priority for some businesses trying to escape or delay some of their public liability.

DLT is certainly ideal regarding the reliability of information, but it drastically changes the boundaries of public knowledge. In this regard, there are some important limitations, especially for smaller and innovative businesses, which could be harmed by too much publicity. Overall, the unlimited sharing of information through DLT needs to be carefully investigated. Semi-public blockchains could offer a good compromise for these issues (Itabashi and Garcia, 2021).
4.2.2 Using Shared Ledgers for Reporting

Most literature about DLT focuses on recording specific transactions, such as payments using virtual currencies. Cai (2019) reviewed several projects using tokens, whose purpose is to replace traditional accounting ledgers with some shared, DLT-based, token-based ledgers. Although some authors criticize the feasibility of such initiatives (Coyne and McMickle, 2017), others propose the use of DLT to replace traditional databases (Weigand et al., 2020, Patel and Lal Das, 2020). In this research, we assume that technology and scalability issues will improve in the future and mitigate the current costs of mining.

Patel and Lal Das (2020) proposed a blockchain application in order to share university transcripts without disclosing personal information to third parties. This system is particularly interesting for bookkeeping and reporting because it deals with non-quantitative information such as images etc.

For example, a receipt could be produced by a seller and made available to the customer based on DLT. Another idea from the Patel and Lal Das (2020) application would be to share images of invoices or receipts for SMEs that report VAT. This could considerably reduce the need for tax audits and the administrative burden of companies that do not have a systematic information system for that purpose.

Financial reporting using DLT is investigated in Weigand et al. (2020). They adapted the accounting concept for transactions (basically, a sales transaction in IFRS) and the reciprocal commitments of parties in a formal representation. Based on that ontological approach, they proposed a DLT-based application in order to record and share financial information.

In their model, each entry should include the following elements (Weigand et al., 2020, 9).

- Event identifier (EID),
- Transferor type – Customer or Provider (or more specialized role), that specifies the context view for the transfer,
- Event type – Offer, Agreement, Fulfilment or Settlement of Transfer, Performance or Contract obligations, Realization, Other Recognition, Reclassification, Revaluation (or more specialized subtype),
- Date or Period, and
– Currency Unit,
– Provider and Customer identification,
– Local currency units with the spot exchange rates.

This system is based on shared ledgers between clients and suppliers, as in the triple entry bookkeeping system described by Grigg (2005). The first column in the ledger example infra corresponds to the shared ledger, which can be automatized with a smart contract.

Fig. 2: Example of shared ledger between provider A and customer B (Weigand et al., 2020).

In the Weigand et al. (2020) model, all transactions would be labelled in digitized resources (tokens), but they acknowledge that some reporting systems like Hyperledger Fabric can use the traditional accounting categories of assets, and not only tokens, in order to report economic transactions. Our experiment follows their suggestion with some technical improvements that we will detail in the next section.

4.3 Research Design and Technical Choices

Several blockchain platforms are used or experimented with by companies. The results of a worldwide survey conducted by Blockdata (2021) are presented in Table 1.
### Table 1: Corporate usage of blockchain platforms, data computed by the authors based on the Blockdata survey (Blockdata, 2021, 15).

<table>
<thead>
<tr>
<th>DLT Platform</th>
<th>Number of companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyperledger Fabric</td>
<td>26</td>
</tr>
<tr>
<td>Ethereum</td>
<td>17</td>
</tr>
<tr>
<td>Quorum4)</td>
<td>11</td>
</tr>
<tr>
<td>Corda</td>
<td>8</td>
</tr>
<tr>
<td>Hyperledger Sawtooth</td>
<td>3</td>
</tr>
<tr>
<td>AxCore</td>
<td>3</td>
</tr>
<tr>
<td>Hyperledger5)</td>
<td>3</td>
</tr>
<tr>
<td>BitCoin, GumboNet, Ant Blockchain, Medilegder, Multichain</td>
<td>2 each</td>
</tr>
<tr>
<td>Theta Blockchain, Diem, FISCO BCOS, OpenSC, Dragonchain, Baseline (check), MadNetwork, DAML (SC language), Zilliqa, Flow, Fiducia, Energy Web Chain, Ripple, Cardano, FiMAX S3C, Aura, Medilegder, Mastercard Blockchain, private blockchain</td>
<td>1 each</td>
</tr>
<tr>
<td>Not disclosed</td>
<td>2</td>
</tr>
<tr>
<td>Unclear</td>
<td>15</td>
</tr>
<tr>
<td>None</td>
<td>26</td>
</tr>
</tbody>
</table>

We have chosen Hyperledger Fabric as a platform for this experiment. Hyperledger Fabric is a permissioned platform with an administrator that does not have its own cryptocurrency, but that allows the creation of a token / tokens. We used a smart contract program to create tokens / a token, and we registered transactions off-chain for the experiment.

The original system of Hyperledger Fabric does not allow for a great variety of transactions: creation, sale, information update and removal of a token (“Asset”). In order to increase the diversity of entries, we have created other categories: Liability, Equity, Profit and Loss. The accounts used in double entry bookkeeping are classified in these categories by means of a tag that appears in the definition of the item.

The experiment consisted of journalizing several types of entries, and subsequently generating a balance sheet automatically from these entries. In this paper, we describe in detail the process for the version of Hyperledger Fabric web that we have used. The balance sheet was
generated using the ending balance of all “asset”, “liability”, “equity” tagged accounts, with “equity” also including “profit” and “loss” tagged accounts.

4.4 Summary of the Experiment

4.4.1 Construction of the System

The first step of the experiment was to install Hyperledger Fabric v2.4.2 on a local computer to access the blockchain platform. The world state database that we used was ‘CouchDB’ because the data can be saved in JavaScript Object Notation (JSON), which was convenient for the subsequent generation of financial statements.

The main program used for the experiment was ‘Fabric Test Network’, which is designed for testing, learning and operation verification on a local computer. The program is accessible from the Hyperledger Fabric website. The main difference with the normal version of Hyperledger Fabric is that this simplified version requires only two peer organizations and one administrator to operate it, and that consensus is based on a Raft protocol at each node.

The main program was modified for the purpose of the experiment as follows:

a) Since the search and computation of data tend to reduce the speed of the network and interrupt transactions when implemented directly on chain, we created an off-chain database for computational purposes. This database was generated and updated automatically using a specific program written in the main program.

b) A smart contract was created to issue tokens, which was also written into the main program.

c) The usual version of Hyperledger Fabric records issuance, transfer, information update, and the write-off of assets. In order to create a double-entry bookkeeping system, we added liability, equity profit and loss as new categories – in addition to assets – by means of new functions embedded in a smart contract. The smart contract model also included the automatic tagging of the journal entry to reflect the categories impacted by the transaction.
d) Tags are necessary to retrieve information directly from Hyperledger Fabric. We used the following tags: date of transaction, account category (asset, liability, equity, profit and loss), account name, owner, amount, and for asset accounts quantity. In order to trace transactions affecting the same item, we also included another tag called “control number”.

e) Some entries require third party identification, for example, contribution to capital or transfers of tokens. The counterpart must then communicate their ID in a readable format. The ID was included in the journal entry for the verification of the recipient.

In the blockchain network, we created two participants, “organization 1” and “organization 2”, which operate one node each and which validate the transactions and add information to blocks. Additionally, an administrator “orderer” was created, whose role was to decide the order of transactions and the creation of new blocks. This was done by creating certificate authorities (CA) for each of the three parties involved.

Lastly, we created a channel of transactions. In Hyperledger Fabric, it is possible to create several channels in a network, so that some participants join one channel, while others join another. In our experiment, we used only one channel because there were only two participants, however, this function is particularly interesting regarding the disclosure of information (see section 5 infra).
4.4.2 Journal Entries

Several transactions were recorded using double-entry bookkeeping, for example:

- Increasing contributed capital
- Borrowing from the bank
- Purchasing equipment
- Purchasing merchandise
- Sale of merchandise etc.

We also recorded an accounting adjustment to reflect unsold inventory at year end.

Let us explain in more detail the example of a capital increase realized on 1st April 2022, for an amount of 500,000 units. Table 2 below presents the corresponding journal entry in traditional bookkeeping.

<table>
<thead>
<tr>
<th>Date</th>
<th>Account</th>
<th>Debit</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1</td>
<td>Cash</td>
<td>500,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equity</td>
<td></td>
<td>500,000</td>
</tr>
</tbody>
</table>

Table 2: Journal entry for a capital increase.

In Hyperledger Fabric, this was recorded in several steps. First, we created an entry for the issuance of stock, which becomes an issuance of coins in our system. Each coin is worth 10,000 units, so the company issued 50 coins.
test-network $ peer chaincode invoke "${TARGET_TLS_OPTIONS[@]}" -C mychannel -n token_erc20 -c '{"function":"Mint","Args": ["50"]}'

2022-09-11 17:01:06.292 JST 0001 INFO [chaincodeCmd] chaincodeInvoke-OrQuery -> Chaincode invoke successful. result: status:200

Next, we recorded the transfer of ownership of coins to the investor. We assumed that the investor had communicated his ID to the company in order to embed ownership information into the entry.

test-network
$ RECIPIENT="eDUwOt049cmVjaXBpZW50LE9VPWNsaWVudCZPb3JnYXBlLm9yZzIuZXhhbXBsb2dSb2dpdC5mb3QuY29tLEw9SHVyc2xleSxTVD1IYW1wc2hpcmcz1VSw=="
test-network $ peer chaincode invoke "${TARGET_TLS_OPTIONS[@]}" -C mychannel -n token_erc20 -c '{"function":"Transfer","Args": ["'$RECIPIENT'",50"]}'

2022-09-10 03:24:38.735 JST 0001 INFO [chaincodeCmd] chaincodeInvoke-OrQuery -> Chaincode invoke successful. result: status:200

Lastly, we recorded the capital increase itself, which in double-entry bookkeeping corresponds to the sentence “equity increases by 500,000 and assets increase by 500,000”. This is the main entry of the transaction, and we tagged it as follows:

- Transaction date 20220401
- Control number B0001,
- Account name Xyzdeposit
- Owner Xyz
- Amount 500,000
- Quantity 1.

The corresponding record in Hyperledger Fabric was as follows.

+ node addAssets.js 20220401 B0001 XyzDeposit1 Xyz 500000 1

Adding asset:Date:20220401 Type:asset ID:B0001 AssetName:XyzDeposit1 Owner:Xyz Price:500000 Quantity:1

+ node addEquity.js 20220401 B0002 XyzEquity1 Xyz 500000

Adding equity:Date:20220401 Type:equity ID:B0002 EquityName:XyzEquity1 Owner:Xyz Price:500000
4.4.3 Financial Statements

In traditional bookkeeping, the balance sheet and income statement are prepared at year end by computing the ending balance of accounts, proceeding with some adjustments in value, and then aggregating the resulting information. In our experiment, adjustments were recorded on the chain, and we used an off-chain Javascript-based program to search for debits and credits affecting an account, compute the ending balance and compile all ending balances in the financial statements.

Below is an example of requests for information regarding assets held by Xyz.

```bash
+ peer chaincode query -C mychannel -n basic -c '{"Args": ["QueryAssetsByOwner", "Xyz"]}

[{
  "Date": "20220405", "ID": "B0005", "Type": "asset", "AssetName": "XyzEquipment1", "Owner": "Xyz", "Price": 300000, "Quantity": 1}, {
  "Date": "20220415", "ID": "B0006", "Type": "asset", "AssetName": "XyzGoods1", "Owner": "Xyz", "Price": 100000, "Quantity": 10}, {
  "Date": "20220409", "ID": "B0007", "Type": "asset", "AssetName": "XyzDeposit3", "Owner": "Xyz", "Price": 300000, "Quantity": 1}, {
  "Date": "20220415", "ID": "B0008", "Type": "asset", "AssetName": "XyzDeposit4", "Owner": "Xyz", "Price": 120000, "Quantity": 1}]
```

It is important to stress that the program can be run on any date, and does not require much effort to process, so that financial statements can be generated almost instantly and at no cost. The reason for that is that closing adjustments in value are assumed to be recorded on the chain. Also, the financial statements program could be embedded directly in the chain, but it would slow down the recording of new transactions, so we decided to leave it off-chain.

Table 3 below shows the final output of the experiment: the retrieval process at the top and financial statements at the bottom.
Chapter 4  An Experiment on Double Entry Bookkeeping and Financial …

Table 3: Financial statements generated from information automatically retrieved.

In the last section at the bottom, the two columns on the left, “asset” and “liability and equity” are the ending balance sheet. On the right, “loss” and “profit”, constitute the income statement. Net income appears on both statements for 20,000 units. The upper part of Table 3 just shows the iterations of the retrieval process after each transaction.

4.5 Conclusion and Discussion on the Results

As far as the experiment appears successful, we believe that distributed ledger technology could be used as a means to provide more timely and verifiable information to stakeholders. In terms of the administrative
burden, the decentralized organization of the network implies additional records, such as the verification of identity in case of a transfer of ownership. On the other hand, the potential benefits of automatization would certainly exceed these supplementary tasks.

Besides, it is important to note that companies using this system would not be involved in the preparation of the financial statements. Even if they remain responsible for the original input of information, the risk of fraud in the final output decreases considerably, since a balance sheet that is generated automatically cannot be modified by the enterprises (Dai et al., 2017, Bible et al. 2018). This aspect would drastically change the responsibility of corporate directors and auditors (Deloitte, 2016, Bible et al., 2018, Desplebin et al., 2018).

We found through our experiment that Hyperledger Fabric allows the creation of several channels (set of entries) that can be used to differentiate access to the data. For example, some entries could be shared with customers, and others with the tax administration in a manner that protects privacy and trade secrets. This aspect is particularly important given that blockchains are not foolproof (Sako and Furukawa, 2021) and do not fully ensure the privacy of individuals (Narula et al., 2018).

Besides, the traditional limitations of blockchain regarding costs, scalability and speed (Gountia, 2019, Kusunoki, 2021) would remain if this system were to be generalized among businesses, even the environment of a permissioned blockchain. For that reason, it appears necessary to investigate further the infrastructure to be used for the FIRE ecosystem.

The challenges remain for future research and we can already identify several areas of improvement. A first approach, proposed by Itabashi and Garcia (2021), would be to select information and share only entries that are important to third parties. The rest would remain in local databases, traditional information systems or sidechains.

A second approach would be to reduce the quantity of data necessary for each entry. For example, instead of replicating information used in traditional journal entries as we did in this experiment, we could condense transactions with a single code or a label.

Last but not least, the simplest way to solve the issue in the short term would be to divide the ecosystem into several subsystems, in order to reduce the number of entries treated by each blockchain network.
However, given the exponential increase of corporate financial data, this may not provide a viable solution in the long term.

References


Ledgerium (2019). Blockchain accounting system. Available at: https://www.ledgerium.net/home/.


Abstract: Forest deductions are calculated based on the acquisition value of the forest and the disposable income. The total number of forest deductions that forestry owners are allowed to make during the holding period shall be calculated based on the acquisition value of the whole property, the property’s registered assessment value and the forest’s registered assessment values according to the main rule in Chapter 21 Section 12 IL (the Income Tax Act). In my post-doc project, I will examine problems regarding the income taxation of forestry, specifically how to determine forest deductions. This is the first article in this post-doc project and in this article, I will describe the rules on the kind of data that are being registered on forestry assessment values and how the registered assessment values on forestry may be used to determine forest deductions. My post-doc project has been financed by a post-doc scholarship from TOR/Skattenytt.

5.1 Introduction

It is said that the forest’s contribution to the fight against climate change is of the greatest importance. Climate change affects more or less all countries throughout the world and affects the conditions for most of society’s sectors, including agriculture and forestry. With climate change in mind, forests need to be managed sustainably. However, there are divided opinions about what constitutes sustainable forestry. A forest as a collective good with people’s rights and the goal of biological diversity at the forefront stands often in conflict with property rights and the forest
owner’s interest in immediately making use of the forest. At the same time, the demand for forest products is increasing. Hence, the necessary efforts to create a coordinated financial system that promotes sustainable solutions for agriculture and forestry is required. In Sweden, income tax on forestry is based on the idea that there is a long period of time that passes from the trees being planned until the trees can be felled. During this time, the value of the forest may change for different reasons, for example, if part of the forest property is sold. These values of the forest are also directly linked to the taxpayer’s right to make forest deductions when, for example, selling felling rights. Because of this, these forest values need to be registered correctly.

At the end of the 1960s, a real estate data reform was initiated. A new system based on automatic data processing was introduced at the registry and registration authorities. The system was called the real estate data system. The reform was fully implemented in September 1995. From the beginning, that system consisted of the property data system, the property register, the registration register and certain information from the property assessment. In 1995, a special investigator was summoned to review the constitutional regulation of the real estate data system and submit proposals for the necessary constitutional changes. At that time, the constitutional regulation dated back to 1973–1974. Some changes in this regulation were carried out after the new system had been implemented in 1995, but a comprehensive review had not been performed. The Swedish Tax Agency uses registration systems like these as a basis for decisions on forest deductions.

The increased amount of information in the property data systems as well as new user groups and forms of use with increasingly advanced technology raises questions regarding income taxation on forestry and puts them in a new light. The purpose of this article is to make an inventory from an income tax law perspective regarding the registration of

---

1 See SOU 2002:40, del 1, p. 43 Fall Johan, Miljöskatter och Januariöverenskommelsen, Svensk skattetidning, nr 8, 2019, p. 473–492.
forestry assessment values that are used as a basis for decisions on forest deductions and decision-making on income taxation on forestry.

Questions of interest are as follows:

1. What kind of data is being registered on forestry assessment values?
2. How may the registered assessment values on forestry be used to calculate forest deductions?

The questions will be examined using the legal dogmatic method. Using the legal dogmatic method here entails that the problems will be analyzed based on legal sources such as legislation, treaty texts, convention texts, preliminary works, legal practice and doctrine. By analyzing legal problems based on the legal sources, you can also interpret and systematize the applicable law. You may also give suggestions on how the legal problems can be solved. By allowing the content of the legal basis material to influence the argumentation, the conclusions also receive legal support.

The article only brings up physical forest owners in accordance with Chapter 21 Section 9 IL, and therefore rules concerning legal entities or trading companies that own forest properties are not covered. The article will also not discuss forest accounts, forest damage accounts, real estate regulations, splitting, severing or amalgamation. Due to this, the equalization rule in Chapter 21 Section 13 is only dealt with in a general manner and Chapter 21 Sections 21–41 IL on forest accounts and forest damage accounts are not brought up in the article.

Firstly, the rules on which assessment values must be registered for forest and shoe properties are described. Secondly, an introduction is given to the rules in Chapter 21 IL on income taxation of forests. Thirdly,
the article discusses the main rule in Chapter 21 Section 12 IL for a calculation of forest deductions and total deduction area. The article ends with conclusions and concluding remarks.

5.2 Digitalization of Forestry Data

In the past, it was proposed that properties and land should be divided into different kinds of property types and different types of ownership. The classification of the property should be based on the use or nature of the property. One goal with this classification was, among other things, that it should facilitate the formation of assessment units and the valuation. If assessment units are formed based on this classification, property types and types of ownership could be combined so that the result is economic units. These economic units would be easy to value and should therefore form special assessment units.

Therefore, the committee recommended that the assessment units should be specified with regard to the property to be included in the unit. Each such type of assessment unit should, according to the committee, only include properties that belong to a specified combination of property types and ownership. The committee believed that built-up assessment units should in most cases contain only one type of building, as the division into assessment units should be made so that each assessment unit constitutes an economic unit. According to the proposal, the building type farm building and owned arable land, pasture land, forest land and forest impediment shall be attributed to agricultural units. According to the proposal, all agricultural and forestry land within a municipality, which has the same owner, should constitute a taxation unit if this land is part of the same utilization unit.

Today, the Property Assessment Act (1979:1152) FTL, regulates the kind of data that should be registered for forestry assessment values. The rules on the registration of forestry assessment values can be found in Chapter 4 FTL. According to Chapter 4 Section 1 FTL, properties shall

---

constitute assessment units, unless otherwise prescribed. These assessment units shall be taxed separately. If separate parts of a property have different owners, the property must be divided into assessment units according to the ownership relationship, Chapter 4 Section 2 FTL.

Accordingly, each property is divided into assessment units. These assessment units may, for example, consist of detached houses and land for such a building (small house unit), owner-occupied apartments and land for such a building (owner-apartment unit), apartment building and land for such a building (apartment house unit), Chapter 4 Section 5 p. 1–3 IL. The provision states which combinations of building types and types of ownership can be included in a taxation unit of a certain specified type. According to Chapter 4 Section 8 FTL, taxation units must include farm buildings, arable land, pasture land, productive forest land with felling restrictions, productive forest land without felling restrictions, forest impediments or other land that is part of a farming unit. There have also been changes to the FTL that were to be applied for the first time in 2011.

These changes pertained to the definition of forest land, so that it would conform with the corresponding definition in the Forest Protection Act. Forest land is now divided into productive and unproductive forest land. Common to these types of land is that they basically constitute forest land, which according to the definition means that they consist of land within a contiguous area where the trees have a height of more than five meters and where trees have a crown closure unit of more than ten percent or enjoy conditions allowing them to reach this height and crown closure without production-enhancing measures.

For productive forest land, this means in addition that, according to accepted assessment criteria, it can produce on average at least one cubic meter of wood per hectare and year. Unproductive forest land is land which in and of itself is forest land but which does not meet the requirements above regarding conditions in terms of timber production. Unproductive forest land constitutes, together with trees and shrubland, forest impediments. Trees and? bushland can briefly be said to be land within a contiguous area that is not forest land because it does not meet the above-mentioned requirement for tree height and crown closure unit
and where trees do not enjoy the conditions to be able to fulfill these requirements.\textsuperscript{12}

The definitions can be schematically described with the figure below:\textsuperscript{13}

![Diagram showing forest land and trees and shrubland]

5.3 Income Taxation of Forests

The rules on the income taxation of forests can be found in Chapter 21 IL. According to Chapter 21 Section 4 first paragraph IL, deductions due to the sale of forest land (forest deductions) may be made on a property in Sweden that is taxed as an agricultural unit and is a capital asset according to the provisions in Chapter 21 Sections 5–19 IL. When forest land is acquired, the compensation refers to a certain part of the land and to a certain part of a forest stand. If taxation were to take place in full when the forest stand has been felled at the time of the acquisition, it would mean that a withdrawal of invested capital, usually referred to as a capital withdrawal, is taxed. The purpose of a forest deduction is to avoid the taxation of capital withdrawals. This has been considered desirable because capital withdrawals are not regarded as income and are therefore not deemed to entail a tax liability. The taxation of capital withdrawals is thus considered to be contrary to the principle of fiscal capacity. Forest deductions are thus a clear and direct consequence of the principle of fiscal capacity.\textsuperscript{14}

\begin{itemize}
\item \textsuperscript{12} Prop./Government Bill 2010/11:21 p. 11.
\item \textsuperscript{13} Prop./Government Bill 2010/11:21 p. 11.
\item \textsuperscript{14} See Björkqvist, Jakob, Skogsavdrag i ljuset av skatteförmågeprincipen, Skattenytt, årsskrift 2016 p. 83–104.
\end{itemize}
According to Chapter 21 Section 4 second paragraph IL, forest deductions may not be made based on income that is taken up for taxation after all land or all productive forest land that is part of the business activity has been acquired by a new owner. When calculating a forest deduction, the forest deduction must be calculated based on the forest’s acquisition value, the deduction area, and the forest income on which the deduction is based, Chapter 21 Section 5 IL. Forest income and forest revenue can, for example, be obtained by selling forest raw materials. Forest raw materials can be sold, for example, through the granting of felling rights or through root sales. The granting of felling rights means a transfer of the right to harvest forest. A root sale means that the forest owner sells a certain measured quantity of forest standing on the root, while the felling right option means that the amount of timber is determined after the felling has taken place.15

According to Chapter 21 Section 6 second paragraph IL, the forest deduction is the maximum amount a property owner has the right to deduct during his holding period. Deductible forest income is the sum of the tax year’s income due to the granting of felling rights and 60 percent of the tax year’s income due to the sale or withdrawal of forest products. Forest revenue also refers to insurance compensation for forests and forest products, Chapter 2 Section 6 third paragraph IL. According to Chapter 21 Section 9 IL, a forest owner may, during his holding period, make forest deductions of a maximum of 50 percent of the forest’s acquisition value. Except for rationalization acquisitions according to Section 10, deductions for a certain taxation year may be made with a maximum amount corresponding to 50 percent of the forest income that forms the basis of the deduction. According to Chapter 21 Section 11 IL, forest deductions may not be made with an amount that is less than SEK 15,000. According to the main rule in Chapter 21 Section 12 IL, the acquisition value of the whole property and the assessment value of the forest units form the basis of the calculation of the total amount of forest deduction that the owner can make during his or her holding period of the property (the total forest deduction area). The income from

15 See Bjuvberg, Jan, Periodisering av ersättning för avverkningsrätt – vem ska fråga Bokföringsnämnden? Svensk skattetidning, nr 2, 2018 p. 122.
the forest then forms the basis for calculating the forest deduction for a certain taxation year.

It is also important when calculating the acquisition value to know how the transfer took place. If, for example, the acquisition has taken place through purchase or exchange, the main rule in Chapter 21 Section 12 IL may be applied when calculating the total forest deduction area. If the provisions in Chapter 21 Section 12 IL give a misleading result and therefore cannot be applied, the adjustment rule in Chapter 21 Section 13 IL is applied when calculating the total forest deduction area. The adjustment rule applies if an application of the main rule would give a value that deviates from the real compensation for forest and productive forest land. If so, the acquisition value is the amount that can be considered to correspond to the real compensation, Chapter 21 Section 13 IL first paragraph.\(^{16}\) If compensation has been paid in the event of property regulation or splitting because the value of the forest and productive forest land that has been added to the taxpayer’s property exceeds the value of the forest and productive forest land, an amount corresponding to the compensation shall be considered as the acquisition value, Chapter 21 Section 13 IL second paragraph.\(^{17}\)

If a part of the taxpayer’s productive forest land is sold to a new owner, the taxpayer’s acquisition value and deductions are reduced to the same extent as the reduction in the value of the forest and the productive forest land in the business, Chapter 21 Section 17 IL. The rule in Chapter 21 Section 17 IL thus means that if, for example, an individual trader sells forestland, the forest’s acquisition value and the total forest deduction area must be reduced to the corresponding extent.

5.4 Forestry Deductions According to the Main Rule in Chapter 21 Section 12 IL

As previously stated, an individual trader may make forest deductions of a maximum of 50 percent of the acquisition value during the entire


Chapter 5 Income taxation of forestry, forest deduction and digitalization

holding period. 50 percent of the acquisition value of the forest thus corresponds to the forest deduction area, Chapter 21 Section 9 IL. The total forest deduction area is then calculated according to the regulations in Chapter 12 and Sections 5–19 in Chapter 21 IL. The main rule in Chapter 21 Section 12 IL is applied if a property is acquired through purchase, exchange or in a similar way. According to Chapter 21 Section 12 IL, considered as the acquisition value as much of the compensation for the property as the part of the property’s assessment value that relates to forestry, constitutes the entire assessment value at the time of acquisition. As previously stated, through forest deductions, forest owners may deduct half the acquisition value of the forest during the period of ownership.

Forestry includes productive forest land with growing forests and land that facilities the use of or need for forestry. The calculation of forest deductions takes place through a standardized calculation where the forest deduction area is calculated as follows; the purchase price times the assessed value of the productive forest land divided by the total assessed value.

Example:

Calculation of the total forest deduction area during the holding period according to the main rule in Chapter 21 Section 12 IL:

An agricultural unit with associated forest land is acquired through purchase for SEK 5 000 000. The assessed value for the entire agricultural unit amounts to SEK 3 000 000, of which the assessed value for the forest (forest and forest land) amounts to SEK 1 200 000.

Calculation of a forest deduction:

- 1200 000/3 000 000 = 0.4, Chapter 21 Section 12 IL
- 0.4 * 5 000 000 = SEK 200 000, Chapter 21 Section 6 paragraph 1 IL
- 2 000 000 * 0.5 = SEK 100 000, Chapter 21 Section 9 IL
- Forest deduction = SEK 1 000 000, Chapter 21 Section 9 IL, Chapter 21 Section 6 paragraph 2 IL
  - The acquisition value of the forest = SEK 200 000

18 See also Helgesson, Ragnar, Hur bör framtida utgifter för nyplantering av skog perioderas? Skattenytt, TEMA EG och skatter, 1995, p. 132–133.
The total deduction area for forest deductions during the holding period = half the acquisition value = SEK 1 000 000.

Calculation of a forest deduction for a certain taxation year:
- The sum of the tax year’s income due to the granting of felling rights is SEK 500 000. Deductions for a certain taxation year may be made with a maximum amount corresponding to 50 percent of the forest income that is the basis of the deduction. In this case, SEK 500 000 is the basis of the forest deduction.
- 500 000 * 50 percent = SEK 250 000 in forest deduction that year.
- 1 000 000 – 250 000 = SEK 750 000 left in total forest deduction area after the current year’s forest deduction.

According to what follows from the main rule, it is therefore important how you value the forest and the assessment value of the forest. When applying the main rule in Chapter 21 Section 12 IL, the assessment value of the forest is used to calculate the total forest deduction that the owner can make during his or her holding period of the property. Previously, forest cases occupied a significant part of the Supreme Administrative Court’s working time, but they have now almost disappeared. This is probably connected with the 1979 forest taxation reform. Von Bahr expresses that the need to estimate the volume of growing forests at different times disappeared from the 1981 assessment. According to Von Bahr, what is now decisive for the size of forest deductions is, in principle, only the value of the forest at the time of the acquisition of the property, i.e. normally what the property owner paid for the forest, and the value of felled (sold) forest.\(^\text{21}\)

Chapter 21 Section 16 IL states that if a property is acquired through an inheritance, will, gift, division of property or in a similar way, the following applies when calculating the acquirer’s deductions. If the acquisition includes all land or all productive forest land in the previous owner’s business, the acquirer takes over the previous owner’s acquisition value. The acquirer is considered to have made forest deductions with the same amount as the previous owner. If the acquisition covers only part of the productive forest land, the acquisition value for the acquirer

is the same as the previous owner’s acquisition value and the value of
the acquired forest and productive forest land constitutes the value of all
forest and productive forest land in his business when the acquisition
takes place. The acquirer is considered to have made the same level of
forest deductions as the previous owner is considered to have made on
the acquired part. If the acquisition covers less than 20 percent of the
value of all forest and productive forest land in the business and it is not
a question of a non-profit share of a property, the new owner’s acquisition
value and scope for deduction is zero.

In the agreement with the forest buyer (usufructuary), there is often a
plan that determines how the payment is to be made, a so-called payment
plan. The alternative method of taxation of compensation for felling
rights is therefore often called payment plan taxation. In order for the
method to be applied, according to the legal text, Rydin expresses that
these two criteria must be met. Firstly, it must be a question of compen-
sation for felling rights and secondly, the payment of this compensation
must take place over several years.22

HFD 2020 ref. 9 was about a person who had sold felling rights to a
forest owner?, where the compensation was to be paid over several years.
The person who had sold felling rights had chosen to apply Chapter 21
Section 2 IL by using a so-called payment plan and had consequently
only been taxed on the amounts he had received. He intended, as part
of a generational change, to leave his entire business with all the assets
including the forest property to his two sons as a gift. The transfer would
also include the untaxed claims regarding the granted felling rights. He
applied for an advance notice to know whether the assignment of the
claims would result in him being taxed on income that had not yet been
paid but was about to be paid according to the payment plan.

The Tax Court concluded that the tax liability for future payments
according to the payment plan could be taken over by the sons when
transferring the entire business as a gift to them. Therefore, the transfer
did not mean that the taxpayer would be taxed for the remaining number
of claims according to the payment plan. As a justification, the board/Court? stated that the wording of Chapter 21 Section 2 IL does not

22 Rydin, Urban, Undantagsregleringen för beskattning av ersättning för avverkningsrätt,
prevent the sons from taking over the tax liability for future payments. The board/Court? also referred to the legal case the Supreme Administrative Court 2011 ref. 79. HFD 2011 ref. 79 pertains to how a taxpayer obtains a commercial property with forest land as a gift when the previous owner has made forest deductions without being taxed before handing over the property as a gift. The question in that case was whether the taxable person who took over the property had an obligation to return the forest deductions that the previous owner had made when the taxable person sold the property. This obligation to return forest deductions made by a previous owner was tried regarding the continuity principle that otherwise prevails in beneficial transfers of the type in question. The Supreme Administrative Court concluded that the taxpayer had an obligation to return the forest deductions that the previous owner had made according to the continuity principle.

In case HFD 2020 ref. 9, the Supreme Administrative Court stated that Chapter 21 Section 2 IL only regulates the time of taxation and has no significance regarding the tax liability as such. According to the Supreme Administrative Court, a transfer of the tax liability cannot therefore be based on this rule in itself. The Supreme Administrative Court further stated that there is no specific rule that the tax liability for claims regarding felling rights for forests can be transferred as a gift to a recipient (such rules exist for certain other incomes in the business income type). According to the Court, tax liability for income can only be transferred if there is support for this in the law. Consequently, the transfer of a claim as a gift does not exempt the owner from tax liability for future payments for the felling rights. As a result of the transfer of the future payments according to the payment plan, the taxpayer no longer fulfilled the two criteria for applying Chapter 21 Section 2 IL. Because of this, the Court concluded that the taxpayer therefore had to be taxed in the year in which the entire business was transferred to his sons.

Kleist expresses that it may be noted that a relatively extensive continuity rule is found in Chapter 44. Section 21 IL pertains to assets that are taxed according to the rules for capital gains, but there is, as the Supreme Administrative Court notes, no corresponding rule for current income in the income category business activities. According to Kleist, it could possibly be argued that the principle of continuity is a legal principle that applies to all beneficial transfers, even without direct support in law. The
fact that future payments for the harvesting right accrue to the recipient and that the recipient thereby receives funds to pay the tax could also speak in favor of a transfer of the tax liability for future payments.23

5.5 Conclusions and Concluding Remarks

In the EU’s forest strategy 2030, the Commission promoted skills enhancement to be able to broaden the use of forests, which should lead to a better financial situation for forest owners. To equalize the taxation for a trader in the forestry business, there is the possibility of several provisions. One of these provisions consists of forest deductions. A forest deduction is thus a tool for postponing income taxation of forest income and facilitating self-financing when purchasing forest properties. Because of this, the forest valuation and the assessment value of the forest is important for the size of future forest deductions.

*What kind of data is being registered for forestry assessment values?* Chapter 4 Section 1 FTL states that properties shall constitute assessment units, unless otherwise prescribed. These assessment units shall be taxed separately. There are several kinds of assessment units regarding forests, such as forestland, and forest impediments shall be attributed to agricultural units. In addition, if the property has different owners, the property must be divided into assessment units according to the ownership relationship, Chapter 4 Section 2 FTL.

*How may the registered assessment value on forestry be used to calculate forest deductions?* As previously stated, the owner of a forest property may make a forest deduction when selling forest on a property in Sweden. The property must be taxed as an agricultural unit and must be a capital asset, Chapter 21 Section 1 IL. According to Chapter 21 Section 4, paragraph 2 IL, the forest deduction may only be made by the existing owner of the land. The rules on forest deductions are based on productive forest land. The forest deduction for a certain taxation year is calculated based on the acquisition value of the forest and the income from the disposal of the forest. According to the main rule in Chapter 21 Section 12, the total forest deduction area shall be calculated based on the acquisition value

---

of the whole property and the difference between the assessment value of the whole property and the assessment value of the forest. The result of that calculation corresponds to the acquisition value of the forest. An individual who owns a commercial property with forest land can make total forest deductions corresponding to 50 percent of the acquisition value of the forest during the holding period. If the property is sold or otherwise transferred to another person, the total forest deductions need to be adjusted according to the transfer.

References

Andersson, Daniel, Grylin, Hanna, Kristoffersson, Eleonor (2021), Beskattning av Fastigheter och bostadsrätter. Lund: Studentlitteratur AB
Bjuvberg, Jan, Periodisering av ersättning för avverkningsrätt – vem ska fråga Bokföringsnämnden? Svensk skattetidning, nr 2, 2018 p. 122
Björkqvist, Jakob, Skogsavdrag i ljuset av skatteförmågeprincipen, Skattenytt, årsskrift 2016 p. 83–104
Fall, Johan, Miljöskatter och Januariöverenskommelsen, Svensk skattetidning, nr 8, 2019, p. 473–492
Helgesson, Ragnar, Hur bör framtida utgifter för nyplantering av skog periodiseras? Skattenytt, TEMA EG och skatter, 1995 p. 132–133
Kleist, David, A4 Inkomst av näringsverksamhet, Skattenytt, nr 6, 2020 p. 301–307
Rydin, Urban, Undantagsregleringen för beskattning av ersättning för avverkningsrätt, Skattenytt, 2007 p. 439–455
COM(2021) 554 final
Prepartory work, prop. 2020/21:60
Prepartory work, prop. 2010/11:21
Prepartory work, prop. 1999/2000:2 del 2
Preparatory work, prop. 1978/79:204
SOU 1997:3
SOU 2002:40, del 1
HFD 2011 ref. 79
HFD 2020 ref. 9

106
Abstract: A majority of tax administrations in the Member States of the European Union (EU) are increasingly leveraging machine-learning (ML) technology to perform their fiscal prerogatives. Yet, little information about ML systems has been disclosed to taxpayers regarding the underlying input data, the risk factors learned by machines, and the overall accuracy or fairness of their outputs. The use of ML by tax administrations highlights an inherent lack of transparency regarding algorithmic-based tax risk assessments and the algorithmic selection of taxpayers. Cases such as the Dutch childcare allowance scandal or toeslagenaffaire have shown how such a lack of transparency can have dramatic consequences for taxpayers. This raises the question: to what extent is secrecy necessary for the collection of taxes and how can transparency be upheld in tax algorithmic governance? This question is addressed in two parts. Section 1 presents the state of use of ML systems by tax administrations in the EU. Section 2 delineates the criteria that compose transparency, and applies those normative criteria to the specific context of State secrecy in fiscal algorithmic governance. The analysis shows that, regardless of the reiterated importance of transparency in algorithmic governance in literature, doctrine and jurisprudence, the use of ML by tax administrations is exacerbating the level of secrecy, to the detriment of taxpayers.
6.1 Introduction

The rate at which ML systems used by tax inspectorates have proliferated is nothing short of extraordinary. In less than two decades, ML systems leveraged for fiscal governance have multiplied exponentially, from a handful of EU Member States to more than two thirds of the EU. The use of ML as a tool to perform State fiscal prerogatives has become the norm. ML-based technology is inter alia used to provide direct assistance to taxpayers, to customize default letters sent by the administration, to automatically collect data or select taxpayers for audits (Hadwick, 2022a). These technological tools have leapfrogged the digital transformation of EU tax administrations, so much so that barely any action is currently carried out without the assistance of that technology.

Most notably, with the integration of ML systems, tax administrations are able to process more data and infer more information from taxpayers’ data, disrupting the fragile balance of power between the administration and the administered. Yet, little information regarding these ML systems has been publicly disclosed, primarily by virtue of the fiscal procedural rules of Member States. ML systems have been adopted without legal basis and the rights of taxpayers are systematically barred from accessing any information or details on the models leveraged by their respective administration, including during litigation. Despite the newfound importance of algorithmic transparency in literature and jurisprudence, in the context of fiscal governance, it is only a buzzword devoid of any normative purpose. In complete antithesis to the principle of transparency, fiscal algorithmic governance in the EU is characterized by a codified status quo of institutional secrecy, a fiscal omerta. Seminal cases such as SyRI, eKasa, or SS SIA demonstrate how the lack of transparency bears significant risks to taxpayers’ rights. The events of the toeslagenaffaire revealed that opacity regarding ML algorithms can generate destructive consequences and poses an existential threat to taxpayers. Regardless of the risks to taxpayers, tax administrations in the EU enjoy a literal carte blanche for the development of risk-scoring models. In a context where the use of ML is proliferating at a rapid pace, the fiscal omerta is rendering some fundamental rights entirely moot and obsolete. The opacity in EU fiscal algorithmic governance raises the question: to what extent is secrecy necessary for the collection of taxes and
how can transparency be upheld in tax algorithmic governance? Section 1 demystifies the concept of machine-learning for a legal audience, the different learning techniques employed, and delineates the current state of use of ML systems by the tax administrations of the Member States. Based on a review of the literature, Section 2 presents the criteria that compose the nebulous principle of transparency, and why these criteria bear no normative consequences on tax procedures, rather characterized by a regime of institutional secrecy. In Section 2, the question of whether all of these tenets of institutional secrecy are proportionate to the aim of tax enforcement is examined, and some solutions are presented to enhance transparency in fiscal governance.

6.2 Section 1: The State of Use of Machine-Learning by EU Tax Administrations

The Organization for Economic Co-operation and Development (OECD, 2019) defines AI systems as systems that, for a given set of human-defined objectives, are capable of making predictions, recommendations or decisions and are designed to operate at varying degrees of autonomy. The EU AI High-Level Expert Group (AIHLEG, 2018), the group of experts appointed by the European Commission to provide advice on the EU AI strategy, defines AI systems in a quasi-identical manner. Although the concept of machine-learning (Samuel, 1959) appeared concurrently to the term ‘artificial intelligence’ (McCarthy et al., 1955), it is conceptually and legally recognized as a sub-set of AI (EU AI Act Proposal, 2021).

Machine-learning can be defined as computational procedures that can autonomously, i.e. without being explicitly programmed to do so, improve performance by drawing statistical inferences from data. In essence, machine-learning is nothing more than an autonomous statistical model, or suite of models. From a computer science perspective, a machine-learning system transforms inputs into outputs without being explicitly programmed to do so by a finite set of human-designed algorithms, unlike a traditional software (Mohri et al., 2018). Similarly to any statistical model, the system assigns mathematical coefficients or ‘weights’
to any individual input and adds the inputs to obtain a weighted sum (Sammut et al., 2011). The results of the weighted sum are then normalized with an activation function, which expresses results between a range of figures, for instance, as either 0 or 1 (Hill et al., 2011).\(^1\) The particularity of a ML system, what distinguishes it from a traditional statistical model and makes it capable of autonomous learning, is the process of ‘error backpropagation’. As illustrated in Figure 1, error back-propagation consists of using previous erroneous outputs as new inputs to the system. At each cycle of backpropagation, when the errors are fed back as new inputs, the system adjusts the weights thus increasing or decreasing the coefficients associated with specific inputs. By adjusting the weights, the system autonomously isolates the most important inputs to improve its performance. The machine-learning algorithm then learns to generate a statistical model, of either a static or dynamic nature. Typically, a ML system is composed of several units, so-called perceptrons, to produce finer-grained results. Together, these perceptrons form a ‘neural network’ and multiple layers form a ‘deep neural network’ (Nigrin, 1993). Figure 1 below is a schematic representation of a perceptron.

![Single Layer Perceptron](http://sumanthrb.com/ml/perceptron/)  

\(^1\) Hence, in essence the activation function decides whether the neuronal unit is activated or not.

It is interesting to note that ML is often referred to as a novel ‘disruptive’ technology, yet in fact it is more than half a century old. Originally created in 1957, the ML system of Rosenblatt was designed to ascertain whether the picture presented was a triangle. The system was fully analogous, i.e. not a digital computer, with visual sensors that would analyze pictures of 16 by 16 pixels (Rosenblatt, 1958; Rosenblatt, 1960; Olazaran, 1993). The simple recognition and binary classification of a shape may seem like a trivial exercise. However, classifying the most straightforward shape is a multifactorial exercise involving the processing of lines, corners, reverberation of lights and shadows, etc. (Chan et al., 2002). Whether by a human or by a machine, such classification is by no means an easy cognitive feat. Through the analysis of vast amounts of pictures, the ML system was capable of inferring statistical correlations, creating a statistical model that could be applied to future inputted pictures.

Systems used for tax risk assessments work in a very similar manner. These systems are presented with previous known examples of taxpayers that have and have not committed fraud or were compliant and non-compliant. By analyzing these examples, the systems draw statistical correlations and deduce what variables can be regarded as indicating a risk of fraud. Together, these risk indicators form a statistical model used to predict the risk of tax fraud/non-compliance for future taxpayers and transactions. This technique is referred to as supervised learning, because the correct output, i.e. who is a fraudster and who is not, is supposedly already known by the tax administration (Hoogendoorn et al., 2017).

The tax administration also makes use of unsupervised learning techniques where the data is unlabeled, i.e. the correct output is not known (Hadwick, 2022b). Clustering is an example of an unsupervised learning technique used by tax administrations (OECD, 2016). Clustering is the act of organizing groups (‘clusters’) whereby the objects or datapoints in one cluster are similar, and dissimilar to objects belonging to other clusters (Aggarwal, 2018). Figure 2 below is a schematic representation of a clustering algorithm.
Clustering can be regarded as the most important category of unsupervised learning techniques, as it serves as the basis for many unsupervised learning algorithms (Arroyo et al., 2016). Via clustering many functions can be performed such as classification and outlier detection. For the tax administration, clustering is used to classify similar and dissimilar taxpayers to predict tax evasion. Clustering is also used to detect abnormal behavior and outliers, such as under-reported income, by calculating the distance of points within a cluster. Points at the very edge of a cluster are likely to be outliers, indicative of potential tax evasion.

Even as a fiscal governance tool, ML-based technology is certainly not a new phenomenon. ML was already used in 2004 with, for instance, XENON, a ‘spider’ system designed by tax administrations in the Netherlands, Denmark and Sweden to automatically collect taxpayer data online (European Commission, 2006). Nowadays, at least 18 out of the 27 Member States’ tax administrations use ML systems on a regular basis (Hadwick, 2022b). Additionally, Eurofisc members developed Transaction Network Analysis (TNA), a ML data-matching system specifically designed to detect and prevent carousel fraud (OECD, 2021). Hence, in some areas of taxation, ML systems are already used consistently throughout the EU. ML systems perform several functions for tax administrations: taxpayers assistance through the use of chatbots (OECD, 2019; Vero Skatt, 2021); automated data collection with ‘spiders’ or ‘web-scraping’ algorithms (CIAT, 2017; Loi n°2019-1479);

---

the detection of risks through clustering or network analysis (Juhasz, 2021); the selection cases for audits via risk management systems (RMS) (OECD, 2016; Revenue Authorities, 2014; Federal Ministry of Austria, 2018); or nudging, by adapting the language used on communications sent to taxpayers (van Hout, 2018; van Luts et al., 2019). By far the most prevalent function for which ML systems are used by tax administrations are RMS tools to select taxpayers for audits. All 18 Member States’ tax administrations that use ML exploit one or more of such risk-scoring systems (Hadwick, 2022b). Moreover, the Commission points out that even in Member States where ML is not used for the algorithmic-based selection of taxpayers for audit, their tax administrations use traditional statistical approaches and data analytics to determine which taxpayers should be audited (European Commission, 2022). Hence, the use of statistical risk indicators for tax enforcement is a constant throughout the EU.

6.3 Section 2: Algorithmic Transparency as the New Buzzword

In recent years, algorithmic transparency has been hailed as the new keyword, to quell citizens’ fears of AI. Eminent scholars on AI and data protection (Hildebrandt, 2012; Pasquale, 2011; Pasquale, 2015; Pasquale et al., 2014; Wachter et al., 2019), have stressed the importance of transparency to combat the risks of algorithmic governance. The OECD and the EU, through the Commission (2021; EU AI Act, 2021), the AI HLEG (AIHLEG, 2019) or AI Watch (Misuraca et al., 2020; Manzoni et al., 2022) have highlighted the paramount necessity of transparency as a pre-condition for citizens’ trust in an open and democratic society. The significance of transparency as a principle of law is also codified in Article 11 of the Treaty on the European Union (TEU, 2012). Even in the niche isolated world of taxation, reference to the importance of transparency have been made on several occasions. In the case of Systeem

---

4 Out of the 60 ML systems identified, 32 could be qualified as risk-scoring algorithms or risk-management systems, see Hadwick, 2022.
Risico Indicatie (SyRI, 2020; SUWI Wet, 2020), a ML risk-scoring system used by the Dutch tax administration to select taxpayers for audit, the Court of the Hague halted the use of the system by virtue of the lack of transparency of the legislation governing the system. The Court ruled that, having regard to the risks discrimination of SyRI, transparency was primordial to verify whether these risks are sufficiently neutralized. In eKasa (eKasa, 2021), the Constitutional Court of Slovakia ordered to temporarily end the use of the eKasa system, finding that the ML system had not been authorized through the prior adoption of a legislative measure. The system was meant to act as an electronic cash register system and Enterprise Resource Planning (ERP) system, automatically transferring a wide array of data on both buyers and sellers to the Slovak tax administration for the detection of VAT fraud. The data transferred was subsequently processed by an ML system to detect risks and devise risk indicators for the selection of taxpayers for audit. The Constitutional Court found a grave breach of the principle of legality, but also advised the legislature to adopt specific safeguards, all of which related to transparency (eKasa, 2021, § 112 et seq.). A very similar reasoning can be observed in CJEU SS SIA (SS SIA, 2022), where the Court found that a request by the Latvian tax administration for the transfer of large bulks of data, to be processed by automated and non-automated means, violated the GDPR. In particular, the CJEU asserted that the request for information was contrary to Article 5(1) of the GDPR, namely the principles of fairness, lawfulness and transparency, by virtue of the lack of legislative measure authorizing the transfer. In each of these cases, transparency is viewed as an important safeguards against the risks of algorithmic governance. The lack thereof is systematically invoked as the ratio decidendi to rule against the integration of ML systems.

Despite the multiple iterance of the importance of transparency for data protection, algorithmic governance and even democracy, the concept is hardly ever defined in a comprehensive manner in legislation. Although being a fixture of EU constitutionalism, and an even older pillar of Western philosophy (Kant, 1795; Hobbes, 1651; Mill, Bentham, Montesquieu, de Tocqueville as cited in Gosseries, 2005), the concept of transparency is undeniably nebulous. Cynically, one could say that perhaps because of this elusive meaning, it is so heavily brandished as a pillar
of digital governance. Upon analysis of the literature, three normative axes can be inferred from the principle of transparency:

Firstly, subjects must be sufficiently informed about an official activity – a decision, measure, norm, law, etc. – both prior to the activity, throughout the process, and after its adoption or conclusion (‘publicity’).

Secondly, the information should be easily accessible and provided in a clear, concise and intelligible manner (‘accessibility’).

Thirdly, prior to the official activity, procedures should be established to ensure that the governing body is properly regulated, supervised or monitored, that the governing body can be held liable in case of ‘torts’ and that subjects can obtain reparations (‘accountability’).

For the purpose of this paper, the focus will be specifically on publicity, the axis most concerned with tax secrecy. Prima facie, there are three channels for taxpayers to obtain information on the ML models used by tax administrations: through the law, upon exercise of their data subject rights to information and access, and before the courts through disclosure requests. All of which are lacunary in the specific context of fiscal algorithmic governance.

First, regarding the transparency of legislative norms, upon comparative legal review of the 18 Member States whose tax administrations make use of ML systems, only 4 have a law which mentions some of the ML systems used (Hadwick, 2022b). Most Member States do not even prescribe in their tax codes that the tax administration is empowered to make use of such technological tools. No Member States have published a complete inventory of the models used by their respective tax administrations, or at least an inventory of the models that exhibit a risk of conflict with taxpayers’ rights (Hadwick, 2022a). In theory, the principle of legality prescribes that a measure that generates a risk to the exercise of natural rights should be regulated through legislative norms, and thus should be communicated to the public (Venice Commission, 2016). Currently, respect of the principle of legality is far from being the norm.

Second, access to information on ML systems will also be denied to taxpayers who make a specific request for it. Indeed, because ML

---

5 For the purpose of this paper, torts simply means ‘wrongdoing’, not necessarily a civil law torts, but also including criminal wrongdoing and violation of taxpayer fundamental rights.
systems are used to assess tax risks and thus also to detect and predict risks of fraud, these systems are used to investigate crimes. Accordingly, tax procedural rules of Member States foresee that access to data on ML systems used by tax administrations, for example, statistical risk indicators, is barred from taxpayers with the argument that it could potentially prejudice the investigation of a crime. This limitation to the right of access is explicitly foreseen by the GDPR in Article 23(1), sub-paragraph (e) and (h), and Article 15(1) of the Law Enforcement Directive (LED). In the context of the prevention of crime, a limitation on the right of data subjects to be informed of data processing operated with their personal data is also prescribed in Article 13 (3)(b) LED. Consequently, taxpayers can lawfully be barred from being informed that they were subjected to data processing by ML systems and denied their right to access any information regarding these systems. In addition to these EU secondary law instruments, limitations to the right of access and right to information are also prescribed in Member States’ tax procedural codes. In Member States such as Belgium (Loi du 5 Septembre 2018), France (Arrêté CFVR, 2021) and Poland (STIR, 2017), the limitations of habeas data rights are prescribed in the norms which regulate the use of data and the use of ML systems by the administration. In other Member States such as Germany, these limitations are prescribed directly in tax codes (AO, 2022). In both situations, the reasoning is the same: disclosing details on ML systems, in particular risk indicators, would jeopardize the investigation or prevention of a crime, hence access to such data is excluded. Since systems for tax risk assessments are used on all taxpayers, whether suspected of fraud or not, taxpayers are systematically deprived of their rights as data subjects.

Third, even in the case of an administrative recourse against a tax administration or in the context of a trial, taxpayers are barred from accessing details on the ML systems used by their tax administration. This limitation in the context of judicial proceedings, is explicitly provided in, for instance, Section 88(5) (4) of the German Tax Code.\(^6\) As a result, 

\(^6\) Abgabenordnung, Sec. 88(5) (4): “Einzelheiten der Risikomanagementsysteme dürfen nicht veröffentlicht werden, soweit dies die Gleichmäßigkeit und Gesetzmäßigkeit der Besteuerung gefährden könnte” – ‘risk-indicators should never be made public’ – this includes the context of judicial proceedings.
taxpayers who hold legitimate grievances over an ML system used by tax administrations, for instance, a taxpayer who believes to be the subject of discrimination, cannot exercise disclosure rights. As legitimate as it may be, this request will automatically be denied by virtue of State secrecy. Effectively, the obligation of disclosure and the equality of arms in a potential trial are completely turned on their head, to the extent that the rights to data protection, to non-discrimination and to a fair trial become moot. Conclusively, in the context of taxation, publicity is a normative ‘market failure’. Taxpayers are not afforded any points of reference to understand what data is processed, with what sort of technological tools it is processed and what the outcome of the processing is. Taxpayers cannot know what types of ML systems are used by their respective administration, whether in the law, as data subjects or as defendants in a trial.

This opacity is based on an illegitimate fear that transparency would enable some taxpayers to circumvent fiscal risk assessments. Yet, the consequences of a lack of transparency are very real and seriously erode taxpayers’ rights. This opacity generates a strong power asymmetry in favor of the tax administration. It disrupts the balance of power between the administration and the administered in the constitutional order. In fact, the risks of such opacity have already manifested in the Dutch childcare allowance scandal, or toeslagenaffaire (Hadwick et al., 2021). In this case, taxpayers showed reliable evidence of being the victims of unlawful ethnic profiling by a tax risk assessment tool of the Dutch tax administration. Yet, for more than eight years their grievances fell on deaf ears by virtue of the impossibility for them to access information on the ML systems used by the administration. Ultimately, the lack of publicity in the toeslagenaffaire led to the resignation of the entire Dutch cabinet, and the discrimination of 35,000 taxpayers caused irreparable harm, led to forced separation of children from their families and costs of half a billion euros in public funds for compensation (DutchNews, 2021). If the judiciary or the DPA had been informed that the Dutch tax administration was using discriminatory risk indicators, such as ethnicity, this scandal could have been avoided outright.

It is important to note that aside from grave statistical malpractice, such as in the toeslagenaffaire, discrimination can occur fairly easily when resorting to ML models for public governance. Even with an impeccable
computational procedure, discrimination and errors can result from factors such as biased data, imbalanced classification or incorrect labels. Yet, in a governance context, where the target population is so heterogenous as the entire cohort of taxpayers, these factors will occur more often than not. For instance, ensuring that the training data is representative of the entire population to avoid a sample bias requires rigorous vigilance and extremely granular data. The same can be said of correct labeling which necessitates regular updates long after the algorithm has been properly trained to avoid longitudinal fallacies. The list of potential biases in data collection illustrates how complex it is to carry such a process without any mistakes (Mehrabi et al., 2022). Even with perfect data, the computational procedure itself may generate discriminatory features. Often these biased risk indicators will follow neutral and sound policy choices. For instance, targeting individuals with foreign bank accounts or businesses with high prevalence of physical cash. These attributes are empirically proven to be indicative of potential tax evasion. Yet, as features of a model, these attributes would generate prohibited indirect discrimination against foreign taxpayers. Transparency would enable checks and balances by other governmental organs or citizens themselves, to verify whether risks of discrimination or data protection infringements have been properly considered by the administration.

In such a context, completely barring all taxpayers from any information about the data processed or risk indicators used in ML systems, both in the law or through the exercise of their data subject rights, is manifestly disproportionate. Taxpayers even with knowledge of the data or features of the model cannot game the system. Risk indicators used in the model relate to objective characteristics of taxpayers. Taxpayers, whether natural or legal persons, cannot modify all personal characteristics and factors of production without it being detected by the administration in some shape or form. Discrepancies from one year to another, a sudden change in revenue or unusually high purchases would automatically raise red flags. For more than 95% of taxpayers, the tax administration is capable of completing their tax returns without any input from the taxpayer, simply by compiling documentation from third parties (Bohm, 2021). Most OECD countries have dozens sometimes a hundred different typologies of risk indicators that are continuously updated (OECD, 2017). Knowledge of some statistical correlations cannot enable someone to
continuously cheat the whole system without insurmountable economic burdens. Simply put, cheating would be more costly than compliance. In addition, risk-scoring algorithms are but one kind of algorithm used by tax administrations among many. Risk indicators only relate to one specific type of algorithm, namely risk-scoring algorithms. Even if all risk indicators were disclosed, other ML algorithms would not be affected and would still be able to detect tax evasion. Accordingly, the interest of taxpayers in knowing what data is processed and how, both in the law or through specific requests, greatly outweighs those of an administration.

Moreover, even if you acknowledge the need of the administration to maintain some secrecy, barring disclosure in the context of litigations against the administration is both dangerous and nonsensical. Technological solutions exist to test the compliance of a model with the rights to non-discrimination or data protection, without opening the black box or conveying the internal logic of a model. Technical processes such as counterfactual explanations, for example, through machine-learning models such as Local Interpretable Model-Agnostic Explanations ‘LIME’ (Ribeiro et al., 2016; Wachter et al., 2017), enable the review of a model without accessing any sensitive details. These solutions are model-agnostic, i.e. they perform on any ML model, and provide satisfactory explanations interpretable even by laymen. Invoking tax secrecy to completely deny any access to the model, even in litigation, is by far the most intrusive solution an administration can opt for. Developing a simple API to counterfactually test some benchmarks is a costless solution that would protect taxpayers’ rights while guaranteeing the same level of secrecy for the administration. In such a context, when solutions exist to enable the review of a model while maintaining a form of black box, the current omerta promulgated by the administration is manifestly disproportionate to the aim pursued.

6.4 Conclusions

While ML systems have been used for almost two decades, taxpayers’ fundamental rights have been thoroughly neglected during all that time. Within the EU digital constitutional order, the principle of transparency perfectly illustrates this appalling neglect. The status quo is one of secrecy,
an institutional law of silence authorized by Member States’ legislatures. Little information on the ML systems used by tax administrations is disclosed to taxpayers. Either in legislation, as less than a quarter of Member States have an actual legal basis that authorizes the use of ML by their respective tax administrations. Nor upon request by taxpayers, as tax procedural rules forbid taxpayers to access details on ML systems based on an illegitimate fear of administrations that it would hinder fraud investigations. Even when taxpayers hold legitimate grievances and substantiated claims, access to information is outright denied rendering their right to data protection, to non-discrimination and to a fair trial effectively moot. This opacity is not without consequences and has already led to dramatic cases such as the toeslagenaffaire. Accordingly, the digital transformation of the tax administration poses an existential threat to taxpayers’ rights.

It is clear that the current policy of institutional secrecy of EU tax administrations is neither necessary nor proportionate to the aim pursued. The vast majority of taxpayers use pre-filled in tax returns and the administrations can complete the quasi-totality of tax returns without any input from the taxpayers. In such a context, additional transparency through the disclosure of some details on the ML systems used or the data processed, would not hinder tax enforcement. Moreover, technical solutions, such as counterfactual explanations, already exist and enable the review of ML systems without disclosing sensitive details or the inner workings of a model. Consequently, maintaining complete secrecy and upholding the legal black box, is unnecessary and disproportionate to the aim of not hindering tax enforcement. By no means will such secrecy render an administration better or more effective, while the harm generated by the omerta for an administration’s legitimacy and for taxpayers’ rights are considerable. Despite the existence of technical solutions to uphold fundamental rights, EU legislatures are opting for a regime of heightened surveillance, inquisitorial against taxpayers. In the long term, such opacity coupled with the digital surveillance regime instituted will only antagonize taxpayers, and serve as a catalyst for less compliance and less cooperation with tax inspectorates.
References

Abgabenordnung, Sec. 32c (1) 2. (2022) (AO).
High-Level Expert Group on Artificial Intelligence (AIHLEG) (2018). *A Definition of AI: Main capabilities and scientific discipline.*
Ireland Revenue Authorities (2014). *Code of Practice for Revenue Audit and other Compliance Interventions.*
à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Art. 89, 1° and 2° (2018).

Manzoni et al. (2022). *AI Watch Road to the Adoption of Artificial Intelligence by the Public Sector* (Joint Research Centre, Office of the EU).


Presentation of Bøhm, M. former Deputy Director at the Danish Tax Administration and member of the TFTC at the OECD – retrieved from: https://


Vero Skatt (Finland’s Tax Authority) (2022, July) on chatbot ‘Virtanen’ : https://www.vero.fi/en/About-us/contact-us/chat_with_the_tax_authoritie/.


Wet houdende regels tot vaststelling van een structuur voor de uitvoering van taken met betrekking tot de arbeidsvoorzieningen en sociale verzekeringswetten 29 november 2001 (SUWI wet), Article 64 & 65 (2001).
Chapter 7
The Current Corporate Income Tax Rule Architecture & Automated, Real-Time Taxation – Would the Necessary Prerequisites of Today’s Tax Rules Have to Be Changed?

Abstract: Income taxation handled by AI and carried out in real time (ARTT) is promising in many ways. It could, for example, save a lot of time and money for both companies and tax administrations, be based on facts rather than estimates and probably also help prevent economic crime. But what are the obstacles and how would taxes and taxation actually work in such a context? This chapter includes a discussion on whether current substantial corporate income tax rules are compatible with ARTT or if their design will have to be changed to make it possible to apply them based on automatically generated data. It is argued that many of today’s tax rules are not suitable for an ARTT context and that significant changes in current income tax principles are probably required for ARTT to work.
7.1 Introduction

As pointed out in the OECD Tax Administration 3.0 report, there are a number of promising possibilities with new technologies and procedures in taxation. Such a development would also have an enormous impact on a number of questions outside taxation, such as investments, integrity, crime prevention, transaction costs etc. This paper does not, however, concern those risks and possibilities, but the possibility of making such a system work. I will here, from a “legal technical tax perspective”, critically look at some of the challenges of automatically created and/or distributed “raw” financial data and automated, real-time income taxation (below referred to as ARTT, for Automated, Real-time Taxation). This paper mainly concerns the procedures of taxation, but the main point is to try to show that implementing the kind of new tax procedures discussed here (ARTT) is likely to require major changes, not only in (1) developing more sophisticated algorithms etc. and (2) changes to today’s tax procedures (in a broad sense) and as regards (3) the creation of new ways to produce and distribute financial data on which to base the taxation, but also (4) concerning today’s substantial tax rules and principles of taxation (and probably also those of financial reporting). Some of these questions (such as making legal AI work) have been discussed a great deal in the literature, but not the issue that is the focus of this paper, i.e. the provision of relevant data for the said use, and the need to change the tax rules so

---

1 Many thanks to (in alphabetical order) Bo Harald (Senior Advisor at the Finnish Council of Regulatory Impact Analysis and previously Nordea), Magnus Kristoffersson (Örebro University), Peter Lindholm (Swedish Tax Agency), Gustav Lindkvist (Gustav Lindkvist Förvaltningsprocess) and Jan Sjösten (Swedish Tax Agency) as well as participants in seminars/conferences at the universities of Linköping and Örebro, for highly valuable feedback on previous versions of this paper. All remaining errors and shortcomings are my own.


3 The new procedures of taxation discussed here concern in particular the procedures that are transforming today’s income tax, especially regarding corporate income taxation, from a highly manual procedure, handled on a yearly basis (see Ch. 2), into something that is automated and where tax is calculated (perhaps also paid) in real time – close to transactions.

4 See, for example, Ashley (2017) and Gardner (1987).
that they work well with the data that could or should realistically be made available.

Thus, what we are discussing here, is 1) a new kind of system where data is created and shared automatically and more or less instantly and continuously (i.e. RAW data, as they are unprocessed on delivery) with (at least) the tax authorities which, 2) based on this data and with the help of AI, automatically apply income tax rules and 3) that this application means that taxation is finally determined in such a way that it does not require tax returns to be submitted on an annual basis or that yearly general decisions are made on taxation. We are thus, as a thought experiment, looking at a system for automated, real-time income taxation. An exciting idea, to say the least. It may entail fantastic possibilities. But would it work under current substantial tax rules?

I will start by looking at how conventional taxation works. To the extent that this legal and administrative technique is to be replaced by ARTT, we have to offer another way that would replace the functions of today's model – and preferably in a satisfactory way. Thus, in the following section, I will first (Ch. 2) describe how conventional taxation works, thereafter (Ch. 3) I will problematize this from the perspective of using ARTT under today's tax rules and scout for some what I imagine would be necessary changes in the tax system, for ARTT to work. Chapter 4 gives a concluding, brief general reflection on the possible way forward.

The questions discussed below are long, and it would seem, give rise to almost countless further questions and many different areas of expertise. This makes delimitations necessary.

1. This paper does not concern what would be legal (for example, in relation to current constitutional law), moral, rational or desirable, nor about the necessary technology as such. The analysis is only concerned with data, tax rules, and the automatic application of the latter in relation to the former.

2. The examples of current tax rules are taken from Swedish income taxation. That means that some of the rules that are applicable will be accounting rules; for that reason, accounting is of some importance here, although it is not discussed in its own right. VAT and excise taxes are not discussed below, and nor is international legislation or national legislation in other countries. However, there is reason to
Jan Kellgren

presume that the examples and line of reasoning below have a level of general validity, outside corporate income taxation and outside Sweden.

3. In terms of AI, the perspective here is limited to what kind of AI is to be expected to be possible within a fairly foreseeable future. I am therefore not discussing “general super IQ AI” or some such, but rather AI of today’s standard (oriented towards the purpose discussed here) and somewhat extrapolated beyond that. Nor am I discussing a possible future where sensors are superintelligent and can record and report feelings and intentions etc. Instead, I am speaking about rather simple sensors, like GPSes, thermometers, cameras etc. – and of course such data that can be derived from invoices etc. So, no “all seeing eye” etc.

4. Neither the coding of the tax law so that it works for AI purposes, nor making AI interpret the law (including case law, legal principles, preliminary works etc.) as such, will be discussed in this paper. Here, I will simply assume that it will be possible for AI to understand and interpret tax rules (which, as will be discussed below, is not the same as applying these tax rules in real life cases).

5. This paper mainly concerns real-time definitive taxation, not “just” real-time preliminary estimations and real-time payments of preliminary taxes.

---

5 These are really important questions, and there is a complex relationship between the coding and the drafting of laws. See, for example, Governatori, G. et al. (2022).
6 “Definitive” in the tax context seems to be a relative term, considering the possibilities of appeals and reviews. What is meant here by definitive is that the taxation is not provisional in the sense that the intention is to make a final decision later on – not that there would be no possibility to make an appeal or review.
Chapter 7 The Current Corporate Income Tax Rule Architecture …

7.2 The Point of Departure: The Modus Operandi of Conventional Taxation – A Taxonomy of Tax Rule Application

7.2.1 Introduction

The design of a typical tax (and other) rule is that it refers to something outside the norm; a state of affairs or an event or something like that (this is the factual side of the norm, but as long as only the rule is concerned, the facts of the case are only abstractly expressed). If this (whatever it is) is the case, the rule provides a legal consequence of some kind. When applying the rules, the facts of the actual case have to be investigated and, through interpretation, related to the rule(s) in order to decide whether or not it is applicable (or how it is to be applied). Basically, this is no different in a ARTT context, but, as will be discussed in chapter 3, there are certain significant differences with regard to the facts, the interpretation of the rule and (it will be argued) how the rules can or should be designed.

7.2.2 The Substantial Tax Rule

The law can relate to many kinds of facts and situations. For example, when deciding in tax cases, you might have to make sure that facts such as these actually hold true.7

- What is the civil law background for this transaction or situation and how should the answer to that question affect taxation?8 How does the civil law background affect the accounting and how does the accounting in turn affect the taxation in this case?9

---

7 These examples are questions that sometimes will have to be answered when applying Swedish income tax law.
8 Civil law could be of importance within income taxation for different reasons, for example, if its classifications are to be seen as binding for a tax question or if civil law is of importance for evaluating the economic substance (for example, the likelihood of a loss in a civil law court case).
9 See Kellgren (2012).
• How are these kinds of transactions to be handled within accounting and are they correctly handled in this case, by this company?\textsuperscript{10}
• Does this kind of cost seem to be relevant as a means to increase the profit of the company?
• What where the insights or intentions of the Management of this company with regard to this project?
• Is this a non-profit organization?
• Was it XX’s intention to save tax through this rather odd series of transactions and, if so, how much would have been saved, had it been accepted by the tax authorities, and compared to what?
• Will we be able to sell this product once it is fully developed, and when and at what price?
• Did they bribe him/her, in the sense that is meant in the rule prohibiting deduction of such costs?
• Is this an R&D cost? What are the plans, goals and possibilities regarding R&D project X?
• Is the company likely to lose in court against X and, if so, how much will it likely have to pay, and when?
• Does the second transaction (T2) change how we look at the first one (T1)?
• What is the current value of that intangible asset?

Such necessary prerequisites and complexities may not be easy to handle when applying the law, nevertheless they are there, and they are handled manually.

7.2.3 Getting the Required Data into the Decision-Making Process
As shown above, the necessary prerequisites of many rules call for varied and sometimes “subtle” kinds of information (such as insight, intention, relevance or “degree of”). Beyond that, the law sometimes, explicitly or implicitly\textsuperscript{11}, allows the taxpayer to make choices with regard to how to use tax law. These choices may be with regard to the assessment and

\textsuperscript{10} Accounting law must often be understood and properly applied at least in Sweden, where accounting is often more or less incidental in relation to taxation.

\textsuperscript{11} See Kellgren (2012).
classification of facts, such as the size of a future cost or perceiving an asset as an expendable equipment, or choices between alternatives explicitly provided for in rules. The taxpayer might be free to choose between, for example, different rules, valuations and procedures. These choices are also a kind of data, currently sometimes needed for taxation. Especially within corporate income taxation, the taxpayer supplies many such facts, through a degree (not seldom a high degree) of manual labor and sometimes subtle and complex estimations.

7.2.4 Interpreting the Norm
Interpreting the norm is done manually with the help of the doctrine on the proper use of legal sources. Every lawyer knows the basics of this process, and we are well aware that it is not purely a mathematical or logical process, but that it is also a (to some degree) normative one, partly based on personal judgement.

7.2.5 Evaluating the Data: Facts and Evidence
The data and evidence available in each case are assessed in relation to the relevant tax rules. This is carried out manually, but the process can be aided by different kinds of algorithms, statistics etc. The bottom line, however, is that the judge (etc.) has to decide what to believe happened (or what has been proved to have happened) and what the situation was or is, based on the evidence.

7.2.6 Applying a Norm on the “Facts” of the Case
Traditionally, the application (or not) of a norm on the “facts” of the case is also carried out manually. It is important to emphasize that although there are plenty of straightforward cases and legal sources (doctrine, case law etc.), the application of a norm on the “facts” of the case is often a highly complex procedure from a philosophical perspective. It concerns what you think of the norm and the correct interpretation and application of the norm in relation to the specific case and the data available. To a certain extent, it is certainly a “manual” intellectual process – where facts, traditions and logics but also normative judgments on the part of

---

12 See, for example, Tontti (2004) and Rissland (1987).
the judge meet in a way that is not fully expressed in either the written grounds for a decision or fully explored in empirical research.

7.2.7 Final Remarks

The above-mentioned steps are handled by the parties and sometimes by a judge. Some data is already today delivered automatically, but a great deal is handled manually and processed through evaluation, choice etc. by the taxpayer (instead of being delivered automatically as raw data). Further, new facts and evidence can be requested and supplied. The further assessment of the said data and the interpretation and application of the tax rules are then mostly handled manually. This process leaves some room for discussion and debate both regarding the facts of the case and the interpretation and decision. With this background, let us now see how these steps might be handled within an ARTT context.

7.3 Fully Automated Real-Time Taxation – Problems and Necessary Adaptations

7.3.1 Setting the Scene – Minimal Changes, but ARTT Taxation

The fact that tax rules, as they are currently formulated, seem likely to cause problems when it comes to application within an ARTT context is discussed in a wider perspective below. However, in the ARTT context, taxation is carried out in real time, so a basic prerequisite for this scenario is that the rules are at least changed in exactly that way – from annual assessments to real-time assessments. So, let us say, as a thought experiment, that the tax rules are the same, except for the fact that they are (written so that they are) applied in real time, and let us have a look at how this would seem to meet the requirements in ARTT taxation. The focus lies on probable difficulties regarding the use of today’s tax rules (with the above-mentioned adjustments for real-time taxation) and on discussing the nature of changes in today’s substantial income tax rules and principles when switching to ARTT taxation.

It is important to note here that we are not only speaking about (1) the use of AI when applying tax law, but on this taking place (2) on
automatically generated and delivered data and (3) is carried out (more or less) in real time.¹³ When AI is applying the law in a more conventional, manual annual process, it is fully possible to submit and request manually submitted data, estimations, predictions and preferences etc. and also to have some kind of dialogue vis-à-vis the taxpayer. In that case, things can be largely old school, much like when, for example, a judge is applying the law in a tax case, with the exception of a situation where AI makes (or suggests) a decision. However, in a fully-fledged ARTT context, there is no room for asking the parties (for example, a company) for more information, such as data, estimations and preferences. Within our ARTT scenario, only information that is already available can be used. Needless to say, AI could identify additional information needs and request this information – but, at least in these cases, that it is no longer real-time taxation.

7.3.2 Getting the Required Data into the Decision-Making Process – or Coping Without, by Asking for Less or Other Facts?

We must contemplate the following: is it possible to create an automated data production that would make it possible for AI to make tax decisions in relation to today’s tax rules? As many of today’s rules take aim at quite subtle qualities in the facts of the case (see 2.2), it would seem very hard indeed to automatically create data that could make AI (even a highly bright one, and regardless of whether it is highly skillful at the abstract interpretation of laws) handle all those kinds of states of mind, plans, relations insights etc., referred to in the tax norm.

Perhaps, or even probably, it would be possible to handle some, or even many, of today’s rules, (1) exactly as they are. And perhaps it would be possible to (2) adjust some of the necessary conditions in today’s tax rules just slightly, so that the rule would have close to the same function as it does today, but be better adapted for ARTT technology. However,

¹³ As Kristoffersson E., 2021 points out, Sweden started applying automated decision-making in many fields of tax law already in the late 1970s and as Donahue (2018) points out “On a practical level, lawyers should be aware that software powered by AI already carries out legal tasks. Within a few years, AI will be taking over (or at least affecting) a significant amount of work now done by lawyers”.

135
I find it very hard to believe that necessary conditions like intent, plans, real value etc. would be possible to manage based only on automatic data, run through (even a super bright) AI (see also, just below, on “phantom images”).

All tax rules have a decisive point in time (or period) on which the tax assessment should focus (often it is the time of a transaction or the end of the year). It is debatable, for reasons of both predictability and legality, under what conditions the development (different kinds of new facts) after this point in time (ex post assessment) should be taken into account by the courts. Nevertheless, it should be said that such an assessment is not possible if definitive taxation takes place in real time – instead, taxation will have to be managed on a purely “now” basis.

Thus, it seems like (3) some rules would have to be changed more radically. This would be needed even for a very well-educated, highly intelligent human judge, if she had to apply the law based only on daily fresh raw data – such data simply do not support the kind of conclusions and assessments necessitated by many of today’s income tax rules. Thus, the necessary prerequisites of the tax rules must be made compatible with the possibilities and limitations of ARTT technology.

Thus, in this hypothetical case, the rules are to be changed to (automated) real-time taxation. This gives rise to a number of dilemmas. One example is that it will be hard to handle future major deductions and, in the case of progressive taxation, expected income for the rest of the tax year (to avoid uneven tax burdens over time). Another example regards matching. It is often argued that income and expenses should be matched. Perhaps this would be too tricky to carry out on a real-time basis that it should be changed into something like day-by-day, or week-by-week, taxation – at least if tax payments are also in real time. Otherwise, taxation would risk being very “stochastic”, in some cases – high income one day, high cost the next, on the same deal. A week-by-week taxation payment would make it easier to manage at least some level of matching of income and expenses (but would probably fail to take into account more future expenses connected to transactions/income in the present). A somewhat longer period than (more or less) literally real time would also reduce the work burden; in the case of valuation etc. it is not schematic but

---

14 See Kellgren et al. (2019).
Instead calls for some manual estimations. Manually managing complex estimations on a real-time basis (such as every minute) is, needless to say, simply out of the question. The above applies for basically every kind of manual well thought through estimation (classification, valuation etc.), today made once a year. For example, the same could be said for debt valuations.

In all probability, *far more schematic solutions* for this kind of manually made estimations by the business management today and that are currently carried out once a year, would turn out to be necessary. However, the solutions do *not* necessarily have to be *fully* schematic. Instead, new information (for example, regarding a court case, an asset or events on the stock market) could be allowed to affect the taxation.

It would also be possible to perform some posts, such as the depreciation of assets, in advance, *manually* and more seldom, but calculated day-by-day. Needless to say, that would *not* be an automated process, but it would make it possible for an AI to calculate the tax on a daily basis. Thus, certain information and estimations, choices etc. could be processed and delivered manually and in advance. However, this would no longer be fully-fledged ARTT.

In fact, the substantial tax rules must probably be changed in many ways, in order to blend well with the ARTT way of taxation. This is discussed more below. However, nobody knows exactly what kind of necessary conditions, in the future, that will be possible to handle within the said context. No doubt, computer power, skillful programming and big data (a lot of data from many and various data points) makes it possible to create “*phantom images*” of many things – such as perhaps insights, probabilities etc. Most probably, what is possible to manage automatically is also to an extent a moving target, as technology develops, but I am convinced that some of today’s rules have such a clear “human aspect” that they would not work (well or at all) within an ARTT context.15

Certainly, there are also many easy, or even obvious, decisions when tax law is applied. In those cases, ARTT taxation would often be possible. An example of this kind would be road tax (based on automatically taken photographs combined with AI-interpreted license plates) and, in many cases, the taxation of salaries (where it can be based on control data such

---

15 See more about problems connected to such rules, Ashley (2017) Ch. 2.
as cash flows).\textsuperscript{16} An interesting real life example is the French swimming pool tax, based on an artificial intelligence computer vision system.\textsuperscript{17}

7.3.3 Interpreting the Substantial Tax Rule and Evaluating the Data As Facts and Evidence

There are already a lot of things AI can do, and actually already does, in terms of understanding data/facts and interpreting and applying the law – and in the future, it will (gradually) be able to perform even more impressive tasks. I think AI may very well handle many questions regarding the interpretation and application of the law. But there are also truly and deeply difficult cases, not least many of the cases currently handled in supreme tax courts. There are difficulties in interpreting the law and in evaluating the facts available as evidence of which both can be extremely onerous.\textsuperscript{18} In the foreseeable future, the courts will probably be better at handling those cases – just as they have handled them so far, but perhaps aided by AI and big data.\textsuperscript{19} At least as long as it comes to interpreting tax laws as they are written today, I think it would be a very big step indeed to leave every case to AI – and too much of a step, at least for the relatively foreseeable future. However, AI could probably apply tax rules in relation to simple data in many cases.\textsuperscript{20}

Gradually adapting the tax laws to ARTT technology would extend the number of tax cases that could be handled more or less automatically. Many easier questions could probably be fully handled by ARTT technology, even in corporate taxation. Perhaps this would be the way forward – applying ARTT technology where it works well but going “human mode” (with no real-time decision making, but more often than yearly) where that works better. This would mean something of a “parti-

\textsuperscript{16} See also note 13.

\textsuperscript{17} See https://arstechnica.com/information-technology/2022/08/france-reveals-hidden-swimming-pools-with-ai-taxes-them/ (2022-12-16).

\textsuperscript{18} Not least, the use of AI for evaluating evidence can give rise to biased judgments due to statistics being used in a way that is inconsistent with sound principles of justice.

\textsuperscript{19} See for example note 15.

\textsuperscript{20} It could be noted that the goal for the Finnish tax administration was that the taxation of individual taxpayers would be as automated as possible (https://www.vero.fi/en/About-us/finnish-tax-administration/the-development-of-digitalization-in-tax-administration/towards-automated-taxation/ 2022-11-22).
tioned solution” of the modus operandi of taxation, where some rules are handled within an automated process and others are kept old school. As technology, legislation and know how regarding ARTT taxation develops, the proportion of the total number of tax issues that could be handled automatically and in real time will increase substantially.

7.4 The Way Forward?

To some extent, and from a legal technical standpoint, Automated Real-Time Taxation (ARTT) is pretty easy to establish. However, handling every tax issue the ARTT way would be quite another thing – and probably not realistic, at least not as long as we stick to today’s tax rules and principles. Many of today’s – not seldom thoroughly thought thorough – principles for corporate income taxation (and accounting, which is not very well covered in this paper) would then be jeopardized. But still, ARTT taxation is in many respects highly promising, so it certainly seems worth trying to take taxation in that direction.

What would, in that case, be the proper way forward? My answer is perhaps not very thrilling; it is “go hybrid” and “take it step-by-step”. Let me break this down into four aspects.

1. The data (facts, choices and estimates etc.): Create and send data automatically (once questions of integrity, trade secrets etc. are solved), but, until we (humanity, the technology and the rules) are ready for the next step, leave and process certain information manually. In that way we will complement ARTT technology and have all the necessary data that the current tax rules necessitate. The, thus delivered, big data will potentially be of great use for tax administrations, for example, for crime prevention, regardless it is used for full ARTT or only part ARTT.

2. AI: Use AI on said ARTT data and also on manually crafted data, as far as it works well, which is a step-by-step process – and increasingly can be handled through AI as it (and its surrounding systems, such as data) improves and the tax rules are adapted for this context. Until we are there, and to the extent we are not, let us keep up the manual application of law as far as it is needed (but probably not as seldom as on a yearly cycle). While it is undoubtedly wise to proceed cautiously when taking major significant steps, whose effects cannot be fully anticipated, it is also
very likely that \emph{once the step is taken, creativity will be re-energized} – when it can create real-life benefits and the new situation, with its at that time current needs, conditions etc., are better known. The art of swimming is not perfected until you are working on it actually in the water…

3. \textbf{Real-time taxation}: Head in the direction of real-time taxation, but keep a keen eye on the difficulties. Maybe real-time taxation should be seen as something basically \emph{preliminary}, that, after a certain time, is not preliminary anymore. That would give the tax administrations some leeway to see if things are correct or if the AI system made a mistake, if the data was corrupt (and how and why) or if subsequent transactions are somehow connected to previous transactions in such a way that the substance does not match the form etc. The taxpayer could use slightly simplified principles for the calculation of automatic and daily provisional tax payments, in order to review them and make some fine-tuning adjustments (e.g., if a non-deductible item has been accidentally deducted). In this way, many of the benefits of real-time taxation would also be achieved. However, the last step – to switch to real-time \emph{definitive} taxation – could come later. It should be noted that many of the difficulties discussed above with real-time definitive taxation would also apply to provisional taxation – but these difficulties, and errors, would be easier to live with in a constitutional state, as they can subsequently be discovered and adjusted for. Another possible instrument to experiment with in this context would be a process whereby a provisional tax assessment would have to be approved periodically by the taxpayer and by the tax administration.

4. The substantial income \textbf{tax rules}: If we want to go into ARTT, the tax rules must be made suitable for this – unless they already are, which is probably often the case. The rules must “ask for” data that can be automatically generated and that are suited for AI application. This should probably be managed step-by-step, for example, chapter-by-chapter in the Income Tax Act. Adapting tax rules to ARTT may lead to a loss of some of the qualities of today’s tax law and tax procedure. At least, there is a risk of that. Kristoffersson believes that future tax rules for ARTT might have to have a more \emph{“simple”} and \emph{“binary”} character\footnote{Kristoffersson M., (2022). I see “binary rules” as rules taking aim at numbers rather than other facts.}, and, in many cases,
that is probably true. Perhaps a realistic scenario would even be a move towards some kind of transaction tax. Anyway, with a hybrid, step-by-step method, the process can be controlled, tested, evaluated – and gradually improved. Tax rules that are hard to combine with ARTT would need to be thoroughly inventoried. In the end, I suspect many of today’s qualities in income taxation would be lost, if we went “full ARTT” in corporate income taxation. However, perhaps even more would be gained in terms of lowered transaction costs and new ways (perhaps different kinds of transfer payments) to realize that the objectives that current income tax rules have helped to achieve have been conceived and implemented. Perhaps, sooner or later, a switch to ARTT taxation would fundamentally change the way we look at how we ought to tax ourselves. In the end, this all boils down to a parliamentary issue – what kind of tax laws, tax technology and tax procedures do we want? Regardless of this, only the possible is possible.

References
OECD, Tax Administration 3.0: The Digital Transformation of Tax Administration, OECD 2020.


Chapter 8
ViDA – VAT in the Digital Age

Abstract: The European Commission proposed a series of measures called ViDA (VAT in the Digital Age) in December 2022. The initiative aims to modernize the VAT system, making it more beneficial for businesses, more resistant to VAT fraud, and promoting digitalization. The proposal contains three parts: 1) a real-time digital reporting system based on e-invoicing; 2) updated VAT rules for the platform economy; and 3) a single VAT registration for businesses selling to consumers across the EU. The first part intends to fight VAT fraud, simplify procedures, and save businesses €4 billion annually in compliance costs. The second part makes platform companies in specific sectors responsible for collecting and remitting VAT when their users don’t. The third part expands the one-stop-shop (OSS) system to all businesses selling to consumers, potentially saving businesses €8.7 billion annually. Despite broad agreement on the proposal, the timeline and lack of clear definitions have drawn criticism. The proposal is seen as a step towards modernizing the VAT system, but concerns remain about its complexity and potential increased burdens on businesses.

8.1 Introduction

On December 8, 2022, the European Commission proposed a series of measures under the name ViDA, VAT in the Digital Age (COM/2022/701 final). The proposal aims to modernize the VAT system, making it more beneficial for businesses and more resilient to VAT fraud. It also promotes digitalization. The objectives include modernizing VAT reporting obligations, addressing the challenges of the platform economy, avoiding multiple VAT registrations in the EU, and improving the function of the tool implemented for declaring and paying VAT on distance sales of goods.
The ViDA proposal comprises three parts: 1. A real-time digital reporting system based on e-invoicing, 2. updated VAT rules for the platform economy (PDS – platforms and deemed supplies), and 3. a single VAT registration (SVR) for businesses selling to consumers across the EU. The ViDA proposal is expected to be approved by December 31, 2023. The first pillar is planned to enter into force on January 1, 2028, whereas the second and third pillars are planned to enter into force on January 1, 2025. This chapter describes the three parts of the proposal and the current developments. At the end of the chapter, the author offers her concluding remarks.

8.2 A real-time digital reporting system based on e-invoicing

In the ViDA proposal, a real-time digital reporting system is proposed. The system will be based on e-invoicing, which will give the EU Member States a more efficient tool to use in the fight against VAT fraud, especially carousel fraud. The idea is to simplify cross-border transactions for companies by removing difficult procedures and streamlining processes. This measure is intended to recoup up to €11 billion a year for the Member States over the next ten years. The businesses will save €4 billion a year over the next ten years in compliance costs (European Commission, 2022).

The reporting obligations will be modernized by introducing digital reporting requirements (DRR). Through this, the information that needs to be submitted by each taxable person will be standardized. Each transaction will be reported in almost real-time to the tax authorities. Since the tax authorities will already have information about the transactions, there will be no need for recapitulative statements anymore, which will reduce the administrative burdens for the companies. There will be a common template, which will be harmonized with the standard set up in Directive 2014/55/EU on electronic invoicing in public procurement. Data extracted from the e-invoices would be transmitted to an EU database called the central VAT information exchange system or VIES. Member
States will also have the option to move towards a digital reporting system for domestic transactions (COM/2022/701 final).

The rationale for this proposal is that the VAT Directive stems from the 1970s, a time when the reporting requirements were not digital. The VAT Directive creates a barrier by not allowing compulsory e-invoicing. The latter is necessary to meet the current global trend, which is a shift from traditional VAT compliance towards real-time sharing of transaction-based data with tax administrations (COM/2022/701 final).

Some Member States already apply DDRs and similar tools in addition to the requirements in the VAT Directive for VAT returns. Some require the transmission of monthly reports of business transactions, whereas others require the real-time submission of invoices. Some Member States apply the real-time or almost-real-time transmission of invoice data to the tax authorities, and others apply the submission of tax and accounting data or VAT records. The use of different models creates compliance issues for companies that conduct business internationally. The compliance costs due to the different reporting systems are estimated at €1.6 billion annually (COM/2022/701 final).

The proposed system enables the member states to remove the current inefficient system with recapitulative statements from 1993, which is outdated and not fit for the digital economy. The recapitulative statements do not contain data at the transaction level but only for each taxable person for a certain period. The recapitulative statements do not enable systematic cross-matching with intra-Union acquisitions, and they are too slow to reveal carousel fraud before it has happened.

### 8.3 Updated VAT rules for the platform economy

Platforms that facilitate passenger transport and short-term accommodation have become important players in the market. In many cases, there is no VAT on such transactions because the suppliers are private individuals or small businesses. This makes the playing field unequal since these services are normally subject to VAT. Even when individuals and small businesses are obliged to charge VAT on their services, it may be difficult
for them to understand that and how they should deal with the VAT. In order to solve this problem, the platform companies in those sectors will become responsible for collecting and remitting VAT to tax authorities when their users do not (European Commission 2022).

Before the platform economy, the fact that private individuals and small businesses do not have to charge VAT was not considered to distort any competition in the market. When they, together with many other private individuals and small businesses, supply their services over an Internet platform, they reach out jointly and become important players in the market. For instance, the price for accommodation on a platform is 8 to 17% lower than a regional hotel’s average daily rate. Up to 70% of the suppliers on these platforms are not registered for VAT. The situation is similar with regard to the passenger transportation platforms. Both the accommodation and passenger transport platforms compete directly with the hotel and taxi sectors (COM/2022/701 final).

Following the Council Directive 2011/16/EU of February 15, 2011 on administrative cooperation in the field of taxation and the amendment in Directive 2021/514/EU, the so-called DAC 7, platforms are required to collect information about the supplies that they facilitate and about the persons that are doing business over the platforms. Platforms are burdened by different requirements in different Member States regarding the timeframe and format of this information. Therefore, there is a need for more harmonization in this field (COM/2022/701 final).

Through this part of the proposal, there will be a deemed supply from the platform by which platforms will account for VAT on the underlying supply where no VAT is charged by the supplier. The currently VAT-free supplies of short-term accommodation and passenger transportation will consequently be subject to VAT. The place of supply rules will be clarified, and the transmission of information from the platforms to the tax authorities will be more harmonized (COM/2022/701 final).
8.4 A single VAT registration for businesses selling to consumers across the EU

When providing electronic services and telecommunication services, as well as supplying goods cross-border within EU to private individuals, there is already a one-stop-shop (OSS) system in place. Under this system, the taxable persons engaging in such businesses has the possibility to register for VAT purposes only in one Member State and fulfil their VAT obligations via a single online portal in one single language. The OSS is proposed to be expanded to all businesses that are selling to consumers. The aim is that businesses, especially small and medium sized enterprises, will save €8.7 billion a year in registration and compliance costs over the next ten years (European Commission 2022).

Registering for VAT in another member state results in increased VAT compliance costs. The estimated one-off cost is €1 200, and the minimum yearly compliance cost amounts to €2 400 for a small or medium-sized company and €8 000 for an average business. The already-existing OSS has been a great success. Businesses carrying out business that has cross-border elements but does not qualify as “distance sales” still have to register and comply with several Member States. An extension of the OSS to more transaction types will further decrease the need for multiple VAT registrations.

8.5 Current developments

On May 25, 2023, the European Parliament’s Committee on Economic and Monetary Affairs (ECON) proposed a prolonged deadline for the first part of the proposal, the real-time digital reporting system based on e-invoicing. The ECON proposed a prolongation of one year. Furthermore, the transaction reporting deadline was proposed to be prolonged from two to ten days after the transaction took place (ECON 2023).

On June 16, 2023, the Economic and Financial Affairs (Ecofin) Ministers discussed the proposal. The ministers reached a broad agreement on harmonizing the reporting of intra-Union supplies in the form of a real-time digital reporting system based on e-invoicing. However, some
member states were concerned about the implementation date. Some member states wanted more flexibility in domestic reporting. Most member states supported the proposal of updated VAT rules for the platform economy. France and Ireland were concerned that the proposal would distort competition. Several countries asked for more extensive platform reporting to be considered. The third proposal, the single VAT registration for businesses selling to consumers across the EU, was the most popular, with almost unanimous agreement. Some countries, however, commented on the implementation date (ECOFIN 2023).

In the literature, the proposal has been criticized for not being detailed and clear enough. For instance, the concepts of short-term accommodation and passenger transport are not defined in the directive or implementation regulation. This has the potential to make it unclear in which cases the platforms are obliged to charge VAT and when they are not (Merkx et al., 2023).

The Confederation of Swedish Enterprise has questioned whether the proposal is efficient in combating VAT fraud. The Confederation is positive about the increased use of e-invoices but finds the timeline for their implementation too short. The proposal includes the abolishment of collective invoices. The Confederation is critical to this abolishment, as to the fact that the invoices must be issued within two days. Furthermore, it requests clearer definitions and presumptions regarding the platform proposal. It also finds that the proposal should be dealt with in parts rather than as one (CFS 2023).

8.6 Concluding remarks

The overall aim of the ViDA proposal can be described as “adapting the VAT system to a digital context.” It is, however, far from the vision in the OECD’s report Tax Administration 3.0, where “tax just happens” (OECD 2020). The proposal still requires the fulfillment of heavy reporting obligations and the issuance of VAT invoices, even in electronic form.

I sympathize with the remark from the Confederation of Swedish Enterprise that the proposal should be dealt with in parts rather than as one proposal. Adapting the VAT system to the digital context is too broad a common denominator. The proposed rules for the platforms
facilitating short-term accommodation and passenger transport stand out from the other proposals since they introduce a system for certain sectors where supplies from non-taxable persons become taxable. The other two proposals concern the collection, reporting, and administration of VAT, but they do not change the foundations of the VAT system as such.

The first pillar, a real-time digital reporting system based on e-invoicing, is a paradigm shift in how to report cross-border trade. The abolishment of recapitulative statements is a small relief for the companies’ administration in comparison to the new reporting obligation, where every cross-border transactions shall be reported in almost real-time. E-invoicing and real-time reporting have great potential when they are fully implemented and cover all transactions. The Member States are free to implement e-invoicing and real-time reporting for all transactions, which would enable the abolishment of VAT returns. As long as the paper form still exists for domestic transactions and not all transactions are reported in real-time, the administrative burdens for the companies will necessarily increase.

The central VIES system will be a huge database. This is a difference in comparison to the current VIES, where the recapitulative statements are stored in national databases but accessible through the VIES interface (Merkx et al., 2023). Since information on all taxable persons’ taxable cross-border transactions will be available in the same database, the risk of exposure to hacking should not be underestimated. At the same time, the tax authorities get efficient tools in their fight against VAT fraud, which is an important interest that may outweigh the cybersecurity issues.

The second pillar, namely the deemed transactions for platforms facilitating short-term accommodation and passenger transport services, is, in my view, the most controversial proposal. The idea behind it—to restore the competitiveness of hotels and taxi companies—is understandable. The proposal, however, raises a lot of questions. What the Commission has done is that it has selected two sectors and decided that transactions in these sectors should be taxed even when non-taxable persons supply them. This is a huge derogation from what normally applies in the EU VAT system. The motivation for it—that the prices are lower for an AirBnb or an Uber in comparison with a hotel or a conventional taxi—is, in my view, not convincing. The quality of the services that you get when you hire a professional instead of a private individual is normally higher,
which motivates a higher price. To have special, disadvantageous VAT rules for two sectors but not for others creates boundary and delimitation issues. Furthermore, the more derogations from the main rules, the more complex the VAT system becomes and the higher the compliance costs. I doubt that this is the right way to go.

The third pillar, with a single VAT registration, is maybe the least controversial part of the proposal since it concerns expanding the OSS system that is already in place. The accounting software is already adapted to provide the output needed for OSS. Expanding it to all transactions with cross-border elements seems efficient and less burdensome for businesses than registering for VAT in other Member States.

To sum up, regarding the first pillar, having one e-invoicing and reporting system for cross-border transactions and one for domestic transactions will cause the taxable person increased difficulties in complying. It is, however, an important step in the right direction, where the VAT returns may be abolished. The second pillar makes services supplied by non-taxable persons taxable. This is a fundamental derogation from the VAT system and needs good reasons. The third pillar makes the OSS system more available, which is a positive development.

References


oru.se/journalarticle/EC+Tax+Review/32.3/ECTA2023018 (Merkxx et al. 2023)
Yurii Orzikh

Chapter 9
Accounting Regulation and Financial Reporting under Ukrainian Legislation

Abstract: The article discusses the challenges and modifications in accounting and financial reporting in Ukraine, especially in light of the ongoing war and digitalization. The article highlights the difficulties of studying this topic due to the abnormal state of affairs caused by the conflict and the associated issues arising from the harmonisation of Ukrainian law with EU standards.

The article provides a historical context for Ukraine’s economic and legislative conditions, with a focus on the impact of the conflict and digital transformation initiatives. It mentions a number of legal acts implemented for digital transformation, such as the Concept for the Development of Ukraine’s Digital Economy and Society in 2018–2020 and the Memorandum of Understanding for the Development and Implementation of the Financial Reporting System.

“What is the current state of accounting and financial reporting legislation in Ukraine?” The research employs the legal-dogmatic method, analysing the current positive law as stated in written and unwritten European or (inter) national rules, principles, concepts, doctrines, case law, and annotations to the literature.

The article discusses in more depth the state regulation of accounting and financial reporting in Ukraine, as well as the responsibilities of various government agencies such as the Ministry of Finance of Ukraine, the National Bank of Ukraine, and the State Treasury Service of Ukraine. In addition, it addresses the current accounting and financial reporting laws in Ukraine, including the application of International Financial Reporting Standards (IFRS) and the categorization of companies according to their size and financial indicators.
The article concludes with a comprehensive overview of the accounting and financial reporting environment in Ukraine, highlighting the challenges posed by the conflict and the ongoing digitalisation efforts.

9.1 Introduction

Conducting this research dedicated to accounting regulation and financial reporting under Ukrainian legislation, on the one hand, and the digitalisation of accounting and financial reporting in Ukraine, on the other, I faced several difficulties which, I assume, I should mention to begin with.

Firstly, I have to say that this study addresses how regulations function during a war. Therefore, this study is narrow because wartime is an abnormal state of affairs, and the law must somehow operate in this abnormal temporary situation. However, studying this topic without considering the war and its drastic impact on the state of affairs is simply impossible, or otherwise, it would make this study irrelevant.

Secondly, there is always a risk of being lost in translation. Although there are unified terms explaining and describing the subject, the national legislation is originally not in English and, therefore, losses of meaning are unavoidable despite the fact that Ukrainian legislation is being harmonised with EU standards continuously.

9.2 Background

Before the wholesale invasion on 24 February, Ukraine somehow had got used to existing in a partial occupation and an ongoing armed conflict in the eastern parts of the country. The Ukrainian economy, businesses, and just ordinary people had just endured the ordeal of Covid 19. Then, 24 February 2022 came, dividing the world into a “before” and “after”. Indeed, it is too far from making any conclusions on the role of that day in the history of the world, not only Ukrainian history, and this is largely what Yurii Lotman talked about in his work “On poets and poetry: Analysis of poetic texts” (Lotman, 1996).
Nevertheless, war is still a part of day-to-day life in Ukraine affecting legislation enormously. It has revealed gaps in places where they could not be imagined. Hence, it has provoked legal scholars and practitioners to think of possible ways of overcoming those gaps within the framework of the rule of law and fundamental principles of law but without a particular legal norm or rule in the national legislation.

Many laws have been adopted during the current war, and not all of them are perfect. However, it is not about merely criticising legislators or other government bodies but about revealing the imperfections of some decisions and their possible undesired outcomes that might echo in the practical application of the law.

It is also worth mentioning a few legal acts that have been adopted as a framework for the ongoing digital transformation. It started with the program act No. 67-p adopted on 17 January 2018 by the Cabinet of Ministers of Ukraine, i.e. the Concept of the Development of Ukraine’s Digital Economy and Society in 2018–2020 (Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii, 2018). The action plan for this Concept was adopted simultaneously with the Concept by the Cabinet of Ministers. On 3 March 2021, the Cabinet of Ministers of Ukraine adopted the Concept for the Development of Digital Competences and the Action Plan for Its Implementation (No. 167-p) (Pro skhvalennia Kontseptsii rozvytku tsyfrovykh kompetentnostei ta zatverdzhennia planu zakhodiv z yii realizatsii, 2021).

Another significant legal act on the digitalisation of accounting and financial reporting processes is Memorandum of Understanding No. 102/15 for the Development and Implementation of the Financial Reporting System signed on 18 December 2017, by the Ministry of Finance of Ukraine, the National Bank of Ukraine, the National Commission for State Regulation of Financial Services Markets, and the National Securities and Stock Market Commission of Ukraine (MEMORANDUM No. 102/15 pro vzaiemorozuminnia shchodo rozrobky i zaprovadzhennia systemy finansovoi zvitnosti, 2017). This document is considered the core act regarding the implementation of the XBRL and iXBRL format of electronic financial reporting. The purpose of the Memorandum was to reach a reciprocal agreement on developing and implementing the financial reporting system in Ukraine in compliance
with the International Financial Reporting Standards, firstly, for those legal entities bound by the law to report under the IFRS. Furthermore, implementing the financial reporting system in Ukraine led to the launch of the Financial Reporting Collection Centre (Shcho take SFZ, n.d.).

In 2017, the State Treasury Service of Ukraine created and implemented E-Reporting, an automated electronic reporting system, for its users, i.e. entities using budget funds. Its operation and implementation began as part of the 2016–2018 Action Plan for the Modernization of the Accounting System in the Public Sector, approved by Order No. 1038 of the Ministry of Finance of Ukraine dated 28 November 2016 (Shchodo zaprovadzhennia AS “Ye-Zvitnist”, 2018).

The E-Reporting system envisages the creation of a personal electronic office (usually called “cabinet” or “e-cabinet” in Ukrainian) for administrators (recipients) of budget funds (budget holder) who prepare and submit financial and/or budget reports to the State Treasury Service of Ukraine. The State Tax Service of Ukraine provides another option for e-reporting via its portal cabinet.tax.gov.ua where tax and financial reports can be created and sent.

However, the issues related to the financial reporting terms and standards will be covered in detail later in this paper as an issue of administrative and criminal liability for the failure to submit reports, for submitting reports with errors (intentionally or unintentionally), or for the late submission of financial reports by certain legal entities.

As was concluded in an article from 2020 “The process of reforming the legal regulation of accounting and financial reporting in Ukraine, which began with the aim of improving the national accounting system and financial reporting pursuant to the requirements of international standards and EU legislation, has currently covered three important areas: (a) re-examination of the relevant regulatory legal acts (adopting new and/or improving existing ones, filling gaps, eliminating collisions, etc.); (b) creation and development of the professional organizations of accountants and auditors; (c) improvement of their professional education system.” (Bodnar, Reznikova, Patsuriia, Radzyviliuk, & Kravets, Accounting and financial reporting of economic entities: adaptation of Ukrainian legislation to the standards of the European Union, 2019.) and now another improvement to this legislation can be added – the adaptation of the current legislation to the state of war.
9.3 Research Question

Considering the circumstances which are currently affecting Ukraine’s economy, legislation, and policy, the research question can be formulated as follows: “What is the current state of the accounting and financial reporting legislation in Ukraine?” Answering this question will surely touch upon such mainstream questions as the digitalisation of accounting and financial reporting, adaptation and harmonisation of Ukrainian legislation with the EU and international standards, etc.

9.4 Research Method

A legal-dogmatic method is used for this research as a core method. However, it goes without saying that general research methods, such as analysis, synthesis, comparison, and analogy are also used. As Jan Vranken states in his article, legal-dogmatic research concerns researching current positive law as laid down in written and unwritten European or (inter) national rules, principles, concepts, doctrines, case law and annotations in the literature (Vranken, 2012). However, this approach provokes another question, which I will only mention because it is out of the scope of my work. This question is directly connected with what we consider as the sources of law. We should accept that neither in legal tradition nor in written national or international law will we find any universal answer to this question. Although no one will challenge the fact that written law is a source of law, which automatically leads to the analysis of the Ukrainian legislation in accounting and financial reporting before and during the full-scale invasion.

9.5 State Regulation of Accounting and Financial Reporting in Ukraine

State regulation of accounting and financial reporting in Ukraine consists of implementing relevant functions by the authorities and their structural units.
The Ministry of Finance of Ukraine is the main body responsible for regulating the accounting and financial reporting methodology, approving the National Accounting Regulations (Standards) and National Accounting Regulations in the Public Sector (Standards), shaping and implementing government policy in the field of accounting and auditing, as well as other issues (Pro bukhhalterskyi oblik ta finansovu zvitnist v Ukraini, 1999).

According to the Regulation ‘On the Ministry of Finance of Ukraine,’ it shall not interfere with the activities of specific enterprises and targets its direct influence on the government authorities under its control and the enterprises under its governance (Polozhennia pro Ministerstvo finansiv Ukrainy, 2014).

At the same time, the Ministry of Finance of Ukraine is charged, among other things, with such tasks as ensuring internal control and performing audits in the Ministry of Finance and enterprises, institutions and organisations under its governance (please see the list of these enterprises on the website of the Ministry of Finance (Derzhavni pidpryiemstva ta ustanovy, shcho nalezhat do sfery upravlinnia Ministerstva, 2021); approving the implementation by state-owned undertakings, including private-sector undertakings (except banks) in which the state owns 50% of the shares (interest) or more; raising internal long-term and external loans; providing guarantees or sureties for such liabilities, etc. (Polozhennia pro Ministerstvo finansiv Ukrainy, 2014).

Thus, the Ministry of Finance has the right and obligation to only influence the activities of those undertakings that fall within the scope of its governance, which usually includes state-owned undertakings or private-sector undertakings where the state owns 50% of the shares (interest) or more.

In relation to the undertakings under the governance of the Ministry of Finance, the latter exercises internal control over their activities and performs internal audits. Moreover, the Ministry may issue direct orders to establish, liquidate, or reorganise undertakings under the governance of the Ministry of Finance (Subclauses 24, 25, Clause 10 of the Regulation on the Ministry of Finance of Ukraine) (Polozhennia pro Ministerstvo finansiv Ukrainy, 2014). In this case, we are talking about the establishment of legal entities qualified by the Civil Code of Ukraine as public-law legal entities (see Article 81 of the Civil Code of Ukraine).
Ukraine) (Tsyvilnyi kodeks Ukrainy, 2003) and by the Economic Code of Ukraine as state-owned unitary and state-owned commercial enterprises (see Articles 73 and 74 of the Economic Code of Ukraine) (Hospodarskyi kodeks Ukrainy, 2003).

In relation to the undertakings under the governance of the Ministry of Finance, the latter appoints and dismisses heads of such undertakings, as well as decides on bringing them to disciplinary liability (Subclause 25-1, Clause 10 of the Regulation on the Ministry of Finance of Ukraine) (Polozhennia pro Ministerstvo finansiv Ukrainy, 2014).

Attention should be paid to the governmental-regulatory activities of the Ministry of Finance. The Ministry of Finance of Ukraine has the right, within the limits of its powers, and is even obliged to issue orders, which are governmental-regulatory acts and are subject to registration by the Ministry of Justice of Ukraine, and to control their implementation and application. Orders of the Ministry of Finance shall be binding upon the central executive authorities, their territorial bodies, local authorities, enterprises, institutions, and organisations, regardless of their form of ownership, and individuals. The binding nature of the orders of the Ministry of Finance on actually all undertakings and individuals cannot be qualified as a direct influence of the Ministry of Finance on the activities of specific undertakings, since its orders are not individual acts, nor are they intended to regulate the activities of any particular undertaking, except for undertakings under the governance of the Ministry of Finance or undertakings in which the state owns 50% of the shares (interest) or more.

By issuing relevant orders, the Ministry of Finance ensures the formation and implementation of the government policy in the field of accounting and auditing, carries out state regulation of accounting, drafts a strategy for the development of the national accounting system, defines the unified methodological principles of accounting and compiling financial and budgetary reporting, ensures and implements the adaptation of accounting and auditing laws in Ukraine to EU legislation which is a part of the Action Plan on the Implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other, approved by Resolution of the CMU of 25 October 2017, No. 1106 (Bodnar, Reznikova, Patsuriia, Radzyviliuk, & Kravets, ...
Particular attention should be paid to the powers of the Ministry of Finance of Ukraine to provide individual clarifications on accounting and auditing issues, which are not governmental-regulatory legal acts by nature but, at the same time, the practice of such clarifications in Ukraine shows that they can be used in practice as a guideline for the application of the law. Thus, the Ministry of Finance of Ukraine, without having the official right to do so, carries out an unofficial interpretation of the legislation since the act of clarification cannot be carried out without an appropriate act of interpretation. However, a particular issue may arise here. Will the clarification issued by the Ministry of Finance still be legitimate and legal if we assume that it is the wrong interpretation, while, at the same time, it will be used by the local executive bodies and a specific legal entity, in respect of which it was adopted, will agree with it?

In addition, the Ministry of Finance regulates the accounting and reporting procedures of legal entities that are state budget holders and local budget holders according to the National Public Sector Accounting Regulations (Standards) approved by the Ministry of Finance.

In turn, the State Treasury Service controls the accounting of revenues and expenditures of the state and local budgets, the preparation and submission of financial and budgetary reporting by holders of the budget funds (Polozhennia pro Derzhavnu kaznacheisku sluzhbu Ukrainy, 2015).

In relation to banks, their accounting and financial reporting are regulated by the National Bank of Ukraine. According to the legislation of Ukraine and specifically Article 6 of the Law of Ukraine ‘On Accounting and Financial Reporting in Ukraine,’ Ukrainian banks are public joint-stock companies obliged to report according to the International Financial Reporting Standards (IFRS) and their taxonomy, and also according to the procedure established by the National Bank of Ukraine. Resolution No. 75 of the National Bank of Ukraine dated 4 July 2018 approved the Regulation on the Organisation of Accounting in Banks of Ukraine, Clause 23 of which states that ‘Accounting and financial reporting of a bank shall be based on the principles outlined in the Conceptual Framework for International Financial Reporting Standards’ (Polozhennia pro orhanizatsiiu bukhhalterskoho obliku v bankakh Ukrainy, 2018).
Separately, according to Article 69 of the Law of Ukraine ‘On Banks and Banking Activity,’ the National Bank of Ukraine shall establish the following for banks and/or banking groups: the list and forms of reports or requirements for forms, periodicity and deadlines for reporting, the procedure for submission and publication of financial statements (annual financial statements, annual consolidated financial statements, interim financial statements, consolidated interim financial statements), consolidated and sub-consolidated statements.

At the same time, the procedure for submitting financial statements approved by Resolution No. 419 of the Cabinet of Ministers of Ukraine dated 28 February 2000 does not apply to bank activities. Banks are guided by the Instruction on the Procedure for Preparing and Publishing Financial Statements of Ukrainian Banks, approved by Resolution No. 373 of the Board of the National Bank of Ukraine dated 24 October 2011, which is based on the requirements of the International Financial Reporting Standards for disclosing information in financial statements.

Summing up, we can say that the main government bodies that carry out the state regulation of accounting and financial reporting in Ukraine are the Ministry of Finance of Ukraine, the National Bank of Ukraine (for banks as a special category of legal entities), and the State Treasury Service of Ukraine.

Certain aspects of accounting and financial reporting regulation are also performed by the State Tax Service of Ukraine (Subclause 2, Clause 6 of the Regulation on the State Tax Service of Ukraine). However, these aspects are limited to the control function aimed at verifying the correctness and completeness of the financial result before taxation according to the National Accounting Regulations or the IFRS (Polozhennia pro Derzhavnu podatkovu sluzhbu Ukrainy, 2019).

We cannot ignore the National Securities and Stock Market Commission, which regulates the procedure for reporting by subjects managing assets of non-state pension funds and the requirements for such reporting, as well as establishes the procedure for public joint-stock companies to disclose information about their activities based on the International Financial Reporting Standards (Pro Natsionalnu komisiu z tsinnykh paperiv ta fondovoho rynku, 2011). The NSSMC also operates the Financial Reporting Centre, to which the financial statements prepared under IFRS requirements are submitted.
9.6 Aspects of Current Accounting and Financial Reporting Legislation in Ukraine

The distinctive feature of accounting development in Ukraine lies in the fact that for over 70 years accounting science has been developing according to the model of command economy. (Hora & Chyzevska, 2013) It can be said that the adoption of a framework law defining the basic aspects of legal regulation of accounting and financial reporting in Ukraine in 1999 was the start of a long process of shaping a modern model of accounting and financial reporting in Ukraine.

For example, the possibility of applying the International Financial Reporting Standards and the relevant taxonomy appeared on 1 January 2012 in the form of Article 12-1 of the Law ‘Application of International Standards’ (Pro vnesennia zmin do Zakonu Ukrainy “Pro bukhhalterskyi oblik ta finansovu zvitnist v Ukraini”, 2011). The implementation of the IFRS in the Ukrainian legal system was thoroughly examined in an article from 2013 by Yang, J. H., Kakabadse, N., & Lozovskyi, D. (Yang, Kakabadse, & Lozovskyi, 2013).

Thus, this Article defines the list of entities and their obligation to apply the IFRS and prepare financial statements based on the taxonomy of financial statements in a single electronic format. These entities include:

- public interest entities (securities issuers admitted to trading on stock exchanges, insurance companies, banks, credit unions, non-state pension funds, and undertakings classified as large undertakings according to their indicators and requirements of the Law of Ukraine ‘On Accounting and Financial Reporting in Ukraine’) (Khto maie zvituvaty?, 2022);
- other entities in the form of public joint-stock companies (listed companies);
- parent companies of groups that include at least one public interest entities;
- parent companies of a large group;
- companies operating in the extractive industry;
- companies providing financial services other than insurance and pension support;
companies engaged in non-state pension support;
- companies that carry out auxiliary activities in the fields of financial services and insurance, except for auxiliary activities in the field of insurance and pension support (e.g., activities of insurance agents and brokers) (Pro zatverdzhennia Poriadku podannia finansovoi zvitnosti, 2000).

However, it is an issue, which is still the subject of discussions between scholars, of what and how should be done by those undertakings (companies) which are not obliged to report according to the international standards (IFRS) but which decided to start to report and maintain accounting according to the international standards (FOMINA, SEMENOVA, & BEREZOVSKA, 2022).

Since 1999, the Law of Ukraine ‘On Accounting and Financial Reporting in Ukraine’ has been amended many times, and the latest amendments were made during the martial law period in Ukraine in order to speed up the approximation of the Ukrainian legislation to international standards.

It was in 2022 that the groups of companies were divided into appropriate categories at the legislative level based on the average staff size in the group, its net income from the sale of products (goods, works, services), and the booked value of assets.

<table>
<thead>
<tr>
<th>Group type</th>
<th>Criterion Balance sheet total¹</th>
<th>Net turnover from sales of products (goods, works², services)</th>
<th>Average number of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small groups</td>
<td>Up to EUR 4,000,000</td>
<td>Up to EUR 8,000,000</td>
<td>Up to 50 employees</td>
</tr>
<tr>
<td>Medium-sized groups</td>
<td>Up to EUR 20,000,000</td>
<td>Up to EUR 40,000,000</td>
<td>Up to 250 employees</td>
</tr>
<tr>
<td>Large groups</td>
<td>More than EUR 20,000,000</td>
<td>More than EUR 40,000,000</td>
<td>More than 250 employees</td>
</tr>
</tbody>
</table>

¹ The official exchange rate of UAH against foreign currencies (average for the period) calculated based on the official exchange rates of the National Bank of Ukraine set for EUR during the respective year is used.

² Ukrainian legislation, unlike many other European countries, contains a distinction between ‘work’ and ‘service’. Moreover, the term ‘work’ in this case has nothing to do with labour relations. One of the main features that distinguishes work from a service...
Prior to these changes, groups of companies were mentioned only indirectly or at the level of specific national standards (regulations) (Pro zatverdzhennia Natsionalnoho polozhennia (standartu) bukhalterskoho obliku 2 «Konsolidovana finansova zvitnist», 2013) or International Financial Reporting Standards (Mizhnarodnyi standart bukhalterskoho obliku 27 (MSBO 27). Konsolidovana ta okrema finansova zvitnist, 2012) and did not contain a clear gradation of types of groups.

Moreover, it was with the amendments of 19 July 2022 that the definition of the term ‘group’ was first enshrined at the legislative level, that is a group of legal entities consisting of a company that controls other companies (parent company) and all companies controlled by it (subsidiaries) (Article 1) (Pro bukhalterskyi oblik ta finansovu zvitnist v Ukraini, 1999), which has a broader meaning compared to the National Accounting Regulation, NAR (Standard) 2 ‘Consolidated Financial Statements.’ The definition of ‘control’ of one company over another is in turn given in the official translation of International Accounting Standard 27 (IAS 27) “Consolidated and Separate Financial Statements”. Control, according to IAS 27, is the power to govern the financial and operating policies of another entity so as to obtain benefits from its activities (Mizhnarodnyi standart bukhalterskoho obliku 27 (MSBO 27). Konsolidovana ta okrema finansova zvitnist, 2012). IAS 27 contains the criteria for determining the existence of control, which it would be interesting and appropriate to compare with the criteria for the existence of control specified in the NAR(S).

Thus, according to Clause 13 of IAS 27, control is presumed to exist if a parent undertaking owns, directly or indirectly through subsidiaries, more than one half of the voting rights of an entity (unless it can be clearly demonstrated that such ownership does not constitute control).

According to Clause 7 of NAR(S) 2 ‘Consolidated Financial Statements,’ a subsidiary is considered to be controlled by a parent company when all of the following conditions are met:

---

in Ukrainian private law is the existence of a tangible object, which is to be created in the course of performing work or taking action by a contractor transforming an existing tangible object (the repair, modification or transformation of a tangible object), whereas services are characterised by actions whose value is consumed/used in the process of their provision. Classic examples in this sense are transportation services, insurance, agency and brokerage activities in stock markets, etc.
1) the parent company has power over the subsidiary;
2) the results of the subsidiary’s activities will directly lead to changes in the composition and value of assets, liabilities, equity of the parent company;
3) the parent company has the actual ability to exercise power.

NAR(S) 2 ‘Consolidated Financial Statements’ also provides, in its appendix, specific examples of powers that are considered to be authoritative in the context of Clause 7 of Section I. NAR(S) does not contain an exhaustive list of such examples of powers, as evidenced by Subclause 5), which, on the one hand, makes it possible to qualify, if necessary, certain authorities as powers even if they are not on the list, and on the other, may become a point for abuse by the relevant government bodies and disputes with them.

An important factor in the approximation of Ukrainian accounting and financial reporting to the international standards is that the state has undertaken to publish international standards in the state language (Ukrainian) on the official website of the Ministry of Finance of Ukraine (Article 12-1) (Pro bukhalterskyi oblik ta finansovu zvitnist v Ukraini, 1999).

The latest amendments to the Law of Ukraine ‘On Accounting and Financial Reporting in Ukraine’ has also affected the procedure for submitting and publishing financial statements, but this issue will be discussed in another part of this paper.

9.7 Procedure for Presenting and Disclosing Financial Statements under the Legislation of Ukraine (in Peacetime and under Wartime)

This part of the article will review in detail the procedure for presenting corporate financial statements, the bodies to which financial statements are presented, the form in which they are presented, the need for their disclosure, etc. It is important to note that, according to the current leg-
islation of Ukraine, financial statements do not constitute a trade secret, are not confidential, and are not classified as restricted information, unless otherwise stipulated by law³.

According to Article 11 of the Law of Ukraine “On Accounting and Financial Reporting in Ukraine”, corporate financial statements shall be compiled based on accounting data and shall be presented in a manner and at a time approved by the Cabinet of Ministers of Ukraine, and for banks – by the National Bank of Ukraine.

The procedure for presenting financial statements, the need and the procedure for their disclosure, and the list of bodies to which financial statements are presented shall depend on the type of undertaking, the category of the undertaking, and the type of the group of undertakings⁴.

The law defines four categories of undertakings which copy the provisions of Article 3 of the Directive 2013/34/EU of the EU (Directive 2013/34/EU of the European Parliament and the Council, 2013) in their entirety:

<table>
<thead>
<tr>
<th>Undertakings category</th>
<th>Balance sheet total⁵</th>
<th>Net turnover from sales of products (goods, works⁶, services)</th>
<th>Average number of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro undertakings</td>
<td>Up to EUR 350,000 inclusive</td>
<td>Up to EUR 700,000 inclusive</td>
<td>Up to 10 employees</td>
</tr>
<tr>
<td>Small undertakings</td>
<td>Up to EUR 4,000,000 inclusive</td>
<td>Up to EUR 8,000,000 inclusive</td>
<td>Up to 50 employees</td>
</tr>
<tr>
<td>Medium-sized undertakings</td>
<td>Up to EUR 20,000,000 inclusive</td>
<td>Up to EUR 40,000,000 inclusive</td>
<td>Up to 250 employees</td>
</tr>
<tr>
<td>Large undertakings</td>
<td>More than EUR 20,000,000</td>
<td>More than EUR 40,000,000</td>
<td>More than 250 employees</td>
</tr>
</tbody>
</table>


⁴ An overview of the types of groups of enterprises is given in another part of this article.

⁵ The official exchange rate of UAH against foreign currencies (average for the period) calculated based on the official exchange rates of the National Bank of Ukraine set for EUR during the respective years shall be used.

⁶ Ukrainian legislation, unlike many other European countries, distinguishes the terms “work” and “service”. See another part of this article that covers this issue.
For most undertakings operating in Ukraine, financial statements shall be compiled according to the NAR(S), which differ for the private and public sectors. However, some authors justify the necessity of creating a unified Conceptual Framework for financial reporting regardless of the type of the entity (Savina, Pozniakovska, & Miklukha, 2021). NAR(S) are approved by the Ministry of Finance of Ukraine, with further registration of the regulatory act by the Ministry of Justice of Ukraine and its publication in the manner established for acts of the Ministries. Most of the existing and current national regulations (standards) govern the activities of private sector undertakings (30 of them) vs. nine standards applicable to public sector undertakings. The typical structure of the national accounting standards comprises basic terms, the order of accounting, object identification and assessment, and the reflection of information in reporting (Hora & Chyzevska, 2013).

NAR(S) in the public sector was drafted based on the IAS for the public sector and is provided for legal entities that are budget spending units, the State Treasury Service, and compulsory state social and pension insurance funds.

Financial statements are compiled according to the international standards in two cases: compulsory compilation for specific undertakings, and voluntary compilation for all undertakings that are not obliged to

---

7 https://zakon.rada.gov.ua/laws/show/493/92#Text (On the State Registration of Regulatory Legal Acts of Ministries and Other Executive Authorities, Decree No. 493/92 of the President of Ukraine of October 03, 1992); https://zakon.rada.gov.ua/laws/show/731-92-%D0%BF#Text (Regulation on the State Registration of Regulatory Legal Acts of Ministries and Other Executive Authorities, approved by Resolution No. 731 of the Cabinet of Ministers of Ukraine of December 28, 1992). The Procedure for the official promulgation and entry into force of regulatory legal acts issued by the Verkhovna Rada of Ukraine, the Cabinet of Ministers, and the President of Ukraine is regulated by Decree No. 503/97 of the President of Ukraine of June 10, 1997. This decree sets out a list of printed media that currently have an electronic version duplication, the publication which is considered to be the official promulgation of Laws and other acts of the Verkhovna Rada of Ukraine, Resolutions and other acts of the Cabinet of Ministers of Ukraine, as well as acts of the President of Ukraine. Additionally, this decree defines the procedure and the term of the entry into force of regulatory legal acts of the above-mentioned agencies.

8 For the list of entities that are budget holders, please see Article 22 of the Budget Code of Ukraine https://zakon.rada.gov.ua/laws/show/2456-17#n458.

9 An overview of such undertakings is given in another part of this article.
report under the IFRS and have independently decided to maintain their records under IFRS.

Currently, financial statements shall be presented to the following entities:

- the State Statistics Service of Ukraine – for all legal entities, regardless of their organisational and legal form of management and ownership;
- the State Tax Service of Ukraine – for income taxpayers who, in the cases stipulated by law, present annual financial statements as part of their income tax returns;
- the State Treasury Service of Ukraine and the Accounting Chamber – for spending units of state and local budgets, the compulsory state and social insurance funds;
- the National Bank of Ukraine – for banks operating in Ukraine;
- the Ministry of Economy of Ukraine and the Ministry of Finance of Ukraine – for ministries, other central executive bodies whose sphere of management covers economic entities of the public economy sector;
- the Financial Reporting Collection Centre – for all legal entities reporting voluntarily or compulsorily based on the financial reporting taxonomy under the International Financial Reporting Standards.

Special attention should be paid to the fact that the Financial Reporting Collection Centre is a kind of additional entity that accumulates financial statements of undertakings reporting under the IFRS. For example, according to Clause 8.5. of the Instruction on the Procedure for Presenting Financial Statements by Ukrainian Banks (Instruktsiiu pro poriadok skladannia ta opryliudnennia finansovoi zvitnosti bankiv Ukrainy, 2011), a bank shall present consolidated interim financial statements in hard copy to the Banking Supervision Department and publish them by posting them on the bank’s website on or before the 30th day of the second month following the reporting period. Thus, the bank shall not only present financial statements to the National Bank of Ukraine and publish them on its website, but shall also present its statements to the Financial Reporting Centre (Khto maie zvituvaty?, 2022).

Income taxpayers shall present financial statements in a unified electronic format – XML document (Poriadok obminu elektronnymy
This format was introduced along with the adoption of Order No. 729 of the Ministry of Revenues and Duties of Ukraine (currently, the State Fiscal Service of Ukraine) of November 29, 2013 within the framework of the implementation of the Concept of Creation and Functioning of the Automated System “One-Stop Window for Electronic Reporting” and the Action Plan for its Implementation (Format (standart) elektronnoho dokumenta zvitnosti subiektiv hospodariuvannia, 2014). This format was introduced even before Ukraine introduced a unified format for presenting financial statements for undertakings presenting their statements under IFRS to the Financial Reporting Collection Centre in a unified iXBRL format.

**Mandatory publishing** on their webpage or website is provided for the following types of legal entities within the following periods:

| Until 30 April of the year following the reporting period | – Main budget holders (spending units) | – annual financial statements;  
| – annual consolidated financial statements; |
| Until 30 April of the year following the reporting period | – Public interest entities (except for large undertakings that are not securities issuers)  
| – Public joint-stock companies-Subjects of natural monopolies in the national market11  
| – Undertakings operating in the mining industries (extractive industries) | – annual financial statements;  
| – annual consolidated financial statements;  
| – audit reports;  
| – management reports;  
| – consolidated management reports;  
| – report on payments made to government;  
| – consolidated reports on payments made to government; |
| No later than 1 June of the year following the reporting period | – Large undertakings that are not securities issuers  
| – Medium-sized undertakings |

---


<table>
<thead>
<tr>
<th>Reporting Period</th>
<th>Financial Statements and Reports</th>
<th>Reporting Period</th>
<th>Financial Statements and Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>No later than 1 June of the year following the reporting period</td>
<td>- Other financial institutions; - Non-state pension funds belonging to micro undertakings and small undertakings;</td>
<td>No later than 1 June of the year following the reporting period</td>
<td>- Small undertakings that are economic entities of the public economy sector</td>
</tr>
<tr>
<td></td>
<td>- annual financial statements; - annual consolidated financial statements; - audit reports; - management reports; - consolidated management reports;</td>
<td></td>
<td>- annual financial statements; - audit reports (if mandatory audit of financial statements is required by law);</td>
</tr>
<tr>
<td>No later than 1 June of the year following the reporting period</td>
<td>- Parent companies of a large group that belong to the category of large undertakings (except for investment entities that do not compile consolidated financial statements according to the international standards)</td>
<td>No later than 1 June of the year following the reporting period</td>
<td>- annual consolidated financial statements compiled according to the international standards; - audit reports; - consolidated management reports; - consolidated reports on payments made to government;</td>
</tr>
<tr>
<td>No later than 1 June of the year following the reporting period</td>
<td>- Parent companies that are also subsidiaries and, according to the requirements of NAR(S) or IFRS, do not present consolidated financial statements</td>
<td>No later than 1 June of the year following the reporting period</td>
<td>- annual consolidated financial statements of its parent company, - audit reports of the parent company, - consolidated management reports;</td>
</tr>
<tr>
<td>No later than 1 June of the year following the reporting period</td>
<td>- Central executive body that implements the policy in the field of treasury servicing of budget funds (State Treasury Service of Ukraine) (Polozhennia pro Derzhavnu kaznacheisku službu Ukrainy, 2015)</td>
<td>No later than 1 June of the year following the reporting period</td>
<td>- annual consolidated statements on the general property status and performance of public sector entities and budgets</td>
</tr>
</tbody>
</table>

An important innovation in the changes that took place in the summer of 2022 was the release from the mandatory compilation and presentation of annual consolidated financial statements of large group companies that belong to the category of large undertakings. This change was intended to reduce the administrative burden on large companies, which are already subjected to high levels of regulatory requirements. However, the requirement to provide consolidated management reports remains unchanged, as these reports are essential for monitoring and oversight purposes.

12 Except for the report on payments made to government and the consolidated report on payments made to government.
Chapter 9 Accounting Regulation and Financial Reporting under Ukrainian …

of consolidated financial statements and a consolidated management report for small and medium-sized groups of undertakings, except for those that include at least one public interest entity. That is, these groups have the right to compile and present such statements, but they are under no obligation and, therefore, they cannot be held liable for failure to compile or present financial statements. At the same time, if small and medium-sized groups decide to compile and present such financial statements, they shall be liable for the accuracy and completeness of the information. The implementation of such exemptions was another step in the harmonisation of national legislation with EU standards because under Article 23 of Directive 2013/34/EU small and medium-sized groups are also exempted from the obligation to draw up consolidated financial statements and a consolidated management report, except where any affiliated undertaking is a public-interest entity (Directive 2013/34/EU of the European Parliament and the Council, 2013).

Please note that the deadlines for disclosing and presenting financial statements may differ and also depend on a number of factors that characterise the reporting legal entity. Thus, the Procedure for Presenting Financial Statements establishes the deadlines for presenting annual financial statements and interim financial statements of legal entities of private law (including non-entrepreneurial companies) and legal entities of public law (state and municipal legal entities, ministries and departments that have the status of a legal entity, etc.) As a rule, most undertakings (micro undertakings, small undertakings, non-entrepreneurial companies and undertakings that maintain simplified bookkeeping) present financial statements on or before 28 February of the year following the reporting year (Pro zatverdzhennia Poriadku podannia finansovoi zvitnosti, 2000).

All undertakings that are obliged to publish annual financial statements shall present to the state statistics and tax authorities a statement of financial position (balance sheet) and a statement of profit and loss and other comprehensive income (income statement), except for consolidated financial statements, for the reporting year on or before 28 February of the year following the reporting year. Instead, companies that use the IFRS to compile financial statements shall present them to the Financial Reporting Collection Centre by the deadline established for disclosing such information (Pro zatverdzhennia Poriadku podannia finansovoi zvitnosti, 2000).
The presentation of revised financial statements is allowed only in the manner established for financial statements subject to revision. At the same time, regulatory legal acts do not establish deadlines for presenting revised financial statements based on the results of the audit and independently identified errors or for other reasons.

Wartime has changed the way undertakings present their financial statements and their obligation to publish financial statements in different ways. Undertakings that did not present interim, annual financial statements and consolidated financial statements during the period of martial law or the state of war within the period specified in this Procedure shall present such statements within three months after the termination or cancellation of martial law or state of war for the entire period of non-presentation of such statements (Pro zatverdzhennia Poriadku podannia finansovoi zvitnosti, 2000).

In addition, as early as on 3 March, 2022, the Law of Ukraine “On the Protection of Interests of Subjects of Reporting and Other Documents during Martial Law or the State of War” (Pro zakhyst interesiv subiektiv podannia zvitnosti ta inshykh dokumentiv u period dii voennoho stanu abo stanu viiny, 2022) was adopted, which applies to almost all types of reporting except for tax reporting, and does not apply to banks. This law establishes the need to present and publish, inter alia, financial statements in hard and/or soft form within three months after the termination or cancellation of martial law or the state of war for the entire period of non-presentation of statements. The specific aspect is that the inability to present statements or documents must be objectively confirmed in fact for each particular reporting entity. Administrative and criminal liability for failure to present or late presentation and non-disclosure of financial statements shall also not be imposed during the period of martial law or the state of war, as well as within three months after its termination.

Separately, regarding the reporting of banks to the National Bank of Ukraine, the NBU Board adopted Resolution No. 41 of 7 March, 2022 “On Compiling and Presenting Financial Statements during Martial Law” (Pro skladannia ta podannia finansovoi zvitnosti v period zaprovadzhennia voennoho stanu, 2022), which effectively suspended the obligation to compile, present, and publish financial statements by banks that are unable to do so due to the introduction of martial law in Ukraine because of the military aggression of the Russian Federation.
against Ukraine. The Resolution states, firstly, that the NBU shall not apply penalties on the banks’ failure to meet the deadlines for presenting and disclosing financial statements during the period of martial law and within three months after its termination or cancellation. At the same time, it should be noted that the NBU is not the only body that has the right under the legislation of Ukraine to apply measures of influence to banks or bring them to liability. Secondly, it is established that Ukrainian banks, during the period of martial law and within three months after its termination or cancellation, shall present to the NBU financial statements in hard copy or a scanned copy thereof sent via email and signed with a qualified electronic signature.

References


Chapter 9 Accounting Regulation and Financial Reporting under Ukrainian …


Mais Qandeel

Chapter 10
Blockchain Application in Information Ecosystems: The Right to Privacy in Cyberspace

Abstract: This chapter explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in enhancing the protection of human rights in the application of financial information retrieval ecosystems. In this chapter, the legal analysis of such an application focuses on data protection, specifically privacy. Thus, it first discusses how blockchain technology application plays a vital role in realising and challenging data protection. In essence, the chapter seeks to establish how such technological enhancement will securely facilitate governmental and business operations in dealing with data/information from a human rights perspective.

10.1 Introduction

The transformative prospects of distributed ledger technology (DLT) have attracted great interest. Financial institutions are investing heavily in the initial applications of DLT technology. DLT has been used in various applications to enhance efficiency, reduce costs, and ensure immutability, traceability, security, and transparency. In the application of financial retrieval systems, the way data is collected, reported, stored, used, obtained, processed, shared is of utmost importance. Businesses must provide their financial data to the public authorities, depending on the jurisdiction and domestic regulations in place. This data is mostly provided digitally on an annual or monthly basis, which is surrounded by certain complexities and concerns. The existence of an ecosystem that
enables businesses and authorities to submit and retrieve data, respectively, provides a digitalized environment with certain probabilities that facilitate the conduct of financial information.

At the same time, this digital ecosystem is encircled with/surrounded by human rights concerns, particularly the protection of individual (data) privacy. Privacy refers to individuals’ rights to entirely possess, control and govern the transmission of their own data as to how, when, with whom and how, and for how long. This also concerns the authorization granted to other actors, whether other individuals, public authorities, or corporations. As protected in international, regional and domestic regulations, the right to privacy is one of the main pillars where data is concerned. The question of privacy becomes significant when involving personal and sensitive data. Additionally, the question of the type of technology that is used in such an ecosystem is of great significance. Blockchain technology is today utilized as a harbour of many digital activities, including financial information storage; hence, an attentive assessment of the legal implication of such technology in relation to privacy is needed.

This chapter explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in enhancing the protection of human rights in the application of financial information retrieval ecosystems. In this chapter, the legal analysis of such application focuses on data protection, specifically privacy. Thus, it first discusses how blockchain technology application plays a vital role in realizing and challenging data protection. In essence, the chapter seeks to establish how such technological enhancement will securely facilitate governmental and business operations in dealing with data/information from a human rights perspective.

---

10.2 Features of the Ledgers

This section does not intend to provide a comprehensive and detailed description of distributed ledger technology or fully examine its technical characteristics. It rather sheds light on the main features of ledgers, specifically blockchain technology, and focuses on the portrayal of these features and their connection to privacy issues. The ultimate purpose of this portrayal is to provide an assessment of the challenges and opportunities of blockchain technology when used as a data hub for information ecosystems. To appreciate (data) privacy protection, it is central to look at the current pronounced characteristics of blockchain technology and assess its capabilities.

Distributed ledger technology can hold transactions and interactions to secure communications in a complex information environment, which are at the origin of data creation and collection. In recognition of the importance of accurate and timely information as a precondition for human rights, blockchain technology is a significant framework to increase accountability and transparency for the prevention of human rights abuses. Several questions should be asked: what is distributed ledger technology? What is blockchain technology? What are the distinguishable characteristics of blockchain technology? And what is their connection with privacy? These questions are discussed briefly in this section.

Distributed ledgers are a model of decentralised records where data can be upheld in storage points that are connected. Distributed ledger technology can be defined as “a system for value transactions running on a peer-to-peer (P2P) network that is distributed and does not require a central authority to intermediate those transactions.”2 Blockchain technology is a form of distributed ledger technology, and in the financial world, it can be described as an “accounting book”.3 It is one of the most used and well-known applications for ledgers. Blockchain technology is simply, as the name suggests, a “ledger of transactions, or blocks, that form to make a systematic, linear chain of all transactions ever made.

---


While the blocks themselves are highly encrypted and anonymized, the transaction headers are made public and not owned or mediated by any specific person or entity.”

Blockchain can be public, alliance/hybrid and private. For the purpose of any intended application of blockchain in a financial information system, it is important to note the permissioned-private blockchain is assumingly the tool to be utilized. Notably, other applications of blockchain technology benefit from being public. Although it was its initial purpose, blockchain technology has moved beyond cryptocurrencies. It has been applied in several application areas such as supply chain management, banking and finance, digital authentication, smart contracts and asset trading. Blockchain technology, in essence, has the potential to transform businesses and their legal and regulatory implications. Remarkably, it could be used in both the public and private sectors. It is, indeed, a potential booster of development and innovation. Blockchain technology has many features, upon which it has gained its popularity. In the process of analysing the legal issues and implication of this technology in relation to privacy, it is vital to identify the main characteristics of blockchain technology.

The main relevant characteristics or features are i) decentralization, ii) cryptography and iii) immutability. First, decentralization is one of the main disguisable characters of blockchain. Instead of relying on a centralized ledger, “many data storage points (nodes) are all connected with each other and store all data simultaneously, together constituting

---


the common ledger… [it] requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device.”

To put it simply, instead of relying on an intermediary to confirm the data transfer, blockchain requires consensus on such data. This feature creates the potential to increase and foster data security due to the absence of intermediaries.

Second, cryptography refers to the fact that the data stored on blockchain is securely reliant on authorized access. While some blockchains are public, others are private and need a special private key to access. Blockchain maintains “confidentiality of the content and participants in each transaction… [the only one] with the correct key can access the details associated with a specific record.” Access to data that is stored on blockchain technology can only be elaborately accessed by an authorized person who holds the ‘access key’. From an information security point of view, cryptography can be considered to partially contribute to the fulfillment of the C.I.A. information security triangle, namely, confidentiality, integrity and availability of information. The designed cryptographic nature of the blockchain increases cybersecurity and could be sufficient to resist hacking and security threats. Cryptography is vital to ensure that the transferred and stored data is secure, which is coupled with the idea of privacy.

Third, immutability means, in simple terms, that all data and transactions that exist on blockchain cannot be edited, reversed, altered or

---


deleted. It “refers to the fact that no participant in a blockchain initiative can tamper with a transaction once it is agreed upon.”\textsuperscript{14} This unique characteristic of blockchain technology makes it extremely transparent\textsuperscript{15} and ensures authenticity, where the manipulation and corruption of data cannot be inflicted. This is what can be identified here as \textit{transparency by design}. Immutability scores high in blockchain technology design, hence the name \textit{immutability by design}. At the same time, this very same characteristic has raised concerns regarding errors that have occurred and enforceability issues. At the European level, for instance, this immutability characteristic explicitly opposes compliance with the erasing requirements imposed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), particularly the right to erasure / be forgotten.\textsuperscript{16}

Although these characteristics of blockchain technology are surrounded by claims of increasing cybersecurity,\textsuperscript{17} some studies on the security and privacy of blockchain technology have shown that “many applications [of blockchain] have fallen victim to successful cyberattacks.”\textsuperscript{18} There are several challenges concerning and notable attacks on blockchain applications that have occurred in the last few years.\textsuperscript{19} For example, the hacking of Mt.Gox, a Bitcoin exchange resulting in 473 million US dollars’ worth of losses, and Ether currency where USD 53 million were wrongly channelled to a third party, and in some of the attacks “[t]he White Hat Group breached the wallets using the same vulnerability as the attackers and funneled the funds into the group’s

own account.” In 2022, Binance, the world’s biggest cryptocurrency exchange, suffered a hack, targeting vulnerabilities in its blockchain that serves the assets transfers between networks, with loses estimated at USD 570 million. Such attacks are only examples of the vulnerabilities that surround blockchain application. Simply put, blockchain technology, despite all the promising features, can be and has been subject to cyber-attacks. Blockchain’s vulnerabilities are predominantly coupled with privacy concerns. The attacks targeted against blockchain applications genuinely raise concerns in connection with network communications as “privacy leakage is gradually increasing.” In response to privacy concerns, some data brokers (database providers) have attempted to minimize sensitive identifiable information. Attacks that lead to, among others, communication interferences, damage or corrupt data, and access to confidential and sensitive data, including biometric and metadata, can result in breaches to the protected right to privacy.

10.3 The Right to Privacy in Cyberspace

The right to privacy in cyberspace has attracted enormous attention at all levels – national, regional and international. Such attention is present in the application of technologies in all fields, whether in law, judiciary, finance, informatics, governance and public sectors, among others. Concerns about the right to privacy, in particular, data privacy have been continuously raised. In the application of blockchain technology in financial information systems, concerns about data privacy cannot be

---


ignored. In order to ensure the privacy requirements of the data when transferred, retrieved, processed, used, stored, shared and obtained, the nexus between data privacy and blockchain must be understood. This is the purpose of this section.

The protection of human rights generally applies offline and online. Privacy (of data) in the cyberspace has gained special attention, and it is described as “central to the enjoyment… of human rights online… [and] one of the foundations of a democratic society…” The Charter of Human Rights and Principles for the Internet includes data privacy as one of its main pillars. Principle 5: Privacy and Data Protection precisely provides that:

Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

At the regional and domestic levels, (data) privacy is also well-protected. For example, the European General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the Swedish Data Protection Act (2018:218) and California Consumer Privacy Act of 2018 (CCPA) give individuals i) more power and control over their own personal data that governments and businesses collect and possess about them and ii) more privacy protection with very peculiar securities such as the right to know,

---

25 The right to privacy is internationally protected in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, which both provide that: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.
the right to consent, the right to delete/oblivion, the right to opt-out, the right to correct and the right to limit. Blockchain is seen as a challenge to these legal requirements, specific to their contexts and jurisdictions.

The protection of data privacy is well-established. International law, statutory, common law, and constitutional privacy rights rest on diverse assumptions about the nature and purposes of privacy.”

Individuals have the right to control all aspects of their data, as to where it is stored, how, why, and by whom it is used, for what purposes and for how long it is being handled. Derived from its vital significance, privacy has been comprehensively discussed by the United Nations General Assembly (UN GA), Human Rights Council (HRC) and legal scholars nationally and internationally. In its resolution 75/176 of 2020, the UN GA highlighted the obligations of public authorities and business enterprises concerning data privacy. For the interest of this chapter, the subject matters to emphasize are the relationship between public authorities and business enterprises in connection with handling data. The resolution provides that States must take “measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises”, where there must be “transparency measures with regard to requests by State authorities for access to private user data and information.”

In order to protect data privacy, the use of secure and safe technological applications, the choice of what technology to apply becomes central. For this specific need, arguably, blockchain technology can preliminarily offer a promising secure venue for informational ecosystems. This ultimate goal is reflected in the HRC, where it is of utmost importance that public authorities and business enterprises use “technical solutions to secure and to protect the confidentiality of digital communications, including

---


measures for encryption, pseudonymization and anonymity.”

The use of proper technical solutions would, in principle, provide for privacy risk management and governance mechanisms, which is recommended by the UN Special Rapporteur on the right to privacy. This, however, needs to be approached with caution. Technical solutions may be inspired by, for instance, privacy by design and data protection.

Studies have shown that the use of blockchain applications is combined with considerable risks to privacy. In other words, “even when users are hiding behind multiple pseudonyms, these can be correlated and often identify them... the fact that transactions are linked, one can retrieve the full history of all transactions performed on a blockchain.”

This entails that privacy cannot be achieved simply because privacy was never the purpose of blockchain. In order to make blockchain privacy sensitive, it can be combined with other technologies that offer privacy by design where data is conducted to provide authenticity guarantees. For that purpose, it is noteworthy to indicate that, as Ethereum Foundation puts it, “blockchains do NOT solve privacy issues, and are an authenticity solution only... putting [any data] records in plaintext onto a blockchain is a Very Bad Idea.”

As long as the data is stored in an encrypted format, where it cannot be tampered with or deleted, blockchain can

---

moderately satisfy privacy requirements. This, conversely, created other sets of problems, as the data cannot be removed, and long-term data protection becomes a challenge.37

The submission of such a requirement comes in handy when thinking of blockchain technology and its defined characteristics, explicitly encryption, on the one hand. On the other, the much-desired characteristic in some practices becomes a disadvantage for others. When using blockchain technology in information ecosystems, transparency may become a downside, where all information is exposed unwittingly and unnecessarily. The current state-of-the-art shows that blockchain still raises problems as regards, enter alia, privacy issues, namely: pseudo-anonymity, immutability, where failure to meet privacy requirements as such, responsibility, accountability38 and States’ obligations39 become an integral part of the legal discussion of blockchain technology. Eventually, questions concerning law compliance are essential to bridge the gap between law and technology. Whether the law should adopt to technological advancements and features or vice versa is the focus of the next section.

10.4 Law Compliance or Technology Compliance

The disconnect between law and technology can make it difficult to reconcile current data protection laws with the core characteristics of blockchain, such as the lack of centralization, immutability and perpetual data storage. The current state of affairs of regulatory guidance limits opportunities for an effective reconciliation between law provisions and blockchain technology. It is crucial then to think of the law as a flexible protection instrument or reverse that thinking if indispensable. If the law

is deemed hard and inflexible, would the technology have to adopt its features to be law compliant – here technology developers and computer scientists are concerned. This is a remarkable intersection between law and technology.

When computer scientists ensure that technology by-design meets the existing regulatory framework, this creates a type of technology that is law compliant, this is what I call law compliant technology. In this case, lawmakers and judiciary, within the existing legal framework, develop the legal norms and their application. This would not require any ground-breaking rules or be confronted with unforeseeable violations. In the real and digital worlds, this is not the case. Technology has proved that it has no boundaries and comes to challenge the law, not to obey it. Possible legal capacity for extending the scope of existing legal provisions to encompass new activities that should/should not be covered by the law (domestic, regional or international) is questionable. Thus, can the laws and regulations demand that properties of blockchain technology should be changed? This is very unlikely. Regulators tend to put limitations on the use of technologies and address their implications.

Consequently, this limits the discussion to the ability of the law to follow-up technological developments. This is what I identify as technology compliance with limitations. There are two scenarios here to point out: the first scenario concerns whether the law should rapidly be made up to date considering the development and implications of technologies, and the second scenario concerns whether the law should restrict the application of technologies for mitigating risks and preventing violations. The answers to these two scenarios are short. It has been established that blockchains have regulatory issues. As technology develops, the law must adapt rapidly. Simply put, the regulatory framework must be able to address the regulatory and human rights issues, namely privacy, pertaining from the use and implementation of blockchain technologies.

---

The best way, or perhaps the only way, to ensure that blockchain is privacy compliant is to limit its use, depending on the purpose and the sought after benefits. Blockchain enhances transparency but has vulnerabilities. This can be done through legal design and stronger implementation to provide for legal protection mechanisms for privacy-preserving blockchain application. The lawmakers first need to fully understand the technology itself, then design, in consultation with blockchain developers, regulations that fit best. Blockchain governance in the public sector has already been suggested. However, laws must mostly address the legal implications pertaining to the use of blockchain, particularly when sensitive and personal data is involved.

10.5 Conclusions

Financial information continuously involves individual and sensitive data. The use of blockchain technology raises legal issues and privacy concerns. Today, the lack of unambiguous regulations to curb the use of the various types of technologies forces an assessment of the very basic legal principles and existing norms. It might be very unrealistic to expect that the law should step in and address every single application of technology and then foresee its use and misuse. The law should be general in order to accommodate an expansive range of technological applications. Then an assessment of the use of these technologies and their peculiarities becomes a need.

For the very purpose of privacy, the application of blockchain technology as a hub for storing, maintaining, obtaining, sharing, rederiving and using data in a financial information system might not be the best option. However, blockchain technology is a distinct tool if used in combination with other technologies that preserve (data) privacy. This is to ensure that a combination of the most important features that technologies can offer eliminates law non-compliance and provides the best solutions. Changing the human rights approach or making exceptions for each

technology is not a viable legal option. Changing blockchain properties and characteristics does not seem achievable. A new technology that combines the best of all technologies could be the new way. This would possibly bridge the gap between law and technology and would reconcile current data protection laws with the core characteristics of blockchain in the use of financial information systems.

References


Abstract: This paper aims to outline the compatibility profiles of the European principle of free movement of capital with the most recent phenomena of digital taxation, specifically focusing on the role of cryptocurrencies. On this point, the MICA (Markets in Crypto Assets) Regulation, the main features of which will be outlined below, could provide the much needed clarity and legal certainty that all issuers and users of these digital instruments have been eagerly awaiting for some time.

Finally, we aim to examine the current Italian operational framework on the basis of the interpretation of the tax authorities, trying to offer some food for thought on the state of the art.

11.1 Introduction

Recently, technological developments have fostered the emergence of new categories of potential payment methods, the cryptocurrencies, such as electronic and entirely intangible financial instruments, which are placed within a fully decentralised and supranational mechanism. Specifically, the number of different cryptos in the digital area in the global landscape has multiplied several times, generating a system of currencies freely issued by private agents.

This paper focuses on the difficulty of identifying, at Union level, a proper regulatory and supervisory regime, which must necessarily be
compatible with the free movement of capital, enshrined in Articles 63 to 66 TFEU. Article 63 TFEU alone states that the rules on the movement of capital and payments must be in line with the legal obligation to remove all restrictions between Member States, as well as between Member States and third countries.

In any case, the great volatility shown by the market for such virtual currencies does not seem to support the idea that the issuance of such competing coins is the crucial element in determining their survival and dominance over government currencies (Comandini 2020; Carstens 2018; Gasparri, 2015; Waknis 2017). These premises make you realise the growing importance and difficulties of this digital wealth, which to all intents and purposes has made the work of economists and jurists much more burdensome, precisely because of its difficult demarcation and legal qualification in the different branches of the legal system and in the different models of global finance.

11.2 Blockchain Technology and Digital Wealth

Technological innovations related to the use of smart contracts and blockchain are revolutionising the payment and financial services industry (so-called Fintech) and the capital markets. This technology is entering numerous sectors such as real estate (Prop Tech), the regulation of financial intermediaries (Reg Tech), insurance (Insurance Tech) and legal services (Legal Tech). At the centre of this discourse is certainly so-called blockchain technology, literally block chain, which can be framed as a kind of ledger on which all transactions between one user and another are recorded, enabling sic et simpliciter cryptocurrencies to circulate in Web 3.0. This register is the same for all the computer devices that make up the network and each block represents a page of it.

Each blockchain is thus an encrypted environment, inaccessible to the outside world, in which all the information about the transactions executed by users of financial markets is collected, ensuring the immutability and transparency of transactions. Since they are the latest generation of digital instruments, technologically advanced and subject to continuous
experimentation, their use in the financial markets is currently not subject to regulation. On this point, the absence of an ad hoc regulation exposes the protagonists of digital exchanges to considerable risks; reference is mainly made to the anonymity with which a cryptocurrency circulates, not allowing its users to be adequately informed with respect to their counterparts, i.e. the recipient of any payment. In particular, the greatest danger to which one is exposed is that of being unknowingly involved in money-laundering activities or fraud. However, the payment method itself is not to be demonised, indeed its widespread use is to be desired; but before carrying out any transactions, it is essential to ascertain the identity of the counterpart to the contractual regulation.

11.3 The Proposed EU Regulation: Objectives and Milestones

Thus, it seems unquestionable that the operational framework of crypto-assets and cryptocurrencies is far from easy to understand. In fact, it is necessary to reflect on the EU proposal of 24 September 2020 to amend Directive No. 2019/1937, highlighting the clear EU need to intervene in the regulation of crypto markets.\(^1\)

Firstly, this body of legislation is part of the digital finance package, containing measures aimed at exploiting the potential of digital finance in terms of innovation and competition, mitigating risks and also being in line with the pilot scheme on market infrastructures based on distributed ledger technology (DLT).\(^2\) Secondly, it is undisputed that technological innovation should be promoted without undermining the EU’s fair competition regime, guaranteeing consumer and investor protection, and also attempting to move towards a high degree of financial stability

---

1 The European Commission has issued this regulatory proposal entitled Markets in Crypto-Assets (MiCA), which is expected to be fully operational by December 2022.
of crypto-assets, in view of the fact that they are constantly evolving (Befani 2019).

It also points out that EU action has been promoted through two cardinal principles of the system, namely proportionality and subsidiarity. In fact, the proposal is based on Article 114 of the Treaty on the Functioning of the European Union, which gives the Community institutions the power to lay down the most appropriate provisions to achieve the approximation of the laws of the Member States, ensuring the establishment and functioning of the internal market.

The above-mentioned rule also allows the adoption of acts in the form of a regulation or a directive, although, in the present case, it is considered that the choice could fall on a regulation, as it is more appropriate to establish a single set of rules immediately applicable throughout the Single Market.

The above should aim at removing obstacles that could undermine the functioning of financial services, bearing in mind that, as of today, issuers and service providers of crypto-assets cannot fully exploit the benefits of EU freedom, due to the absence of a specific regulatory and supervisory regime, consistent at EU level.

The above should aim at removing obstacles that could undermine the functioning of financial services, bearing in mind that, as of today, issuers and service providers of crypto-assets cannot fully exploit the benefits of EU freedom, due to the absence of a specific regulatory and supervisory regime, consistent at EU level. A legislative proposal for a regulation on cryptocurrency markets, MiCA (Markets in Crypto-Assets), is currently being finalised by the European policy-making institutions. The European Commission presented this proposal in September 2020 and the European Council reached an agreement on the text at the end of November 2021. Since then, it has been under negotiation between the European Parliament and the EU Council, with the aim of reaching a final agreement.

---

3 Recommendation 7 of the final report of the High Level Forum on Capital Markets Union, where it is highlighted that: “only some Member States have already implemented a specific regime to regulate all or part of the activities of some service providers for crypto-assets but in most Member States they operate outside any regulatory regime. Moreover, an increasing number of Member States are considering setting up specific national frameworks to regulate in particular crypto-assets and their service providers.”
The proposed MiCA Regulation provides for a set of common rules in the EU, focusing on legal certainty and adequate legal protection for crypto asset users, which would be applicable to issuers and service providers of these instruments. This framework will replace any existing national regulations on crypto-assets other than those covered by EU financial services legislation. The proposal does not apply to non-fungible crypto-assets, nor to crypto-assets that qualify as financial instruments, deposits, funds, securitisation positions or pension products, among others, to which the legislation in force for each type of financial instrument mentioned above will apply. It applies instead to stablecoins, understood as those cryptocurrencies that aim to maintain a stable value by reference to the value of an official currency, another security or right, or a combination of both.

If these stablecoins fulfil certain requirements, they will also qualify as e-money, as explained below.

The proposal distinguishes between the following classes of crypto-assets: on the one hand, those classifiable as stablecoins, identified as e-money tokens and asset-referenced tokens, and, on the other, other crypto-assets. Specifically, e-money tokens are a class of crypto-assets intended to be used as a medium of exchange and to maintain their stable value, and the issuers of these tokens must be credit or e-money institutions. Asset-backed tokens are a class of crypto-assets other than e-money and issuers of asset-backed tokens are required to create and maintain an asset pool at all times. The latter is formed in the interest of the holders of such tokens and must therefore be separated from the assets of the issuer. The assets in the pool can only be invested in financial instruments with high liquidity and minimal market, credit and concentration risks. Finally, the proposed MiCA Regulation requires that the pool be managed in such a way that it can cope with the liquidity risks associated with the redemption of token holders and cover the risks associated with the assets to which the tokens refer.

All other cryptocurrencies, other than those mentioned above, are included in the scope of the proposal. E-money tokens and asset-backed tokens may also be significant when certain criteria are met or certain thresholds are exceeded, relating to the customer base, the value of tokens issued or the number and value of transactions. The proposal regulates
further aspects of the activities of cryptocurrency issuers and service providers related to these activities.

For the former, rules have been introduced on authorisation, the preparation of the information document on the issuance of cryptocurrencies (‘white paper’), organisation, governance or supervision. The latter can provide different services and the proposal includes rules for each of them, including prudential rules (own funds, insurance policies), organisational rules, rules on client information, safeguarding clients’ funds, conflicts of interest and rules on outsourcing. Credit institutions may be both issuers of crypto-assets and providers of crypto-asset services, and in neither case are they required to obtain a licence to carry out this activity. However, this does not exclude the application of other provisions contained in the proposed MiCA Regulation.

The regulation of cryptocurrency service providers can ensure that the pace of cryptocurrency market expansion is appropriate and avoid excessive accumulation of risk; despite the possibilities of peer-to-peer trading of crypto-assets, the development of intermediaries can be important to increase the scale of the crypto-asset market, implement efficiency gains and reduce information asymmetry. If regulations were to ensure an adequate degree of transparency and prudence of these intermediaries, this could make it possible to effectively control the accumulation of risks associated with crypto-assets, particularly from the point of view of the information required by the regulator and the number of entities to monitor compliance.

Last but not least, the supervision of issuers is the responsibility of the competent national authorities, unless the e-money tokens and asset-backed tokens issued are significant, in which case a European-level supervisory authority in cooperation with a college of supervisors will assume responsibility (Ooi 2022).

11.4 The Italian Cryptocurrency Framework for Direct Taxes: the Role of Practice

Following the description of the characterising features of the MiCA Regulation, emphasis should be placed on the Italian experience of virtual
currency transactions. It seems unquestionable that the uncertainty over the exact legal and accounting framework of cryptocurrencies has significantly complicated the subsequent tax qualification. Tax law provides for different ways of determining income and identifies different moments when a taxable realisation event may arise, depending on whether the object is an asset, a legal tender or an investment of a financial nature. Not surprisingly, the life cycle of cryptocurrencies affects all legal areas of taxation.

The European legislator, which recently intervened in this matter with the legislative resolution of 29 April 2018 of the European Parliament amending EU Directive 2015/849, defines virtual currencies as: “a representation of digital value that is not issued or guaranteed by a central bank or public entity, is not necessarily linked to a legally established currency, does not possess the legal status of currency or money, but is accepted by natural and legal persons as a medium of exchange and can be transferred, stored and exchanged electronically.”

With regard to direct taxes on capital gains realised by companies and citizens, there is no specific tax legislation referring to virtual currencies. However, the Inland Revenue Agency provided guidance on the applicable tax regime and affirmed a full assimilation of virtual currencies to foreign currencies. This interpretation already clashed at the time of its publication with the European Central Bank’s statement that virtual currencies could not be considered to be money (Eurosystem central banks do not recognise that these concepts would belong to the world of money or currency as used in economic literature, nor is virtual currency money, currency or a currency from a legal perspective). The equalisation of virtual currencies with foreign currencies also leads to various problems.

Firstly, there is the difficulty of identifying a unique conversion value as the various exchanges sometimes apply very different prices. Another issue is subsequently the relevance in determining the taxable income of an item that, by its very nature, suffers from significant volatility. With regard to companies, Resolution No. 72/E of 2 September 2016 stated that exchanges of virtual currencies constitute business income for the difference between the purchase price and the sale price and that, at the end of the financial year, the normal value pursuant to Article 9 of Presidential Decree No. 917 of 22 December 1986 (TUIR) becomes relevant for tax purposes. With regard to private individuals, the Regional Directorate
of Lombardy with Interpello no. 956–39/2018 clarified an unfortunate passage contained in the aforementioned Resolution No. 72/E of 2 September 2016, which could have inferred a sort of subjective non-taxability for natural persons not engaged in business activities. The applicable tax regime is always that of foreign currencies.

In particular, Article 67 TUIR and specifically paragraph 1, letter c-ter and paragraph 1-ter are referred to, determining the assumption of tax relevance for all transactions (even simple withdrawals from wallets) where the value of the deposit in virtual currencies has exceeded for seven consecutive days the counter-value of €51,645.69 calculated as of 1 January of the year in which the taxation assumption occurs (Recently cf. Marinello 2022; Calculli 2022).

The interpellation also mentions Circular No. 38/E of 23 December 2013, which clarifies the scope of application of Article 4 of Decree-Law No. 167/1990, extending the obligation to fill in the RW panel of the Form Redditi PF also to foreign financial assets held in Italy outside the circuit of financial intermediaries. This provision, according to the Agenzia delle Entrate, would also be applicable to the case in question given the lack of territoriality implicit in blockchain technology (a protocol in which the accounting records that demonstrate the ability to spend virtual currencies for the subject in possession of a public and private key reside, based on peer to peer and therefore present in identical copies wherever it is downloaded).

With reference to the tax treatment applicable to transactions relating to virtual currencies, as set out in the aforementioned Resolution No. 72/E of 2016, in the absence of specific legislation applicable to the system of virtual currencies, the judgment of the Court of Justice of 22 October 2015 in Case C-264/14 necessarily constitutes a point of reference in terms of the tax rules applicable to them.

More precisely, according to the European Courts, these transactions fall within the transactions ‘relating to currency, banknotes and coins having a value in discharge’ referred to in Article 135(1)(e) of Directive 2006/112/EC.

In light of the above, it is considered that for income tax purposes of individuals holding virtual currencies outside their business activity, the general principles governing transactions involving traditional currencies apply to virtual currency transactions. On this point, pursuant to Article
67(1)(c-ter) of the Consolidated Income Tax Law, ‘capital gains, other than those referred to in subparagraphs (c) and (c-bis), realised through the sale for valuable consideration or redemption of securities not representing commodities, mass certificates, foreign currencies, subject to forward sale or from deposits or current accounts, precious metals, provided they are in the raw or monetized state, and shares in collective investment undertakings constitute miscellaneous income of a financial nature. For the purpose of the application of this sub-paragraph, the withdrawal of foreign currencies from a deposit or current account shall also be deemed to be a disposal for consideration’.

Pursuant to paragraph 1-ter) of the same Article 67, ‘Capital gains deriving from the transfer for valuable consideration of foreign currencies deriving from deposits and current accounts combine to form the income provided that, during the tax period, the balance of the total deposits and current accounts held by the taxpayer, calculated according to the exchange rate in force at the beginning of the reference period, exceeds one hundred million lire (EUR 51,645.69) for at least seven continuous business days’.

Accordingly, forward sales of virtual currencies are always taxable, whereas spot sales generally do not give rise to taxable income in the absence of a speculative purpose, except where the currency sold is derived from withdrawals from electronic wallets for which the average holding exceeds EUR 51,645.69 for at least seven continuous business days during the taxable period, pursuant to Article 67(1)(c-ter) in conjunction with Article 67(1)(1-ter).

For the purposes of the latter provision, withdrawals from wallets are equated with a spot sale, and a spot sale is defined as a transaction in which there is a simultaneous exchange of one currency for a different currency. The euro value of the average stock in virtual currency is to be calculated according to the reference exchange rate at the beginning of the tax period, i.e. on 1 January of the year in which the taxation condition occurs (see Circular No. 165 of 24 June 1998). It is understood that if the condition identified above is not fulfilled, any capital losses realised are not deductible either. Given that there is no official daily price to refer to for the exchange ratio between the virtual currency and the euro at the beginning of the tax period, the taxpayer may use the exchange ratio as at 1 January found on the site where he purchased the virtual
Francesco Paolo Schiavone

currency or, failing that, that found on the site where he makes most of his transactions. This average balance must be checked against all wallets held by the taxpayer, regardless of the type of wallet (paper, hardware, desktop, mobile, web).

For the purposes of any taxation of other income, it is therefore necessary to ascertain whether the conversion of a given virtual currency into another virtual currency (or from virtual currencies into euro or other legal tender) takes place as a result of a forward sale or in the case of a spot sale or withdrawal if the average holding of the wallets has exceeded the euro equivalent of 51,645.69 for at least seven continuous business days in the tax period. Taking into account that, pursuant to Article 67, paragraph 1-bis of the Consolidated Income Tax Law, for the purposes of determining capital gains/losses, the most recently acquired currencies are considered to be disposed of first; in order to determine the capital gain resulting from withdrawals from wallets, which have exceeded the aforementioned average stock, the cost of acquisition must be used, considering the most recently acquired currencies to be disposed of first 8. The income, if received by an individual outside the exercise of a business activity, is subject to substitute tax pursuant to Article 5 of Legislative Decree No. 461 of 1997, currently set at 26 percent.

With reference to tax monitoring obligations, Article 4 of Decree-Law No. 167 of 1990 provides that natural persons, non-commercial entities and simple and equivalent companies resident in Italy that, during the tax period, hold investments abroad or foreign assets of a financial nature, liable to produce taxable income in Italy, must indicate them in their annual tax return. Circular No. 38/E of 23 December 2013 (paragraph 1.3.1.) specified that the same obligation also applies to foreign financial assets held in Italy outside the circuit of resident intermediaries. Therefore, with reference to the holding of virtual currencies by the aforementioned persons, it is considered that this obligation exists because they constitute foreign assets of a financial nature capable of producing taxable income in Italy (Contrino – Baroni 2019).

In conclusion, it is worth recalling that the Tar Lazio’s judgment No. 1077 of 27 January 2020 supported the interpretative line adopted by the Revenue Agency, reiterating that persons holding virtual currencies are obliged to indicate such currencies in box RW of the Income Form – Individuals. For the purposes of completing this box, the counter value in
euros of the virtual currency held on 31 December of the relevant period must be determined at the exchange rate indicated on that date on the site where the taxpayer purchased the virtual currency. In subsequent years, the taxpayer must indicate the counter value held at the end of each year or on the date of sale in the case of virtual currencies sold during the year. Finally, it should be noted that virtual currencies are not subject to the tax on the value of financial assets held abroad (IVAFe) by natural persons resident in the territory of the State, as this tax applies to deposits and current accounts exclusively of a banking nature (see Circular No. 28/E of 2 July 2012).

11.5 Concluding Remarks and Food for Thought

This paper has attempted to offer some food for thought, highlighting how the cryptocurrency phenomenon represents a new and urgently needed issue. It is clear that a comprehensive regulation at EU level, respecting the fundamental EU principles, is an absolute priority today. In addition, methodologically, defining and consequently correctly framing cryptocurrencies, either with institutes proper to modern legal systems or with new, blockchain-based categories, would entail a reasoned and fair tax discipline, avoiding phenomenal shortcuts just to tax.

On the strictly taxation side, it should be noted that, while not disregarding the perplexity arising from the difficulty of assigning cryptos to the category of miscellaneous income, the classification of cryptos as foreign currencies should not be definitively rejected. In fact, the contributory capacity deriving from crypto-assets should be valued in terms of actuality, i.e. the reasonable referability to economic facts (really verifiable and not merely presumed) and actuality, i.e. the existence of a reasonable connection between the moment of taxation and the moment of manifestation in terms of law. Consequently, it seems desirable that a comprehensive regulatory intervention should lead to a scenario in which crypto-to-crypto transactions and transactions remunerated directly in cryptocurrency are not attributed tax relevance, in order to avoid subjecting to taxation merely presumed amounts.
These considerations are coupled with the pregnant characteristics of cryptos, the volatility of which, specifically, leads one to emphasise how complex it is to prove the actual and current ability to pay until full conversion into traditional currency is realised. In addition, the withdrawal of cryptocurrencies differs from the withdrawal of foreign currencies from the current account, as it is clear that the principles mentioned above, i.e. actuality and timeliness, would not be met in the event of loss of private keys or cyberattacks, where in any case a movement of a cryptocurrency from one wallet to another could be configured, but the prerequisites for taxation from a substantive point of view would be missing.

By virtue of these arguments, crypto-assets falling within the scope of EU law could be assimilated, from the point of view of legal qualification, to so-called financial instruments. A regulatory action at the EU level, in the form of a pilot scheme, aimed at enabling market infrastructures to test the application of TLD in the issuance, trading and settlement of financial instruments, could facilitate the spread of primary and secondary markets for crypto-assets, which are similar to financial instruments throughout the single market, while ensuring financial stability and a high level of investor protection. Conversely, for crypto-assets that are currently not regulated by EU legislation, the creation of an EU regulatory framework would lay the foundations for the development of a broader cross-border market, to the benefit of providers and users of such digital instruments.

These reflections are perfectly consistent with what has been said above about EU freedoms not being fully invoked by issuers and service providers for cryptocurrencies at present. Indeed, the identification of a European regulatory and supervisory regime will necessarily have to be compatible with the free movement of capital, enshrined in Articles 63–66 of the Treaty on the Functioning of the EU. It is precisely Article 63 TFEU that stipulates that regulations on the movement of capital and payments must be in line with the legal obligation to eliminate all restrictions between Member States, as well as between Member States and third countries. Thus, the principle of free movement of capital and payments
has a general scope and direct vertical effects, clearly demonstrating the will of the drafters of the TFEU to apply this principle immediately.\footnote{See EC Court of Justice, 14.3.2000, Association Eglise de scientologie de Paris, C-367/98, in Coll., I-5751 26, par. 17, C. just. EU, 26.4.2012; C-578/10 and others, Staatssecretaris van Financiën/L.A.C. van Putten; judgments of 13 November 2012, Test Claimants in the FII Group Litigation, C-35/11, EU:C:2012:707, paragraphs 89 to 93, as well as of 28 February 2013, Beker and Beker, C-168/11, EU:C:2013:117, paragraphs 25 to 31, and, as regards a provision relating to both the free movement of capital and the freedom to provide services, judgment of 26 May 2016, NN (L) International, C-48 /15.}

On this point, reference should be made to the recent ruling of the EU Court of Justice of 27 January 2022 in connection with Case C-788/19, which opens the way for some substantive observations. It emerges from a reading of the ruling that the Spanish tax system uses a tax monitoring system very similar to the Italian one, known under the heading of quadro RW of the income model (Schiavone 2021) whose \textit{rationale} coincides with the desire to ensure the effectiveness of tax controls and combat tax evasion as well as tax avoidance. Well, the Court of Justice of the EU has found the Spanish legislation incompatible with EU law, as the consequences of non-compliance with the obligation to declare, inherent in \textit{cryptos}, are, according to the Court, disproportionate to the objectives that the legislation seeks to pursue.\footnote{Report from the Commission – Accelerating the capital markets union: addressing national barriers to capital flows, 27 February 2017; Joint Roadmap of actions to address national barriers to capital flows, 19 May 2017.}

The justification for this disproportion to EU law coincides with the fact that the deterrence measures envisaged, which have no equivalent in national law for assets located in the country, are likely to dissuade, prevent and limit the possibility of resident taxpayers to invest in other EU states, and this contravenes the free movement of capital, which is essential in the context of EU freedoms. The CJEU’s point of view is quite clear: the obstructionism implicitly proposed by regulations set out in this way, vis-à-vis residents with no fraudulent or evasive intentions, tends to clearly disadvantage the movement of capital within the European...
Union. Recalling that the national legislator cannot be at odds with the EU legislator, in view of the rejection of the Spanish legislation on tax monitoring, one can imagine that this ruling might also have repercussions on the domestic regulatory framework. In fact, such assumptions could lead more than one Member State to rewrite the perimeter of tax monitoring, also softening the system of sanctions in relation to assets held in other EU countries, in order to ensure respect for the free movement of capital under Article 63 ff. TFEU.

Let me conclude by pointing out in a critical tone that perhaps the biggest shortcoming of the MiCA Regulation is the non-inclusion of many crypto-assets, such as Nft, DeFi, metaverse and avatars.

Considering that we are in the final step of approval and its entry into force will be in 2024, nothing would prevent a sudden intervention to reshape the legislation, avoiding later implementations, just when a single and precise framework is needed. Finally, it is important to remember that the regulators and the crypto industry have to learn how to cooperate constructively and creatively. They need to fill each other’s knowledge gaps and experiment together with new products and new rules (Biancotti 2022) hopefully the outcome will not be similar to the ending of “Waiting for Godot” (Beckett 1952).

References


6 As indicated in paragraph 20 of the aforementioned judgment, the need to ensure the effectiveness of tax controls and the objective of combating tax evasion and tax avoidance are among the overriding reasons of general interest capable of justifying the establishment of a restriction on the freedoms of movement (see, to that effect, judgments of 11 June 2009, X and Passenheim-van Schoot, C-155/08 and C-157/08, EU:C:2009:368, paragraphs 45 and 46, and of 15 September 2011, Halley, C-132/10, EU:C:2011:586, paragraph 30).
Chapter 12
The Digitalization of Governance and Tax Administration in Ukraine

Abstract: This study examines the current state of digitization in tax administration in Ukraine and aims to identify the challenges and opportunities it presents. The research provides recommendations for further improvements of the tax administration as a part of interoperable digital public services infrastructure. The study uses a mixed-methods approach, including data analysis from official and public sources, as well as legal framework and regulations analysis. The findings reveal that the main efforts of digitization of tax administration in Ukraine have been focused on digital workplaces and the digital platforms of state services. The future evolution of tax administration may include legal design involving AI techniques and the exploitation of open and linked data. The importance of soft digital infrastructure for human rights protection is emphasized, which includes not just technical solutions but also elements such as policy frameworks, institutional frameworks, digital literacy, data governance, and stakeholder participation.

12.1 Introduction

The digitization of tax administration in Ukraine has been a topic of increasing importance in recent years. With the advent of technology and the increasing use of digital platforms in various industries, the tax administration has also been undergoing a digital transformation. The goal of this research paper is to examine the current state of digitization in tax administration in Ukraine, identify the challenges and opportunities
it presents, and provide recommendations for further improvements in tax administration. The paper will explore the various initiatives and programs implemented by the Ukrainian government to modernize its tax administration system and assess their effectiveness. Overall, this research paper aims to provide a comprehensive understanding of the digitization of tax administration in Ukraine and its potential to improve the efficiency and effectiveness of the country’s tax system as a part of interoperable digital public services infrastructure.

12.2 Method

The research is conducted using a mixed-methods approach, which includes data analysis from official and public sources, as well as legal framework and regulations analysis. Data collection was done by reviewing the relevant Ukrainian government websites, official publications, and other relevant sources to ensure that the research findings are in line with the current understanding of the topic. The data collected from official and public sources were analyzed to understand the current status of the digitization of tax in Ukraine and to identify any trends, patterns, or challenges in the process. The analysis was conducted using a combination of quantitative and qualitative methods to extract meaningful insights from the data. To ensure the validity and reliability of the data and the results of the study, the author has used multiple data sources and cross-checked the information collected from official and public sources.

12.3 Results

12.3.1 Interoperable Public Services

“We are creating a digital state with people at its center. A transparent and understandable state for people. We are starting to change: fewer queues, more life. Diia is the interaction of “the State and I”. Diia is an application in which all the necessary documents are in one place, on your smartphone. Diia is a single portal where you can access all services online: quickly, conveniently, and humanely.” (Diia website, u.d.) This is the information you may find as an answer to the same question on
Chapter 12 The Digitalization of Governance and Tax Administration …

the official website of Diia — a flagship project of the Ukrainian digital transformation reform. “Ukraine has become the third country in Europe to have something like that. Congratulations to our country! It is very important that not a single hryvnia from the state budget was spent on creating this application”, (Diia website, u.d.) President Zelensky said.

Diia was first presented on September 27, 2019, by the Ministry of Digital Transformation of Ukraine as part of the State in a Smartphone initiative. This is how Diia was described by Volodymyr Zelensky at the project presentation: “During the presidential campaign, I said that all of our team dreamt of a ‘State in a Smartphone’. That I dream of drastically changing the format of relations between the state and the citizen. The state should be just a service for the person. Convenient and, most importantly, simple and clear” (Ukraine P. o., u.d.).

By November 2021, the Diia mobile app had become the most downloaded app in Ukraine, according to similarweb.com, and was in regular use by more than 10 million people, or about a quarter of the Ukrainian population, as reported by the Ministry of Digital Transformation of Ukraine. One key factor contributing to the app’s popularity is the streamlined access to public services and the digitalization of important documents (Academy, 2021).

Diia is a word that means “Action” in Ukrainian and is also an abbreviation of “Держава і Я” [Derzhava I Ja] – “State and Me”. The Diia.Digital State project envisages the deployment of an ecosystem that brings together a wide range of services offered by the government and makes them accessible through a single online platform which includes a mobile app and web portal. The main goal of this project is to provide citizens with easy access to important documents, such as passports, driver’s licenses, birth certificates, and COVID certificates. The public services portal, which is an integral part of the project, is designed to provide users with a user-friendly interface for accessing government services. In line with the plan of the Ministry of Digital Transformation, the goal is to make all public services available online by 2024.

It is important to clarify that “State in a Smartphone” and “Digital State” are not the same although they may seem to be so. “State in a Smartphone” was one of the pivotal concepts in Zelensky’s election campaign, while “Digital State” (Diia.DigitalState) relates to specific activities in the domain of digital transformation of government with tangible
results. There also exists a state-owned commercial enterprise “DIIA” (DIIA Company) managed by the Ministry of Digital Transformation of Ukraine. The company was created by the Decree of the President of Ukraine with the goal to “…digitize all state services, eliminate the corruption factor, and make state services understandable and accessible to every Ukrainian” (Diia Company website, u.d.).

However, Diia is the top of the iceberg, all the things services? are produced under the water line. The foundation of digital public services’ interoperability and thus the entire digitalization reform in Ukraine is the system of electronic interaction of state electronic information resources – Trembita, an organizational and technical solution that allows the building of secure information interdepartmental interactions for state authorities, local government bodies, and business entities via the Internet. In the official language, this electronic interaction system is described in the law:

1. The electronic interaction system is used during the implementation of permitting activities, the provision of administrative, social, and other public services, the implementation of other management activities, and state regulation for the implementation of continuous electronic interaction of registers in the cases and to the extent determined by this Law, a law, or another act of legislation, under which registers were created.

2. The exchange of register information in the order of electronic information interaction between registers is carried out exclusively within the System of electronic interaction in electronic form as sets of register data and/or information about their presence or absence in the relevant register, certified using electronic identification established by law.

3. The electronic interaction system ensures the informational interaction of registers through the automated exchange of electronic messages between suppliers and recipients using its modular elements installed in the software and hardware complexes of the corresponding registers (Law on Public Electronic Registers, 2021).

More specifically, electronic interaction is the process of data exchange between two electronic information resources through the software complexes of the recipient (web clients) and the provider (web services). A transaction in the Trembita system is a completed cycle of sending an electronic request message from a web client to a web service, its
processing by the web service, receiving an electronic response message from the web service by the web client, followed by its processing by the web client (Trebita.gov.ua quarterly report (3Q 2022), u.d.).

As regards the third quarter of 2022, Trebita carried out almost 136 million transactions between state registers. And in general, since its launch – more than 1.6 billion transactions. Currently, 75 electronic information resources are connected to the Trebita system, with three joining in the third quarter of 2022. Most transactions – more than 72 million – were conducted between the Diia portal and the State Register of Individuals, i.e. taxpayers (Ukraine, u.d.).

The basis of the Trebita system is the improved Estonian data exchange platform X-ROAD, which is the foundation of e-Estonia and was adjusted for the needs of Ukraine with the support of the European Union projects EGOV4UKRAINE (2016–2021) and EU4DigitalUA (2020–2024). This example of cooperation is very interesting since as of January 2023 Estonia has launched the testing of the mRiik mobile application based on the application code and UI/UX design of the Diia application.

12.3.2 The Digital Transformation of Tax Administration (e-taxes)

The digital transformation of the system of tax administration in Ukraine is based on a single state web portal of administrative services (Diia portal) which serves as a central hub for the provision of online services to taxpayers and aims to streamline and simplify the process of accessing and using such services. The Unified Portal of State Services enables the filing of tax returns, payment of taxes, and access to tax-related information and documents. The integration of the taxpayer’s electronic cabinet (“Електронний кабінет” Ukr., [Elektronnyi cabinet]) with the Diia portal, and the Diia mobile application enables foreigners to obtain information regarding the status of residency of Ukraine electronically, provides access to the application for registration of private entrepreneurs (natural person-entrepreneurs) as a VAT payer and/or application for a simplified taxation system, creation, and submission of licensing applications. In addition to these developments, the taxpayer’s electronic cabinet’s API ensures online access to tax information for tax authorities and other state authorities according to the legislation.
The integration of a taxpayer’s electronic cabinet with the Diia mobile application offers users in turn the convenience of handling their tax in a highly efficient and cost-effective manner by reducing the time required for filing returns and paying taxes from 1–2 days to a couple of minutes. Instead of having to fill out 30 paragraphs of a complicated tax form, Diia users only need to answer four questions. The app also provides the automatic calculation of taxes to be paid based on the revenue provided by the user, which means that this service can also decrease the cost of accountants and tax consultants, as well as reduce the risk of receiving fines from the tax authority. According to polling results, the Diia app increases the transparency of the process by 38.7% which means that private entrepreneurs can easily monitor, create, and file their tax returns and pay their taxes directly through the Diia app (Diia mobile application: evaluation report).

With the help of a special access tool based on an electronic digital signature, the taxpayers’ electronic cabinet allows the taxpayer to interact with the tax authorities in a real-time manner. Electronic document exchange between the taxpayer and the controlling authority is carried out in accordance with the Tax Code, the law of Ukraine of May 22, 2003, No. 851-IV “On electronic documents and the flow of electronic document”, and the law of Ukraine of October 5, 2017, No. 2155-VIII “On electronic trust services” with changes and additions. The taxpayer can authorize natural persons with the right to sign, submit, and receive documents and information through the electronic cabinet on behalf of the taxpayer, and define their scope of authority. A taxpayer becomes a participant in electronic document exchange after sending the first electronic document in the prescribed format to the supervisory body in compliance with the requirements of the legislation.

To ensure fast detection of the riskiest of both subjects (taxpayers) and objects (transactions) for tax audits, the State Tax Service of Ukraine, has developed the XSD file (XML schema definition) of an electronic document of a standard audit file (SAF-T UA). This XSD file is a technical component of the e-audit procedure and is intended to enable taxpayers to create and submit the SAF-T UA file to the tax authority (Ukraine M. o., u.d.). The standard audit file (SAF-T) was developed by the OECD to improve the retrieval of information from taxpayers. This file is easy to use and is designed to carry out tax control measures using
specialized software. The Concept for the introduction of an e-audit for taxpayers was developed by the Ministry of Finance to meet the terms of the Memorandum of Understanding between Ukraine as a Borrower and the European Union as a Lender for Ukraine to receive macro-financial assistance. The Ukrainian Ministry of Finance has adopted an on-demand Standard Audit File for Tax (SAF-T) regime from 27 August 2021 for major taxpayers. However, its implementation was postponed till 1 January 2023 due to COVID-19 disruptions. Due to the legislation, at the request of the tax authorities during the audit, major taxpayers must provide an SAF-T UA within two working days of receiving the request. The legislation also explicitly stipulates that a major taxpayer must have the appropriate software to create an SAF-T UA. The tax authorities, in turn, must have the necessary software to receive documents in the form of an SAF-T UA and publicize the information in the format of electronic documents on their website.

For tax administration of cross-border operations, the Single Window electronic system was launched. This electronic system allows customs and other government authorities to exchange information on goods that have been moved across the state border of Ukraine. It also helps businesses to lodge documents only once at one single data point to obtain all the necessary permits from various government authorities. The data is stored in a single database. In practical terms, the Single Window in customs helps to expedite and simplify the flow of information between trade operators and several government authorities while bringing meaningful gains to all parties involved in cross-border operations. The electronic system of a Single Window for customs or similar systems, is widely spread in developed countries such as Germany, Sweden, Japan, and others. The use of software for transfer pricing control and tax audits based on electronic accounting data is another key aspect of the updated electronic services. This will enable tax authorities to monitor and enforce compliance with transfer pricing rules and may help to reduce the risk of tax evasion and avoidance more effectively.

Overall, the introduction of updated electronic services for taxpayers in Ukraine is a significant development that has the potential to improve the efficiency and effectiveness of the country’s tax system. These services have the potential to provide taxpayers with more convenient and efficient
access to a range of tax-related services and may help to reduce the burden on both taxpayers and tax authorities. At least, they are supposed to.

12.3.3 Prevention and Countermeasures Against the Legalization (Laundering) of Proceeds of Crime

Bordering with the digitization of tax is the digital transformation of prevention and countermeasures against the legalization (laundering) of proceeds of crime, financing of terrorism, and financing of the proliferation of weapons of mass destruction – e-financial monitoring – which is also a topic of extreme importance for Ukraine as it seeks to counteract full-scale military aggression of the state sponsor of terrorism. A key aspect of the digital transformation of e-financial monitoring is the deployment of an “e-cabinet of the financial monitoring system” (“e-кабінет системи фінансового моніторингу”), which allows for the simplified electronic retrieval of information related to the prevention and countermeasures against the legalization of proceeds obtained through crime, financing of terrorism, and financing of the proliferation of weapons of mass destruction. This system also provides for the secure exchange of information between the State Financial Monitoring Service and other relevant organizations. Another important development is the implementation of a modernized analytical component of the financial monitoring service which is planned by the end of 2023. This component, known as the “e-case financial monitoring” system, will integrate all analytical services into a single automated analytical workplace and provide means of operational and strategic analysis, as well as support for electronic case investigations and the creation of aggregated data.

12.3.4 The Unified Register of Convicts and Persons Taken into Custody

The Unified Register of Convicts and Persons Taken into Custody is an important new development in the criminal justice system of Ukraine. Supported by the EU Project “Pravo-Justice” and EDGE, this register is designed to create a single database of information about convicts and prisoners and to facilitate operational communication and cooperation between the various bodies and institutions of the penitentiary system and probation.
One key aspect of the Unified Register is its ability to support the functioning of the special system called Cassandra as a subsystem for recording data on the assessment of the risks of committing a repeated criminal offense. This system uses algorithms of automated conclusions and machine learning to determine the level of risk of recidivism for each person based on factors such as criminal history, housing, education and work, financial situation, and behavior and thinking. By providing more accurate and individualized predictions of recidivism, the Cassandra system can help probation authorities and other relevant organizations manage and supervise offenders more effectively and reduce the risk of reoffending. For instance, the program will automate the preparation of a pre-trial report which describes the personality of the accused and assesses the probability that s/he will commit new crimes in the future. Such a document is supposed to help judges determine the level of punishment.

Another remarkable feature of the Unified Register is its ability to ensure operational communication and cooperation between the various bodies and institutions of the penitentiary system and probation. In addition, the Unified Register will facilitate interaction with other state structures that work with registers, such as law enforcement agencies and other organizations.

A single database for information about convicts and prisoners supported by the Cassandra system might be used by tax authorities in different ways, for example, to identify and investigate individuals who have committed tax-related offenses. It is not hard to assume that tax authorities could use the Unified Register to investigate individuals convicted of tax-related crimes, such as tax evasion or tax fraud. This information could be combined with other data sources, such as tax returns and financial records, to help identify potential tax offenses and to build cases against individuals suspected of violating tax laws. Additionally, the register can be used to monitor the behavior of individuals who have been convicted of tax-related offenses and to identify any patterns or trends that may suggest an increased risk of reoffending. This could help tax authorities identify individuals at high risk of committing tax-related offenses in the future and target them for additional enforcement and compliance measures.
12.4 Discussion

12.4.1 Hard and Soft Digital Infrastructure

The entire success of the digitalization of governance as we see it in Ukraine seems to reveal the level of development of hard digital infrastructure comprising technical components of digital systems and networks. These include the hardware, software, networks, and other technologies that are used to collect, store, process, and transmit digital information that might be categorized as:

- Computing resources: This includes servers, storage systems, and other types of computer equipment that are used to store and process digital data
- Network infrastructure: This includes telecommunications networks, wired or wireless, that connect different parts of a digital system, such as the internet or a local area network (LAN)
- Software: This includes the various types of software that are used in digital systems, such as operating systems, databases, and applications.

Hard digital infrastructures are the foundation upon which digital systems are built and are essential for their functioning. It is important to note that hard digital infrastructure is interdependent on digital infrastructure which refers to the non-technical and organizational components of digital systems and networks – soft digital infrastructure. These components include policies, institutions, regulations, norms, and social practices that shape the design, development, deployment, and use of digital systems. And with this component, not everything seems to be so clear in Ukraine. Issues that still must be addressed are as follows:

- Policy frameworks – these include regulations and laws that govern the use of digital systems and data, such as data protection and privacy laws, cybersecurity regulations, and intellectual property laws.
- Institutional frameworks – these include the organizations and agencies that are responsible for the development and management of digital systems and data, such as government agencies, academic institutions, and private companies.
- Digital literacy – the awareness and understanding of digital technologies and their implications are crucial for the effective use and management of digital systems and data. Deriving from the issues of digital literacy are issues of social and organizational norms which include the customs, practices, and expectations that shape how digital systems and data are used and shared within a society.
- Data governance – how data is collected, shared, stored, and used is governed by a set of policies and procedures to ensure that the data remains accurate, reliable, and secure, that there is transparency in its collection and use, and that the rights of individuals are protected.
- Stakeholder participation – the active engagement of different stakeholders such as government, private sector, civil society, academia, and users is important for the development and maintenance of digital systems.

The example of Russia (officially recognized as a terrorist state)\(^1\), which is a member of the OECD and contributor to the Tax Administration 3.0 report and its satellite Belarus, which reveals remarkable success in both hard and soft digital infrastructure for the economy, do not ensure democracy and freedom. The digitization of governance and data-driven approaches in the public sector can potentially violate human rights in several ways. If digital systems are not designed and implemented with adequate safeguards, they can expose individuals to the risk of data breaches, identity theft, and other forms of misuse or abuse of their personal information. The threats to national security are obvious and articulated by the OECD for instance: Ukraine has to resist extensive

\(^{1}\) On November 23, 2022, the European Parliament adopted a resolution on the latest developments in Russia’s brutal war of aggression against Ukraine including the deliberate attacks and atrocities committed by Russian forces and their proxies against civilians in Ukraine, the destruction of civilian infrastructure and other serious violations of international and humanitarian law amount to acts of terror and constitute war crimes. Considering this, Russia was recognized as a state sponsor of terrorism and as a state that “uses means of terrorism”. As there was no mechanism for the EU to officially designate states as sponsors of terrorism, the Parliament called on the EU and its Member States to put in place the proper legal framework and consider adding Russia to such a list to trigger a number of significant restrictive measures against Moscow that have profound restrictive implications for EU relations with Russia (European Parliament declares Russia to be a state sponsor of terrorism, u.d.).
attempts to destroy administrative data by Russian hackers; the decreased
capacity of service providers due to the lack of employees (due to mobili-
ization or migration); and the difficulty in accessing digital services from
abroad when displaced are all serious issues.

Considering the above, it is important to define which human rights
principles and standards should guide the process of digitization of
governance and whether these human rights principles and standards
correspond to the approaches to digitization of governance. A broad
analysis of international and European law can help us yield several
human rights principles and standards that should guide the process of
digitization of governance. These include:

1. The right to privacy: individuals have the right to have their personal
information protected from unauthorized access, use, or disclosure.
This includes the right to be informed about how their personal
information is collected, used, and shared, as well as the right to have
control over their data. (United Nations, n.d., Article 12), (United
Nations, 1966, Article 17), (Council of Europe, 1950, Article 8),
(Council of Europe, 1981)

2. The right to equality and non-discrimination: individuals have the
right to equal treatment and opportunities, regardless of any grounds
of discrimination. This includes the right to access digital services and
opportunities without discrimination, and to have the same rights
and protections online as offline. (United Nations, n.d., Article 2),
(United Nations, 1966, Article 2), (United Nations, 1979, Article 2),
(United Nations, 2006, Article 5)

3. The right to freedom of expression and information: individuals have
the right to seek, receive, and impart information and ideas without
interference or discrimination. This includes the right to access and
use digital technologies and platforms for the exercise of their free-
don of expression and information including the information on the
principles and algorithms of the digital technologies and platforms
functioning. (United Nations, n.d., Article 19), (United Nations,
1966, Article 19), (Council of Europe, 1950, Article 10), (European
Parliament & Council of the European Union, 2016, Article 85)

4. The right to an effective remedy: individuals have the right to an
effective remedy for violations of their human rights, including the
right to seek redress for any harm or damage caused by the misuse or abuse of digital technologies. (United Nations, n.d., Article 8), (United Nations, 1966, Article 2(3)), (United Nations, 1984, Article 14), (United Nations, 1989, Article 39)

5. The right to participate in public affairs: individuals have the right to participate in the decision-making processes that affect their lives, including through the use of digital technologies and platforms. This includes the right to access information and to have their views and concerns heard and considered in the policy-making process. (United Nations, 1948, Article 21), (United Nations, 1966, Article 25), (United Nations, 1979, Article 7)

These principles and standards are set out in various international human rights treaties and instruments, they apply to all aspects of governance, including the digitization of governance, and should be respected and promoted in the development and implementation of digital governance policies and practices. These principles and standards are not specific to the approaches to the digitization of governance, but rather provide a broader framework for the protection and promotion of human rights in the context of digital transformation. The approaches to the digitization of governance are more specific and focus on how digital technologies and data-driven approaches can be used to improve the efficiency, effectiveness, and accountability of public sector organizations. Such approaches do not necessarily correspond to human rights principles and standards but should rather provide a set of strategies and tools for the implementation of digital governance.

Ukraine has already developed a set of strategic documents such as the Digital Agenda for Ukraine (2018), the Concept of Digital Economy and Development of Society to implement the Digital Agenda of Ukraine, Ukrainian Economic Development National Strategy till 2030, the draft concept for the digital infrastructure development in Ukraine for the period 2020–2023 developed and launched for public debate in 2019.

Ukraine has already legally adopted the Concept and Action Plan for the development of the digital economy and society, but a more modern digital strategy in line with the latest EU strategies is needed. By creating a coherent framework for the Digital Economy and Society Index (DESI) in terms of legal, political, and institutional coordination
and methodology, the Ukrainian government will not only be able to measure and track progress but also further shape digital transformation policy based on data. Self-assessment based on the DESI will allow for the tracking of digital development and comparison with the digital economies of the EU, ultimately contributing to Ukraine’s integration into the EU’s Single Digital Market.

The war has pushed the government to seek European Union membership and thus access to the EU Digital Single Market (DSM), including an alignment with international regulations and standards. The move towards integration in the DSM means a progressive alignment with international regulations and standards on digital practices, which could bring important benefits in terms of the reduction of cross-border barriers to digital trade and the acceleration of Ukraine’s digital economy. OECD policy tools such as the “Going Digital Policy Framework” can also help Ukraine realize its ambitious plans to strengthen and rebuild its digital space. (Digitalisation for recovery in Ukraine, u.d.)

12.4.2 The Future of the Administration of Tax in Ukraine

It is not hard to infer that Ukraine has undergone significant changes in terms of digital transformation of governance and digitization of tax. Various initiatives to modernize the tax system, including the introduction of the electronic filing and payment of taxes, as well as the use of digital tools for tax administration have been implemented. However, it is important to note that despite the progress made, there is still much to be done to fully realize the potential of digitization for the administration of tax in Ukraine, considering key factors that determine the digital future of economies and governance.

The main driving force in the digital transformation of society, at least within the scope of tax, is Industry 4.0, also known as the Fourth Industrial Revolution. The concept refers to the integration of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data analytics into the manufacturing process. It represents a shift toward smart, connected, and autonomous systems that can interact and communicate with each other in real time. Industry 4.0 aims to increase efficiency, reduce costs, and improve the overall performance of manufacturing operations. It also includes the use of technologies such as virtual and augmented reality, cloud computing, and robotics.
Industry 4.0 is expected to revolutionize the way goods are produced, distributed, and consumed, leading to a more sustainable and efficient manufacturing ecosystem.

Industry 4.0 and the digital transformation of the administration of tax are mainly connected in terms of data collection, as Industry 4.0 technologies such as the IoT, can generate vast amounts of data that can be used to improve tax compliance and administration.

As fairly outlined by the OECD “As more interconnections become possible between the different systems that taxpayers use to run their businesses, undertake transactions, and communicate – their “natural systems” – the more it becomes possible to move taxation processes into these systems, subject to appropriate assurance. This digital transformation … has the potential to build-in compliance in an increasing number of areas, to move taxation closer to taxable events, and to significantly reduce the burdens that can arise from using different processes for taxation to those used in taxpayers’ daily lives and businesses. As these opportunities increase, it may be possible to make significant inroads into the structural limitations of current tax administration which can lead to persistent tax gaps, large amounts of uncollected tax debt and continuing, and in some areas growing compliance burdens” (OECD).

The nature of the changes occurring around us through the increasing digitalization of the economy and of society in general allow, and indeed call for, a different model of tax administration. In this model – termed Tax Administration 3.0 in this discussion paper – tax administration processes are increasingly built into the natural systems used by taxpayers in their daily lives and businesses. This will allow the automation and “upstreaming” of many aspects of tax administration, making tax administration more seamless and frictionless over time and bringing potentially significant reductions in administrative burdens (OECD).

The digital future of economy and governance referred to by Industry 4.0 and the Tax Administration 3.0 model were already described within the concept of WEB 3.0 in which computers “… become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A ‘Semantic Web’, which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy, and our daily lives will be handled
by machines talking to machines. The ‘intelligent agents’ people have touted for ages will finally materialize” (Berners-Lee & Fischetti, 1999).

For the “intelligent [tax] agents people have touted for ages” to finally materialize it is a road to go and the end of this road is still unclear and debated, but what is quite obvious for the tax system of Ukraine is that the digitization of the system of tax administration will probably require the implementation of open and linked data and legal design involving AI techniques.

In the domain of taxation, open and linked data can be used to make legal information, such as court decisions, legislation, and case law, more easily accessible and usable. This can help to improve the transparency and accountability of the tax system and can enable the development of new tools and applications for legal research, analysis, and decision-making. Additionally, by using linked data principles, legal information can be interconnected and integrated with other data sources, enabling new insights and connections to be discovered.

Linked data could be used to connect tax authorities with other government agencies or with businesses, to facilitate the exchange of information about tax liabilities, payments, and other tax-related matters. Of course, linked data could also be used to connect different parts of a tax authority’s native systems, such as databases or applications, to facilitate the sharing and integration of tax-related data within the organization. Much of this has already been implemented to some extent but there is still a great deal of room for improvement. Finally, linked data can be used to create a “single view” of a taxpayer’s financial situation, by linking data from different sources and creating a comprehensive profile of the taxpayer. This makes it easier for tax authorities to identify discrepancies or inconsistencies in the data, and to take appropriate action to correct them.

Legal design involving AI techniques – in turn – refers to the use of artificial intelligence (AI) and machine learning algorithms in the design and development of legal systems, processes, and tools. This can include the use of AI to automate legal tasks, such as document review or contract analysis, or to develop predictive models for legal decision-making. It can also involve the use of AI to improve the user experience of legal services, for example, by creating user-friendly interfaces for legal information or advice.
Thus, in the future, tools and algorithms based on artificial intelligence will probably play a larger role in helping to identify and evaluate liabilities and will be increasingly used to administrate tax and make decisions. However, this also invokes the question of liability when the system makes incorrect decisions. Who will be held responsible when an AI-powered system makes an error in processing a tax return or determining a tax liability? Legal frameworks must be in place to address these issues and to ensure that the system is held accountable for its decisions because the line dividing a highly modernized and efficient system of governance from a dehumanized digital concentration camp might be vaguer than it seems.

To ensure successful and effective tax administration digitization in Ukraine, it is evidently of great importance to critically evaluate its progress under the scope of external assessment tools. Such an analysis might protect from self-admiring or other misleading practices and help to define a better development strategy.

It is worth considering exploiting the Maturity Model which serves as a visualized pathway toward the goals of TA 3.0 and a draft of the model was included in the TA3.0 report as one of the building blocks of a future system. Since 2021, ADG members and other administrations can undertake self-assessments and report their results. The actual results of self-assessment show that the model is “…well calibrated and has resulted in useful conversations within tax administrations”. Another mighty tool for the assessment of tax administration in Ukraine is the International Survey on Revenue Administration (ISORA) which provides wide comparative data. The Inventory of Tax Technologies Initiatives (ITTI) might also be useful as it not only helps to assess the actual state of implementation of technologies, covering both tools used by the tax administrations and approaches that will help to lead the digital transformation, but also give insights from case studies and other supporting materials (OECD).

12.5 Conclusions

The digital transformation of the system of tax administration, fees, payments, and duties (e-taxes) is implemented by the deployment of updated electronic services of the taxpayer’s office based on a single state web
portal of administrative services, automation of functions related to the monitoring of the effectiveness of tax disputes by courts, conducting tax audits, storage and exchange of information according to international standards of exchange of financial information, automation of the work of territorial divisions of tax authorities, the formation of an archive of electronic documents.

The initiatives on the digitization of tax administration in Ukraine are implemented on the two foundations which are digital workplaces and digital state platforms.

The digital workplace of a public servant / electronic cabinet of taxpayers are virtual equivalents of a physical workplace that implement the concept of flexibility in the methods of the performance of official duties by public servants, which stimulates their joint work and interaction, and supports decentralized and mobile work environments. The concept of digital state platforms is implemented by the formation of state bodies aimed at simultaneously improving the quality of services, optimizing the number of civil servants, and reducing costs. Digital platforms allow us to solve tasks, and increase efficiency, reducing the cost of the activity and the time of execution. The benefits of both digital workplaces and state digital platforms are the reduction of costs for hardware, office space, and business trips, as well as the elimination of queues and a better quality of service.

The future evolution of the system of tax administration will probably follow a path of legal design involving AI techniques and the exploitation of open and linked data. However, to ensure human rights protections, attention should be paid to the soft digital infrastructure of tax as well. The role of law in the digital transformation of governance and tax administration is to provide a framework for the development, implementation, and regulation of digital technologies and data-driven approaches in the public sector. This can include laws that establish the legal and ethical framework for the use of digital technologies in the public sector, such as data protection and privacy laws. It can also include laws that provide for the development of digital infrastructure, such as laws that promote the deployment of broadband networks and digital services. Additionally, the law can play a role in the oversight and accountability of digital governance, such as through the establishment of independent bodies.
that monitor the compliance of public sector organizations with legal standards and requirements.

Ukraine did not embark on its journey on the path towards the digitalization of public services from a blank page, nor has it reinvented the wheel in this area, the main role of the government – and consequently its main responsibility towards society – is the implementation of digital transformation with due diligence. EU guidance provides a great deal of support in ensuring that existing and new legislation do not compromise interoperability principles and efforts. For instance, the Tax Administration 3.0 report along with the OECD’s Forum of Tax Administration’s maturity model can assist in visualizing the path towards more seamless tax administration and in understanding the contemporary level of maturity of tax administration in Ukraine, help to consider the possible steps it may take over time. The threat is that because of the poor performance of a government – in a broad sense – Ukraine may gain a legal system that is maladapted, outdated, and fragmented.

Overall, the role of law in the digital transformation of governance is to ensure that the benefits of digital technologies are realized in a way that is fair, effective, and accountable. The digitization of government already raises concerns about the accountability and transparency of public sector organizations. If digital technologies are used to conceal or manipulate tax information, they can undermine the trust of citizens in the institutions of governance and the rule of law, which is unacceptable for the state which defends its sovereignty on the battlefield.

References

Chapter 13
Ensuring an Inclusive Shift Towards a Technology-Driven Dialogue Between Taxpayer and Administration: How the Law Can Benefit from a Different Methodology

Abstract: Technology can be viewed from many perspectives, and the methodological engagement with the subject is quite rigorously split in line with the field of inquiry. This hinders the critical exchange of views that could take place in a field of inquiry that spans across so many disciplines. For the field of tax law, it is proposed here to incorporate (aspects of) a phenomenological approach to technology, in order to enhance the inclusiveness of policy-making ex ante. Especially the relationship between taxpayer and tax administration is increasingly influenced by technology, both in terms of communicative engagement as well as in decision-making. To be able to properly take account of the taxpayers’ perspective in these changes, a turn towards a phenomenological approach in technological implementation is proposed in order to break with the earlier trend of ‘trial and error’ policy making with regard to implementation into the workings of tax administrations. This should enhance the protection of fundamental rights ex ante.
13.1 How Technology Shapes and Changes the Dialogue Between Taxpayers and Tax Administrations

‘Technology is changing the world of tax’: a statement so ubiquitous that it can seem hollow. As this often-used statement is not very often measured up to its actual scope from the perspective of the taxpayer, this contribution will try to fill that gap by adopting a non-legal perspective. The central question is whether technology is applied to the same, already existing relationship, actions, and dialogue between taxpayers and tax administrations, or has the very act of taxpaying itself changed because of the application of technologies to this phenomenon? It will be argued here that the latter is true by means of a phenomenological approach to technology. This changed act of taxpaying has legal implications for the way we apply principles (with legal repercussions\(^1\)) in the design of the legislative framework that absorbs new ways of allowing the dialogue between taxpayers and tax administrations to take place. In order to bolster resilience against unfair outcomes in the future, these changes require new ways of looking at this age-old communicative problem between taxpayers and tax administrations. In the specific context of the retrieval of financial information from digitised ecosystems, an important question is what can guide these practices. This paper proposes a stronger focus on ex ante procedural fairness reviews in the design of instruments, as well as an emphasis on inclusive innovation in the design of future governmental policy, to ensure that the future of this new act of taxpaying, and with it the dialogue between taxpayer and tax administration, has a (more) inclusive future. The aim is not to build a new system from scratch, the aim is to provide principles which can guide the law-making procedures

\(^1\) The aim here is not to enter into a discussion on what precisely constitutes a principle of law, as this is a question for legal theory, which has produced a discourse of its own capable of filling entire libraries. However, here the choice is made to use principles in the design of the legislation, thereby ensuring these principles have a direct influence on the legal position of taxpayers, but in this sense they are maybe not directly seen as part of the doctrinal conservative set of legal principles. Nevertheless, their spirit and working force will obviously be inferred within a legal setting. See sec. 3.3. for further elaboration.
surrounding technologies that fundamentally change the interaction between taxpayers and tax administrations.

The difficulty, particularly with the concept of fairness, is that it is difficult to pin down, not least due to its interdisciplinary nature. Fairness in algorithmic application usually refers to systems that are not biased, fairness in taxation to the idea that taxpayers pay a ‘fair share’ or that countries receive a fair share in the division of taxing income between states. Here, to stay closer to the phenomenological (first-person) lever for the assumption of the need of the usage of ex ante procedural fairness reviews, the fairness concept stays closer to this legal-psychological relationship by means of aiming at the ex ante procedural aspects of tax law design. Thus, here, procedural fairness is meant as non-biased technology that has come into existence under inclusive procedures, with the direct participation of taxpayers. Inclusive innovation should ensure participation of all taxpayers.

13.2 An Outline of this Contribution
Firstly, some conceptual and methodological remarks will explain the main strands of thinking on technology within the philosophy of technology, after which the choice for the phenomenological approach that guides the argument throughout this paper will be explained. A brief example will provide some insight into the main argument that there has been a fundamental shift in the dialogue between taxpayer and tax administration, and thereafter we will pick up on the OECD discussions in relation to tax administration and the possible consequences for this dialogue. It is subsequently argued that this creation or integration can best be guided by principles of fairness and inclusive innovation, both working with ex ante reviews by policymakers, to ensure that voices are equally heard in the pre-legislative phase of the design of technology for the future of taxpaying.

For a very good summary of the context and the two fields that deal with the concept of procedural fairness within their own right, with views that allow for an interdisciplinary dialogue, see: Graaf, C. V. de. (2021). Procedural fairness: Between human rights law and social psychology. Netherlands Quarterly of Human Rights, 39(1), 11–29.
13.3 Conceptual and Methodological Remarks: the Use of Phenomenology to Assume a Change in Legal Relationships

This interdisciplinary inquiry aims at shedding a different light on the relationship between taxpayers and tax administrations by using philosophical insights into the role of and for technology within this relationship, in the spirit of the Foucauldian invitation to use the toolkits of other sciences for the advancement of our own inquiries in our respective disciplines (Foucault, 1980, p. 65). Thus, this inquiry is different from the usual contributions in legal discourse in the sense that it is here not solely the legal relationship that is the subject of review, but also the role of technology from a phenomenological angle as part of this relationship to show that the act of taxpaying itself is not the same anymore/is no longer the same with the introduction of new technologies. It is highly important to define the terms that form the basis of this inquiry, in order to (interdisciplinarily) understand one another (Voltaire, 1977, p. 225). In that sense, it is the use of a phenomenological argument for the assumption of a shift in the act of taxpaying itself that requires an adequate legal translation by means of new principles guiding the process. That translation can be found later in this paper by means of the democratic concepts of self-executing norms and checks and balances.

To be able to overcome the conceptual and methodological boundaries that are thrown up by the differences in both starting point and application, the scope of this review requires limitations in order to encompass the different definitions, as well as the assumption of a legal ‘cover blanket’, i.e. a functional framework of fundamental rights with a high degree of generality to make sure that it encompasses the philosophical and empirical conceptualisations of the shaping force of technology in the relationship between taxpayer and tax administration. This legal framework thus requires a strong level of universality, omni-

---

3 A loose act of paraphrasing from the author, as the famous expression ‘Define your terms […] or we shall never understand one another’ is highly relevant in this exercise, and can be read as a necessary invitation to providing context to the terms used, the expression was coined by the French philosopher Voltaire.
present non-discriminatory applicability and functioning institutions for the enforcement of rights, conditions that can only be fulfilled with effective procedures within a rule-of-law based system with a (constitutionally) entrenched respect for fundamental rights.\(^4\) This assumption of a functioning system is a necessary one, because the current inquiry does not go into the most overt situations of hard breaches of rights or the balancing between individual and collective rights in tax collection,\(^5\) but aims to shed a light on issues of design, prior to the use of potential new systems or the building/integration of ecosystems.

### 13.4 A Few Ways to Interpret Technological Advancement

Without aiming at any hierarchy between the different to be defined concepts, the fountainhead of the dialogue in this review is the assumption of a (potential) tax liability by a taxpayer on behalf of a tax administration,\(^6\) as it is the first emergence of a (legal) need for communication between both subjects.\(^7\) This is a relationship established by law, as a

\(^4\) Whereby the scope of this review is necessarily limited to the states wherein one can assume that the basic characteristics of a rule-of-law based legal order are fulfilled. This is obviously a discussion in its own respect, but attachment to these general principles can be assumed to be the case in nearly all EU Member States, as part of the EU Treaties (most notably Art. 2 TEU).

\(^5\) Whereby, it must be noted that especially the legal provisions on the individual rights of taxpayers come closest to the ideas expressed here (for a definition and discussion hereof see: Kokott, J., & Pistone, P. (2022). Taxpayers in international law: international minimum standards for the protection of taxpayers’ rights. Oxford, UK, Hart Publishing, Bloomsbury Publishing Plc, 70-80), although the collective rights vision also serves a purpose for the idea of checks and balances as expressed in section 3.2.

\(^6\) As is also the starting point of the ‘traditional view’ as set out by the OECD in their ‘Tax Administration 3.0’ document, when dealing with the ‘broadly sequential processes’ that are typical for the current system of tax administration. See: OECD (2020), Tax Administration 3.0: The Digital Transformation of Tax Administration, OECD, Paris. Accessible online via: http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/tax-administration-3-0-the-digital-transformation-of-tax-administration.htm (last accessed on 25-10-2022).

\(^7\) Whereby the author is aware of the fact that obviously, legally, there are distinctions to be made between the types of taxpayers that are identified in the law, and thus the
product of a political consideration on the design of the relevant tax system and the choice concerning the connecting factors (nexus) for tax and/or reporting duties. Within this network of (legal) relationships, the causality between the use of technology and the establishment of this relationship is prompted by the need to resolve a communicative issue of an asymmetry of information, whereby, ‘as the already technologically oriented human beings that we are, we will tend to conceive communication as a problem requiring a technological solution’ (Introna, 2017). By ascribing to this notion, the interpretative choice within this inquiry is immediately disclosed as a phenomenological one, which directly tells us something about the role of technology within this inquiry, and requires explanation.

Technology in the dialogue between taxpayers and tax administrations is posited as a communicative tool or artifact. This latter term requires some explanation in itself. An artifact, according to the standard definition, is an intentionally made object which by design aims to serve a purpose. This definition does not restrict itself to tangible objects, and can also include more abstract notions. A specific example here could be that both the letter as well as the email sent by a tax administration to a taxpayer can be an artifact in its own right, whereby its specific character bearer of the tax liability may differ, which then again may also influence the relationship, however, these nuances will only be presented later so as not to congest the current explanatory section.

8 The word network is somewhat controversial here, in the sense that Actor-Network Theory (ANT) uses the same terminology, and could also be applied to the relationships here to provide new insights, especially since its tools of analysis allow a different construction of social interaction, see more elaborately: M. Callon, Actor Network Theory, (Eds. Neil J. Smelser, Paul B. Baltes), International Encyclopedia of the Social & Behavioral Sciences, Pergamon, 2001, at 62–66. For the subsequent discussion, it is important to know that ANT is traditionally part of the constructivist view on technology.

9 Whereby, generally, the first revelation of this relationship is a communicative endeavour, as the taxpayer will be made known (most often still analogically, but sometimes already digitally) of its new status as a (potential) taxpayer. The asymmetric tension is already present in the oftentimes assumed action by the taxpayer on behalf of the administration, which requires confirmation (by payment). Assumptive elements (or legal fictions) are omnipresent in systems of tax law, and necessary for the proper functioning of tax administrations.

10 It must be mentioned that ‘intentionally made object’ as a category exempts the category of by-products.
Chapter 13 Ensuring an Inclusive Shift Towards a Technology-Driven …

teristics and capacities determine the conceptions and attitudes within the communicative setting. A special ontological status for artifacts is a peculiarity of philosophy. Importantly here, information and communication technology (‘ICT’ or ‘IT’12) as such, as well as its components and other manifestations, can be seen as an artifact (Irmak 2012).

This ontological self-standing status of the artifacts or tools within the techno-communicative paradigm can be approached at the hand of three dominant ways of thinking concerning the role of artifacts or tools and their existence within this communicative setting. Firstly, a bare or neutral view of the tool or artifact is defined by availability and the shaping of our capabilities. The artifact enables human capabilities beyond the mere physical. The impact of the artifact (technology) is determined to a greater or lesser extent by its characteristics.13 A tax example would be to say that online bookkeeping tools expand the capabilities of the user to keep track of business transactions and financial information. This thinking, labelled as determinism, is criticised for its flawed causality, and too narrow understanding of the intrinsic qualities of the technology itself, branding it as a passive actor within the grander scheme of societal relationships. Technology is neutral in the deterministic view, a much attacked view.14 The constructivist critique of this view is that technology

11 Whereby, to take an example from my native country the Netherlands, even the envelope in which the letter comes can be deemed an artifact in its own respect, not solely as a neutral holder of the information in a manner that respects the privacy of the receiver of the information, but also in the normative sense in that these have a typical blue colour so that for anyone seeing it, it immediately signals that it concerns an official communication from the Dutch tax authorities.

12 In the case of this review, also the category of information technology (IT) will be deemed to serve a function within the communicative setting, and thus the distinction here is not extremely relevant.

13 To quote Introna (2017) for an example: ‘For example, a technological determinist may argue that the Internet’s open and non-hierarchical architecture can more or less cause a society that uses it to become more open and less hierarchical.’

14 Logically as well: take the example of the bookkeeping tool. Neutrality in the use of the tool does not mean that the tool itself is necessarily neutrally constructed: the tool costs money, which limits access, and might require special types of skills, which again is an access limitation. The availability of the tool must be seen as part of the tool itself in the other schools of thought, as its societal context is a part of the technology itself. Perhaps the most famous example is the discussion on gun control, where the NRA slogan ‘guns don’t kill people, people kill people’ is the most ‘instrumentalist’ politicasation of a
and society co-construct each other, and the technology we use is already encapsulating a ‘script’ that is instructive in the use of the technology, which is given to it by the wider web of social interactions that precede its existence, wherein it can play a part itself (Latour 1991, Verbeek 2006). The result of this interdependency is that technology constructs our behaviour just as much as we construct technology, and without a predetermined outcome. The constructivist outlook is thus very much engaged with society, technology, and the user; as a web of determining forces for the not to be predetermined outcome of the application of technology. As such this theory can provide valuable insights also for the application of technology in taxation, especially from a sociological perspective.


15 The roots of these ideas are best found in the work of Latour, who works with the idea of ‘script’ in most detail. For a concise explanation of the constructivist idea, please see the work of Verbeek. Here, the connection with ANT (see above, fn 8) must be observed, whereby it is important to point out that ANT does not a priori attribute agency to a tool or artifact, or use a strict determinism, it is more a matter of acknowledging the capacity of the tool or artifact as having the potentiality to gain agency or becoming an actor within the network, thus not necessarily reserving these capacities for people (which as the matter of fact is the first strong rejection of ANT: it strongly opposes the idea of different worlds of living/non-living, thinking/non-thinking, etc.).

16 Thereby not fundamentally rejecting the other views within their own right but rather supplementing these views with a more encompassing view which includes the different metaphysical (and not only instrumental) considerations, as can, e.g., be observed in the work of Heidegger, most vividly in his seminal essay on technology, where he brands the
within the sphere of phenomenology and technology, with their own respective different emphases, a common denominator is the insistence on this co-constitutive element of society and technology ‘by being each other’s reciprocal and ongoing condition or possibility for being what they are’ (Introna 2017). Heidegger, in search of the essence (Wesen) of the technology itself, places technology within the idea of ‘enframing’ (Gestell), whereby our natural attitude towards the world is already a world at our disposal, to fulfil our projects, with both our own view of the world and the technology within this world as a product of our technological attitude towards the world around us (Heidegger 1977, p. 2). It is especially this last notion that is extremely insightful for the inquiry here. To illustrate this, it is best to use a simple example. To use those on the altering capacity of technology as given by Arnold; the calculator and word processor are not solely more effective ways to make calculations or do text editing, ‘they change what it is to do mathematics and to write’ (Arnold 2003, page 236). To apply this to our earlier example of simple bookkeeping software: the processing of information through the computer has already made the act itself a different one. Considering the world of tax administrations, taxpayers’ and reporting duties being fulfilled with new technologies, the whole concept of taxpaying has been fundamentally redesigned by means of technology, whereby there is a clear co-constitutive function between technology and taxpaying. In ‘instrumental’ and anthropological’ conceptions (Vorstellung) true in their own respect, but attacks the idea that technology itself is neutral, as this would make ‘us utterly blind to the essence of technology’.

17 Since Heidegger was famously very detailed in the use of language and the specific meaning of the terms he used (sometimes even finding new words to fit his purpose), the German translation is included for the most pivotal terms.

18 A co-constitutive relationship which has been there from the beginning, such as writing, as an artifact of technology, enabled the first forms of bookkeeping. The influence of technology on society, and in this context more specifically, the law, can hardly be overstated. Perhaps the prime example is the invention of the printing press, a technology that changed society so significantly (see, e.g., the most seminal overview thereof: Eisenstein, E. (1980). The Printing Press as an Agent of Change. Cambridge: Cambridge University Press.), that it is hard to choose where to begin to discuss its impact. To stick to the legal field, excellent in-depth accounts exist of the profound changes brought about either from a country perspective (David J. Harvey, The Law Emprynted and Englysshed: The Printing Press as an Agent of Change in Law and Legal Culture 1475–1642, Portland: Hart Publishing 2015), or applied to societal tendencies in general (for a more global view,
that same vein, this contribution works from the premise that it is not the
same act of taxpaying that we are considering with the introduction of
new technologies, which has serious consequences for the way we should
be applying and evaluating the framework of rights that encompasses the
act of taxpaying in this new world.19

Mandatory public country-by-country reporting as introduced in the
EU context is a more sophisticated and recent example par excellence,20
whereby the act of taxpaying, by means of the introduction of a public
reporting duty, is not solely confined to making a payment to the public
purse but has become part of a social dimension.21 In this highly illustra-
tive case, it is technology that enables the reporting, dissemination, and
public access to tax reports, and thus it is technology that fundamentally
changes the act of tax reporting (as a part of taxpaying).

13.6 The Connection to the Legal Sphere

The fundamental aim here is to use the insights from the discussion above
to reflect on the dialogue between taxpayers and tax administrations, in
order to attach specific legal principles to this newly evolving dialogue
that is co-constructed by technology in respect of newly developed and/
or integrated financial ecosystems.

The choice has been made to put the emphasis on two (legal) principles
that should take a stronger role within the legal framework that is sur-
rounding the design of this dialogue, namely ex ante procedural fairness

19 Which is in line with the age-old Aristotelian notion of using a different treatment for
different situations, translated into the idea of non-discrimination.
24 November 2021 amending Directive 2013/34/EU as regards disclosure of income tax
information by certain undertakings and branches, EU OJ L 429/1, 1 December 2021.
21 See the Recitals in Directive 2021/2101 (cited above), which identifies ‘citizens’, ‘inves-
category of ‘all’ as parties interested in reporting of companies, whereby this last category
will be involved through the engagement of civil society: a rather different type of dialogue
than the previously secretive one between taxpayer and tax administration.
and inclusive innovation. It is especially with the knowledge that there is a wide use of artificial intelligence (‘AI’) by tax administrations around the EU for the processing of the ever-growing amount of data, without any changes to the constitutional setting that these new realities need to be embedded in (Hadwick 2022), that the need for the inclusion of new principles within this new dialogue is becoming even more pressing.\(^{22}\)

As the taxpayer-tax administration relationship is one already established by law, and as a matter of law an exercise of state powers, this dialogue is (and will have to be) regulated by (constitutional) law and the limitations on the exercise of governmental powers, placing the subsequent considerations directly in a legal setting.

As in this specific case we are dealing with, the setting-up and/or integration of financial ecosystems for the retrieval of financial information, a few natural limitations to the discussion present itself. Firstly, the dialogue that is being spoken of in this context is thus part of the relationship between taxpayer and tax administration. The difference between relationship and dialogue is significant in the sense that dialogue here stands for the communicative act between the two,\(^ {23}\) which are tied within the relationship. The relationship can be broader than just the dialogue, and does not solely encompass the communicative actions that are part of the relationship. The limitation here thus takes place by means of limiting the review to the direct communicative aspects of the relationship between taxpayers and tax administrations, which then again can be cut up into smaller parts of specific actions. The circle of interested parties is, however, greater than these two, as intermediaries are likely to be involved (as a service provider), and in the context of companies,


\(^{23}\) Etymologically, the word dialogue stems from the Greek διάλογος (dialogos, conversation); its roots are διά (dia: through) and λόγος (logos: the word), whereby it is important to highlight that dialogue has a different spirit attached to it than other forms of communication, which may be less mediative (e.g., discussion). See: Bohm, & Nichol, L. (1996). On Dialogue. Routledge (London, UK), 6 et seq.
stakeholders will assess information to have a better position to evaluate risks taken by the company while the general public can assess the (tax) activities by the company better.\textsuperscript{24} Another technologically driven change, is that when we deal with the setting-up and/or integration of financial ecosystems for the retrieval of financial information, the relationship between taxpayer and tax authority is more communicative, and specifically more compliance focussed instead of fraud focussed, which places the relationship in a customer-service provider setting with the tax authorities as a facilitator of a service which should reduce compliance costs for the taxpayer (Dom et al., 2022).

This clearly demonstrates a new dimension to the legal sphere of which taxpaying is a part. However, in this case, the primary actor that is more closely evaluated is the technology itself, as it is a part of the entirety of the concept of taxpaying (nowadays). Its coming into existence is not by means of action by the taxpayer, but either by service providers (tax) intermediaries and/or the tax authorities.\textsuperscript{25} As can be seen from future outlooks on the process of tax administration by, for example, the OECD, new technologies make the act of tax-reporting and taxpaying ‘more seamless’ and ‘frictionless’, whilst ‘moving away from sequential taxpayer-facing processes and beginning to integrate taxation processes into the systems used by taxpayers as part of their daily lives and businesses’ (OECD 2020, p. 12/13). The idea is either to integrate tax applications into currently-in-use financial ecosystems, such as personal and/or business finances such as banking tools, whereby ‘many digital platforms will also become “agents” of tax administration carrying out tax administration processes within their systems’ (OECD 2020, p. 12). The integration of business and governmental services is the outcome of ‘a shift towards the embedding of more taxation processes into the natural systems that taxpayers use in their daily lives and businesses’ (OECD 2022, p. 6). With this development towards an increasingly real-time taxpaying activity, the earlier observed phenomenological reformulation

\textsuperscript{24} As could be observed in the example of public country-by-country reporting in the previous paragraph.

\textsuperscript{25} Think again of filing or bookkeeping software, but also the automated ways of filing returns nowadays as well as pre-filled in tax returns by means of an exchange of information between banks and tax authorities.
of taxpaying as constituting a new action, and the idea of this new action requiring new legal embedding, becomes a matter of necessity. Especially since the essential component of a dialogue structure might be lost in the process, namely the deliberate and conscious exchange of information between the parties involved.

The Need for a New Interpretation of Old Legal Rules

Two simple premises form the basis of the subsequent discussion, the first being that technology has fundamentally changed taxpaying and that this has become a new activity through technological applications. Arguing in favour of this claim was the main aim of section 5. The second premise, which will be more elaborately dealt with in the subsequent section, is the legal idea that the legislative process should guarantee an outcome that does not infringe on the (individual) fundamental rights of taxpayers. As the appeal here emphasises stronger ex ante procedural safeguards, and inclusive innovation as an inspiration to these safeguards, the conclusion that must be inferred from these two premises is that the application of traditional legal principles must be adjusted accordingly to accommodate the changed technological nature of the relationship between taxpayer and tax administration, if the new technological nature of this relationship gives rise to a possible breach of these rights.

The difficulty with many legal rules, either in statutory law or derived from principle, is that their useful effect usually depends on an action that must have passed in time. Thus, the enforcement of a legal rule generally is a sanctioning occupation. The difficulty of these primary characteristics of the law is that they do not serve the current inquiry, as this aims to guide the process before the adoption of legislation, preferably by already creating obligations on lawmakers before the law takes effect: otherwise the implementation of new technology within tax laws will become a game of trial and error to the detriment of the fundamental rights of taxpayers. Therefore, principles such as respect for privacy and data protection (family life), although extremely relevant to the current inquiry, are left aside here since they are harder to concretely apply in a legislative steering principle for the first-person communicative relation-
ship between taxpayer and tax administration within an ex ante tax legal setting that is connected to the legislative process.  

One specific principle of law with an intrinsic and peculiar connection to tax law can better serve the current purpose, namely the principle of legality, which explicitly requires that tax laws are determined and made known to the public by law. The crux is in the latter part, as under the general and universal principle of legal certainty this means that the law must be known and thus also to a certain degree comprehensible to anyone subjected to this law. When dealing with (AI) systems that fundamentally change the means of communication between the taxpayers and tax administrations, both in substance and in form, it is necessary to attach a new level of ex ante safeguards to the introduction of these new technologies that takes their dialogue-altering qualities into account.

13.7 Ex Ante Procedural Fairness as a Legal Requirement for a New Policy

The idea of ex ante safeguards to make sure that fundamental rights of taxpayers are not breached by an administration that makes use of algorithmic tools in its dialogue with taxpayers (in communication, exchange of tax specific information and decision-making) has already been acknowledged in the eKasa judgment of the Slovakian Constitutional Court (‘SCC’). The SCC held that the protection of collective rights, in the case of tax AI used for the collection of taxes and countering of abuse, cannot trump individual rights, and that technologies that make the former a smoother and more efficient process must take careful notice

[26] Meaning specifically the process itself in this case.
[27] A point also acknowledged by the Slovakian Constitutional Court in eKasa, see: 492, Finding of the Constitutional Court of the Slovak Republic, PL. ÚS 25 /2019-117; as also observed and summarised by Kuzniacki, B., Almada, M., Tyliński, K., Górski, Ł. (2022), at 223–224.
[28] And thereby the act of taxpaying itself.
[29] See case eKasa (cited above), paras. 125–129.
of the latter through specific safeguards. According to the SCC, ‘[i]t is up to the legislator how to materialise this requirement.’

This materialisation is instructed by the SCC in two important respects: firstly, the need for the use of safeguards (in the legislative process) before technology (AI) comes into force (ex ante), and secondly, with a strong emphasis on individual rights, and thus, individual taxpayers. Following this line of reasoning, the question becomes how the legislator is able to materialise the requirements that ex ante reviews bring with them in line with the principle of legality. In other words: how does the legislator inform or make the taxpayer part of the paradigmatic changes that are taking place or incoming, for example, if the OECD’s view of the future functioning of tax administrations becomes a reality? And thus more fundamentally speaking: how can you prevent the development of a discourse by means of trial and error, which would directly undermine trust in the system?

As suggested by some, the explainability of AI systems could remedy the concerns of legality. Another idea has been proposed by the SCC, hinting in the eKasa judgment at keeping the decision-making within hands that can be held accountable, which could concretely mean an obligation of prior identification of the responsible decisionmaker before a tax technology comes into force. In essence, both these lines of thinking can be brought together under the umbrella of accountability. With explainability, the legislator becomes accountable for the explanation of the technology it uses. With the identification of decision-makers, and thus the accountable player, another step is made towards establishing lines between taxpayer and tax authority in the design. In essence, both require an extra effort from the legislative authorities in and after the

30 Ibid. para. 132. Compare also Kokott/Pistone (2022), cited above.
32 Whereby here, it is with reference to the already widely reported cases in which the use of algorithmic technology by governments has taken a turn for the worse. Specific and most shocking from the tax perspective is probably the Dutch Toeslagenaffaire (child benefits scandal), best reported in English here: Hadwick, D., Lan, S., (2021), ‘Lessons to be learned from the dutch childcare allowance scandal: a comparative review of algorithmic governance by tax administrations in the Netherlands, France and Germany.’, World Tax Journal, IBFD, vol. 13, no. 4.
33 Kuzniacki, B., Almada, M., Tyliński, K., Górski, Ł. (2022), cited above.
drafting of new legislation, but both of these standards of accountability do not a priori involve the taxpayer that is subjected to the new technology, and that sees its relationship with the tax authority changed by means of this technology.

13.8 Self-Enforcing Norms and Open Dialogue: on the Necessity of a Seat at the Table for Taxpayers

The above determines two ways of establishing (legal) accountability, one already in place, and one suggestion by the SCC. The shaping value of the principle of legality on the explanation given by lawmakers in their application of technology is difficult to assess. However, with the aim of enhancing the idea of a fair procedure in the drafting phase of legislation, you cannot really take a chance and deem this principle to be self-enforcing in a field of policymaking that is unknown territory to both taxpayers and tax administrations.

A look at the current functioning of checks and balances within this system of law-making shows both a legal and a political accountability, however, both of these are only enforceable after the policy has been made. Therefore, in the spirit of dialogue, it is rather unsettling that the taxpayers themselves are not granted an entrenched right to be part of the considerations at the beginning of the legislative process. A system of checks and balances, if functioning accordingly, makes sure that under the assumption that the actors within a political decision-making system work towards the realisation of their own goals, their powers are distributed in such a way that they will keep each other’s prerogatives within

---

34 Which, in essence, it can also be argued, is already in place as in the end, government responsibility will have to be taken even for systems where there is no directly identifiable decision-maker.

the predetermined boundaries. However, in the current scenario, the question is what the prerogative of the taxpayer even is, or in other words: what power it holds.

Under the current system, this power of the taxpayer is generally only to be found in the accountability of politicians through the democratic processes available in the state, or enforceable in court after the adoption of the legislation. As emphasised in the previous section, technology is not neutral and highly influenced by design, which makes the involvement of citizens in the drafting of legislation by means of fairness assessments with their inclusion in the decision-making process, and not just by experts on their behalf, not only logical but also necessary. How this should be done concretely is a question for sociology, political sciences, psychology, law, and other scientific fields. The main point to take away from the artifacts/tools discussion within the earlier discussion of technology is the fact that technology is not neutral, and that it will never be neutral, as it is shaped by our outlook on the world while shaping us in the process. Taxpayer participation in the drafting phase therefore seems extra critical to ensure a fair (non-biased) outcome, and enhance public perception of technology usage. To do this right for everyone, and not just for the better organised taxpayers that find their way towards public consultations, one principle must play a pivotal role.

13.9 The Necessity of Inclusive Innovation in the Open Dialogue Between Tax Authorities and Taxpayers

When mentioning taxpayers, the difficulty presents itself again that this is a widely diverse group, comprising different entities with different

---

36 See, for the classical formulation of such a system, with remarkable durability: Madison, J. (1788). The Federalist no. 48, accessible online via: https://avalon.law.yale.edu/18th_century/fed48.asp (last accessed 06-10-2022).

37 Whereby it must be mentioned that for obvious reasons, a wide range of taxpayers do not have this power at their disposal (e.g., companies, but also foreign residents).

38 Which is perhaps the only (meagre) exception to taxpayer involvement in the development of tax technologies by tax authorities.
fundamental, social and economic rights (Gill-Pedro 2022). Just as their rights in the post-legislative phase are completely different, so is their standing in the pre-legislative phase. Where companies lack the power of voting to keep politicians accountable, natural persons often lack the ability to engage in a direct conversation with the authorities, or at least 99% of these natural persons, to directly discuss how technology will be part of their future relationship. Furthermore, if you take a look at, for example, the integration of financial ecosystems as proposed by the OECD as a future model for technology usage in tax compliance, both for businesses and individuals, the possibility for the latter to enter into dialogue by means of mediation is through the service provider (who will become the communicator when integration shall take place). This places in particular the individual at a significant distance to the authorities, and most likely especially less well-off individuals, with less access to better resources or the chance to pay more for a better protection of their rights. Add thereto that it is specifically this group which is most likely to be adversely affected by technological change (Lohr 2022), it becomes clear that the inclusion of an ex ante direct dialogue on fairness with these taxpayers is a necessity for any self-respecting democracy that uses technology to change its engagement with its taxpayers.

13.10 Conclusion

This contribution leaves open more questions than it answers, but it opens the window for engagement between disciplines that have previously predominantly been working within the silos of their own discourse. Whereas the legal act of taxpaying seems to be changing rather slowly, the relationship between taxpayer and tax administration is changing very rapidly if you adopt another lens, as was done above. The legal repercussions of this changed relationship are that a shifting emphasis towards ex ante fairness reviews is necessary to give taxpayers a voice and to make sure that innovation in tax technology is not becoming a field of trial and error progress, at the cost of taxpayers’ fundamental rights. How these systems of pre-legislative dialogues on technology should

39 See also the cited articles.
take shape is a question for other fields of science, but that inclusivity within this dialogue is paramount seems obvious. In addition, a proactive government has to be the fountainhead of such future change. That these developments open up the possibility for new civic and democratic participatory and deliberative engagement should provide fertile ground for further interdisciplinary inquiry.

References


Chapter 14
Automation in the Public Sector and the Principle of Non-Discrimination*

14.1 Introduction

Automated decision-making (ADM) processes are challenging the public sector to safeguard the public from discriminatory practices. This raises the question of whether the existing anti-discriminatory laws are sufficient to preserve individuals’ right to non-discrimination, while utilising new technologies to automate decisions in the public sector?

Discrimination is defined as ‘[…] the intended or accomplished differential treatment of persons or social groups for reasons of certain generalised traits’ (Heitmeyer, Salentin, 2022 p. 1). Discrimination is referred to when a person is treated unfairly and differentiated against based on one of the discrimination grounds (Henrard, 2008 p. 3). Article 2 of the Universal Declaration of Human Rights states that everyone is entitled to the rights and freedoms included in the Convention ‘[…] without distinct of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status’ (Universal Declaration of Human Rights (UDHR) Article 2 1948).

Generally, discrimination may occur on the following grounds: race, gender, sexual orientation, religion, nationality, age and disability (Henrard, 2008 p. 3). Discriminatory practices exist but intensify with

* This paper was awarded the best student paper during the FIRE conference 2022.
the use of artificial intelligence (AI) in ADM systems according to the European Agency for Fundamental Rights (FRA, 2022 p. 22). Digital discrimination is defined as:

“[…] a form of discrimination in which automated decisions taken by algorithms, increasingly based on artificial intelligence techniques like machine learning, treat users unfairly, unethically, or just differently based on their personal data […] such as income, education gender, age, ethnicity, religion” (Criado Such, 2019 p. 82).

There has been a surge in decisions being delegated to ADM systems instead of their human counterparts (Criado, Such, p. 84). This has been a cause for concern for legal scholars, in view of the fact that algorithms are able to discriminate methodically and on an extensive scale, surpassing non-digital discrimination (Criado, Such, p. 85). Additionally, spotting discrimination in an algorithm can be difficult, due to the concept of AI systems being black boxes (Borgesius, 2018 p. 15). AI systems can be opaque in their decisions, which ultimately obstruct investigations leading to potentially discriminatory outcomes (Borgesius, 2018 p. 15). COMPAS is an algorithm which is employed by the judicial system in the United States (US). It is applied pretrial or during sentencing to determine an offender’s level of recidivism (Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, 2016 p. 1). A study conducted by the journalist organisation ProPublica revealed the outcomes of such an algorithm as discriminatory. (Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, 2016 p. 1). However, other examples are less discriminatory. For example, Sweden has successfully implemented an ADM algorithm that administers social benefits in the municipality Trelleborg, albeit not without critique. The municipality of Kungsbacka, which is on the list of receiving the algorithm used in Trelleborg, saw 12 out of 16 social workers hand in their notice in protest (Erik Wisterberg, 2018 p. 1). The algorithm boasted of reducing the number of citizens accepting social benefits and that 85% of the people applying were in fact fit to work. In response, the social workers noted that the system struggled to understand the reality of the situation of those applying for social benefits (Erik Wisterberg, 2018 p. 1).
This chapter first discusses AI and its use in the public sector by governmental authorities, such as central governments, local municipalities and organisations under them and the possible discrimination that that generates. Second, this chapter will provide a comparison of different forms of discrimination as they stand. Finally, in order to evaluate whether the current domestic anti-discrimination provisions in Sweden and the US sufficiently safeguard individuals, this chapter analyses the legal framework and practice in both Sweden and the US and discusses ADM in the public sector in light of the principle of non-discrimination.

14.2 The Use of Artificial Intelligence in the Public Sector

AI can today be described as an umbrella term, containing technologies such as machine learning and natural language processing (Kuziemski, Misuraca, 2020 p. 2). AI can be defined as systems which ‘[...] display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals’ (Kuziemski, Misuraca, 2020 p. 2).

The use of AI in ADM is quite prevalent in the public sector (Langford, p. 142, 2020). The public sector is a term which encompasses ‘[...] central government, local governments, and organisations under them’ (Nasrudin, 2020 p. 1). The sought-after use of ADM by public agencies increases the efficiency and lessens the burden of day-to-day tasks that are repetitive and time-consuming. (Kaun, 2021, p. 2047) ADM is frequently used by the public sector, such as different governmental departments, judicial bodies and international organisations (Langford, p. 142, 2020). One example is the courts employing the above-mentioned COMPAS (Langdon, p. 144, 2020), while another is the US department of Treasury employing algorithms in order detect fraud (Electronic Privacy Information Center, n.d)
14.3 The Danger of Artificial Intelligence in the Public Sector

While invaluable to most public administration sectors for the way it decreases costs and for its time-saving qualities, there are dangerous implications pertaining to the use of AI. The critique faced by AI circulates around ‘[…] bias, error, a lack of transparency about how models operate and an overreliance on machines at the expense of human expertise’ (Deeks, 2020, p. 44). An algorithm produces discriminatory decisions when the data that the algorithm was based on is biased or because there is a lack of available data. This creates an unreliable system with decisions that are incorrect (Deeks, 2020, p. 44). How algorithms can produce biased results is showcased by the algorithm called COMPAS. It is used by courts pretrial and during sentencing and was created by Northpoint Inc. ProPublica investigated the COMPAS algorithm, which was used to measure a convict’s risk of recidivism (Larson, Mattu, Kirchner, Angwin, 2016 p. 1). ProPublica found that COMPAS has shown racial bias and discrimination against people of colour who are ‘[…] twice as likely as white defendants to be misclassified as being a higher risk of violent recidivism.’ (Larson, Mattu, Kirchner, Angwin, 2016 p. 1). COMPAS demonstrates how a public sector organisation can cause grave harm to an individual if they employ a biased algorithm in their day-to-day work. Legal scholars argue that ADM systems may carry an inherent risk of bias, which could perpetuate discrimination and inequality (Vetrò, Torchiano, Mecati, 202, p. 2). These biased outcomes may be based on the ‘[…] prejudices of programmers, previous decisions, users and/or the society’ (Criado, Such, 2019, p. 85). In addition, human errors such as a flawed code design or biased training data intended for machine learning algorithms can result in discrimination (FCAI, 2021, p. 1).

Transparency is commonly proposed as a solution for solving algorithms with discriminatory outcomes (FCAI, 2021, p. 1). This solution is based on the idea that through transparency, there will be a clear view of what needs to be fixed (FCAI, 2021, p. 1). The case of the fully automated Trelleborg algorithm highlights the fact that transparency is viewed as important in order to minimise discriminatory outcomes. The algorithm is based on what is known as a decision tree, which functions by reviewing
specific variables found in different databases (Kaun, 2021, p. 2048). A journalist whose request for access to the code behind the algorithm was denied several times, resulting in a legal dispute for the release of the code (Kaun, 2021, p. 2048). The journalist appealed to the Swedish Administrative Court of Appeal for the release of the code, declaring it to fall under the Swedish principle which allows public records to be open to the public (Kaun, 2021, p. 2049). The Administrative Court of Appeal concurred with the journalist’s appeal and ruled that in Sweden ‘[…] source code must be made accessible to the public and is fully included in the principle of public access’ (Kaun, 2021, p. 2049).

14.4 Comparison between the United States and Sweden

If a public sector organisation which employed an ADM system were to produce a discriminatory result, the matter would be solved differently depending on the country in question. Sweden and the US are dissimilar countries in regards to legislation, but both strive to advance technologically and incorporate AI into the works of their authorities. Thus, a comparison of these countries could indicate a common theme in legislative action and approach towards discriminatory ADM. Sweden’s government announced a new authority, the Agency for Digital Government, which was launched to promote open and data-driven innovation (Regeringen, 2019, p. 1). The Agency also works to foster and promote the public authorities’ ability to utilise AI (Regeringen, 2019, p. 1). The US has underlined the urgent need to maintain ‘[…] American Leadership in artificial intelligence’ (GPO, 2019, p. 3967). The US has encouraged the continued research and development of AI and technological breakthroughs of AI by federal governments (GPO, 2019, p. 3967). Additionally, the National Artificial Intelligence Initiative (NAII) was established in order to ‘[…] lead the world in the development and use of trustworthy AI systems in public and private sectors […] and coordinate ongoing AI activities across all Federal agencies’ (Thornberry, 2021, p. 1165).
The US and Sweden have both encountered problems resulting from public sectors employing ADM algorithms. Sweden has seldom exposed individuals to discrimination through ADM and consequently there is a lack of examples (DO, 2022, p. 20). The Equality Ombudsman presented an incident in 2021 as an example of discrimination by governmental agencies using ADM. The military had exposed an individual to discrimination by using ADM. The algorithm automatically excluded individuals applying to the military if they had the medical diagnosis ADHD or autism (DO, 2022, p. 20). The individuals applying were immediately disregarded when they entered their medical diagnosis, without the possibility to undergo an individual examination (DO, 2021, p. 1). While COMPAS has been discussed earlier as an example of discrimination found in an algorithm employed in the US by a public authority, the US healthcare system is currently facing a backlash for using discriminatory algorithms to detect patients with complicated health needs (Obermeyer, Powers, Vogeli, Mullainthan, 2019, p. 1). The algorithm was used as a screening tool in order to alert which patients were to be considered high risk and in need of care. The result indicated considerable disparities between people of colour and white people in relation to medical care and indicated that the algorithm was racially biased (Obermeyer, Powers, Vogeli, Mullainthan, 2019, p. 2). People of colour were not given the same access to care (Obermeyer, Powers, Vogeli, Mullainthan, 2019, p. 1). The discrimination arose as a result of the algorithm’s preference predicting healthcare costs over sickness (Obermeyer, Powers, Vogeli, Mullainthan, 2019, p. 1). Thus, this resulted in substantial racial discrimination.

The legal implications of a discriminatory ADM system differ depending on the country the algorithm is being utilised in. Sweden is currently invested in ensuring that public sector organisations that employ AI and ADM in their work do so conscious of the discrimination that might occur (DO, 2022, p. 5). Sweden’s Equality Ombudsman has scrutinised government agencies’ application of AI and ADM in relation to citizens and the manner in which the authorities regard the risk of discrimination (DO, 2022, p. 5). While many government agencies employ ADM in their work, only 4 of them were found to employ AI in relation to ADM (DO, 2022, p. 29). Out of the 14 government agencies that employ ADM, only 4 of them had frameworks on the subject to ensure that no
discrimination based on gender, ethnicity or age would occur (DO, 2022, p. 31). The Equality Ombudsman drew the conclusion that knowledge about discrimination was inadequate and that local governments, but also other areas of the public sector, must develop and expand their knowledge regarding discrimination in relation to ADM and AI (DO, 2022, p. 37).

Sweden does not have an all-encompassing domestic law regarding the use of ADM. If discrimination due to an ADM occurs in the public sector different domestic laws would deal with matter (Myndigheten för digital förvaltning, 2020, p. 91). Let us take the example of a government agency employing an ADM algorithm that produces discriminatory results. In Sweden, government agencies’ actions are governed by the Administrative Procedure Act (2017:900). This is established in Article 1, which stipulates that the Administrative Procedure Act applies to administrative activities and to ‘[…] the processing of matters at administrative authorities and the processing of administrative matters at the courts’ (Government Office of Sweden, 2021, p. 1). Government agencies are included in the definition of an administrative authority, due to the fact that they fulfil public administrative tasks and are governed by public law (Prop/Government Bill 2016/2017:18). In relation to discrimination, authorities are required to only take action which is supported by the legal order (Administrative Procedure Act, 2017, Article 5). Furthermore, Article 5 also stipulates that government agencies must be objective and impartial in their activities (Administrative Procedure Act, 2017, Article 5). This signifies that it is crucial to the government agencies’ work to not discriminate or be partial in any significant way. The legal foundation for the use of an ADM system by a government agency is to be found in Article 28 (Administrative Procedure Act, 2017, Article 28). According to legal scholars, this Article concludes that administrative decisions can be made through automation and that there is no need for a special regulation in order to obtain the legal support needed to use automation as a form of decision-making (Kristina Ahlström, Article 28, citation 126, n.d). If an individual faces discrimination as in the hypothetical case described above, then there could be a potential breach of Article 5 (Administrative Procedure Act, 2017, Article 5). In Government Bill 2016/17:180, it is clarified that the principles of impartiality and objectivity in Article 5 in actual fact apply, in accordance with Article 1 Section 2, not only to the administrative activities of authorities (such
as case management) but also to all other aspects included in the actual work of the authorities (Prop/Government Bill 2016/17:180, p. 286). This suggests that decisions which are taken through automation, such as with ADM, must fall within the definition in Article 5. Subsequently, if a government agency were to make a decision through an ADM system that discriminates an individual, this decision would be in breach of Article 5, on the basis of Article 5 being applicable to all activities which are conducted by a government agency (Prop/Government Bill 2016/17:180 p. 289). Article 5 explicitly forbids discrimination and other similar forms of bias according to the Government Bill (Prop/Government Bill 2016/17:180, p. 290). Thus, this suggests that if an individual is faced with a discriminating decision from a government agency, issued by an automated decision, it would be rendered unlawful attributable to it breaching the provisions of Article 1 Section 2 and Article 5.

If the same hypothetical case of discrimination were to occur in a municipality instead of a government agency, the Swedish Local Government Act would apply. This is established in Chapter 1 Article 2 of the Local Government Act, which asserts that Sweden is divided into municipalities and county councils, which handle matters described in this regulation or other special regulations (Kommunallagen, 2017, Chapter 1 Article 2). With the new implementation of legal support for automation in the Administrative Procedure Act, the Swedish government also legislated legal support for the use of ADM in the Swedish Local Government Act (Sveriges Riksdag, 2021, p. 1). The legal support for ADM is found in Chapter 6, Article 37. There, it is declared that a committee may delegate the right of decision to an ADM system in a certain case or group of cases (Kommunallagen, 2017, Chapter 6 Article 37). It is stipulated in Chapter 1 Article 2 in the Instrument of Government:

‘The public institutions shall work to promote the opportunity for all to attain participation and equality in society […]. the public institutions shall combat discrimination of persons on grounds of gender, colour, national or ethnic origin, linguistic or religious affiliation, functional disability, sexual orientation, age’ (Instrument of Government, Chapter 1, Article 2, 1974:152).

Based on this Article, it is established that municipalities, which provide vital public services, are under an obligation as public institutions to follow the Instrument of Government (Government Office of Sweden,
Chapter 14 Automation in the Public Sector and the Principle of…

2004, p. 1). On these grounds, the municipalities, as public institutions, are under an obligation to combat discrimination which is based on the discrimination grounds. Additionally, municipalities must also promote the opportunity for all to achieve equality in society. This signifies that municipalities, which are allowed to use ADM in their work, must in their work safeguard against discrimination (Instrument of Government, Chapter 1, Article 2, 1974:152). It can then be argued that if a municipality uses an ADM system which produces discriminatory results, it must be perceived as unlawful due to non-compliance with the provisions in Chapter 1 Article 2 of the Instrument of Government (Instrument of Government, Chapter 1, Article 2, 1974:152).

However, future cases will conceivably be judged in accordance with the provisions in the Discrimination Act (Discrimination Act, 2008:567). This can be garnered from the Swedish military case study from 2021. The Equality Ombudsman found that the military case was in breach of Chapter 2 Section 15.1 of the Discrimination Act (Discrimination Act Chapter 2 Section 15.1, 2008:567). The Discrimination Act contains special provisions pertaining to enrolment procedures in connection with enlistment in the military (Discrimination Act Chapter 2 Section 15.1, 2008:567). It forbids discrimination in admission examinations to join the military and during the enrolment procedure (Discrimination Act, Chapter 2 Section 15.1 2008:567). Although the Discrimination Act does not contain any provisions pertaining to automation, it establishes in Chapter 1 Section 1 that the purpose of the Act is to combat discrimination (based on the discrimination grounds) and promote equal rights and opportunities (Discrimination Act, Chapter 1, Article 1, 2008:567).

Further on, the Act contains conditions concerning the prohibition of discrimination in relation to education services, employment services, social insurance systems, financial aid for studies, unemployment insurance and more (Discrimination Act, Chapter 2, Sections 1, 5, 9, 13, 14, 2008:567). Thus, if discrimination were to occur, the relevant legislation would presumably fall upon the Discrimination Act, depending on the public authority in question. Due to a lack of examples concerning discrimination by ADM algorithms in the Swedish public sector, it is difficult to pinpoint how these domestic laws would function in reality (DO, 2022, p. 20). Consequently, you can only speculate upon the theoretical application of the laws.
The US, in comparison, recently legislated a federal act pertaining to the use of AI in the government. The AI in Government Act of 2020 was created to encourage the federal government to adopt AI technologies (Consolidated Appropriations Act, P.1105, 2020). The term AI is defined in the Act to include: ‘Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets’ (John. S McCain National Defense Authorization Act for Fiscal Year 2019, p. 62, Section 238(g)(1). Machine learning is included in the definition for AI (John. S McCain National Defense Authorization Act for Fiscal Year 2019, p. 62, Section 238(g)(4)). ADM has been defined as ‘[…] the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data’ (ICO, 2018, p. 5). On that account, ADM fulfils the definition of AI in the section due to the system creating decisions without human interference as in accordance with Section 238 (g). Section 104 (a) of the AI in Government Act of 2020 contains different sets of criteria, which include publishing a memorandum regarding the development of policies about agencies’ use of AI technologies (Consolidated Appropriations Act p. 1107, 2020). Additionally, this memorandum shall contain the best procedures for ‘[…] identifying, assessing and mitigating any discriminatory impact or bias any classification protected under Federal non-discrimination laws, or any unintended consequence of the use of AI including policies to identify data used to train AI algorithms as well as the data analysed by AI used by the agencies’ (Consolidated Appropriations Act p. 1107, 2020) Section 104(a)(3)). The memorandum will be sent to agencies which are planning to use AI (Consolidated Appropriations Act, Section 104(a)(1), p. 1107, 2020). Agencies are defined in the Act to include the ‘[…] executive department, military department, government corporation, government-controlled corporation, or other establishments in the executive branch of the government’ (United States Code, Section 3502 of Title 4, 2011). This seems to indicate that if a discriminatory case were to arise, due to the actions of a government agency, the appropriate legal action would fall within the scope of federal non-discrimination laws.
Contrary to Sweden’s single Discrimination Act, the US has several different federal non-discrimination laws, which according to the AI in the Government Act of 2020 will become relevant to cases of discrimination caused by the use of ADM by agencies (Consolidated Appropriations Act, p. 1107, 2020) Section 104(a)(3)). Such federal non-discrimination laws include, for example, the Civil Rights Acts which prohibit discrimination based on the discrimination grounds race, ethnicity, religion, national origin (Future of Privacy Forum, 2014, p. 1). Legal scholars argue that while these laws do not resolve unintentional discrimination by ADM systems, users of automated systems must in their work strive to not breach these laws (Lee, Resnick, Barton, 2019, p. 11). It has been suggested that Congress should clarify how these non-discrimination laws are to be applied to ADM, due to most of them being legislated before the arrival of the internet (Lee, Resnick, Barton, 2019, p. 11). This is in order to establish clearer rules, which in turn might urge creators of automated systems to be vigilant when establishing new systems in order to reduce the risk of discrimination (Lee, Resnick, Barton, 2019, p. 11).

Furthermore, the US is a federation. As a federation, the different states contained within the United States carry the power to create and legislate their own laws (Britannica, p. 1, 2022). Sweden is a unitary and decentralised state, denoting that while it has municipalities and different regions which have competence in certain fields, it is only the Parliament that may legislate laws (European Committee of the Regions, p. 1, n.d). The State of Maryland recently introduced a Bill obliging state agencies that use ADM to only employ ADM services which adhere to AI standards (Maryland General Assembly, 2021, p. 1). The Bill was drafted to restrict government use of ADM. Since no such law currently exists, the standards include an assurance that a system purchased by the states is transparent, fair and evaluated to whether it carries potential risks (Maryland General Assembly, 2021, p. 2). It is further stated in the Bill that ‘any discriminatory act prohibited in current law that is performed through an algorithmic decision system is a discriminatory act that may be the subject of a complaint filed with MCCR’. This indicates a legal measure if an individual is exposed to discrimination. This Bill has yet to be passed, but legal scholars claim that most recent bills on ADM aim to restrict the purchasing of ADM systems by governments (Sanderson, Jordan, Gray, 2021, p. 1). In addition, Washington DC has
Anna Husman

drafted a Bill which would establish government guidelines in relation to the purchase of ADM system (Hasegawa, Hunt, Kudere, Wilson.C, p. 1, 2021). The text acknowledges that most ADM systems are currently unregulated but still used in the public sector by, for example, local governments, courts and healthcare (Hasegawa, Hunt, Kudere, Wilson.C, p. 2, 2021). It defines public agency as including but not being limited to commissions, departments, educational institutions or other state agencies, counties, cities, governing bodies (Washington State Legislature, 2022, p. 1). Section 3 of the Bill stipulates that public agencies employing ADM systems in their work must do so in accordance with the provisions set forth in Sections 4 and 5 of the Bill. Section 4(1) establishes that public agencies are prohibited from using an ADM system ‘[…] that discriminates against an individual, or treats an individual less favourably than another, in whole or in part, on the basis of one or more factors enumerated in RCW 49.60.010’ (Hasegawa, Hunt, Kudere, Wilson.C, p. 3, 2021). RCW 49.60.010 declares that discrimination based on the discrimination grounds such as gender, age, creed, ethnicity, national origin etc is unlawful (Washington State Legislator, p. 1, 2022). Finally, in Section 7, the Bill introduces provisions which enables a person to launch court proceedings against a public agency (Hasegawa, Hunt, Kudere, Wilson.C, p. 8, 2021, Section 7). This can be done provided that the person in question has suffered from discrimination due to the ADM system employed by the government agency ((Hasegawa, Hunt, Kudere, Wilson.C, p. 9, 2021, Section 8). These are some examples of the laws which legislatures in different states are introducing in an effort to remove the risk of discrimination. Nonetheless, the above-mentioned laws have met critique from scholars, due to the inconsistency in the provisions surrounding obligations and requirements (Sanderson, Jordan, Gray, p. 1, 2021).

It could be debated that the two countries are undecided as to how to manage a case of discrimination caused by ADM. The US faced critique at a federal level for being too focused on being the driving force of technological development in AI, without considering the risk of bias, accountability and transparency (Moore, 2021, p. 1). A memorandum stated that federal agencies ought to avoid certain regulatory actions which would ‘[…] needlessly hamper AI innovation and growth’ (Vought, 2020 p. 2). The Equality Ombudsman in Sweden released a report where it was
stated that, in all likelihood, the relevant laws at a domestic level concerning ADM and discrimination were the Instrument of Government which contained provisions on non-discrimination, which developed into the Discrimination Act (DO, 2022, p. 8). Additionally, eSam determined that ADM would face the Administrative Act and in the case of discrimination and AI, it would be evaluated based on the Discrimination Act (eSam, 2022 p. 15). The US, in contrast, has developed a framework called the AI Bill of Rights which aims to guide the deployment and use of automated systems and AI through a set of principles (Whitehouse, p. 4, 2022). The Bill forbids ADM discrimination based on the discrimination grounds, but is not a legal regulation in itself, it is only meant to be a source of inspiration for new AI laws (WhiteHouse, p. 9, 2022).

14.5 Concluding Remarks

There has been a surge in delegating decisions to ADM systems instead of their human counterparts. Public sector use of ADM to increase effectiveness in the work of organisations gives rise for concern among many legal scholars. The risk relates to the risk of individuals being faced with digital discrimination due to ADM. To resolve this, Sweden and the US have introduced different measures. While striving to be first in the technological advancement of AI, different practices and legal solutions have been introduced to combat discrimination by ADM. It must be underlined that Sweden and the US are made up of two different sets of systems. The US is a federation, which means that the country can introduce legislation at a federal and at a state level. Sweden, on the other hand, has a unitary based system, and while municipalities are allowed a measure of self-governance, it is only the Parliament that can legislate laws. In light of this, it is important to comment that the way these countries legislate laws will, undoubtedly, affect the way the issue is handled. This can be observed in the way the two countries have dealt with the issue. Sweden, although this is still under debate, has come to an agreement that if there is a legal issue concerning ADM and discrimination, the Instrument of Government and its non-discrimination principles will lead to the Discrimination Act. Additionally, depending on the part of the public sector at fault, regulations such as the Administrative Procedure Act or
the Local Government Act may come into play. The US, by contrast, has a federal act concerning public sector use of ADM, where it seems that federal laws pertaining to non-discrimination will be used. Depending on the area of discrimination, one of several federal non-discrimination laws will come into play. Additionally, American scholars have, similarly to Sweden, searched for clarification regarding what laws might become relevant if faced with a case of ADM and discrimination. Some have called for Congress to explain how federal non-discrimination laws are to be applied, due to the fact that most were created before the arrival of the internet. At a state level, the purchase and use of ADM by government agencies is what is being legislated currently. Both countries have been criticised and examined for their use of ADM in the public sector from a non-discrimination point of view. Against this background, both countries have taken steps to prevent digital discrimination by automation, but there is still a measure of uncertainty whether this is enough.

To conclude, considering the arguments presented by legal scholars it can be argued that both countries are aware of the issues surrounding ADM and the risk of discrimination. Due thought must be given to the system each country is based on and its cultural background, as a reason for the difference in legislation concerning the topic of ADM. You might conceivably point out that both countries have the idea of using their domestic non-discrimination laws as a basis for cases of discrimination by ADM. However, concerning additional legislation surrounding the governance of the public sector, there are certain differences. While incidents of discrimination by ADM vary between the two countries, legal scholars are currently of the view that both countries are aware of the risk of discrimination and both are in the process of enacting laws on the subject. In conclusion, due to the reasoning of both countries, actively pursuing ways to solve the matter of ADM and non-discrimination, it is not possible to establish whether laws and practices in Sweden and the US are enough to safeguard against discrimination. Thus, they ought to be constantly developed in order to guarantee that the principle of non-discrimination is upheld.
References


Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)


Government documents


Chapter 14 Automation in the Public Sector and the Principle of…


Books/e-books


Journal Articles


Anna Husman


Miscellaneous items


Jeff Larson, Surya Mattu, Lauren Kirchner, Julia Angwin ‘How We Analyzed the COMPAS Recidivism Algorithm’ (2016) ProPublica https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm Accessed 26-10-2022


