transcrime
Joint Research Centre on Transnational Crime

UNIVERSITÀ CATTOLICA del Sacro Cuore

Datacros

This project was funded by the European Union's Internal Security Fund - Police

Project DATACROS

Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structure

ISFP-2017-AG-CORRUPT-823792

Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures

Final report of the DATACROS Project (ISFP-2017-AG-CORRUPT-823792)

www.transcrime.it/datacros/

Authors:
Antonio Bosisio
Carlotta Carbone
Maria Jofre
Michele Riccardi
Stefano Guastamacchia

With the scientific coordination of Ernesto U. Savona

With the support of Massimilano Carpino (Chapter 5)

ISBN: 978-88-99719-25-8

Suggested citation: Bosisio A., Carbone C., Jofre M., Riccardi M., Guastamacchia S., 2021, *Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structures* – Final report of the DATACROS Project.
Milano: Transcrime – Università Cattolica del Sacro Cuore.

Graphic project: Ilaria Mastro (Transcrime – Università Cattolica del Sacro Cuore)

Table of Contents

Executive summary

Project overview

Project DATACROS was funded by the European Union Internal Security Fund - Police (ISFP-2017-AG-CORRUPT-823792). The project has produced:

1) An **aggregate analysis** of corporate ownership anomalies across EU27;

2) A **prototype tool for conducting risk assessment of legitimate companies**, which is capable of detecting anomalies in firms' ownership structure that are indicative of a high risk of collusion, corruption and money laundering.

The project lasted for two years (March 2019-February 2021) and was coordinated by Transcrime – Università Cattolica del Sacro Cuore. The project was the result of a collaboration between the following partners:

- Agence Française Anticorruption (AFA, France)
- Cuerpo Nacional de la Policia (CNP, Spain)
- Investigative Reporting Project Italy (IRPI, Italy)

Bureau van Dijk contributed as data partner.

The problem

There is an extensive body of evidence[1] suggesting that **legitimate companies** play a crucial role in terms of facilitating corruption schemes and money laundering of illicit proceeds (EFECC 2020). Moreover, the **Covid-19 pandemic**, allied with the concomitant introduction of recovery plans by EU Member States (MS) and the organisational effort required to supply vaccines, have provided criminal networks with further opportunities to drain public resources by exploiting legitimate companies to simultaneously engage in corruption, fraud, tax crime and infiltration of public funds (UNODC 2020; FATF 2020). **Complex and opaque corporate ownership schemes** are widely used to conceal illicit profits and are on the increase. According to the World Bank, 70% of corruption cases between 1980 and 2010 involved **anonymous shell companies** (van der Does de Willebois et al. 2011). Scandals such as the "Panama Papers" (ICIJ 2016) and "Paradise Papers" (ICIJ 2017), among others, uncovered a dense and **opaque** network of companies and **trusts** that were solely established to conceal the identity of their beneficial owners (BOs) and the criminal origin of their proceeds. In many other cases, trusts and other opaque **legal arrangements** are misused, wittingly or otherwise, for money laundering activities (FATF 2010). Numerous police investigations[2] have confirmed that **shell companies** serve to obfuscate criminal activities and act as facilitators of pseudo-legal sales, trade-based money laundering, false invoicing and fraud schemes. Corporate structures characterised by **anomalous ownership** have also been exploited in order to conceal money laundering of proceeds from human trafficking (FATF 2018). There is also evidence pointing to the increased **cross-border nature**[3] of money flow schemes: criminals exploit bank accounts, intermediaries and **firms** located in different jurisdictions, including non-cooperative tax havens. Finally, **politically exposed persons (PEPs)**[4] may abuse their position to accept and extort bribes, misappropriate state assets, before proceeding to use legitimate companies, as well as domestic and international financial systems, to launder the proceeds.

1. See section 2.1 for some examples.

2. See, for example, police investigations such as 'Volcano' or 'Matrioska', which are discussed at length in Transcrime's project MORE report (Savona and Riccardi 2018). See also Europol (2018).

3. See, for example, operation 'Webmaster' (Europol 2019) and operation 'Gambling' (Gdf 2015).

4. "Individuals who are, or have been, entrusted with prominent public functions, their family members, and close associates" (FATF 2013a).

The gaps

Technological tools currently available on the market help financial investigations involving legitimate companies. However, these tools have primarily been designed for banks, financial institutions and large corporates (e.g. for anti-money laundering and compliance purposes). **There is a dearth of tools specifically designed for public authorities (e.g., Law Enforcement Agencies, Financial Intelligence Units, Anti-Corruption Agencies, Tax Authorities).**

However, a survey conducted for the purposes of this project amongst **37 public authorities** across 19 EU countries confirmed that there is a **strong need for such tools**. More specifically, the results showed that:

a. 60% of the respondents **do not** currently **use any software** for conducting investigations;

b. 70% of the respondents **would be interested in using software to conduct risk assessments of firms**;

c. 78% of the respondents still rely on private data being provided or local registers, while they do not use global company data repositories.

How DATACROS addresses the problem and gaps

To address this problem and fill these gaps, Transcrime has:

1. Conducted an a**ggregate analysis of ownership anomalies** in 29 European countries[5] (see section 3),
2. Developed the **DATACROS prototype tool**, which is a risk assessment tool that includes two environments that serve different functions:
   a. The **Restricted Area** (section 4.1): a prototype real-time analytical platform that is only accessible to authorised users (e.g., Anti-corruption Agencies, Law Enforcement Agencies), for investigating anomalies in EU firms' ownership structures and conducting risk assessments.
   b. The **Public Area** (section 4.2): a dashboard that is accessible to everyone, for monitoring ownership anomalies across 29 European countries, regions and business sectors at an aggregate level.

1. Aggregate analysis of ownership anomalies

For the purposes of the project, Transcrime has analysed the **ownership structure** of 56 million companies in 29 European countries. By exploiting unique information from the dataset *Bureau van Dijk - Orbis Europe* and other sources (see details in section 3.1.2), the analysis sought to assess the distribution of opaque and anomalous companies across EU territories and sectors. The results of the analysis (see section 3) indicate that:

- On average, 1% of limited companies in EU27 + United Kingdom and Switzerland have ownership links with entities located in a **high-risk jurisdiction**[6]. Luxembourg (8.7%), Cyprus (8.5%), Malta (5.1%) and Belgium (2.9%) are the countries with the highest percentage of companies who have shareholders from blacklisted/greylisted countries.
- On average, 1.2% of limited companies in EU27 + UK and Switzerland are controlled by a **trust**, a **fiduciary**, a **foundation** or another legal arrangement that does not allow the BO to be identified. In some countries, such as the Netherlands (25.6%) and Luxembourg (8.7%), the percentage is much higher.

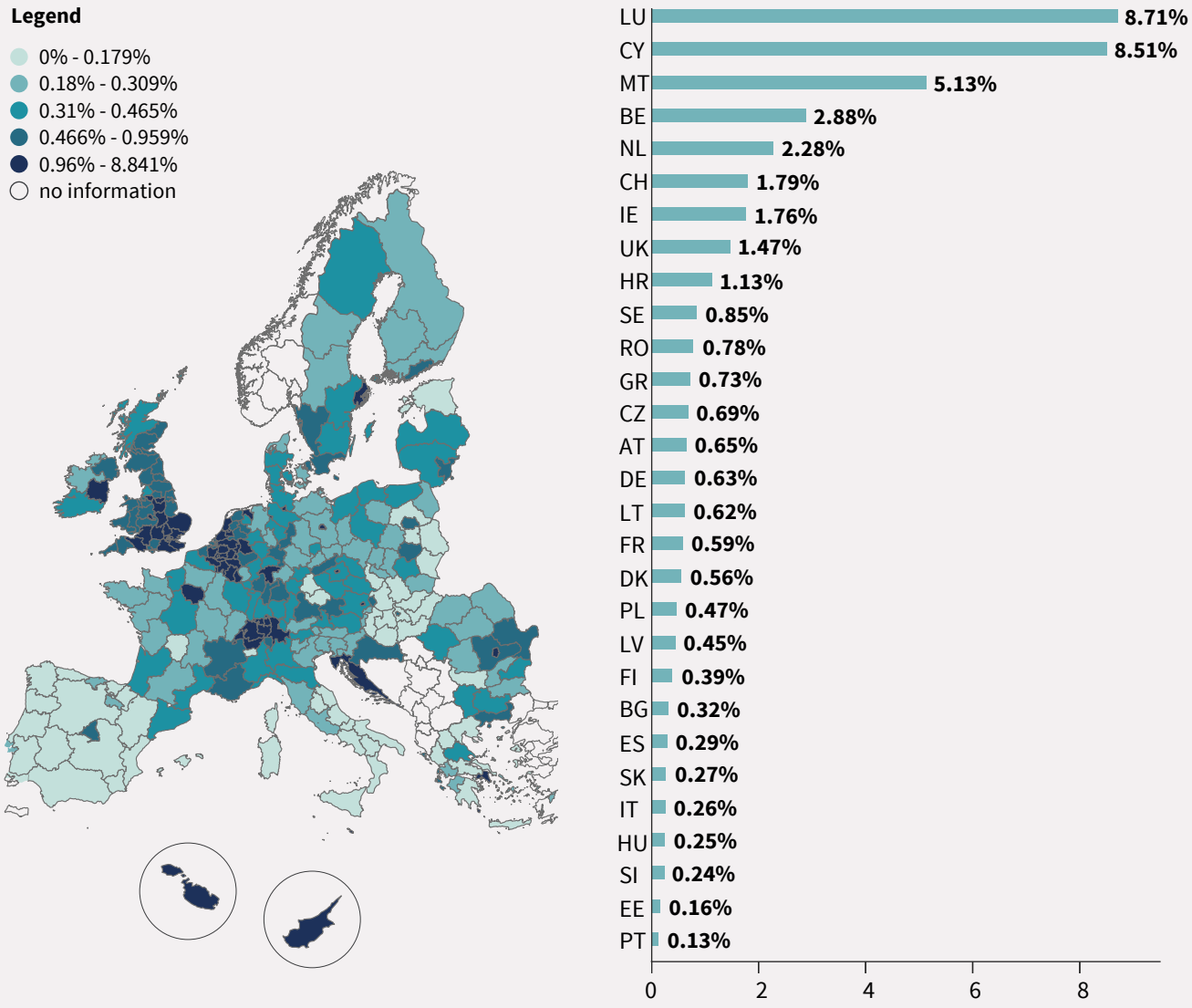
5. EU27 + UK and Switzerland.

6. The following 'blacklists' and 'greylists' were considered within the scope of the analysis: (1) EU lists of non-cooperative jurisdictions for tax purposes (updated 8th November, 2019), (2) Financial Action Task Force black list of non-cooperative jurisdictions and 'grey list' of jurisdictions under increased monitoring in the global fight against money laundering and terrorist financing (October, 2019 statement). See section 3.2.1 for further details.

- Within eight of the analysed European countries[7], 55,352 companies out of 27million (0.2%) are either target of **sanctions**[8] or **enforcement**[9] themselves or are linked to entities and/or individuals included in a sanction list or involved in enforcement cases.

- The analysis demonstrated that companies displaying **anomalies in their ownership structures** are more likely to be related to sanctions and enforcement.

Figure 1 – Percentage of companies with ownership links to blacklisted/greylisted jurisdictions, EU27 + UK and CH (2019)



Source: UCSC-Transcrime's elaboration of Bureau van Dijk – Orbis data, and EU and FATF black and grey lists (2019)

7. Italy, France, Spain, Belgium, Cyprus, Luxembourg, Malta and the Netherlands.

8. Inclusion in one or more global screening and sanction lists issued by various institutions, including, among others: the EU, the US Office of Foreign Assets Control (OFAC), UN, the Bank of England, the US Federal Bureau of Investigation and the US Bureau of Industry and Security (BIS).

9. Enforcement provisions (e.g. arrests, judgments) and court filings around the world were collated by LexisNexis from various sources, including national law enforcement reports, press releases and other statements from public authorities.

2. The DATACROS prototype tool

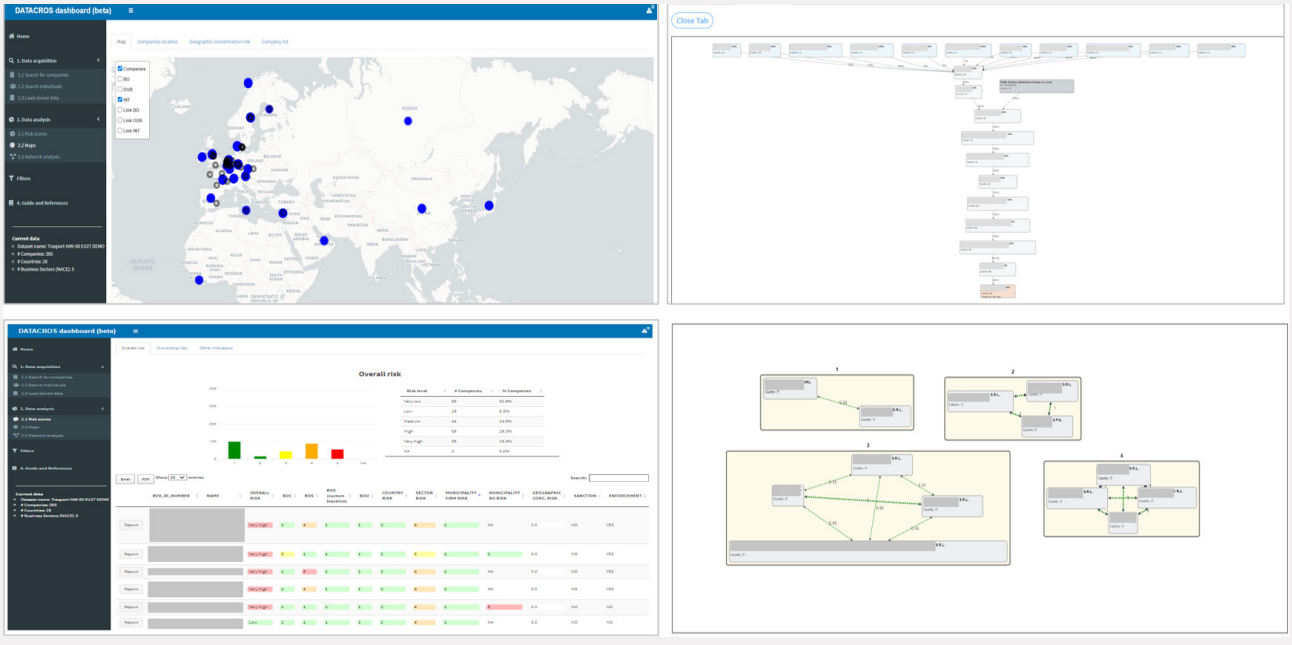
DATACROS produced a prototype tool for conducting risk assessment of legitimate companies, which is capable of detecting anomalies in firms' ownership structure that are indicative of a high risk of collusion, corruption and money laundering.

a. Restricted Area

The Restricted Area of DATACROS is a real-time prototype analytical platform with EU coverage (encompassing 44 countries and about 70 million companies), specifically designed for Law enforcement agencies (LEAs), Anticorruption Agencies (ACAs), Financial Intelligence Units (FIUs) and Tax Authorities (TAs), to support the identification of companies at high risk of corruption, money laundering, tax fraud and other financial crimes. The prototype tool consists of the following features:

- **European cross-border coverage**: it comprises data sources covering the entire EU[10], which, in turn, allows researchers and practitioners to both tackle the transnational nature of organised and financial crimes and to reconstruct cross-border ownership links among firms, entities and individuals;
- **Know-how of criminal schemes**: it exploits the extensive knowledge of criminal schemes generated by Transcrime over more than 25 years of publishing scientific research within high-quality academic journals;
- **Compliance with personal privacy and law enforcement procedures**: It has been designed with the help of legal experts and in accordance with *privacy-by-design* and *by-default* principles (see Chapter 5 for details on the Data Protection Impact Assessment that was conducted).
- **Frontier predictive approaches**: the prototype tool complements traditional approaches (e.g. sanctions list checks) with **innovative machine learning algorithms**, in order to identify hidden patterns and red flags. The risk indicators and algorithms included in the tool have demonstrated a **strong predictive power** for identifying companies (and owners) under sanctions or enforcement. Indeed, the models correctly predicted **83% of companies** targeted by sanction measures and **88% of companies** whose owners were subject to sanction measures (see section 4.1.2 for details).

Figure 2 – Examples of visualizations produced by the DATACROS Restricted Area prototype tool.



10. Company information: Bureau van Dijk – Orbis Europe (encompassing 44 countries and around 70 million companies); Sanctions, enforcement cases on firms: LexisNexis WorldCompliance (coverage: 1.2+ million profiles of entities worldwide)

Our partners in the project (AFA, CNP and IRPI) have reported a **high level of satisfaction** with the tested tool (avg. satisfaction rate: **4.3** out of 5) and have declared that they are highly likely to adopt DATACROS in the future (avg. likelihood: **4.3** out of 5). All Partners declared that **they would recommend** DATACROS Restricted Area to similar institutions.

As well as the positive feedback received by our project partners, the DATACROS tool has also been presented and demonstrated in several meetings and webinars to relevant networks of stakeholders (e.g. AMON – Anti-Money Laundering Operational Network, CARIN - Camden Asset Recovery Inter-agency Network, NCPA – Network of Corruption Prevention Authorities). Several trials have been initiated with public agencies in the law enforcement and anti-corruption domain.

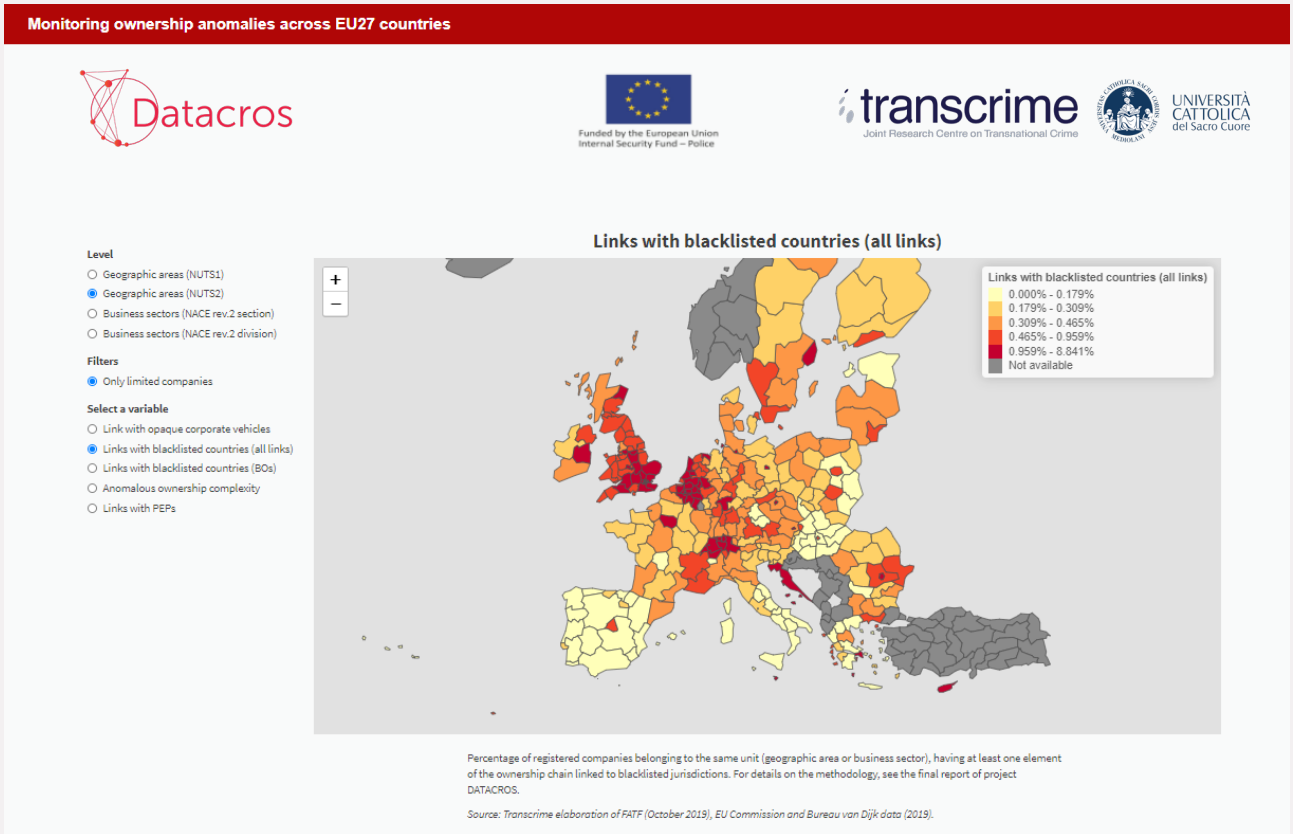
b. Public Area

The project also produced a dashboard for monitoring ownership anomalies across 29 European countries[11], regions and business sectors at an aggregate level. This is based on the aforementioned aggregate level analysis (Section 1). The Public Area is freely accessible to everyone at this link: https://datacros-public-area.app.crimetech.space/

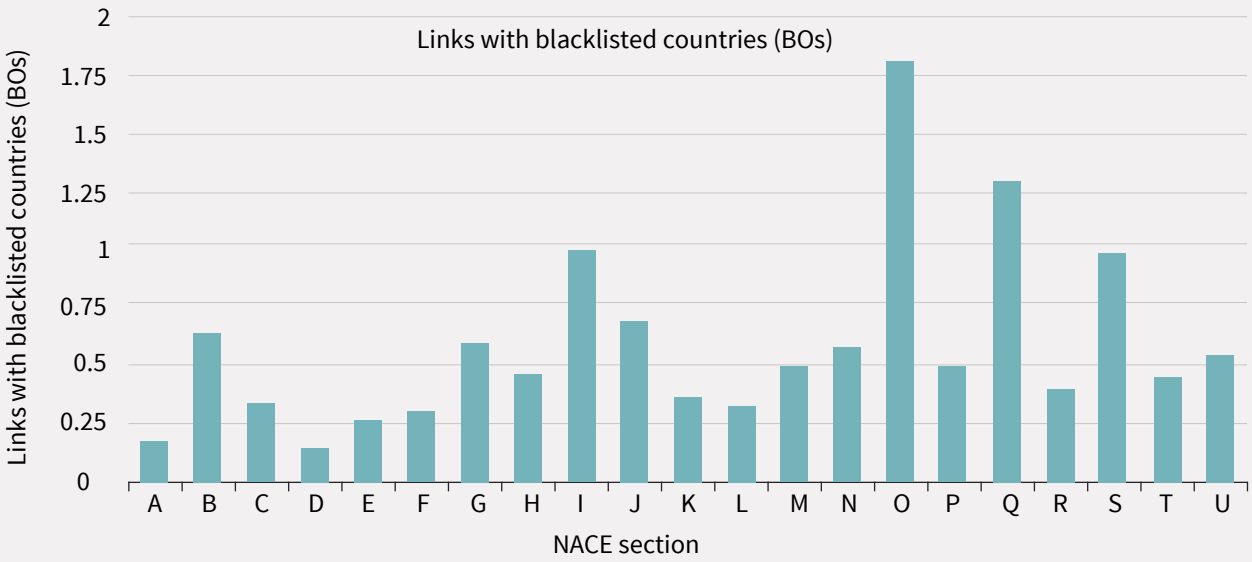
The dashboard includes **interactive maps, charts and statistics** on European businesses, with respect to the following features:

- **Anomalous complexity** of corporate ownership structures;
- Corporate ownership links with **blacklisted/grey-listed jurisdictions**;
- Links with **opaque corporate vehicles**;
- Links to **sanctions** and **enforcement**;
- Links with **PEPs**.

Figure 3 - Examples of visualizations produced by the DATACROS Public Area prototype tool. Representation of ownership anomalies at the country level (left) and sector level (right) , EU 27 + UK and Switzerland (2019)



11. EU27 + UK and Switzerland.



Conclusions and policy recommendations

The opacity of corporate ownership has become a central issue in discussions around global financial crime patterns over the last 15 years. Several measures have been implemented worldwide in order to increase the transparency of firms and their owners, most notably, the establishment of BO registers. However, despite its centrality within these debates, empirical evidence and knowledge around the topic remains limited to a handful of case-studies, while there is a complete absence of large-scale analyses. Moreover, there is a lack of tools that are specifically designed for risk assessment and risk monitoring of firms by public authorities (e.g., LEAs, FIUs, ACAs, TAs).

Project DATACROS has started to address these gaps, by:

- **Proposing an innovative analytical approach** for measuring the opacity of corporate ownership through a set of aggregate risk indicators at the macro level. The analysis we conducted indicates that even **strong and stable economies** within the EU are vulnerable in terms of **corporate opacity and other red flags**.
- **Developing a prototype tool that supports the investigation and risk assessment** of companies potentially involved in corruption, collusion or money laundering schemes. A survey conducted for the purposes of the project confirmed that there is a **strong need among public authorities** in the EU **for a technological solution of this kind**. Although the prototype was based on a database that solely focused on the EU, it was successfully tested by project partners and subsequently requested by a broader set of national and international LEAs and ACAs, which also provided very positive feedback.

These findings lead us to suggest the following recommendations.

Research recommendations

1. **To improve the study of how legitimate structures are misused by organised crime and corruption**: further research shall be produced on the patterns which characterise the businesses misused by organised criminals, and in particular on the variety of ownership structures, legal forms, jurisdictions most frequently employed, so as to identify vulnerabilities to be addressed by future policies (e.g. in the area of company law, AML, anti-corruption).

2. **To improve knowledge of emerging illicit schemes**: further research efforts are required to advance knowledge around the new – and underexam-

ined - financial crime schemes that have emerged with the Covid-19 pandemic. Particular attention should be dedicated to investigating potential illicit conducts and fraud schemes in public procurement procedures for accessing public funds by EU MS and by the European Union.

3. **To improve the mapping of high-risk areas/sectors**: future projects in this area should aim at advancing the understanding of who are the owners of EU companies, but also how they exercise control, to better understand which companies may be at risk of being misused to cover financial crime and other illicit schemes. DATACROS results show that anomalies concentrate in space (in certain EU regions) and across industry (some sectors are more vulnerable than others). Improving and repeating the monitoring exercise could help understanding how risks evolve and change, and how they move across territories.

Policy recommendations

1. **To facilitate integration of company information across EU MS**: the DATACROS analysis shows high levels of ownership interconnections among businesses in the European Union and beyond. This supports efforts and interventions by EU governments and the European Commission in facilitating the integration of business registers across EU MS, and to strengthen existing initiatives in this sense (e.g. the Business Registers Interconnection System infrastructure - BRIS[12], and the Beneficial Ownership Registers Interconnection - BORIS).
2. **To reduce asymmetries in terms of opacity of businesses**: the analysis conducted highlights great differences across business sectors and geographic areas in terms of concentration of companies with anomalous ownership characteristics. Therefore, the results of the project support efforts and interventions by European institutions for harmonising regulations and transparency requirements in the EU (e.g. 4th and 5th AMLD).
3. **To provide supervisor with data analytics solutions**: available data analytics solutions and risk indicators can increase the effectiveness of monitoring and supervision of ownership opacity, rather than overburdening businesses with regulation.
4. **To support public authorities with IT tools**: we recommend that the EU supports the development and improvement of tools which respond to the needs by public authorities identified in Section 2.2, in order to guarantee: a) *more powerful risk assessment algorithms* and richer data sources; b) a *wider set of risk indicators*; c) a more *integrated approach*, by extending the use of the tool to other stakeholders (e.g. FIUs, TAs and competition authorities); d) *enhanced security*, both in terms of IT and personal data protection.
5. **To improve exchange and cooperation among public authorities**: as also highlighted by the new SOCTA 2021, current criminal schemes entail cross-links among corruption, money laundering, organised crime and tax fraud. This calls for the EU to support activities that promote communication, coordination and cooperation among the wide variety of stakeholders active in the fight of corruption, money laundering and other financial crimes (LEAs, ACAs, CAs, FIUs, Tax Agencies, Investigative journalists and civil society NGOs). The aim of these activities should be to: a) *exchange information on crime schemes* and anomaly indicators; b) *share best practices* on investigations and intelligence activities; c) *design integrated approaches* for early-detecting cross-links between corruption, collusion, bid-rigging, organised crime; d) *enhance communication* among public authorities and civil society.

12. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Business+Registers+Interconnection+System

1. Introduction

Project DATACROS was co-funded by the European Union Internal Security Fund - Police (ISFP-2017-AG-CORRUPT-823792).

The project lasted two years (March 2019-February 2021) and was coordinated by Transcrime – Università Cattolica del Sacro Cuore. The partners were:

- Agence française anticorruption (AFA, France)
- Cuerpo Nacional de la Policia (CNP, Spain)
- Investigative Reporting Project Italy (IRPI, Italy)

Bureau van Dijk contributed as data partner.

For details on the consortium and for other news related to the project, visit: www.transcrime.it/datacros/.

1.1 Background, objectives and impact

There is extensive evidence indicating that **legitimate companies** play a crucial role in terms of both facilitating corruption schemes and money laundering of illicit proceeds. Identifying anomalies and red flags based on specific characteristics of companies can help our understanding and detection of risks of corruption or other financial crimes. For this purpose, project DATACROS provided:

1) An aggregate analysis of ownership anomalies across Europe. Overall, Transcrime analysed the ownership structure of 56 million companies across 29 European countries[13]. By exploiting unique information from the dataset Bureau van Dijk - Orbis Europe and other sources (see details in section 3.1.2), the analysis sought to assess the distribution of opaque and anomalous companies across EU territories and sectors.
2) A **prototype tool for risk assessment of legitimate companies**, which is capable of detecting anomalies in firms' ownership structure that are indicative of a high risk of collusion, corruption and money laundering. The **DATACROS prototype tool** includes two distinct environments that serve two different functions:
    - **Restricted Area**: a real-time analytical platform that is only accessible to authorised users (e.g., ACAs, LEAs), for investigating anomalies in EU firms' ownership structures and conducting risk assessments;
    - **Public Area**: a dashboard that is accessible to everyone, for monitoring ownership anomalies across EU27 countries, regions and business sectors at an aggregate level.

The project's outputs can benefit a wide range of stakeholders within the EU and beyond, by:

- Enhancing **police investigations and judicial authorities'** ability to prosecute corruption cases and the laundering of its proceeds, especially cross-border cases;
- Improving the ability of public authorities to detect **cross-links between corruption, tax crime, organised crime and fraud**;
- Allowing **investigative journalists, NGOs and the entire civil society** to check anomalous interactions between businesses, politics and public administration, and expose instances of corporate opacity;
- Increasing the effectiveness of cartel detection by **Competition Authorities**, particularly within public procurement.

13. EU27 + UK and Switzerland.

1.2 Structure of the final report

The final report is structured as follows:

- **Chapter 2** provides a review of the literature and evidence pertaining to the exploitation of legitimate companies for the purposes of concealing corruption and other financial crimes (section 2.1). It then discusses gaps in law enforcement and public authorities' capability to tackle corruption and financial crime though risk assessment and tracing of companies, before proceeding to delineate the results of a survey conducted amongst EU public authorities, which reported a strong demand for technological solutions in this field (section 2.2);
- **Chapter 3** presents the analysis that was conducted to highlight the macro-level distribution of ownership anomalies across EU27 geographical areas and business sectors, and a comparative cross-country overview;
- **Chapter 4** elucidates the technological solution developed during the project, namely the **DATACROS prototype tool**, discussing its two different environments for investigating and conducting risk assessments of companies (**Restricted Area**, section 4.1), and for civil oversight (**Public Area**, section 4.2);
- **Chapter 5** outlines the strategy that was adopted for managing ethical, privacy and data protection issues;
- **Chapter 6** discusses the key messages emerging out of the project, before proceeding to then describe the road ahead.

2. The problem and the gaps to be addressed

2.1 The problem: ownership anomalies and financial crime

There is widespread evidence that **legitimate companies** play a crucial role in terms of both facilitating corruption schemes and money laundering of the illicit proceeds (EFECC 2020).

Complex and opaque corporate ownership schemes are widely used to conceal illicit profits and are on the increase. According to the World Bank, 70% of corruption cases between 1980 and 2010 involved **anonymous shell companies** (van der Does de Willebois et al. 2011). Scandals such as the "Panama Papers" (ICIJ 2016) and "Paradise Papers" (ICIJ 2017), among others, uncovered a dense and **opaque** network of companies and trusts that were established solely to conceal the identity of BOs and the criminal origin of their proceeds. In many other cases, trusts and other opaque **legal arrangements** are misused, wittingly or otherwise, for money laundering activities (FATF 2010). Numerous police investigations[14] have confirmed that **shell companies** act as covers for criminal activities and help to facilitate pseudo-legal sales, trade-based money laundering, false invoicing and fraud schemes. Corporate structures characterised by **anomalous ownership** are also exploited to conceal money laundering of proceeds from human trafficking (FATF 2018, see Case Study 1). There is also evidence indicating the increased **cross-border nature**[15] of money flows schemes, insofar as criminals exploit bank accounts, intermediaries, and firms that are located in different jurisdictions, including non-cooperative tax havens.

Finally, **PEPs**[16] may abuse their position to accept and extort bribes, misappropriate state assets, and subsequently use legitimate companies, as well as domestic and international financial systems, to launder the financial gains.

The problem of illicit schemes involving legitimate companies has been widely acknowledged and addressed by **EU law**. In the last decade, **several measures** have been implemented to increase the transparency of legitimate companies, with the most important of these probably being the establishment of BOs registers in several countries across the globe, as well as within all EU Member States (MS) as per the obligations set out in the **4th and 5th AML Directive** (European Parliament and Council of the European Union 2015; 2018). Despite these aforesaid advancements, extant knowledge on ownership schemes for corruption and financial crime is not particularly developed, primarily due to a lack of data.

Moreover, the **Covid-19 pandemic** and the attendant introduction of recovery plans by EU MS, not to mention the organisational efforts required to supply the vaccines, have presented criminal networks with additional opportunities to drain public resources, by exploiting legitimate companies for the simultaneous use of corruption, fraud, tax crime and infiltration of public funds (UNODC 2020; FATF 2020).

14. See, for example, police investigations such as 'Volcano' or 'Matrioska', which are discussed at length in Transcrime's project MORE report (Savona and Riccardi 2018). See also Europol (2018).

15. See, for example, operation 'Webmaster' (Europol 2019) and operation 'Gambling' (Gdf 2015).

16. "Individuals who are, or have been, entrusted with prominent public functions, their family members, and close associates" (FATF 2013a).

Ownership changes and anomalies observed during the Covid-19 pandemic

In October 2020, Transcrime conducted an analysis of **Italian companies** that changed BOs[17] between the period April to September 2020, which coincided with the first wave of lockdowns to help combat the spread of Covid-19 (Transcrime for Corriere della Sera, 2020).

The results of the analysis showed that, despite a decrease in ownership changes compared to 2019 (43,688 companies changed one or more BO(s), which represented a decrease of 38.7% with respect to the previous year), **more ownership anomalies were observed amongst the new owners**.

In particular:

- **Ownership links with blacklisted/greylisted countries**: 1.3% of these companies have shareholders or BOs registered in blacklisted (or grey-listed) countries[18]. This percentage is **4.5 times higher** than the average for Italian companies;
- **Ownership opacity**: 1.4% of these companies are controlled by a trust, a fund or another legal arrangement that conceals the identity of the individual BO. This percentage is **10 times higher** than the average for Italian companies.

The review of extant literature and the analysis of investigative cases allow for the identification of several anomalies in corporate ownership structures. The next section discusses the following anomalies: 1) Anomalous complexity of ownership structures; 2) Ownership links with high-risk countries; 3) Ownership links with opaque corporate vehicles; 4) Ownership links to PEPs; 5) Ownership links to entities that are subject to sanctions or enforcement.

Anomalous complexity of ownership structures

Criminals can exploit complex business ownership structures to conceal their identity, including the following:

- **Multiple layers of shareholding**: several consecutive layers of interlocking shareholding links (so-called 'Chinese boxes', Transcrime 2018);
- **Circular ownership schemes**: two (or more) companies own (directly or indirectly) shares in each other, therefore jeopardising the identification of BOs with standard shareholding thresholds (Knobel, 2019).

Complex structures pose manifold challenges to investigations and due-diligence processes, in turn, making it more difficult and costly to identify ultimate BO(s), especially when the ownership chain is cross-border and involves entities located in secrecy jurisdictions. Complex ownership chains have been employed in several money laundering, corruption and financial crime cases. 'Chinese boxes' (see Case study 2 below), for instance, are extensively employed for a range of criminal offences, including VAT and tax fraud (Borselli 2011; Hangacova and Stremy 2018), in which either falsified or non-existent financial transactions need to be concealed. Numerous examples can be found in the final report of project MORE (Transcrime 2018).

Other studies have shown the employment of complex ownership schemes for collusive or corruptive behaviours **in public procurement** (Fazekas, Tóth, and King 2013a). These networks can be used to manipulate public procurement, by making bids in a coordinated way and increasing the likelihood of being awarded contracts (Conley and Decarolis 2016; Imhof and Karagok 2017). In fact, cross-ownership links are considered to be relevant red flags for collusion and fraud in this sector (OLAF 2017).

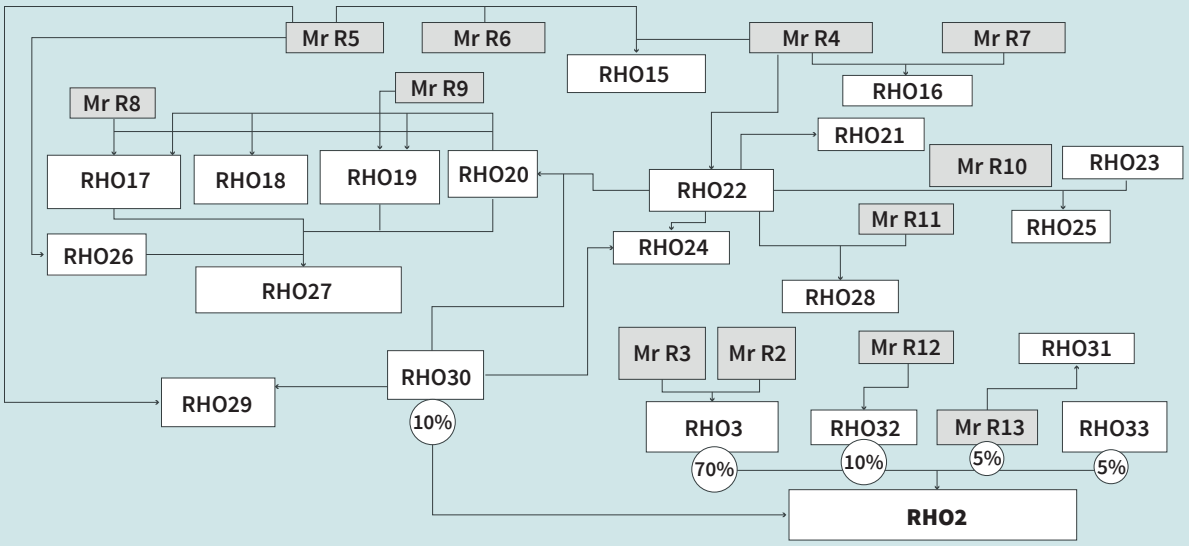
17. Transcrime's elaboration of Bureau van Dijk - ORBIS data (2020)

18. Black and grey lists considered: FATF AML black and grey lists, EU black and grey list on non-cooperative countries for tax purposes (see section 3.2.1 for further details on blacklists)

Case study 1: 'Chinese boxes' schemes

The 2016-17 investigation ***Security*** (by the Italian Anti-mafia District Directorate) revealed the infiltration of legitimate businesses by an organised criminal group (OCG) connected to a Cosa Nostra family (Transcrime 2018). The OCG bribed some retail managers so as to be able to obtain illicit contracts to provide logistics and security services to a supermarket firm, while, simultaneously, systematically issuing false invoices and conducting VAT fraud on a massive scale. The infiltration occurred in the traditional area of influence of the mafia family (Catania, in Sicily), as well as in non-traditional Italian northern regions (Lombardy and Piedmont).

The OCG employed a complex network of figureheads and shell companies (see figure below, in which all firms and owners have been anonymised), with several interlocking ownership links, frequent changes in the legal forms and structures, legal names and registered offices. In order to complicate the shareholding structure yet further, several circular ownership patterns were created. The criminals liquidated the companies when they accumulated excessive tax payables, and soon incorporated new firms to replace the previous ones.



Case study 2: Cross-ownership and collusion in public procurement

In 2018, the Operation 'Comune Accordo' uncovered a network of companies systematically rigging public contracts in the municipality of Corigliano Calabro in the South of Italy (Natrella 2018). In total, the cartel manipulated public contracts for approximately EUR 9 million. The companies presented multiple offers within an agreed range of values in order to increase the probability that they would win to the detriment of the other competitors. Once the tender was awarded, the profits were then split between the members of the cartel: the winning company received 5% of the value of the contract, and the works were subcontracted to the other members without any official authorisation. Interestingly, the 50 companies involved were controlled by the same owner, despite being formally managed by different individuals. Thus, they participated in public contracts and only formally competed against one another. The investigation led to the arrest of 23 people, who were held responsible for various crimes, including bid-rigging, fraud in public supplies, fraudulent misrepresentation, abuse of office and corruption.

However, it is important to underscore here that **the complexity of ownership is not anomalous per se**. In fact, in some cases complex structures are wholly justified on the grounds of the heterogeneity of the business activities carried out by the firm, its geographical reach or financial strategy. Anomalies **arise when companies have an unnecessarily complex corporate structure**, with respect to both the nature of their activities and their characteristics (e.g. a small retail company with limited annual turnover, controlled by a BO through several interlocking layers of ownership). In DATACROS, Transcrime has developed metrics to highlight at what point the complexity of an ownership structure can be said to be statistically anomalous (see Chapter 3).

Ownership links with high-risk countries

The fact that countries with **low levels of financial** and **corporate transparency** are used to conceal the proceeds of financial crime is well-established (Does de Willebois, Van der et al. 2011; FATF 2014; 2012; van Duyne and van Koningsveld 2017a; Garcia-Bernardo et al. 2017a; Aziani, Ferwerda, and Riccardi 2021). Criminals exploit businesses established in these jurisdictions, because it makes it easier to conceal both the criminal origin of their proceeds and their identity as BOs.

Case study 3: Tax fraud and links to tax havens in the Vieux port of Marseille

For years, an OCG from Marseille, France, controlled several transport companies active in the Vieux-port of Marseille, and, most notably, had a monopoly over the ferries that connected the Frioul archipelago (Le Parisien 2009). The investigation – which brought sentences of up to two-years imprisonment - revealed that the OCG set up a complex fraud and money laundering scheme, including a double ticketing system, which also involved off-shore companies registered in the British Virgin Islands.

The scheme allowed the OCG to conceal several million euros from TAs from 1996 to 2006. The group was ultimately accused of tax fraud, money laundering, bankruptcy fraud and asset misappropriation (Tribunal de Marseille 2009).

Nevertheless, **identifying these jurisdictions** is not a straightforward exercise, and there remains a lack of consensus around the answer to this question. For instance, the Financial Action Task Force (FATF) issues (and periodically updates) a list of non-cooperative countries from an AML perspective, or of countries under increased monitoring.[19] The FATF black and grey lists delineate those countries that, albeit to different extents, are considered to have deficient anti-money laundering (AML) and counter-financing of terrorism regulatory regimes. These lists are produced through conducting an in-depth assessment of both a country's level of technical compliance with the FATF Recommendations and their ability to effectively implement AML requirements (FATF 2013b). However, several scholars have pointed out biases in the assessment methods used by the FATF (Halliday, Levi, and Reuter 2014; Levi, Reuter, and Halliday 2018; van Duyne and van Koningsveld 2017b). Similar blacklists have also been issued at the EU level, both in the AML domain – i.e. the list of 'high-risk third countries' produced by the European Commission (European Commission 2020b) - and in the tax domain – i.e. the EU list of non-cooperative jurisdictions for tax purposes (European Commission 2020a). Indeed, these official blacklists are not always aligned with the evidence stemming from

19. The first (the so-called 'Blacklist') includes countries that are publicly identified in the statement "High-Risk Jurisdictions subject to a Call for Action" (previously entitled "Public Statement"). The second ('Grey-list') includes "Jurisdictions under Increased Monitoring".

judicial and police operations, and from major media investigations such as *Panama Papers* or *Paradise Papers*. Other measures of financial secrecy and money laundering risk across countries exist, chief among which is the Financial Secrecy Index (FSI), which is a composite indicator issued by the Tax Justice Network (TJN) every two years (Tax Justice Network 2018; 2020). However, it is important to stress that all these rankings and lists are subject to methodological or political biases (see Riccardi 2020 for a comprehensive review).

In DATACROS, Transcrime has developed a novel methodology through which to measure ownership links to firms located in high-risk jurisdictions (see Chapter 3).

Ownership links with opaque corporate vehicles

Another risk factor that can be identified in the ownership chain of legitimate companies is the presence of legal arrangements, such as **trusts, fiduciaries, foundations** and certain types of investment funds, which, by statute, do not allow for the identification of BOs. **Trusts**, for instance, are legal arrangements introduced by common law jurisdictions, in which the legal title and control of an asset are separated from the beneficiary of that asset (Law, 2009). In a typical trust, a "settlor" transfers the legal title of assets over to a "trustee" who, in accordance with the declaration of trust, must hold these assets for the benefit of certain "beneficiaries". Despite the legitimate purposes for which trusts were conceived, **the separation of legal and beneficial ownership** makes trusts useful for those seeking to distance and disguise their connection with property that has been used for, or generated via, criminal activities. Furthermore, in many jurisdictions there is no registration requirement for a trust, since they are viewed as private arrangements and their existence is not a matter of public record. Trusts are therefore well suited to be used as secrecy vehicles by those wishing to launder the proceeds of illicit activities (Riccardi and Savona 2013). In these cases, they are often used as the last layer of secrecy in complex corporate structures spanning multiple jurisdictions, with trust assets, Trust and Company Service Providers (TCSPs) and BOs located in different countries.

Case study 4

Diepreye S. P. Alamieyeseigha was a Nigerian politician who was Governor of Bayelsa State in Nigeria from 1999 to 2005. He was arrested in London in September 2005 by the London Metropolitan Police on suspicion of money laundering offences (van der Does de Willebois et al. 2011). At the time of his arrest, the Metropolitan police found about £1m in cash in his London home (registered in the name of a company). He returned in Nigeria after fleeing the UK - allegedly dressed as a woman- where he was impeached and dismissed from his political position. He was accused of participating in corrupt activities and enriching himself by tens of millions of dollars' worth of internationally held monetary assets and property holdings, often registered in the name of corporate vehicles (CVs). On July 2007, Alamieyeseigha pleaded guilty to all charges.

The misuse of trusts and corporate vehicles was an essential part of his scheme to obscure the ownership of his assets. Alamieyeseigha created at least five CVs to separate his identity from the legal ownership and control of several financial and real estate assets. Most of the CVs were private limited companies in several jurisdictions (Seychelles, British Virgin Islands, Bahamas, South Africa), managed through a variety of trusts and company service providers.

In particular, Alamieyeseigha settled "the Salo Trust" in the Bahamas, which in turn controlled a company called Falcon Flights Inc. In 2001, Alamieyeseigha received on his UK account a deposit of US$1.5 million from a state contractor; the deposit was immediately converted into bonds and transferred to the portfolio holdings of Falcon Flights Inc. The existence of the trust separated Alamieyeseigha from beneficial ownership and control of the assets, adding another layer of complexity to those who would have tried to discover that he did own such assets.

There is **extensive evidence** on the employment of such legal arrangements in money laundering cases, ranging from laundering of grand corruption to the more recent Malaysia's 1MDB (Knobel 2019; van der Does de Willebois et al. 2011). The FATF and other institutions have previously stressed the threats posed by these legal arrangements (FATF 2006; 2010b; OECD 2001; HM Revenue & Customs 2010). As a result, BO identification has evolved in several countries in order to also allow the identification of BOs for legal arrangements (see, for example, IADB and OECD 2019; HM Revenue & Customs 2010). However, these measures have been criticised for allowing only formal identification of BOs, while scepticism over their effectiveness remains, especially in the case of certain investment funds (Knobel 2019) and types of foundation, such as the Dutch *stichting* (OECD 2019b; Netherlands Chamber of Commerce - KVK 2020).

In DATACROS, we have developed metrics to detect and measure the extent of ownership links of firms with opaque corporate vehicles (see Chapter 3).

Ownership links to Politically Exposed Persons (PEPs)

While there is no global definition of a PEP, most countries have based their definition on the one proposed by the FATF (FATF 2013a), which defines a PEP as "*an individual who is or has been entrusted with a prominent public function*". Due to their role and influence, it is recognised that PEPs are in positions that **can potentially be abused for the purpose of committing money laundering and related predicate offences**, such as corruption and bribery, as well as conducting activities related to terrorist financing (Rose-Ackerman and Palifka 2016; World Bank 2011). **The evidence-base** for PEPs exploiting legitimate businesses for illicit schemes is sizeable. Malaysia's former prime minister, Najib Razak, was linked to the multibillion-dollar 1MDB scandal (Agence France-Presse 2015), in which billions of dollars were allegedly looted from a state fund set up to promote development. In 2019, an OCCRP investigation uncovered the Troika Laundromat (OCCRP 2019), a $8.89 billion scheme that allegedly allowed corrupt Russian politicians and organised-crime figures to launder funds, evade taxes, hide assets abroad and carry out other illegal activities. In the ICIJ leaked datasets - Panama Papers and Paradise Papers - there were over 300 offshore companies linked to 140 PEPs in over 50 countries (Haberly 2020).

In light of the risks associated with PEPs, the FATF Recommendations and the 5th EU Anti-Money Laundering Directive (AMLD) require the application of additional AML/CFT measures to business relationships with PEPs. However, it is important to stress that these requirements are **preventive** in nature, and, as such, should not be interpreted as stigmatising PEPs for being involved in criminal activities.

Ownership links to entities subject to sanctions and enforcement

In some instances, ownership structures may include links with individuals or companies included in a **sanction list**, which designates the individuals, entities or countries that are prohibited from certain business activities or transactions. They are issued by numerous institutions, such as the United Nations, the EU, the US Office of Foreign Assets Control (OFAC), the Bank of England, the US Federal Bureau of Investigation, or other country regulators and LEAs. Sanctions seek to curb illegal activities, terrorist financing, nuclear and arms proliferation, and other activities deemed to be a threat to the security of a nation (King, Walker, and Gurulé 2018). Therefore, ownership links with **sanctioned entities can be considered a risk factor** that a firm is involved in illicit schemes. However, it is important to underscore here that sanctions, despite being issued at an individual level, as opposed to towards entire countries, are often geographically oriented against certain countries, and structurally biased to accomplish specific foreign policy and security goals (see Riccardi 2020 for a review). Therefore, such lists should be assessed carefully, and the presence of a ownership link with an individual or a company on these lists should not be automatically interpreted as meaning they are involved in criminal activities.

Moreover, companies may have owners or managers/directors with prior **enforcement** provisions (e.g. arrests, judgments) or who have been reported in media articles of being involved in negative events that potentially link them to illicit activities (e.g. money laundering, financial fraud, drug trafficking, financial threat, organized crime, financial terrorism). Therefore, to conduct a comprehensive risk assessment of a company, it is important to check if all the related entities have either prior enforcement provisions or adverse media coverage that could potentially signal a risk of being connected to illicit schemes.

2.2 The gaps

2.2.1 Context

As described in the literature review in section 2.1, criminals adopt increasingly sophisticated methods to move their illicit money across the globe, often by exploiting legitimate corporate structures. Investigative authorities have a hard time keeping pace with the criminals, which ultimately impacts on their capacity to trace and seize illicit proceeds. Indeed, Europol estimated[20] that **EU authorities annually confiscate** only 1.1% of total criminal profits across the EU, which is estimated by Transcrime (2015) to amount to EUR 110 billion. This results in a net loss for the economy and society, not to mention additional costs for citizens and businesses. This loss builds, among other things, upon specific weaknesses in the capabilities of European law enforcement and judicial authorities, namely:

- **Lack of knowledge** of how criminals exploit legitimate business structures and move illicit money across different domains (see section 2.1 for some examples). Despite the notable interest in this topic, the empirical evidence and knowledge remains limited to a handful of case-studies, while large-scale analyses are wholly lacking, with the exception of some recent work (Garcia-Bernardo et al. 2017b; Aziani, Ferwerda, and Riccardi 2020; Riccardi, Milani, and Camerini 2018a; Ferwerda and Kleemans 2018). One of the reasons for the lack of empirical research is the shortage of reliable corporate ownership data;
- **Difficulties** in **identifying cross-border links** among firms, entities and individuals, also due to the challenges of international cooperation, especially when secrecy jurisdictions and opaque corporate ownership structures are exploited. The identification of individuals who ultimately control a business - the so-called BOs – has been facilitated by the establishment of Ultimate Beneficial Ownership (UBO) registers, introduced by the 4th (and then 5th) EU AMLD (European Parliament and Council of the European Union 2015; 2018). Based on the 5th EU AMLD, EU MS have to make the UBO registers publicly accessible by the beginning of 2020. However, a legitimate interest is still required in order to be able to access the UBO registers for information on trusts and such like (Global Witness 2020). While most of the registers have been implemented by MS in 2020, doubts remain over their level of accessibility, as well as the limitations and exclusions posed by privacy and data protection regulation. Moreover, it is difficult to verify the accuracy of the information provided by companies themselves, and, hence, it remains entirely possible that those individuals who need to conceal their identity will continue to make use of figureheads and fictitious BOs.

20. See Europol's EFECC launch report (2020) (https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime) and Europol (2016), which estimates that only 1.1% of criminal profits are confiscated yearly by EU authorities (https://www.europol.europa.eu/publications-documents/does-crime-still-pay)

- **Difficulties** in properly **managing all the digital evidence collected**, and making it compliant with governing laws at both the EU and national level, with specific reference to IT security and personal data protection requirements (e.g. those stemming from EU Directive 680/2016 and GDPR), so as to ensure its admissibility in court proceedings.

- **Lack of tools** specifically designed for LEAs, FIUs, ACAs and TAs for risk assessment and risk management of companies in the anti-financial crime domain. The solutions currently available on the market are **mostly designed for the private sector**, such as banks, financial institutions and other obliged entities involved in AML and compliance activities. In order to explore the existence of this gap, Transcrime **conducted a survey as part of project DATACROS in 2019**: the detailed results of the survey are reported in the next section.

2.2.2 Exploratory survey

In September 2019, Transcrime conducted an exploratory survey among potential stakeholders[21] of the DATACROS tool. The aim of the survey was to:

1. Verify the existence of **gaps** in terms of tools for risk assessment and risk management of companies in the anti-financial crime domain.

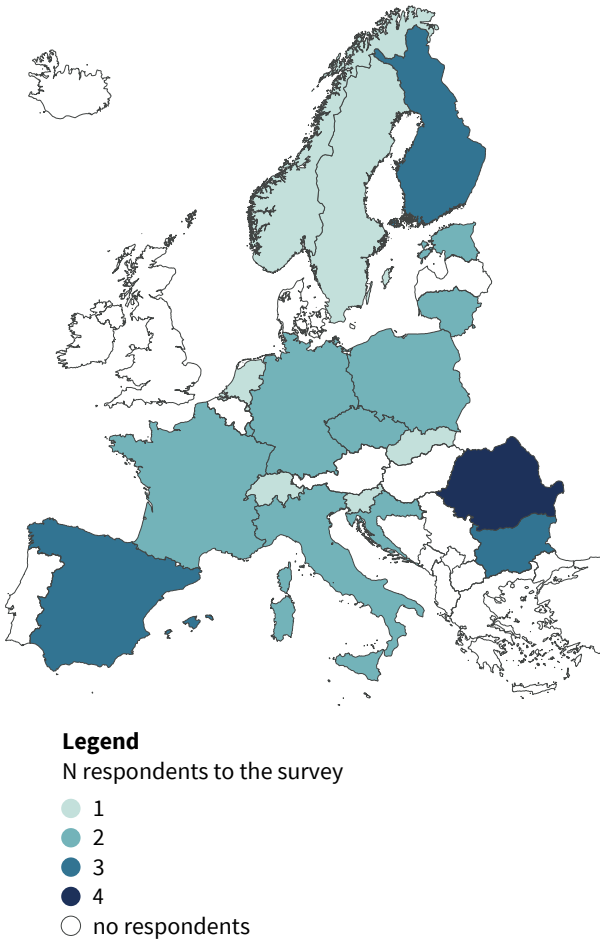
2. Understand the **operational needs** and **requirements** for developing the DATACROS prototype tool.

Respondents

Table 1 shows the number of respondents from each type of institution; in total, 37 authorities[22] from 19 countries responded to the survey.

Table 1 –Number of respondents (by type of institution) and the location of the responding institutions

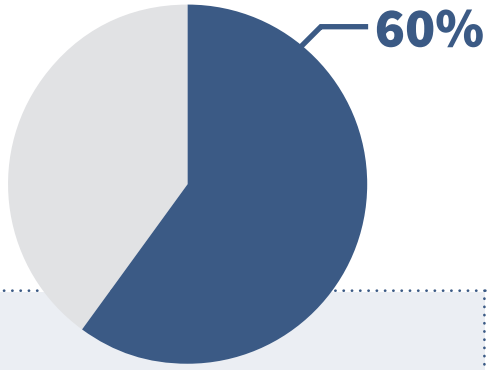
Type of institution	Contacted	Respondents
Police and other law enforcement agencies	95	20
Anti-corruption agencies	29	7
Competition authorities	29	5
Judicial authorities	29	2
Investigative journalists and NGOs	3	2
Tax Authorities	15	1
Total	**185**	**37**



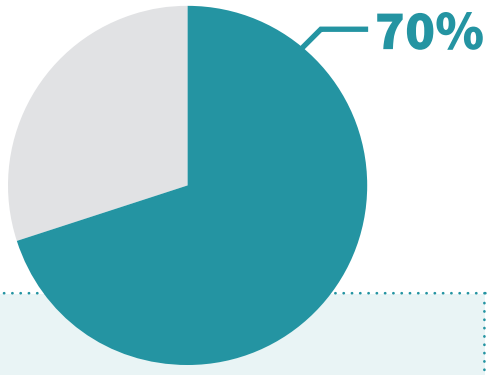
21. (1) Anti-corruption agencies (ACAs); (2) Police and other Law Enforcement Authorities (LEAs); (3) Competition Authorities; (4) Judicial authorities; (5) Tax authorities (TAs); (6) Investigative journalists and civil society organisations.

22. Out of a total of 185 that were contacted (average response rate: 20%)

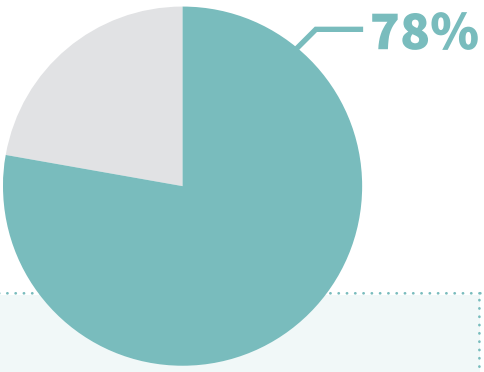
With regards to the **gaps and weaknesses** identified, the survey confirmed that:



60% of the respondents currently **do not use any software** when conducting investigations in the anti-corruption or anti-financial crime domain



70% of the respondents **would be interested in using software for firms' risk assessment**



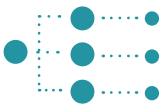
78% of the respondents still rely on **data provided by companies themselves** or **local registers**, while they do not use any global company data repositories.

The survey also identified the main **operational needs** and **requirements for the respondents' institutions**. The answers indicated a **strong interest** for **software solutions** capable of providing automatic analyses when conducting investigations or due diligence within the anti-corruption or AML domains. The **most relevant functions** required were:

BO identification (*All respondents*)

Identification of links among companies – shareholders and directors (*All respondents*)

Identification of ownership links with secrecy jurisdictions (*All respondents*)



Identification of anomalously complex ownership structures (*LEAs*)

Identification of links with PEPs (*Anti-corruption Agencies*)

Other functions suggested by respondents were:

- Analysis of the links between companies and sanctioned individuals or companies (All respondents)
- Analysis of geographical concentration of companies (All respondents)
- Possibility of customization of specific functions (All respondents)
- Analysis of the links with recently created or dissolved entities (All respondents)
- Analysis of bidding behaviour of companies (Competition Authorities)

3. Aggregate analysis of ownership anomalies

As described in section 2.1, there are several anomalies and risk factors based on the characteristics of companies, which can help us to understand and detect risks of corruption or other financial crimes, such as:

- Anomalous complexity of ownership structures
- Ownership links with high-risk countries
- Ownership links with opaque corporate vehicles
- Ownership links to PEPs
- Ownership links to entities subject to sanctions and enforcement

In order to advance extant knowledge on ownership opacity, Transcrime has developed ***risk indicators*** associated with the previously identified ***risk factors*** (Section 2.1) The analysis presented in the following sections allows for the measurement of ownership anomalies at the **micro** (i.e. firm) level, and assesses how they distribute across Europe at the **macro** (i.e. across business sectors and geographical area) level. In addition, the analysis explores the relation between the calculated indicators and certain contextual variables at the macro level (e.g. socio-economic variables, structural business statistics, financial secrecy, etc). Finally, a focus on the ownership anomalies displayed by companies participating in European public procurement, is reported in section 3.1.3.

Some selected findings from the analysis can also be freely explored through interactive maps the Public Area of the DATACROS tool (see section 4.2 for details), which is available via the link: https://datacros-public-area.app.crimetech.space/

3.1 Data and Method

Operationalisation

Building on the experience it gained in projects IARM and MORE (Savona and Riccardi 2017; Transcrime 2018), Transcrime has further developed a methodological approach to measure the opacity of business ownership at both the micro (i.e. firm) and macro (i.e. business sector and geographical area) level, by exploiting unique information from the dataset Bureau van Dijk - Orbis Europe and other sources (see details below). To achieve these objectives, the ownership anomalies and companies' red flags that are displayed in the table below are operationalised and measured as follows:

Table 2 – Risk factors considered in the analysis and operationalisation

Risk factor	Description	Operationalisation[23]
Complex corporate structure	A company presents a **complex ownership structure** that is not justified by its size or business sector	1. Reconstruction of full ownership chain of companies 2. Identification of peer groups (i.e. groups of companies with similar characteristics) 3. Calculation of BO distance of companies 4. Clustering of BO distance across peer groups for identification of statistical anomalies in the complexity of companies' corporate structure
Links to high-risk countries	A company presents **ownership links with high-risk countries**	1. Reconstruction of full ownership chain of companies 2. Identification of companies' owners/shareholders located in blacklisted/greylisted jurisdictions
Links to opaque corporate vehicles	A company presents **ownership links with opaque corporate vehicles** (trusts, fiduciaries, investment funds)	1. Reconstruction of full ownership chain of companies 2. Identification of companies' owners that are opaque corporate vehicles and do not allow for identification of BOs
Links to PEPs	A company has ownership **links with PEPs**	1. Reconstruction of full ownership chain of companies 2. Matching companies and individual names with PEP lists 3. Identification of companies' owners/shareholders that are PEPs
Links to entities subject to sanctions or enforcement	A company has ownership **links with entities with prior enforcement provisions or who are included in a sanction list**	1. Reconstruction of full ownership chain of companies 2. Matching companies and individual names with sanctions and enforcement lists 3. Identification of companies' owners/shareholders subject to sanctions or enforcement

Data

The exploited data includes:

1. **Business ownership data**: information on 56 million companies across 29 European countries[24] was retrieved from *Orbis Europe*, a dataset provided by Bureau van Dijk[25]. In order to guarantee both cross-country and cross-sector comparability, only limited companies with information on the ownership structure are included in the analysis – while the full results can be navigated in the Public Area[26] of the DATACROS tool. The resulting dataset contains information on **13.4 million companies** and around **20 million BOs**[27]. The coverage of ownership information is represented in Figure 4.

2. **Sanctions and enforcement**: information on companies and companies' owners that were either included in a sanction list or associated with enforcement cases are obtained from 8 countries[28] using *LexisNexis WorldCompliance* and matched with

23. See section 3.1.2 for further details.

24. EU27 + UK and Switzerland.

25. The extract provides a snapshot of European businesses as of June 2019.

26. https://datacros-public-area.app.crimetech.space/

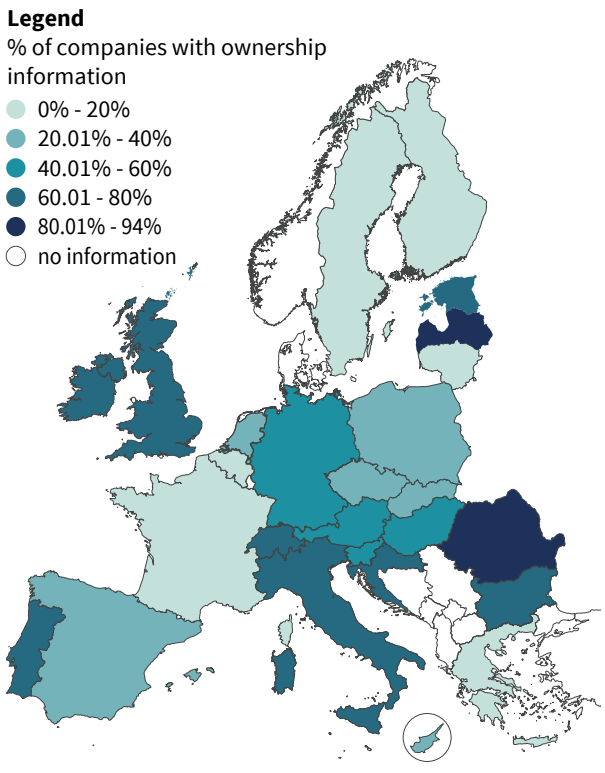
27. The BOs of a company (or entity) are those individuals who ultimately own or control it. Bureau van Dijk identifies them by reconstructing the ownership chain of the company, until finding natural persons with shareholdings above a certain level. Since there is no consensus on the notion of control, for the purpose of this study we set the minimum threshold at 10% of shareholding at each level of the company ownership chain. This threshold is in line with the current development of the EU AML Directives.

28. Italy, France, Spain, Belgium, Cyprus, Luxembourg, Malta, and the Netherlands.

Orbis data. This involves:

- *Enforcement lists*: companies and individuals with enforcement provisions (e.g. arrests, judgments) and court filings around the world, collated by LexisNexis from various sources including national law enforcement reports, press releases and other statements from public authorities. For the purposes of this analysis, all categories of crimes and predicate offences covered by LexisNexis are considered;
- *Sanction lists*: companies and individuals included in one or more of the global screening and sanction lists issued by the following institutions: the EU, OFAC, the United Nations, the Bank of England, the US Federal Bureau of Investigation, the US Bureau of Industry and Security (BIS) and others[29].

Figure 4 – Percentage of companies with available ownership information, EU27 + UK and CH (2019)



Source: Transcrime's elaboration of Bureau van Dijk – Orbis data (2019)

3. **Data on PEPs**: Data on PEPs are obtained from 8 countries[30] using *LexisNexis WorldCompliance* and matched with Orbis data. WorldCompliance covers 2 million structured profiles of PEPs globally. It adopts a PEP definition that is in line with FATF standards; specifically, the following categories are included as "primary PEPs": heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned enterprises, and senior political party officials. Moreover, other individuals are also included in the data as "secondary PEPs": these are individuals who are related to PEPs by hereditary, marriage, or civil partnerships, as well as individuals who are socially or politically connected to PEPs.

4. **Country blacklists**: the following black and grey lists are considered for the purposes of the analysis:
   - *Tax domain*: the EU list of non-cooperative jurisdictions for tax purposes updated as of 8th November, 2019 (European Commission 2019), which groups together countries that encourage abusive tax practices, and ultimately erode EU MS' corporate tax revenues (European Commission 2019);
   - *AML/CTF domain*: FATF lists[31] of non-cooperative jurisdictions (or jurisdictions under increased monitoring) in the global fight against money laundering and terrorist financing (FATF, October, 2019 statement). In particular, two lists are included:
     - *Call for action* (or so-called 'blacklist') identifies countries that are evaluated by the FATF as non-cooperative in the global fight against money laundering and terrorist financing, who are flagged as "Non-Cooperative Countries or Territories" (NCCTs);
     - *Other monitored jurisdictions* (or so-called 'grey-list') identifies jurisdictions that have strategic AML/CFT deficiencies for which they have developed an action plan together with the FATF (for more information, see FATF 2017; 2019).

29. For more information, see https://risk.lexisnexis.com/global/en/products/worldcompliance-data.

30. Italy, France, Spain, Belgium, Cyprus, Luxembourg, Malta, and the Netherlands.

31. In the AML/CTF domain, we decided to employ the FATF list instead of the EU list of high-risk third countries for the following reasons: 1) Ownership data included in the analysis are from 2019, and in 2019 the EU list had not been issued; 2) The FATF list has the advantage of also covering EU countries (potentially), which are excluded by definition by the EU list; 3) The EU list has a very high correlation with the FATF list (see Riccardi 2020).

Table 3: Black and grey lists of countries used for the study (Updated as of October/November 2019)

List	Countries
EU blacklist of non-cooperative jurisdictions for tax purposes (08/11/2019)	American Samoa, Fiji, Guam, Oman, Trinidad and Tobago, United States Virgin Islands, Vanuatu, Samoa
EU grey-list of non-cooperative jurisdictions for tax purposes (08/11/2019)	Anguilla, Antigua and Barbuda, Armenia, Australia, Bahamas, Barbados, Bermuda, Bosnia and Herzegovina, Botswana, Belize, British Virgin Islands, Cape Verde, Cayman Islands, Cook Islands, Curacao, Jordan, Maldives, Marshall Islands, Mongolia, Montenegro, Morocco, Namibia, Nauru, Niue, Palau, Saint Kitts and Nevis, Saint Lucia, Seychelles, Swaziland, Thailand, Turkey, Vietnam
FATF AML blacklist (October 2019 statement) - *Call for action*	Iran, Democratic People's Republic of Korea
FATF AML grey-list (October 2019 statement) - *Other monitored jurisdictions*	Bahamas, Bouvet Island, Cambodia, Ghana, Iceland, Mongolia, Palau, Papua New Guinea, Tajikistan, Tunisia, Yemen, Zimbabwe

5. Data on contextual variables at the country level are retrieved from various sources, and then used to test the potential path of the correlation with macro-level measures of ownership anomalies. Several heterogeneous categories are identified, including demography, economy/finance, taxation, OCGs/other crimes, corruption/governance indicators, financial secrecy and money laundering, among others (Table 3).

Table 4– List of country-level contextual variables and relative descriptions

Category	Variable	Description
Demography	Population (EUROSTAT)	Total resident population in EU countries (Jan 2019).[32]
Economy/ Finance	GDP per capita (EUROSTAT)	Ratio of real GDP to the average population (2019).[33]
	Bank Credit (WB)	Financial resources provided from domestic banks to the private sector with respect to GDP (2018).[34]
Taxation	Nominal tax rate (KPMG)	Nominal corporate income tax rate (2017).
	Effective tax rate (Torslov et al. 2020)	Estimation of effective corporate tax rate corrected by missing profits (2020).
	Corporate Tax Haven score + components (TJN)	Indicator measuring the attractiveness of a country for tax avoidance purposes (2019).[35]
OCGs/Other crimes	Italian mafias presence (Transcrime elaboration)	Presence of Italian mafias in Italy and abroad (2010-2017).

32. https://ec.europa.eu/eurostat/data/database

33.https://ec.europa.eu/eurostat/databrowser/product/page/SDG_08_10

34.https://datacatalog.worldbank.org/domestic-credit-private-sector-gdp-3

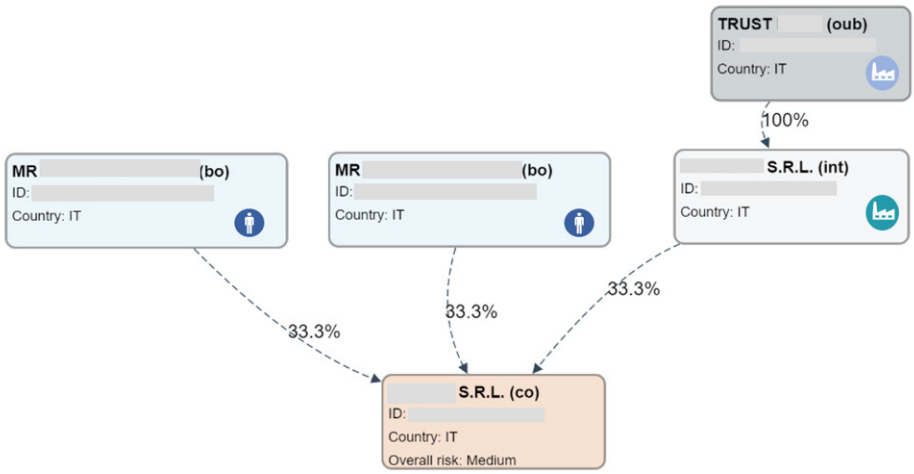
35. https://www.corporatetaxhavenindex.org/en/

Category	Variable	Description
Corruption/ governance Indicators	Government effectiveness (WB)	Indicator measuring the quality of public services, civil service and its independence from political pressures, quality of policy formulation and implementation, and a country's credibility with respect to its stated policies (2018).[36]
	Rule of Law (WB)	Indicator capturing perceptions of the extent to which agents have confidence in and abide by the rules of society (2018).[37]
	Corruption Perception Index (Transparency International)	Indicator ranking countries based on how corrupt the public sector is perceived to be by experts and business executives (2019).[38]
	Control of Corruption (WB)	Indicator capturing perceptions of the extent to which public power is exercised for private gain (2018).[39]
Financial Secrecy	Financial Secrecy Index + components (TJN)	Indicator ranking jurisdictions according to their secrecy and the scale of their offshore financial activities (2020).[40]

Methodology

For each company in the sample, the full ownership chain connecting the company to its BO(s) is reconstructed. In each case, entities owning more than 10% of the share capital at each ownership level are identified, up to any individual ultimate beneficiary at the top of the chain (i.e. the BO). If it is not possible to identify an individual at the top of a chain, then the top shareholder is referred to as the *Other Ultimate Beneficiary* (OUB). Moreover, all entities separating a company from its BOs or OUBs are labeled as *intermediate shareholders* (INT). After metrics at the firm level are calculated, descriptive statistics are then computed for each country, territory (NUTS1, 2, 3 level[41]) and business sector (NACE section and division level[42]). The next sections provide a summary of some of the results that have been obtained, while the full results are accessible in the Public Area.

Figure 5 - Illustration of different actors across the ownership structure of a company (CO), including Beneficial Owners (BOs), Other Ultimate Beneficiaries (OUBs) and intermediate shareholders (INTs).



36.https://databank.worldbank.org/databases/governance-effectivenes

37. https://datacatalog.worldbank.org/rule-law-estimate

38. https://www.transparency.org/en/cpi

39. https://datacatalog.worldbank.org/control-corruption-percentile-rank

40. https://fsi.taxjustice.net/en/

41. https://ec.europa.eu/eurostat/web/nuts/background

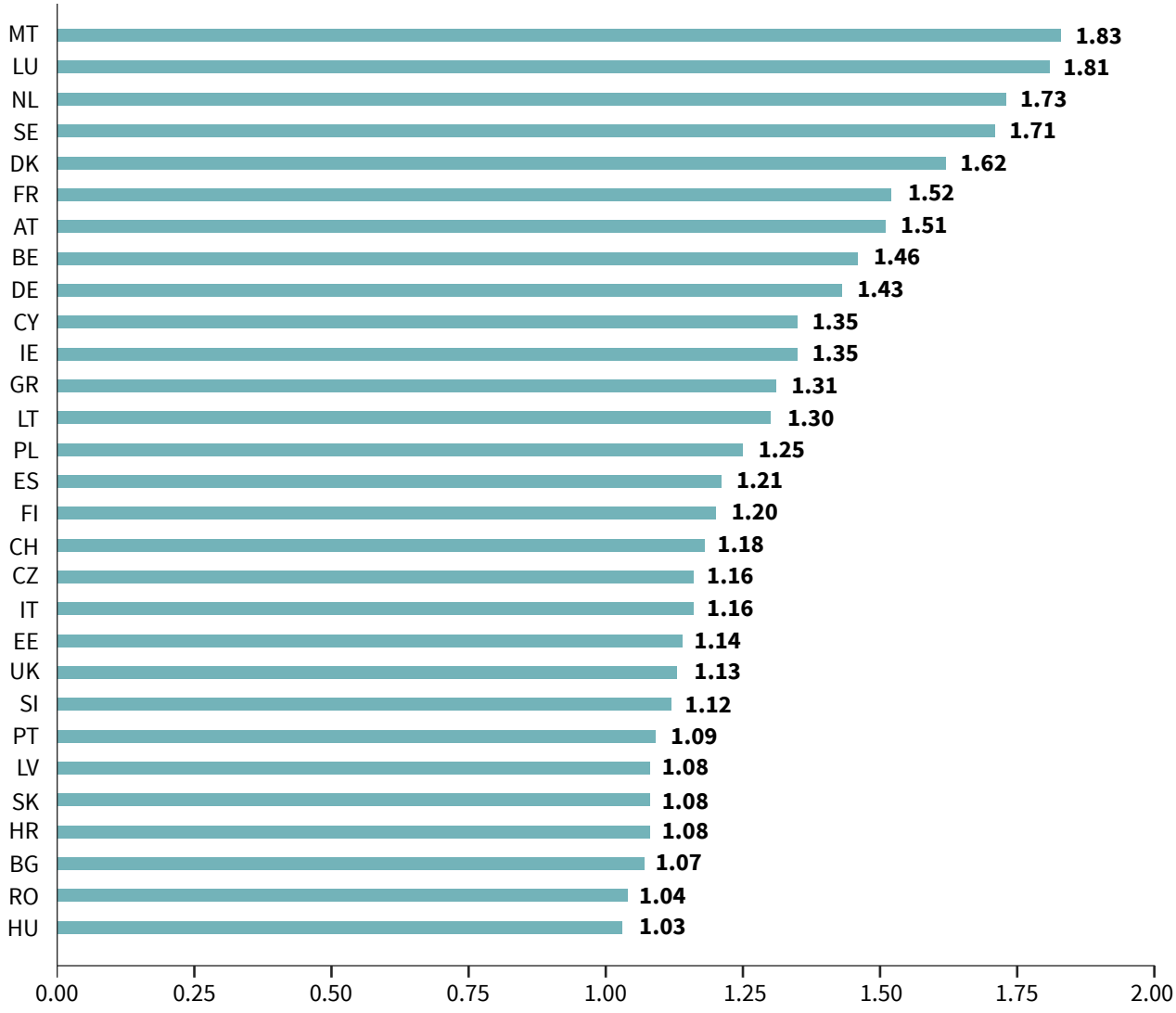
42.https://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_NOM_DTL&StrNom=NACE_REV2&StrLanguageCode=EN

3.2 Results

Complexity and anomalous complexity of ownership structures

The first analysed business ownership risk factor is the **anomalous complexity of corporate ownership** across European regions and business sectors. The higher the complexity of a company, the more difficult it is to trace its BOs, and the greater the risk that the company may be used to conceal criminal profits and/or individuals (Knobel 2021). Complexity of businesses is analysed by looking at what is known as the *BO distance*. This measure represents the number of steps that separate a company from its BO(s). When the *BO distance* is equal to 1, then the company is directly controlled by its BO(s). The higher the *BO distance*, the greater the level of complexity of the company structure. The average *BO distance* is calculated for all the companies in the sample, and the average observed values are computed at both the territory and sector level. The average EU value observed is **1.21**.

Figure 6 - Average BO distance across European countries (EU27 + UK and CH, 2019)

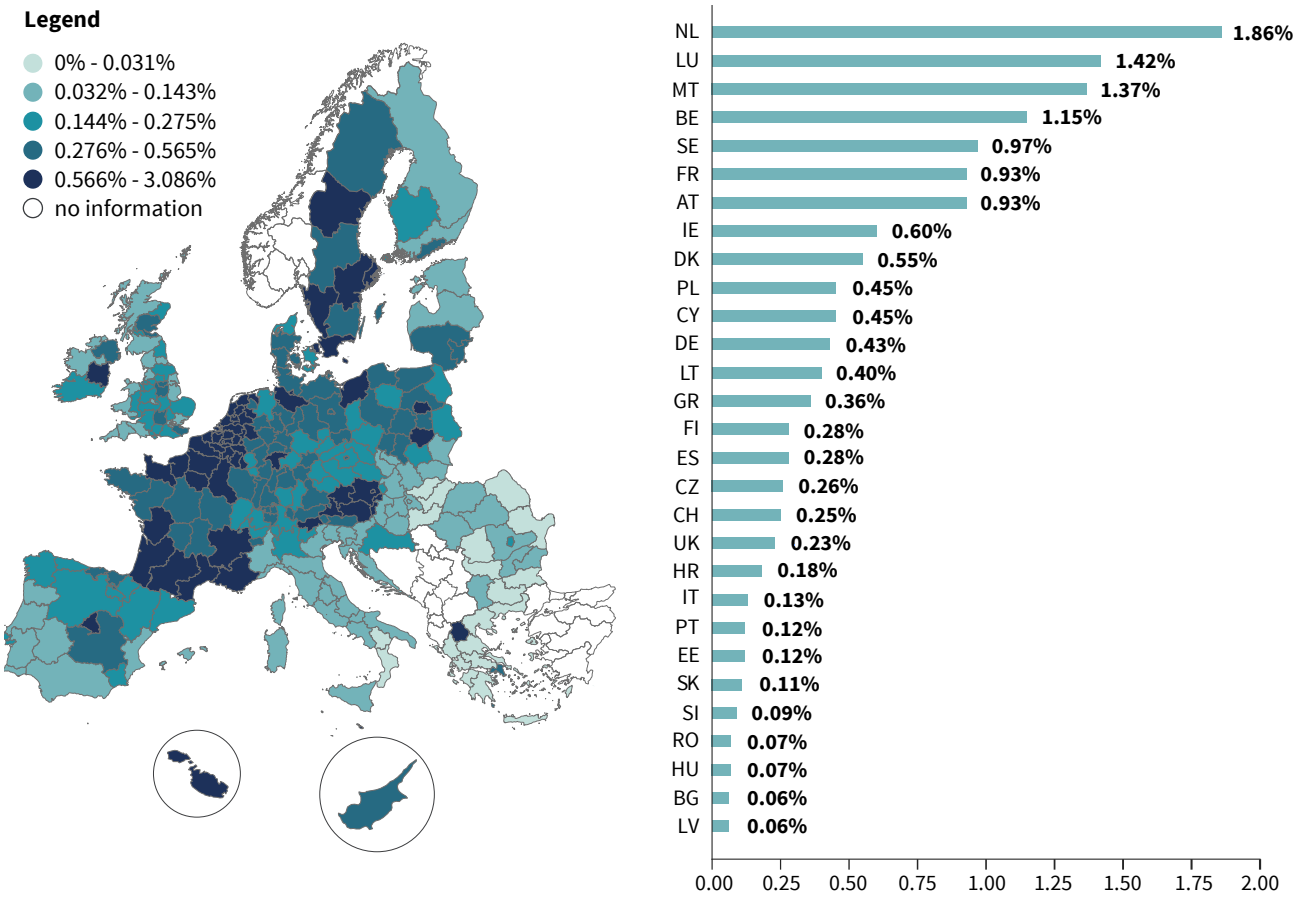


Source: UCSC-Transcrime's elaboration of Bureau van Dijk – Orbis Europe (2019) data

From Figure 6, one can discern that the country that displays the highest average *BO distance* among European countries is **Malta (1.83)**, followed by **Luxembourg (1.81)**, **the Netherlands (1.73)**, and **Sweden (1.71)**. Conversely, the lowest values are observed in Hungary (1.03), Romania (1.04) and Bulgaria (1.07). However, as discussed in section 2.1, it is important to underscore here that a **complex ownership structure is not anomalous per se**, and that, in fact, the observed differences might be due, in part, to the larger number of foreign direct investments (FDI) and multinational companies in some areas, countries, and business sectors. **Anomalies arise when companies have an unnecessarily complex corporate structure** that is not justified by the nature and the size of their activities. Therefore, to take that into account, the sample is segmented into groups of peer companies (so-called peer groups), that is, groups of companies active in the same business sector and with a comparable dimension. The distribution of *BO distance* within each peer group is computed and then divided into 5 classes using a K-means clustering algorithm. In this way, every company in the sample is assigned a *risk score* (range 1-5) called **BOC**[43], which indicates **anomalous complexity with respect to its peer companies**.

Figure 7 shows the percentage of limited companies with maximum value in the calculated **BOC *risk score* of anomalous complexity** (i.e. % of firms with BOC = 5 on total registered firms). While the **EU average value is 0.3%** the **Netherlands** presents, by far, the highest concentration of anomalously complex companies (1.9%), followed by **Luxembourg** (1.4%) and **Malta** (1.4%).

Figure 7 – Percentage of companies with ownership structures characterised by anomalous complexity, NUTS2[44] (EU27+ UK and CH, 2019)



43. Business Ownership Complexity

44. NUTS is the current territorial classification adopted by the EU. It lists 104 regions at NUTS 1, 281 regions at NUTS 2 and 1348 regions at NUTS 3 level.

When one considers the correlation with contextual variables at the country-level (Table 4), it appears that high levels of anomalous complexity of ownership tend to be positively associated with variables identifying wealthy European countries (GDP per capita) with well-developed financial markets (i.e. value of bank credit over GDP) and stable institutions (in terms of control of corruption, rule of law, government effectiveness). No significant correlation is observed against measures of financial secrecy. These results may be read twofold. On the one side, they confirm that corporate complexity, even when corrected by peer-group benchmarks, may still be representative of the presence of multinational firms and foreign investments and not necessarily of anomalous or even illicit behaviour. On the other side, they confirm that our knowledge about which geographical areas are 'risky' remains limited. While most official blacklists (in both AML and tax domains) include developing countries and offshore jurisdictions, these data point out that even **strong and stable economies**, including within the EU, present some risks in terms of **corporate opacity**. This result calls for further research on the issue of corporate ownership complexity, in order to better understand when complexity represents a higher risk in terms of potential illicit behaviour, and when it is instead mirroring other legitimate determinants.

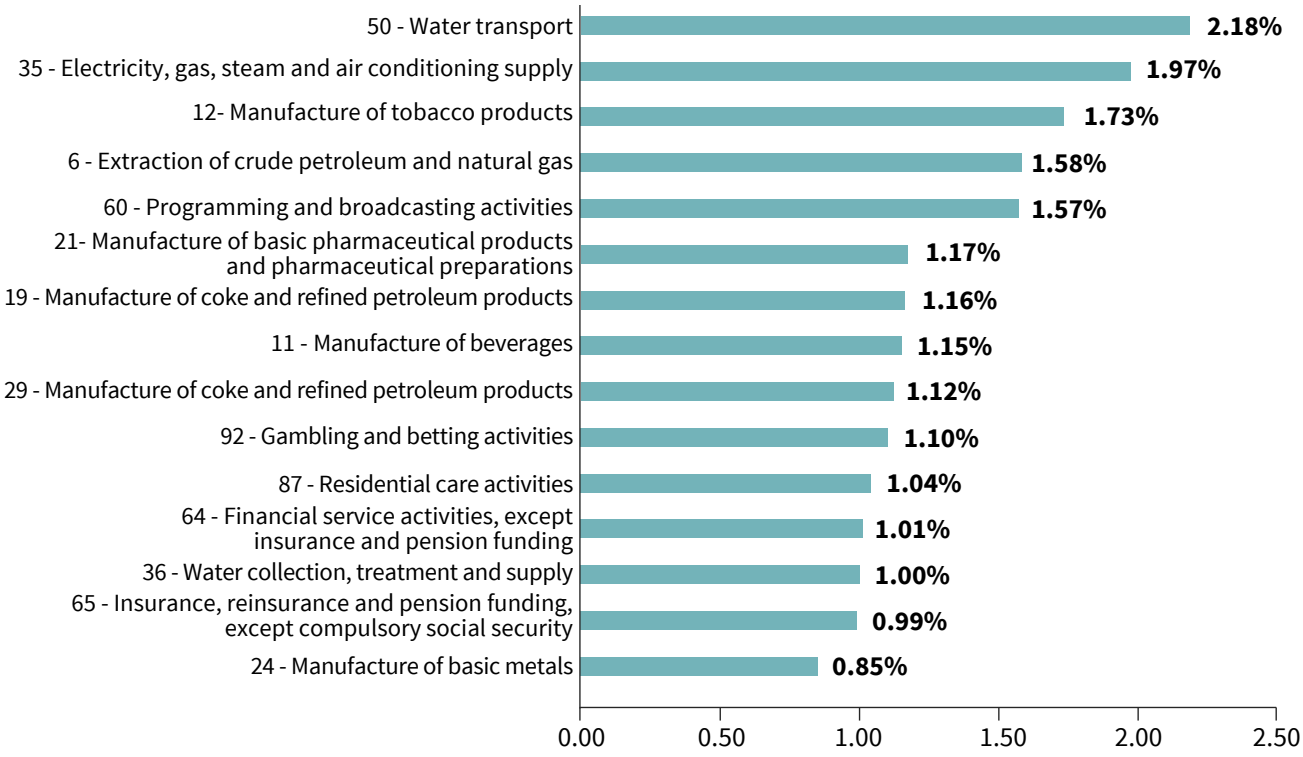
Table 5 – Correlation between the percentage of companies with anomalous complexity and contextual macro variables at the country level (EU27+ UK and CH, 2019)

Macro category	correlated variables	Correlation coefficient	p-value
Economy/Finance	GDP per capita (EUROSTAT)	0.57***	0.001
	Bank Credit (WB)	0.38**	0.044
Taxation	Nominal tax rate (KPMG)	0.60***	0.001
Corruption/governance Indicators	Government effectiveness (WB)	0.46**	0.011
	Rule of Law (WB)	0.48***	0.008
	Corruption Perception Index (Transparency International)	0.46**	0.015

The table displays the Pearson's correlation coefficients statistically significant over a 99% CI (***) and a 95% CI (**).

The result of the analysis conducted at the sector level (NACE rev.2 division) is displayed in Figure 8. Some of the business sectors with the highest density of anomalous complex companies, such as **water transport** (NACE division 50) and **gambling** (NACE division 92), have also been found to be more vulnerable towards criminal infiltration and money laundering, in terms of previous research (Transcrime 2018; Savona and Riccardi 2017) and police investigations (DIA 2019; 2017; 2016).

Figure 8 - Percentage of companies with ownership structures characterised by anomalous complexity, NACE rev.2 classification (2019)



Ownership links with blacklisted/greylisted countries

When a company has ownership links with countries with high levels of secrecy, it is more difficult to carry out financial investigations and trace BOs. Therefore, there is a higher risk that these companies could be used to hide individuals and proceeds related to criminal activities (Tavares 2013; Tax Justice Network 2015). In order to understand the level of business ownership links with secrecy jurisdictions, we match ownership data with **black and grey lists of risky jurisdictions** issued by EU and FATF (details in section 3.1). In this way, it is possible to identify, within each territory and sector, the percentage of companies with BOs, INTs, OUBs that are linked to risky countries.

Across the EU, the average percentage of companies with ownership connections to blacklisted/greylisted jurisdictions is **0.91%**. As depicted in Figure 9, **Luxembourg** (8.7%) and **Cyprus** (8.5%) are by far the countries with the highest **density of business ownership connections with blacklisted/greylisted jurisdictions**. The sub-country analysis also shows that some specific areas of Belgium (Brussels and Liège), the Netherlands (North Holland and Utrecht) and the UK (London) present noticeable concentrations. The lowest values are observed in Portugal (0.1%), Estonia (0.2%) and Slovenia (0.2%). Moreover, it can be seen (Figure 10) that in some countries, such as Belgium, Switzerland and the UK, a relevant portion of the links to blacklisted countries are to BOs (i.e., individuals). Hence, it is likely that some of these ties are driven by factors that are not related to financial secrecy or opacity, such as the **presence of foreign residents** in the domestic country, the **attractiveness** in terms of **the ease of starting a business**, and the presence of tax incentives for individuals. In other countries, such as Cyprus, Luxembourg and the Netherlands, a major proportion of the links to blacklisted countries are not related to individuals, but rather to other companies that are intermediate companies (INTs, i.e. firms somewhere in the ownership chain between the firm itself and its BOs) or other ultimate beneficiaries (OUBs, i.e. firms and corporate vehicles which are at the top of an ownership chain and do not allow for the identification of BOs - see Figure 5 for further details on these entities).

Figure 9 – Percentage of companies with ownership links to blacklisted/greylisted jurisdictions, EU27+ UK and CH (2019)

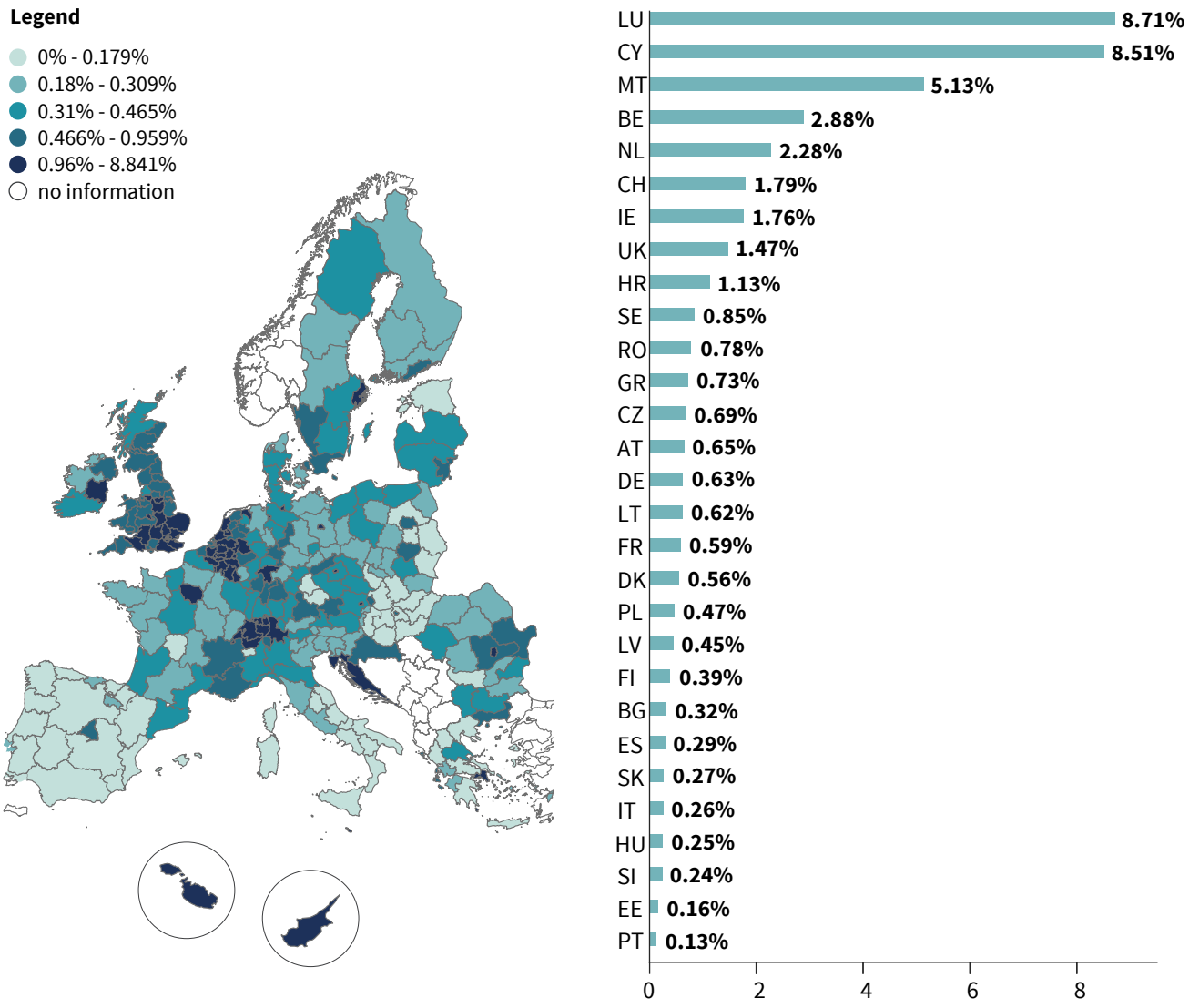


Figure 10 – Percentage of companies with ownership links to blacklisted jurisdictions, by type of owner/shareholder (i.e., BOs, OUBs, INTs), EU27+ UK and CH (2019)

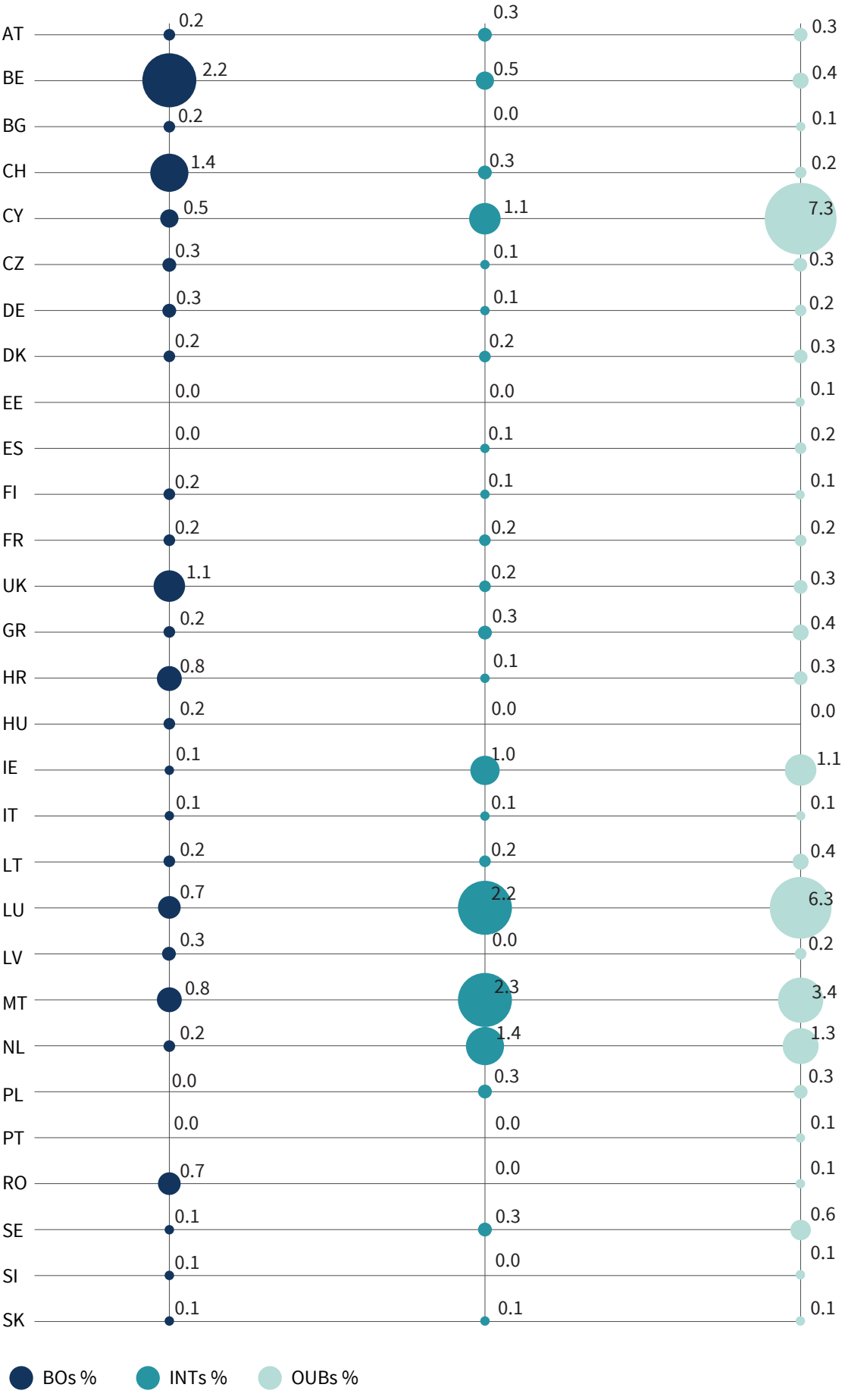


Table 5 reports the results of the correlation between the percentage of companies with *ownership links with blacklisted/greylisted* countries and the contextual variables considered at the country level. As with the previous variable (*anomalous complexity*), the results draw attention to the fact that high volumes of links to blacklisted/greylisted jurisdictions are observed in countries with wealthy economies (GDP per capita) and developed financial markets (bank credit). It is also evident that there is a correlation with metrics of favourable tax regimes, both in terms of effective tax rate (Torslov et al. 2020) and indicators in this domain (e.g. the Corporate Tax Haven score by TJN and some of its sub-components). Therefore, countries with lower tax rates have a higher ratio of companies linked to owners from blacklisted/greylisted jurisdictions, that, in turn, can display exiguous or even null effective tax rates, such as British Virgin Islands, British Cayman Islands and Jersey. Moreover, the percentage of *ownership links with blacklisted/greylisted* countries also shows a positive correlation with measures of financial secrecy (e.g. Financial Secrecy Index).

Table 6 – Correlation between the percentage of companies with ownership links with blacklisted/greylisted countries and contextual variables at the country level (EU27+ UK and CH, 2019)

Macro category	Correlated variables	Correlation coefficient	P-value
Economy/Finance	GDP per capita (EUROSTAT)	0.46**	0.013
	Bank Credit (WB)	0.42**	0.025
Taxation	Effective tax rate (Torslov et al. 2020)	-0.42**	0.038
Financial Secrecy	Financial Secrecy Index (TJN)	0.46**	0.011
	Subcomponent: Harmful Structures[45]	0.37**	0.049
	Corporate Tax Haven score (TJN)	0.53***	0.003
	Subcomponent: LACIT[46]	0.43**	0.021
	Subcomponent: Loopholes&Gap[47]	0.44**	0.016
	Subcomponent: Anti-Avoidance[48]	0.39**	0.035

45. *Harmful Structures.* This sub-component of the Financial Secrecy Index assesses the availability of four harmful instruments and structures within the legal and regulatory framework of a jurisdiction (https://fsi.taxjustice.net/PDF/15-Harmful-Structures.pdf, source TJN). In particular, it measures whether a jurisdiction: 1) issues or accepts the circulation of large banknotes of its own currency (of value greater than 200 EUR/GBP/USD), 2) has companies with unregistered bearer shares; 3) has a domestic legislation providing for the creation of Series Limited Liability Companies (LLCs) or of Protected Cell Companies (PCCs); 4) does not effectively prevents the administration of trusts with flee clauses.

46. *Lowest Available Corporate Income Tax Rate, LACIT (https://corporatetaxhavenindex.org/PDF/1-Corporate-Income-Tax-LACIT.pdf, source TJN).* This sub-component of the Corporate Tax Haven Score reflects the tax avoidance risk of countries by scaling the lowest available corporate income tax rate against the spillover risk reference rate of 35%. The range of values goes from 0 (no tax avoidance risk) to 100 (maximum tax avoidance risk). Therefore, a positive correlation with the macro-level indicator of ownership links with high-risk countries confirms the possible coexistence - in some countries - of profit shifting incentives and exploitation of corporate structures involving "tax heaven" jurisdictions.

47. *Loopholes&Gap (https://www.corporatetaxhavenindex.org/PDF/CTHI-Methodology.pdf, source TJN).* This subcomponent of the Corporate Tax Haven Score focuses on various exclusions and exemptions that can be used to shrink the tax rate or base. Therefore, the highlighted positive correlation supports the hypothesis of a possible relation between our risk indicator and practices of profit shifting and tax avoidance.

48. *Anti-Avoidance (https://www.corporatetaxhavenindex.org/PDF/CTHI-Methodology.pdf, source TJN).* This subcomponent of the Corporate Tax Haven Score reflects the extent to which jurisdictions enact robust rules constraining tax avoidance and profit shifting.

Ownership links with opaque corporate vehicles

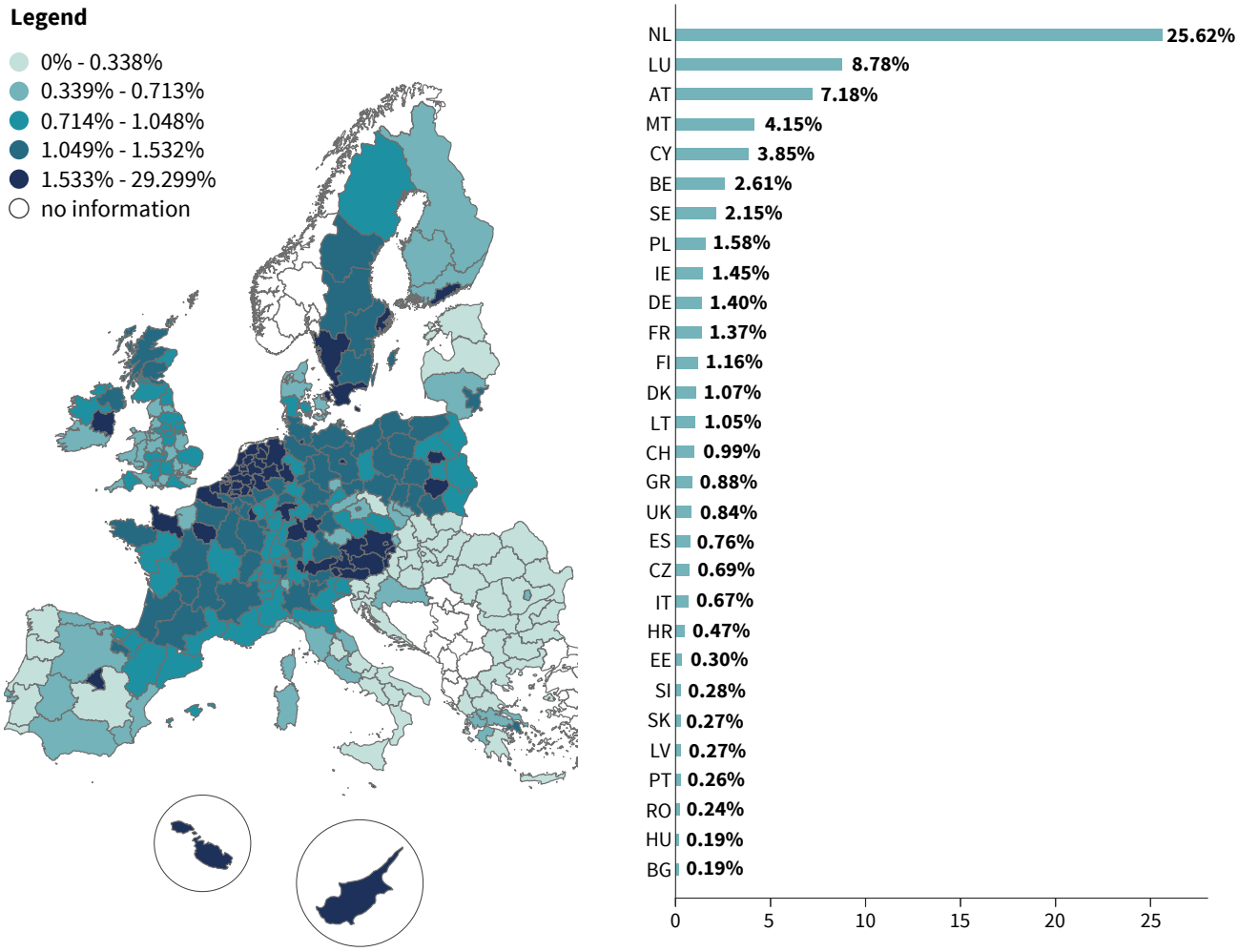
The identification of BO(s) of a company is not possible in some cases for several reasons. For instance, if a company's share capital is highly fragmented (such as is the case with many listed companies), then there might be no individuals that own more than 10% or 25% of the shares. In other cases, specific corporate vehicles can purposefully be used to conceal the identity of individuals at the top of the ownership chain.

In this section of the analysis, we identify **all those companies that have as the ultimate owner a corporate entity, such as a *trust*, a *fiduciary*, a *foundation* or an *investment fund*, which does not allow for the identification of the individual BO(s)**. The underlying hypothesis here is that the more difficult it is to correctly identify BOs, the higher the risk that the company could be used to conceal illicit activities (see section Ownership links with opaque corporate vehicles). Evidently, in most cases these corporate entities are used for legitimate purposes, but the existence of such legal forms at the top of the ownership chain has been identified as a risk factor that must be taken into account by both global organisations involved in the prevention of money laundering, corruption and financial crime – such as the FATF, OECD –, by the EU money laundering/terrorist financing supranational Risk Assessment (SNRA, European Commission 2019a) and the directives issued in this field by the EU (European Parliament and Council of the European Union 2015; 2018).

Across the EU, on average, **1.45%** of companies are controlled by a trust, a fiduciary or a fund that does not allow for the identification of a BO. As illustrated in Figure 11, the analysis outlines high values in **the Netherlands**, where 25.6% of the limited companies in our sample are in fact controlled by an opaque corporate vehicle. This is most likely connected to the extended domestic use of Dutch foundations (so-called *stichting*). These are legal arrangements similar to foundations (they are created to pursue philanthropical and non-profit objectives), but in the Netherlands they are also routinely used to control for-profit limited or unlimited firms. These legal arrangements are widely used for a range of legitimate purposes, namely: as a structural measure to split legal and beneficial ownership of shares and to concentrate voting control on such shares within the board of the *stichting*, and for strategic or defensive purposes within international transactions. However, given their specific nature, it is not very meaningful to talk about 'owners' of a *stichting*, and for this purpose they may be misused for hiding the identity of the ultimate beneficiaries (OECD 2019a). This vulnerability has been stressed by various agencies, such as the OECD, who in its 2019 report underscored that: "*Foundations in the Netherlands are not systematically required to keep identity information concerning all beneficiaries. An obligation should be established in both the European Netherlands and the Caribbean Netherlands for foundations to keep identity information concerning all beneficiaries*" (OECD 2019a).

In future research, it may be worthwhile to further investigate the use of trusts, foundations or other legal arrangements across the EU27, as their diffusion appears to depend largely on the country, as depicted in the map below with respect to **Luxembourg** (8.8%), **Austria** (7.2%), **Malta** (4.1%) and **Cyprus** (3.9%).

Figure 11 – Percentage of companies with ownership links with opaque corporate vehicles that do not allow for identifying BOs (2019). NUTS2 (left), EU27 + UK and CH (right)



Source: UCSC-Transcrime's elaboration of Bureau van Dijk – Orbis Europe (2019) data

Table 6 shows a positive correlation between this measure and measures of financial secrecy, in particular with a sub-component of the FSI - the *Trusts & Private Foundations* indicator. This captures whether a jurisdiction has (or does not have) a central register of trusts and foundations (whether these are local structures, or foreign law structures administered by locals), which is publicly accessible via the internet, and/or if a country prevents resident trustees from administering foreign law trusts, and if a country provides legislation for the creation of private purpose foundations.[49] The positive correlation with this indicator means that, the lower the transparency concerning trusts and private foundations in the country (as measured by the TJN), the higher the likelihood that local firms are ultimately controlled by a legal arrangement (measured through our indicator. Or, in other words, countries with less transparent regulation on trusts and private foundations (as measured by the TJN) are more likely to have a higher percentage of firms that are owned by these types of corporate entities.

49.https://fsi.taxjustice.net/Archive2013/KFSI/2-Trusts-Foundations-Register.pdf.

Table 7 – Correlation between the percentage of companies with ownership links with opaque corporate vehicles and contextual variables at the country level (EU27+ UK and CH, 2019)

Macro category	Correlated variables	Correlation coefficient	P-value
Economy/Finance	GDP per capita (EUROSTAT)	0.37**	0.048
Corruption/ governance Indicators	Rule of Law (WB)	0.38**	0.041
	Control of Corruption (WB)	0.37**	0.049
Financial Secrecy	Financial Secrecy Index (TJN)	0.40**	0.033
	Subcomponent: Trusts & Private Foundations	0.50***	0.005
	Subcomponent: Harmful Structures	0.39 **	0.037
	Corporate Tax Haven score (TJN)	0.69 ***	0.000

The table displays the Pearson's correlation coefficients statistically significant over a 99% CI (***) and a 95% CI (**).

Correlation among ownership risk indicators at territorial and sectoral level

It is relevant to notice that the three opacity indicators analysed in the previous sections (i.e. *anomalous complexity, links with high-risk countries, links with opaque corporate vehicles*) display positive correlation at country level, regional level (nuts2) and sectoral level (NACE rev.2 division) – see figure below.

The strongest statistical correlations are observed at country level (a.), while smaller but significant correlation are observed at regional level (b.). On the contrary, little to no dynamics are observed at sector level.

Therefore, at territorial level, the three risk indicators tend to move in the same direction even though the overlap is only partial. This result suggests that:

1. Each risk indicator may capture different facets of corporate ownership characteristics (some are discussed in the previous sections).

2. Concentration of anomalous companies seems to be driven by country level-dynamics, such as national legislations and regulations (see previous sections for details), rather than by industry-driven factors.

Table 8– Correlation among ownership indicators at: a) country level; b) sub-country level (NUTS2); c) sector level (NACE rev.2 division), 2019

Anomalous complexity of ownership structures	1		
Ownership links with high-risk countries	a. 0.52*** b. 0.46*** c. 0.22**	1	
Ownership links with opaque corporate vehicles	a. 0.78*** b. 0.58*** c. 0.07	a. 0.36* b. 0.23*** c. 0.10	1
	Anomalous complexity of ownership structures	**Ownership links with high-risk countries**	**Ownership links with opaque corporate vehicles**

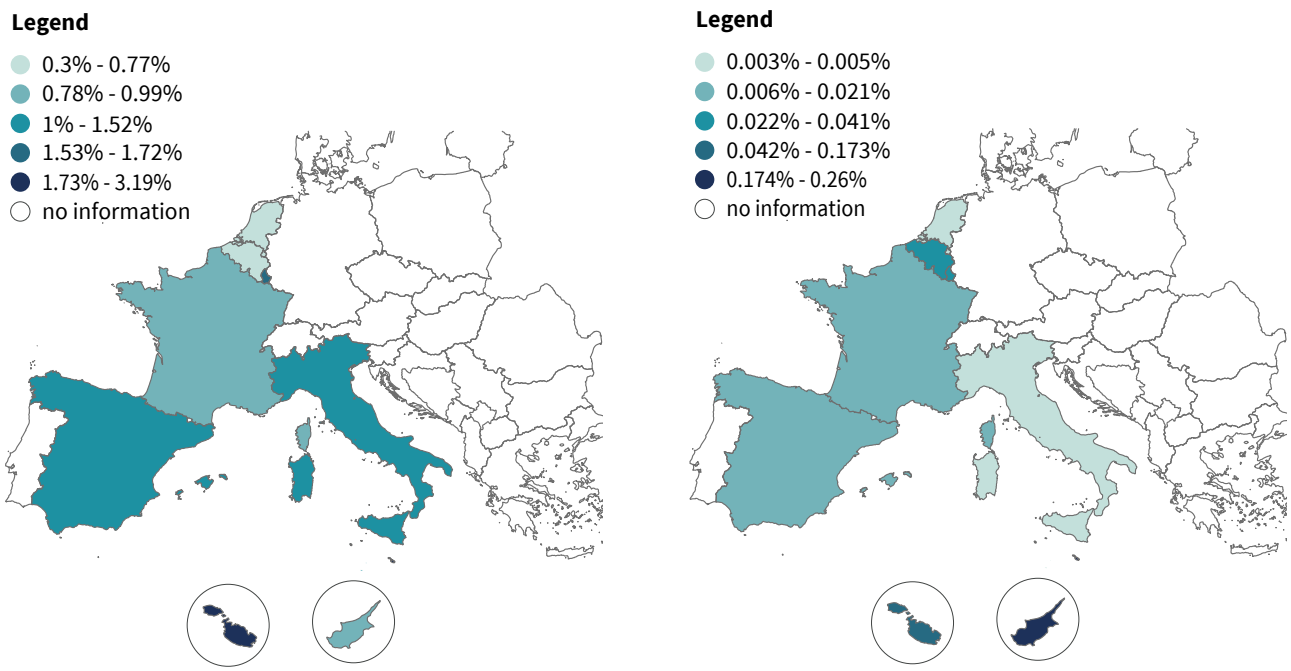
Links to entities subject to sanctions or enforcement measures

To analyse the distribution of sanctions and enforcement cases across territories and business sectors, the information obtained from Orbis Europe is matched with data from LexisNexis World Compliance. Such information is retrieved – and analysed - for eight EU MS: Italy, France, Spain, the Netherlands, Belgium, Malta, Cyprus and Luxembourg. These countries are selected because of their relevance for the geographical scope of the project and because of data availability.

Overall, the number of companies that are subject to sanctions or enforcement, or who have owners who are subject to sanctions or enforcement, amounts to 55,352 out of 27 million (0.2%). The geographical distribution of World Compliance flags on companies at the country level is discussed below. In particular, Figure 12 presents the distribution of companies with enforcement flags (on the left) and sanctions (on the right), divided by the total number of limited companies registered in that territory. It is worthwhile to note that 1% of all Maltese companies appear to be targeted by enforcement measures, while a lower percentage is observed in the case of Cyprus (0.50%). The Netherlands (0.13%), France (0.12%) and all the remaining countries display lower percentages. Despite a lower density, a similar ranking is observed when considering companies included on a sanction list, with Malta (0.19%) and Cyprus (0.04%) at the top of the distribution.

Figure 12 shows the percentage of companies with BOs targeted either by enforcement measures (left) or sanctions (right). With respect to BOs targeted by enforcement measures, Malta shows a higher density than all the other countries (3.2% of domestic companies); Luxembourg (1.6%), Spain (1.5%) and Italy (1.1%) also show high ratios, as is clearly discernible on the map. With regard to sanctions on BOs, Cyprus is the country that presents the highest density (0.26% of all BOs), followed by Malta (0.17%) and the other countries.

Figure 12 – Percentage of companies with a Beneficial Owner subject to enforcement (left) and sanctions (right), 8 countries (2019)



Source: UCSC-Transcrime's elaboration of Bureau van Dijk – Orbis Europe (2019) and LexisNexis WorldCompliance data

These results should be interpreted cautiously. On the one side, they may mirror current risks and evidence of investigations, as also reported by national and international authorities. For instance, in Malta, despite the strict controls of the local supervisory authorities, several investigations in recent years have highlighted the infiltration of Italian OCGs within domestic companies, particularly in the online gambling sector (DIA 2019; 2017; 2016)[50] and, despite the progresses made, some areas of improvements have been also highlighted by Moneyval and the European Commission (European Commission 2020c, Moneyval 2019). However, it is also possible that these results reflect the effectiveness of local authorities in terms of their ability to target criminal behaviour of companies and their owners: higher rates of enforcement flags among companies and owners may mirror more effective activity of local LEAs. Also, since data on enforcement comes from the Lexis Nexis screening of open sources, the variability of flags may be due to different media coverage and awareness across the jurisdictions in the sample, which may hamper the cross-country comparability of results. Therefore, further research is needed to understand the actual extent of enforcement on companies and their owners. If possible, recurring on official statistics rather than on secondary sources such as media news would improve this analysis; but, given the lack of publicly available judicial and police statistics, this is the best available source which could be employed in this type of assessment nowadays.

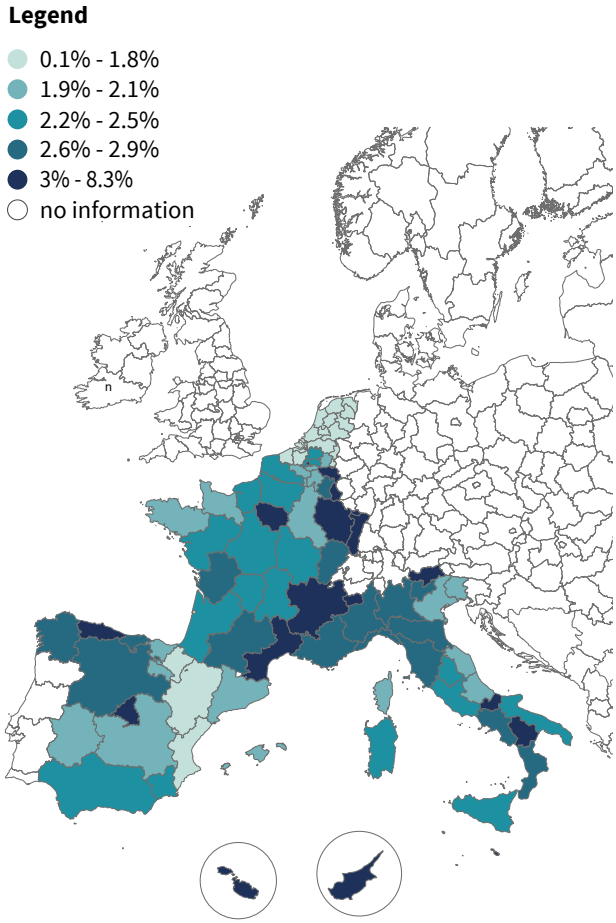
50. For instance, 'Operation Gambling', by the Italian DIA, Carabinieri, Police and Guardia di Finanza (2015), revealed a global network of gaming businesses, some of them established in Malta, which were used by the Italian 'Ndrangheta to run illegal gambling activities in Italy and elsewhere.

Links to PEPs

The FATF defines PEPs as "*individuals who have been entrusted with prominent public functions*" (FATF 2013a) . Within the context of AML and anti-corruption, the presence of PEPs is classified as a factor that enhances the level of risk between business clients and, as such, is subject to increased due diligence by ACAs and other relevant financial institutions.

For the purposes of the analysis, we compute the percentage of companies owned by PEPs in eight EU MS: Italy, France, Spain, the Netherlands, Belgium, Malta, Cyprus and Luxembourg. For these countries, we match the information obtained from Orbis Europe with data on PEPs obtained from LexisNexis WorldCompliance (for further details see the *Data section above*).

Figure 13 – Percentage of companies with Beneficial Owners flagged as PEPs in the WorldCompliance database, 8 countries (2019), NUTS3



Overall, in the 8 analysed countries there are **79,621** BOs of domestic companies flagged as PEPs. Some metropolitan regions (e.g. Madrid, Paris), Languedoc-Roussillon, Malta and Cyprus have the highest percentage of limited companies with at least one PEP amongst their BOs. Malta and Cyprus have figures of 8.3% and 4.8%, respectively. Luxembourg (3.9%) and France (3.1%) are close behind, while all other analysed countries display percentages below 3%.

As highlighted in section 2.1, it is important to stress that having links with PEPs should in no cases be regarded as evidence of criminal activities. However, FATF Recommendations and the 5th EU AMLD do require the application of additional AML/CFT measures when engaging in business relationships with PEPs. Further research should focus on deepening our knowledge of this area by investigating the relations between the business and political sectors within specific countries. Once again, it is important to stress that the coverage and reliability of the compliance lists provided by *WorldCompliance* may vary across countries, thus causing some limitations in the comparability of the results.

3.3 Focus: ownership anomalies of companies participating in European public procurement procedures

Public procurement involves a huge amount of money and resources (it accounts for 14% of GDP within the EU) (European Commission 2017). For this reason, it is vulnerable to corruption and other illicit practices that undermine competition (Rose-Ackerman and Palifka 2016; Soreide 2002). Given the economic relevance of this sector and its attendant vulnerabilities, a specific analysis was carried out on a sample of companies that were awarded public tenders in Europe. The analysis presented in this section specifically aims to assess the usefulness of ownership indicators in the identification of potentially corrupt suppliers in public procurement procedures.

Data and methodology

Data on public contracts awarded in the 28 EU MSs between 2018 and 2019 (N=2,684,068) are retrieved from *Opentender*[51]: they include both information on contracts (e.g. type of procedure, number of bidders) and winners (e.g., official name, city, postcode). Contracts without information on winners are dropped. The database includes 494,242 contracts that were awarded to 146,545 companies. These are then joined with the datasets used for the analysis discussed in the previous section, in order to retrieve ownership information for the companies. As a result, 33,762 companies are uniquely matched (23% of the total).[52] To ensure consistency with the previous analysis, the sample is restricted to public limited and private limited companies. Therefore, the final dataset includes **27,378 companies registered in 28 European countries** that were awarded a total of **112,085 contracts**.

The analysis aims to compare two groups of companies: **winners of non-transparent procedures and winners of transparent procedures**, defined as follows.

51. Opentender is a publicly accessible platform developed as part of the H2020 project DIGIWHIST (https://digiwhist.eu/). It gathers up public procurement data collected from official sources across 35 jurisdictions (including among the 28 EU MSs). The platform can be accessed at the following link: https://opentender.eu/all/start.

52. Since the Opentender dataset did not include company unique identifiers (e.g., VAT number), the matching was performed using company name and postcode.

1. **Non-transparent procedures** are defined as contracts awarded with single bidding or after a negotiated procedure without the publication of the tender notice. Single bidding refers to cases in which only one bid is submitted during the tendering period and, hence, is indicative of a poor level of competition. Previous research has demonstrated that a high presence of single bidding in procurements correlates with other indicators of corruption at country level (Charron et al. 2017; Fazekas and Kocsis 2020; Mungiu-Pippidi 2016). Also, previous research has shown that countries with a lower quality of government are more likely to rely on **negotiated procedures without publication of the tender notice** (Chong, Klien, and Saussier 2015). These kind of procedures are considered non-transparent because they "make it very easy to provide information to one bidder while concealing it from other bidders" (Fazekas, Tóth, and King 2013b).

2. **Transparent procedures** are defined as all the procurement procedures that recorded at least two bidders and have been awarded through any other procedure (e.g., open, restricted, etc.).

Anomalies in companies' ownership are compared between the two groups of companies. In particular, the following measures - as discussed in previous sections - are calculated: 1) anomalous complexity of ownership structures; 2) ownership links with high-risk countries; 3) ownership links with opaque corporate vehicles; 4) ownership links to PEPs.

Results

Table 8 shows the results of the comparison. Overall, the analysis shows that anomalies in companies' ownership are more common among winners of non-transparent procurement procedures. In particular:

- 1.7% of winners of non-transparent procedures display **anomalously complex ownership structures**, against 1.2% of winners of transparent tenders. The difference between the two groups is statistically significant. As discussed in section 2.1, companies could exploit complex ownership schemes to hide collusive or corruptive agreements in public procurement (Fazekas, Tóth, and King 2013a).

- 1.1% of winners of non-transparent contracts are tied via shareholding **links to blacklisted/greylisted countries**, against a 0.8% observed among winners of transparent tenders. The difference between the two groups is statistically significant in this case too. This result supports the hypothesis that companies may exploit blacklisted/greylisted jurisdictions to launder corrupt proceeds and conceal their BOs.

- The analysis does not find a statistically significant difference between the two groups in terms of number of **volume of links to opaque corporate vehicles**. This result may need a further investigation, but it is probably driven by the extensive use of Dutch *stichting* in the Netherlands (see discussion in section 3.1.2). However, excluding this case, the use of opaque corporate vehicles that do not allow to identify the BO appear to be significantly more common among companies participating to non-transparent procurement procedures.

- 5.5% of winners of non-transparent contracts has **links with PEPs**, compared to 4.3% in the comparison group. This result is consistent with previous research on corruption in public procurement: companies may indeed exploit current or former political office holders to get contracts to the detriment of virtuous bidders (Rajwani and Liedong 2015).

Table 9 - Comparison between winners of non-transparent procedures and winners of transparent procedures across ownership anomalies

Ownership anomalies	Sample	Winners of non-transparent procedures	Winners of transparent procedures	Difference
Anomalous complex ownership structures (max BOC)	Whole sample	**1.7%**	1.2%	0.51%***
Links to blacklisted/ greylisted countries	Whole sample	**1.1%**	0.8%	0.27%*
Unavailability of BO information	Whole sample	3.5%	**3.7%**	ns
	Without NL	**3.1%**	2.6%	0.51%*
Links with PEP	BE, CY, ES, FR, IT, LU, MT, NL	**5.5%**	4.3%	1.15%*

Note: Highest percentage among the two groups are reported in bold. Significance levels are reported for the Chi-square tests: + 0.10 * 0.05 ** 0.010 *** 0.001 (ns=not significant). Sample size: Whole sample (N=27,378); Whole sample without NL (N=26,559); Sample including BE, CY, ES, FR, IT, LU, MT, NL (N=9,142).

Analyses at country level highlight some interesting patterns. For instance, in Germany 2.5% of winners of non-transparent procedures is linked to opaque entities, 1.8% has a particularly complex ownership structure and 1.0% are linked to blacklisted/greylisted jurisdictions (respectively, 1.5%, 0.9% and 0.3% in the comparison group). Interestingly, a high percentage of Danish and Dutch winners of non-transparent contracts had anomalously complex ownership structures (respectively, 8.9% and 7.8%) compared to winners of transparent ones (respectively, 2.7% and 4.6%).

Overall, the results are consistent with the analysis presented in section 3.1.2 and confirm that ownership risk indicators can support the identification of more risky suppliers also in the public procurement domain.

3.4 Concluding remarks

The analysis conducted and displayed in Chapter 3 has mapped risk factors of ownership within legitimate businesses across EU countries, regions and business sectors. The results suggest that the analysed anomalies tend to be concentrated within specific geographical areas and business sectors. In the procurement domain, it shows that companies with anomalous ownership are more frequent among participants of less transparent procurement procedures. However, our knowledge of risky "hot-spots" with respect to ownership opacity remains limited. While most official blacklists (in both AML and tax domains) include developing countries and offshore jurisdictions, our analysis emphasises that **strong and stable economies**, even within the EU, can even present some vulnerabilities in terms of **corporate opacity and other red flags**.

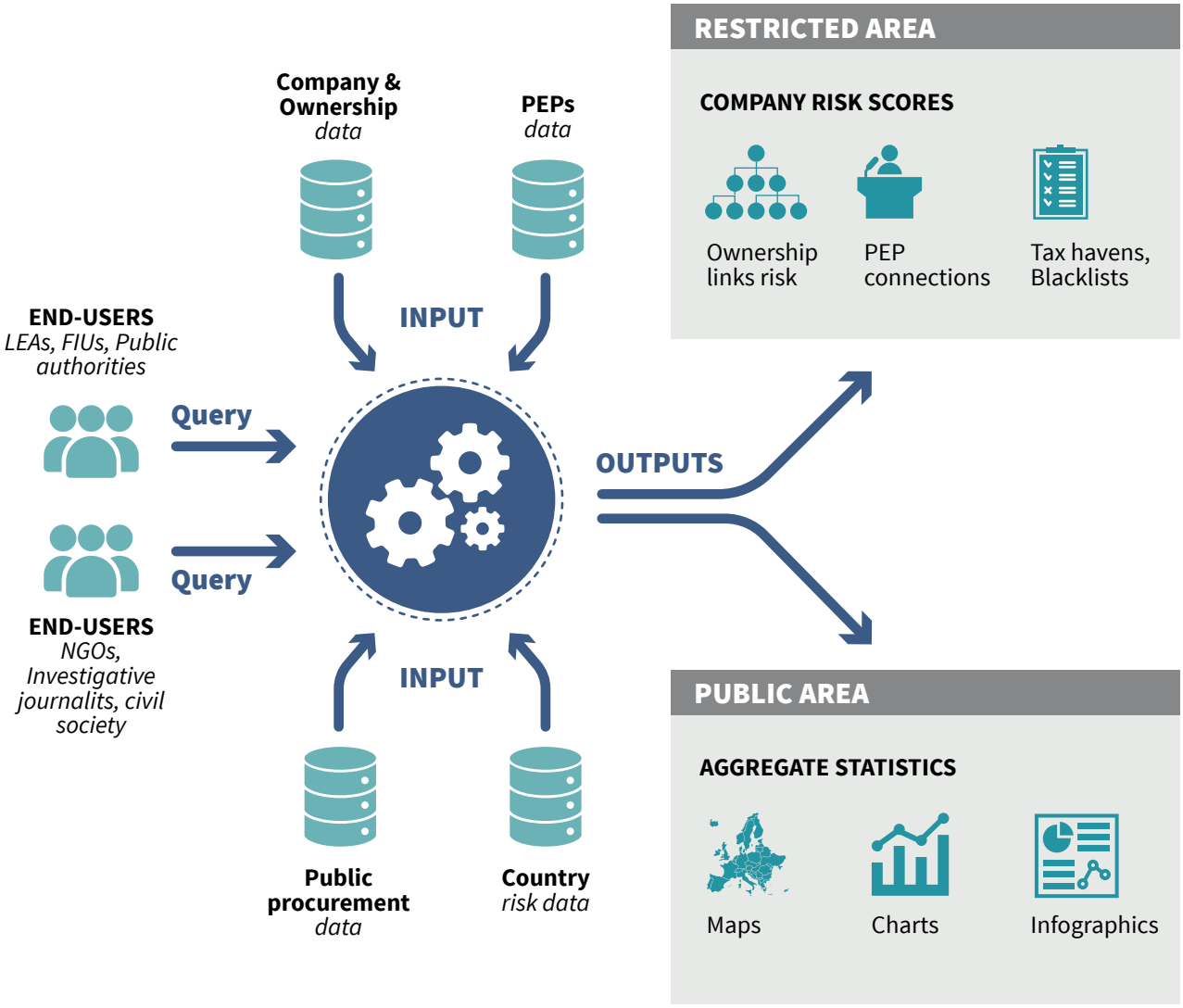
Future research in this area should try to improve the understanding of *who are the owners* of EU companies, and *how they exercise control*, to better understand which companies may be at risk of being misused to cover financial crime and other illicit schemes.

4. The prototype tool

Transcrime has developed the **DATACROS** prototype tool to **address the problem and fill the gaps identified in Chapter 2**. The **DATACROS prototype tool** includes two distinct environments that serve different functions:

- **Restricted Area**: a real-time analytical platform that is only accessible to authorised users (e.g., ACAs, LEAs), for investigating anomalies within EU firms' ownership structures and to assess their risk (see section 4.1);
- **Public Area**: the dashboard is accessible to everyone, for monitoring ownership anomalies across EU28 countries, regions and business sectors at an aggregate level (see section 4.2).

Figure 14 – Schematic representation of DATACROS Restricted Area and Public Area



4.1 Restricted Area – a prototype tool for investigation and risk assessment

The Restricted Area of the **DATACROS prototype tool** is a real-time prototype analytical platform with EU coverage, which is specifically designed to support (and go hand-in-hand with) LEAs and ACAs in the identification of companies at a high risk of corruption, money laundering, tax fraud and financial crimes. It has been designed in order to address the problem and close the gaps identified in Chapter 2. The platform is a prototype accessible only to authorised users (LEAs, ACAs, and other selected authorities) that is limited in scope and requires further enrichment and improvement. Nevertheless, it has thus far been successfully tested by our project partners and an array of relevant authorities at the EU level. It comprises the following features:

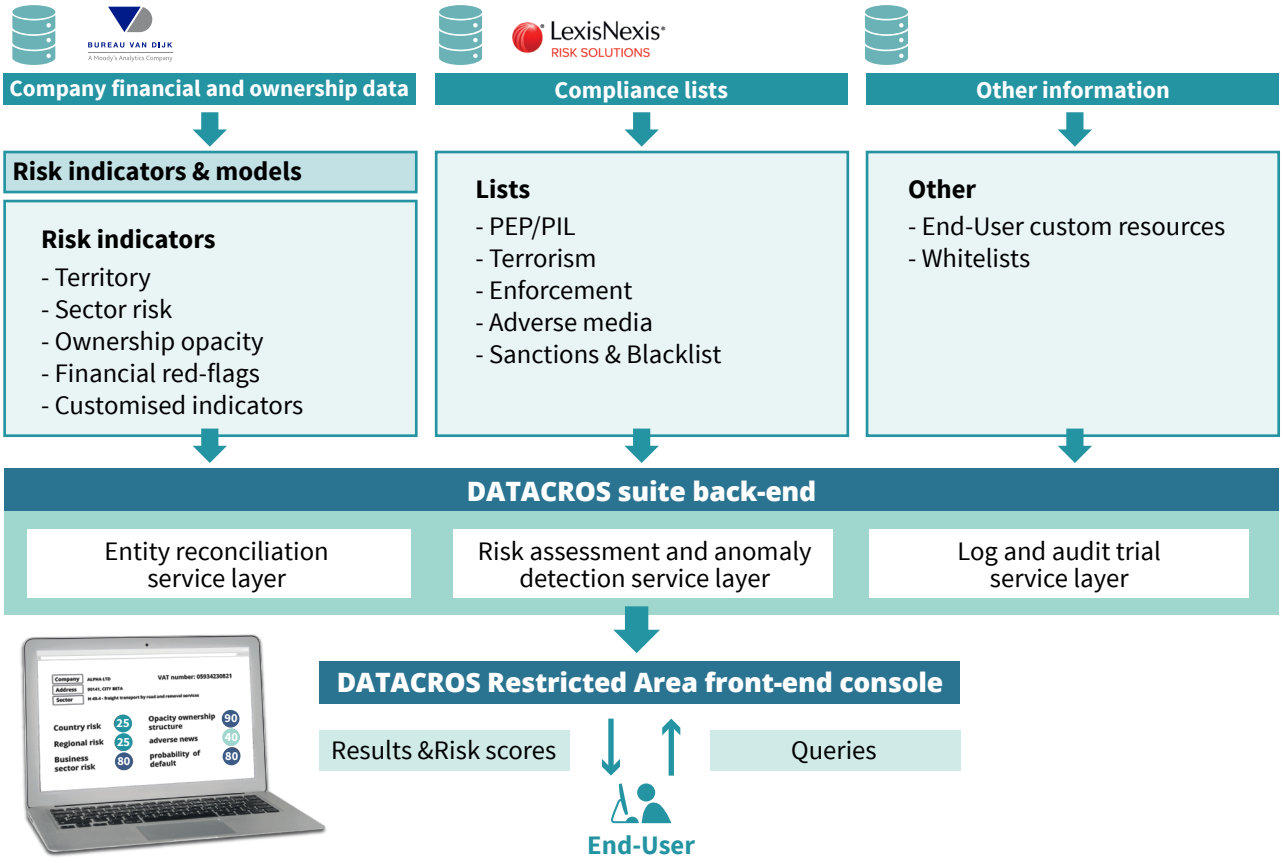
- **European cross-border coverage**: it contains data sources with EU coverage[53], and allows LEAs and end-users to both tackle the transnational nature of organised and financial crime, and reconstruct the cross-border ownership links between firms, entities and individuals.
- Know-how of criminal schemes: exploits the unique knowledge of criminal schemes generated by Transcrime through more than 25 years of publishing scientific research in high-quality academic journals[54] (Aziani, Ferwerda, and Riccardi 2021; Riccardi, Milani, and Camerini 2018; Savona, Riccardi, and Berlusconi 2016; Jofre et al. 2021) and conducting EU-financed projects[55].
- **Compliance with personal privacy and law enforcement procedures**: the Restricted Area was designed with the help of legal experts in accordance with *privacy-by-design* and *by-default* principles (see Chapter 5 for further details on the Data Protection Impact Assessment that was conducted).
- **Frontier predictive approaches**: The restricted area risk scoring includes machine learning approaches and predictive modelling. The prototype tool complements traditional approaches (e.g. sanctions list check) with **innovative machine learning algorithms**, in order to identify hidden patterns and red flags. The risk indicators and algorithms included in the tool have been empirically tested during the project and have been found to have a **strong predictive power** in terms of identifying companies (and owners) subject to sanctions or enforcements. The models correctly predict **82.6% of companies** targeted by sanction measures and **88% of companies** with owners subject to sanction measures (see section 4.1.2 for details).

53. **Company information**: *Bureau van Dijk – Orbis Europe* (coverage: 44 countries and 79 million companies); **Sanctions, enforcement cases** on firms: *LexisNexis WorldCompliance* (coverage: 1.2+ million profiles of entities worldwide)

54. See, for instance: Aziani A. et. al., 2020, "Who are our owners? Exploring the cross-border ownership links of European businesses to assess the risk of illicit financial flows", *European Journal of Criminology* (in course of publication); Riccardi M. et al., 2019, "Developing an indicator to assess the risk of money laundering across territories: an application to Italian provinces", *European Journal of Criminal Policy and Research*; Savona et al., 2016, *Organised crime in European businesses*, Springer. Jofre M., Bosisio, A., et al. (forthcoming, 2021). "*Money laundering and the detection of bad entities: a machine learning approach for the risk assessment of anomalous ownership structures*". Working paper presented at the 2021 Bahamas AML Research Conference

55. Transcrime has coordinated or participated in various projects in the area of corporate ownership transparency (EBOCS and BOWNET), money laundering and financial crime (IARM, MORE), organised crime (PROTON, OCP, ARIEL, FLOWS), and corruption (DIGIWHIST).

Figure 15 – Representation of DATACROS Restricted Area data sources and architecture



4.1.1 Functions and use cases

The Restricted Area of **DATACROS prototype tool** provides public authorities with a platform that is able to:

1. 1. Trace and reconstruct **cross-border links between firms**, individuals and related entities (e.g. BOs, shareholders, manager and directors)

2. 2. **Identify and map anomalies** and risk factors in companies' ownership structures (e.g. owners from blacklisted/ greylisted jurisdictions, unjustified complexity, presence of trusts, fiduciaries or other opaque corporate vehicles)

3. 3. **Score companies and related entities** through the use of risk indicators to orient and prioritize investigations. The indicators are calculated based on firms' observable characteristics (e.g. territory, sector, ownership structure, financials)

4. 4. Identify links with firms targeted by previous **sanctions** or **enforcement measures**

5. 5. Detect **cartels and clusters of firms** that may signal collusive behaviour (e.g. participants in public procurement)

6. 6. Allow for **identification of PEPs** at the national and EU level (source: WorldCompliance), as well as at the local level in selected countries.[56]

7. 7. Allow customization by LEAs or other end-users with proprietary data (e.g. internal blacklists/white lists)

56. Italy (Source: Ministry of Interior), France (Source: Répertoir national des élus), Spain (Portal de Entitades Locales).

This section presents some explanatory examples and use cases that outline the main functions of the platform.

Use case 1: Law Enforcement Agency using DATACROS to investigate financial crime

A LEA receives suspicious transaction reports (STRs) from the local FIU, which contains identifiers of several hundred companies/individuals that are suspected of being involved in money laundering schemes.

1. The LEA is able to upload the list of involved companies and individuals as a single batch (reducing investigation time).
2. DATACROS automatically collects data via API from various sources and processes it;
3. In DATACROS, the LEA is able to:
   a. Reconstruct the **full ownership structure** of all the reported companies (see Figure 17 and identify shareholders and BOs.
   b. Visualize **risk scores** that are calculated for the firms being screened (see Figure 20); the risk classification operated by the tool supports the prioritization of further investigation/due diligence (e.g. by highlighting the firms to focus the enhanced audit and paper checks on).
   c. Identify **links between companies in the list** (e.g. through common owners, directors, addresses, geographical ties), which can help to visualize potential coordinated behaviour in the same criminal scheme (see Figure 18), and **identify the key actors** that are enabling the potential illicit flows.
   d. Detect **links with blacklisted/greylisted jurisdictions** (see Figure 22), entities targeted by **previous sanctions** and enforcement, or **links with PEPs** (Figure 21).

Figure 16 – Search: companies can be searched using various search criteria, e.g. company name, national ID, sector, territory. It is also possible to search for individuals connected to companies, i.e. shareholders, BOs, managers/directors

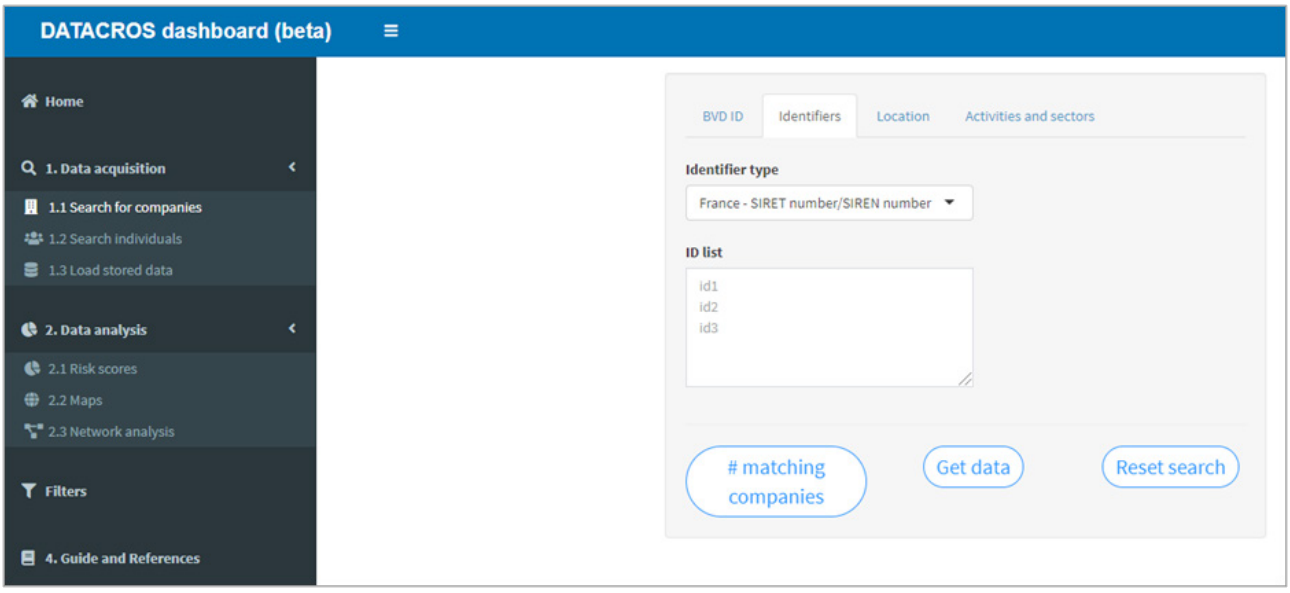


Figure 17 – Ownership analytics: Reconstruction of a complex ownership chain in the DATACROS Restricted Area

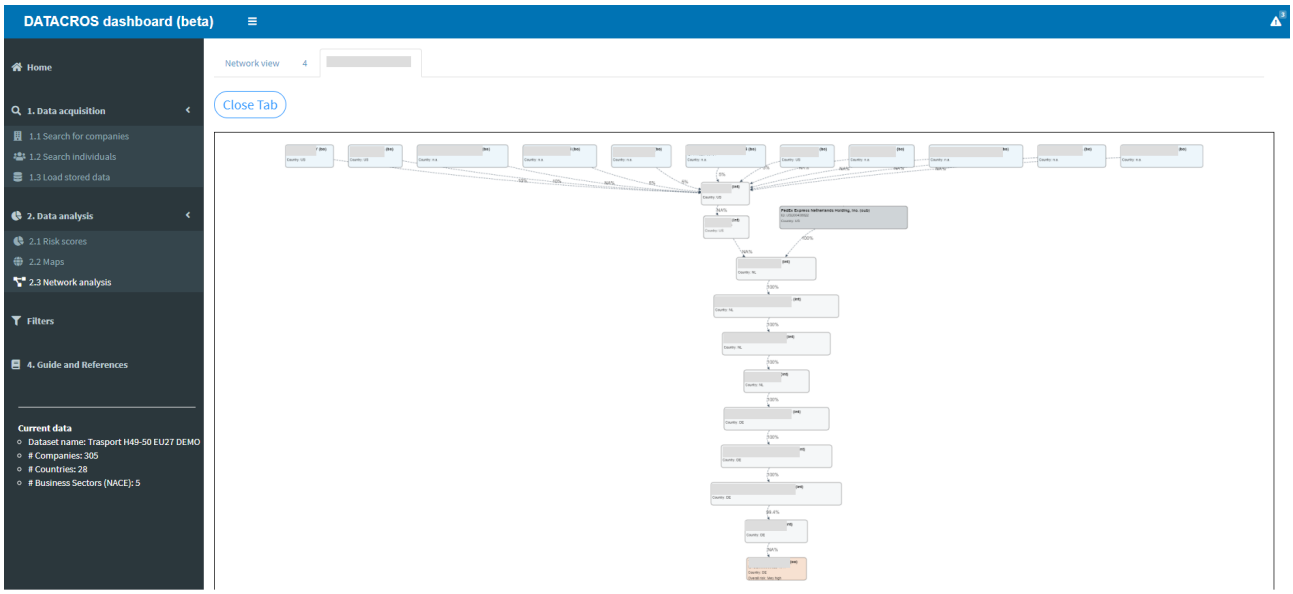
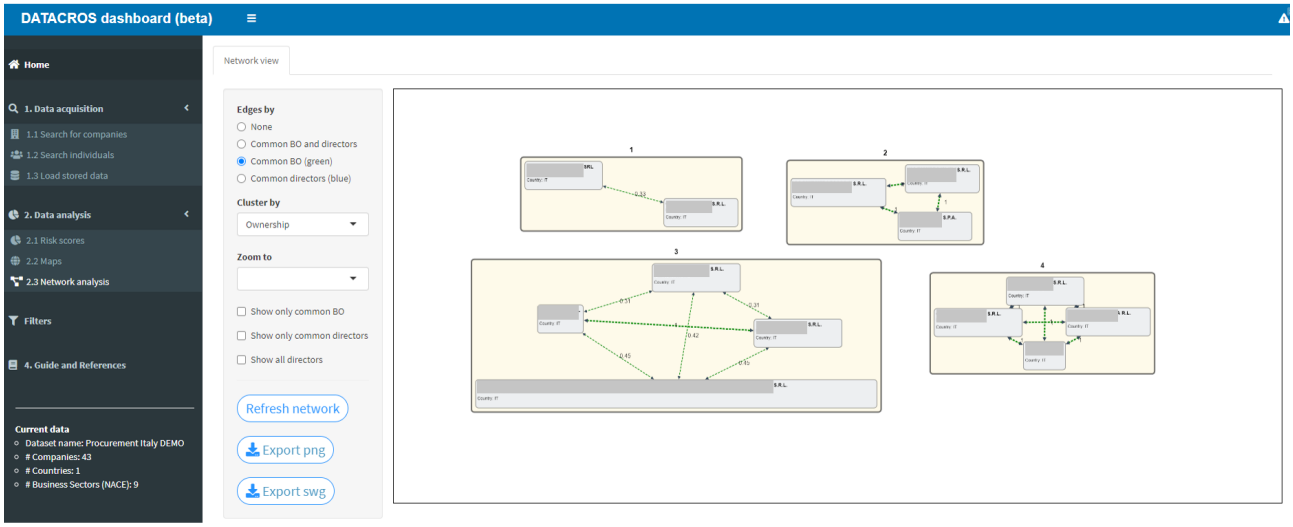


Figure 18 – Network analytics: Identification of networks of connected companies (ownership links) in the DATACROS Restricted Area



USE CASE 2: Anti-corruption agency using DATACROS to detect corruption and collusion within public procurement

An Anti-corruption agency needs to monitor companies participating in public procurements within certain areas to prevent corruption and collusion. The Agency uses DATACROS to carry out due diligence and risk assessment of all the companies, and detect red flags and high-risk companies on which to focus enhanced due diligence checks and audits:

1. The Agency uploads companies' names or national IDs (Figure 16) on DATACROS;
2. DATACROS calls via API the sources and collects the information;
3. In DATACROS, the Agency is able to:
   a. Classify all companies into risk classes (Figure 20);
   b. Supplement risk scores with other red flags (evidence of sanctions, enforcement, links with PEPs);
   c. Identify links between participants in the same bid, which can highlight collusive behaviour. This is done through: (a) reconstruction of ownership/directorships common links (see Figure 18); (b) identification of scores of anomalous geographical concentration.
   d. Detect potential corruption red flags and collusive cartels and filter out those firms at highest risk, who will then be the subject of enhanced due diligence checks and audits.

Figure 19 – Risk scoring: risk profile calculated by DATACROS algorithms for a selected company, based on its characteristics and calculated risk indicators

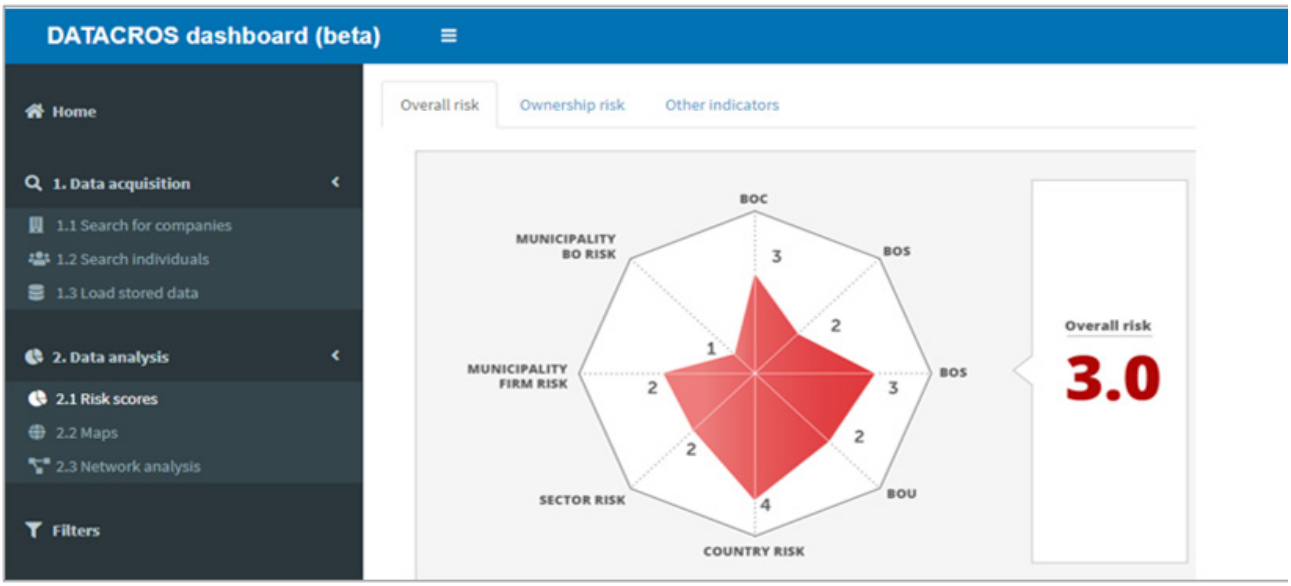


Figure 20 – Risk scoring: example of triage of a portfolio of selected companies based on the calculated risk profiles

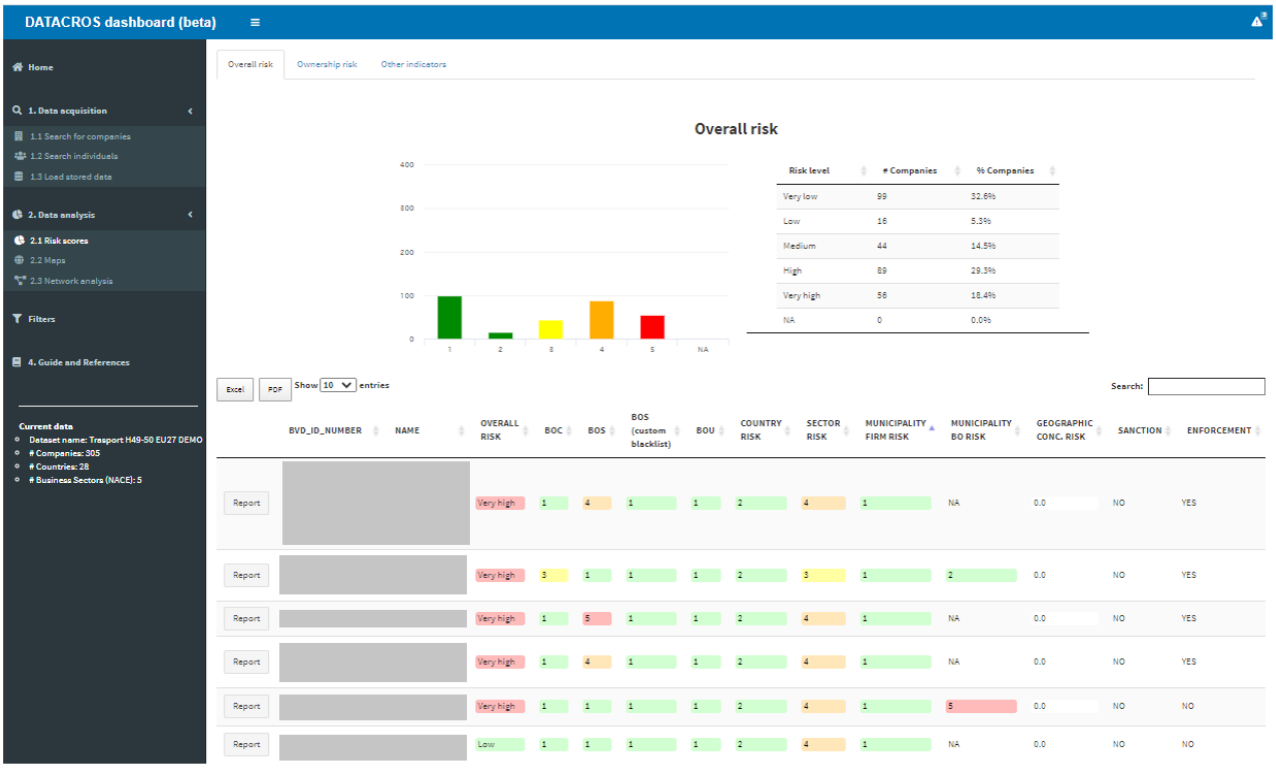
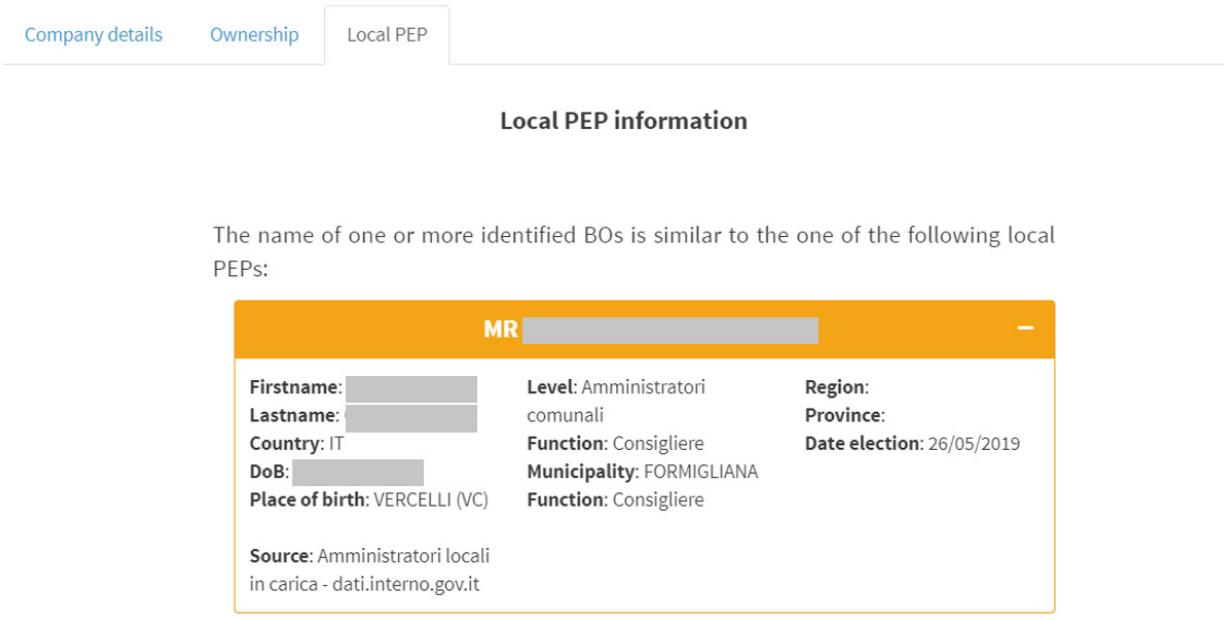


Figure 21 – Local PEP identification: example of a local PEP identified as matching the name of an identified BO of a selected company



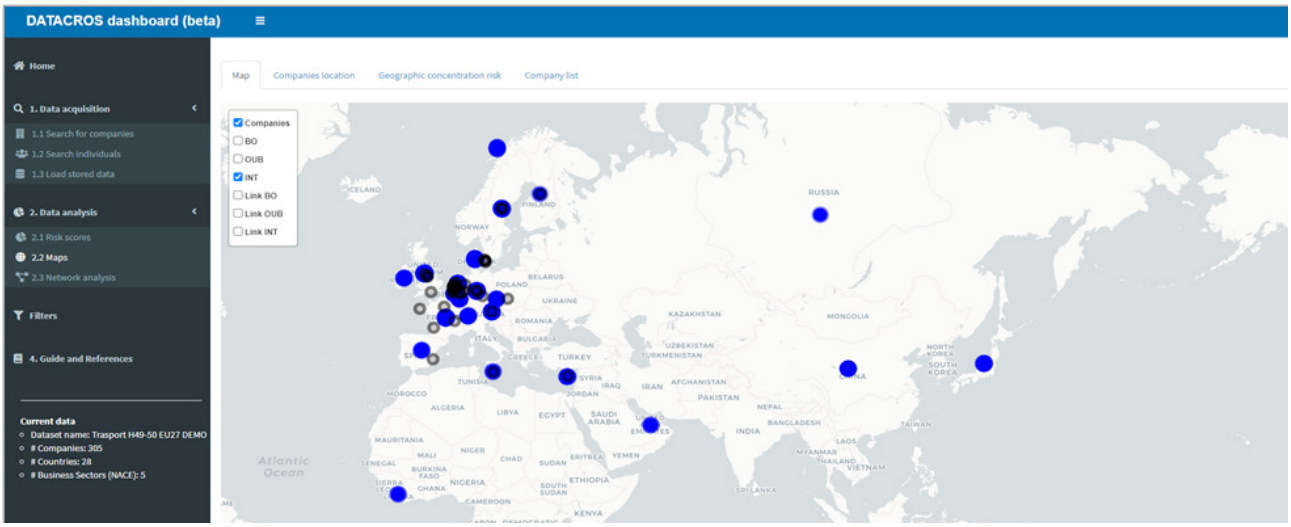
USE CASE 3: Tax agency using DATACROS to map tax fraud risks within a specific business sector/region

A tax agency can use DATACROS services in an aggregate fashion for mapping and monitoring tax fraud across business sectors and geographical areas.

1. The agency filters in DATACROS all firms that are operating in a certain sector (e.g. land transport sector) and within a certain area;
2. DATACROS collects the relevant data via API and processes it to attribute a set of risk scores to each company.
3. The agency can identify in real-time which and how many firms are characterised by high-risk scores. In particular, it can visualize:
   a. which companies have links with non-cooperative tax jurisdictions;
   b. which companies are controlled through trusts, fiduciaries, foundations (and other corporate entities benefiting from fiscal advantages);
   c. complex cross-border ownership structures, employing "Chinese-Box" schemes or circular ownership paths.

All these activities can help the agency to gain a comprehensive risk map, which can help them to both plan policies and allocate resources for its operations.

Figure 22 – Geo analytics - Map displaying the location of selected companies (black dots), beneficial owners, shareholders and related entities (blue dots). Links to blacklisted/greylisted jurisdictions can be identified.



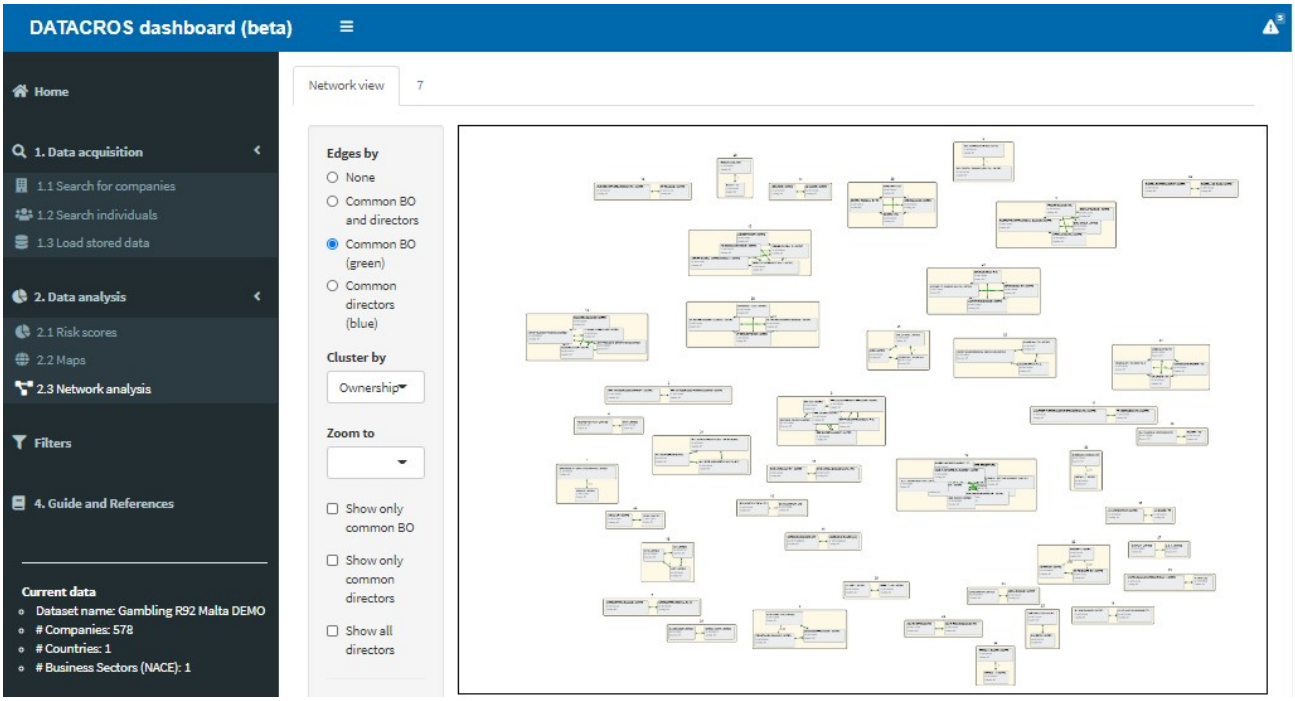
USE CASE 4: Competition authorities using DATACROS for analyisng market concentration

A Competition Authority can use DATACROS services in an aggregate fashion for investigating the level of market concentration and identifying corporate ownership groups across business sectors and geographical areas.

1. The agency filters in DATACROS all firms that are operating in a certain sector (e.g. gaming sector) and within a certain geographic area;
2. DATACROS collects the relevant data via API and reconstructs the full ownership structure of the companies active in that segment of the economy;
3. The authority can identify in real-time which and how many firms are connected through ownership or management links (see Figure 23).

All these activities can help the agency to gain a comprehensive view of the corporate groups operating in specific market segments, which can help them to calculate market concentrations and support market inquiries.

Figure 23– Network analytics: Identification of networks of connected companies (ownership links) across a market segment (business sector and/or geographic area)



4.1.2 Predictive power of DATACROS ownership risk indicators

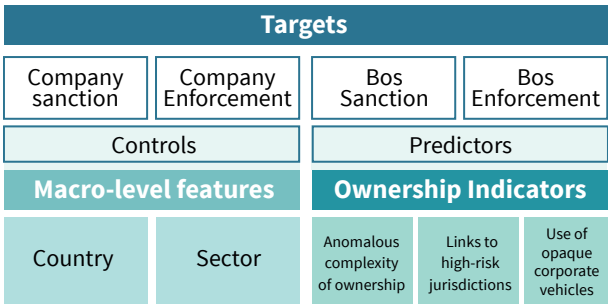
The DATACROS tool allows for the early detection of risk factors within legitimate companies, by complementing traditional approaches (e.g. sanctions list search) with **machine learning algorithms** that attribute **risk scores** to companies, in order to identify hidden patterns and red flags. The **predictive power** of these algorithms has been **validated** by training and testing several models for identifying companies that are potentially involved in illicit activities. The results confirm that the risk scoring algorithms included in DATACROS have a **strong predictive power** in terms of identifying companies (and owners) that are subject to sanctions or enforcement (see full details in Jofre et al. 2021).

For the purposes of validation, the dataset described in Chapter 3 was used to test the predictive power of ownership anomalies in identifying companies involved in illicit activities. The following information was considered:

- As **target** variables: *WorldCompliance* flags (**sanctions** and **enforcement**);
- As **predictors**: anomaly indicators of ownership as calculated in Chapter 3;
- As **controls**: a set of country-level and sector-level variables.

The considered dataset involves information on 3,064,089 million limited companies registered in the nine European countries from where enforcement and sanction data has been retrieved[57].

Figure 24– Information used to validate the predictive powers of DATACROS with respect to ownership risk indicators



57. Belgium, Cyprus, Spain, France, UK, Italy, Luxembourg, Malta and the Netherlands.

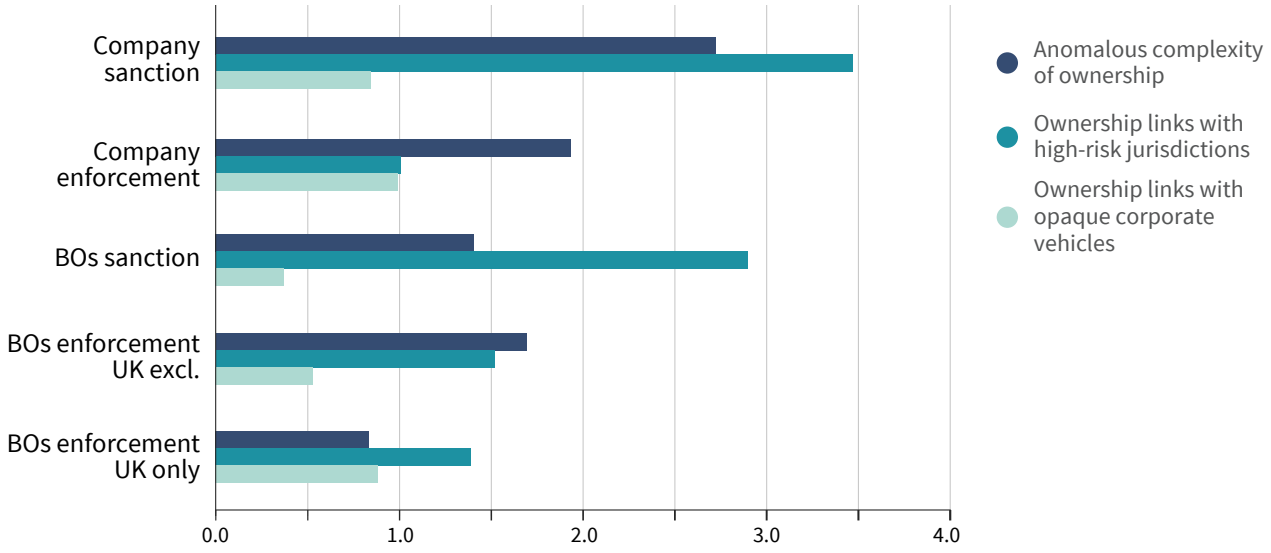
Several machine learning models have been implemented, both for the detection of sanctions and enforcement cases and for the assessment of the predictive performance of the ownership risk indicators, including: logistic regression, Naïve Bayes classifier, stacking of the previous two models, decision trees, bagged trees and random forests. All methods have been optimised and fitted using a training set, and further validated on a test sample, which ultimately ensured a non-biased estimation of the predictive ability of the model and risk indicators. A robustness analysis based on logistic regression was also performed to assess the stability of the results when cases from a certain country or business sector are excluded.

Satisfactory performance was achieved by all the considered machine learning methods, particularly regarding sanction offences. In the case of logistic regression, the algorithms correctly predict **83.3% of sanctions on companies and 88% of sanctions on owners**. The prediction of companies and owners not subjected to sanctions or prior enforcement is also good. The lowest performance occurs when predicting owners in the UK who have either been subject to or not subject to enforcement, which is suggestive of a more complex country-specific phenomenon.[58]

Regarding the predictive ability of the indicators, it is observed that ownership links with high-risk jurisdictions is notably important for detecting most offences, particularly with respect to sanction cases. Regarding anomalous complexity, there is evidence of its ability to predict sanctions and enforcement on companies. Finally, ownership links with opaque corporate vehicles appear to be less relevant in terms of predictive power.

Figure 25 – Predictive power of DATACROS risk indicators. Overall predictive power of the model (up), and relevance of various indicators of anomalous ownership complexity (down)

Logistic regression (Performance on the test set)	True positive rate	True negative rate
Company sanction	0.833	0.872
Company enforcement	0.679	0.729
BOs sanction	0.879	0.851
BOs enforcement excl. UK	0.615	0.564
BOs enforcement only UK	0.548	0.522



58. In the case of Bos who are subject to enforcement, the results are presented in such a way that isolates the UK from the rest of the sample, as the number of UK criminal cases is extremely large compared to the other countries considered.

While the results are stable across the whole sample, some country-specific and sector-specific patterns are observed. For instance, in Italy, Cyprus and Spain the *anomalous ownership complexity* is a stronger predictor of illicit behaviour by companies. *Ownership links with high-risk jurisdictions* and *ownership links with opaque corporate vehicles* are more relevant for identifying sanctions and enforcement in Malta and the Netherlands. At the sector level, we observe that *anomalous ownership complexity* and *ownership links with high-risk jurisdictions* are major determinants of enforcement and sanction offences in the *financial and insurance sector*, while *ownership links with opaque corporate vehicle* is an important factor for identifying the most offences in the *Wholesale and retail trade and Transporting and storage sectors*.

To conclude, the risk indicators included in DATACROS **have demonstrated a strong predictive power**, confirming the relevance of corporate ownership opacity as a key element for identifying companies at a higher risk of committing financial crimes. Firms with *1) anomalous complexity of ownership*, *2) ownership links with high-risk jurisdictions*; and *3) ownership links with opaque corporate vehicles* are, in fact, more prone to engage in illicit activities. Finally, it is important to underscore here that country-specific and sector-specific patterns should also be taken into consideration in order to improve extant understanding of this phenomenon.

4.1.3 Feedback from partners and end-users

A survey was conducted amongst the project partners (*AFA, Cuerpo Nacional de la Policia, IRPI*), who reported a **high level of satisfaction** with the tool they tested (avg. satisfaction rate: **4.3** out of 5) and declared that they were highly likely to use DATACROS in the future (avg. likelihood: **4.3** out of 5). All partners reported that **they would recommend** the DATACROS Restricted Area to similar institutions.

Over the course of the project, the DATACROS Restricted Area was presented and discussed in dedicated meetings with **relevant networks of stakeholders**:

1. *CARIN network*, global network of Asset Recovery Offices;
2. *AMON network*, European network of law enforcement involved in AML investigations;
3. *NCPA network*, European (and global) network of anti-corruption authorities.

Following these presentations, several public authorities requested to activate their trial access to the tool.

4.2 Public Area: a tool for civil oversight

The **Public Area** of DATACROS is a dashboard environment for monitoring ownership anomalies across European countries[59], regions and business sectors at an aggregate level. The dashboard is freely accessible to everyone at the following link: https://datacros-public-area.app.crimetech.space/.

It includes **interactive maps, charts, and statistics** on European businesses, namely:

- Anomalous complexity of ownership structures
- Ownership links with high-risk countries
- Ownership links with opaque corporate vehicles
- Ownership links to PEPs

The tool comprises the following data sources:

1. **Business ownership data**: information on 56 million companies across 29 European countries[60], retrieved from *Orbis Europe* - a dataset provided by Bureau van Dijk. The data provides a snapshot of European businesses as of June 2019;
2. **Country blacklists**: EU black and grey lists of non-cooperative jurisdictions for tax purposes (November, 2019), as well as the FATAF black and grey lists of non-cooperative jurisdictions in the global fight against money laundering and terrorist financing (October, 2019).

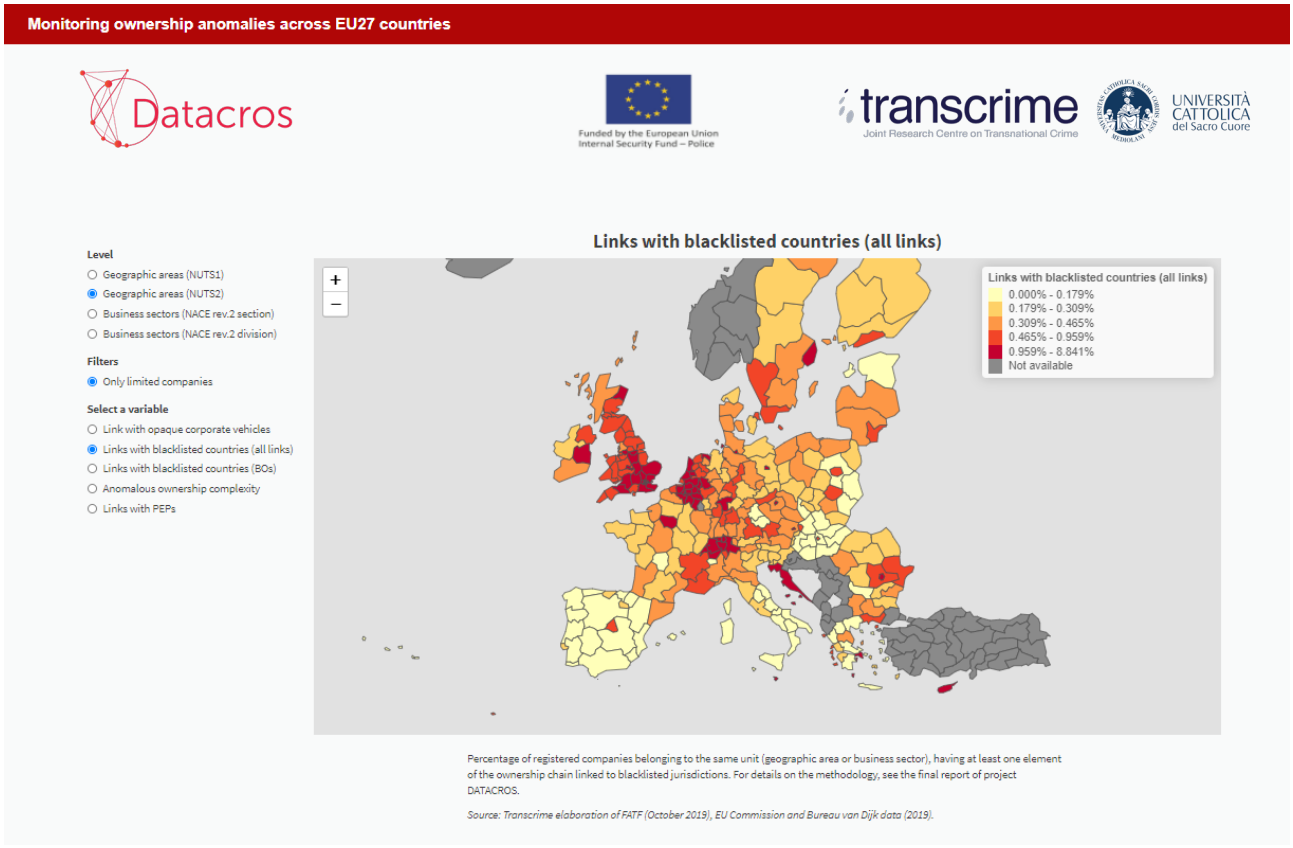
59. EU27 + UK and Switzerland

60. EU27 + UK and Switzerland.

Functions

The Public Area of the DATACROS tool allows the user to navigate between aggregate statistics that were calculated by Transcrime as part of the analysis of ownership anomalies in the EU presented in Chapter 3. Ownership anomaly scores are calculated for all private limited companies and public limited companies registered in EU27 + UK and Switzerland. This set includes 13.4 million companies, and it is discussed in detail in section 3.1.1.

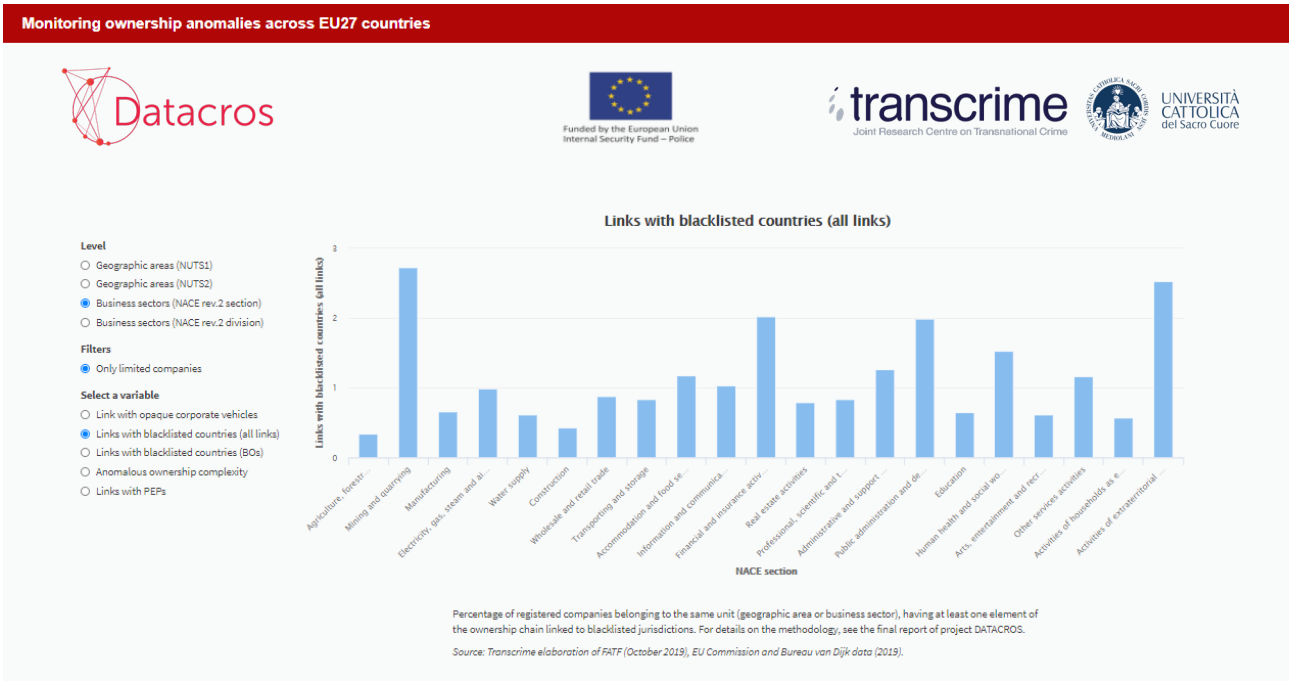
Figure 26 – Public Area of DATACROS: Representation of ownership anomalies at the regional level (NUTS2), 29 European countries (2019)



Through the filter section on the left-hand side of the dashboard, the user can select:

- **Level of representation**: aggregate metrics can be displayed at *regional level* (e.g. NUTS1, NUTS2, see Figure 25) or *sector level* - following the NACE rev.2 classification, with a more general sector classification (section level, see Figure 26), or more specific (division level).
- **Variables**: anomalies and risk factors, as presented and discussed in Chapter 3:
  - *o Anomalous complexity of ownership structures*
  - *o Ownership links with high-risk countries*
  - *o Ownership links with opaque corporate vehicles*
  - *o Ownership links to PEPs*

Figure 27- Public Area of DATACROS: Representation of ownership anomalies at the sector level (NACE rev.2, section), 29 European countries (2019)



USE CASE 5: Investigative journalists using the Public Area of DATACROS for monitoring anomalies at the sector level

Investigative Journalists can use the Public Area of DATACROS services for observing the presence of ownership anomalies at aggregate level across business sectors and geographical areas. This in turn can be used for:

- Identifying new patterns leadings to potential stories e.g. a geographic area showing an anomalous concentration of companies with BOs from high-risk countries;
- Confirming on-going investigations and corroborating stories involving companies active in high-risk areas and sectors.

5. Management of ethical, privacy and data protection issues

This chapter provides an overview of the activities that were conducted[61] to manage the **ethical, privacy and data protection issues** associated with project DATACROS. As planned in the Overview Report (Deliverable 2.1, 30 Sep 2019), we completed a *Data Protection Impact Assessment* (DPIA) for the Restricted Area of DATACROS.

5.1 Overall strategy

At the beginning of the project, a **preliminary risk assessment** was conducted to identify the potential ethical, privacy and personal data protection issues. The adopted management strategy included two main steps:

1. **Data source compliance assessment**: this assessment was conducted to verify that the data sources used in the tool complied with ethical, privacy and protection standards. The objectives of the assessment were as follows: a) to ensure privacy by design and privacy by default as per article 25 of the GDPR; b) to carry out a risk analysis and assessment of the data subjects' rights and fundamental freedoms as per article 24 of the GDPR; c) to ensure the effective exercising of data subjects' rights.
2. **Data Protection Impact Assessment (DPIA)**: this impact assessment was conducted to analyse, identify, and minimise the data protection risks associated with the project. For the purposes of DATACROS, a DPIA was conducted using the template issued by *Commission nationale de l'informatique et des libertés (CNIL)*[62].

61. The activities outlined in this chapter were carried out with the support of Massimiliano Capino

62. CLIN is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data.

5.2 Data protection impact assessment (DPIA)

A DPIA is required when the processing operations pose an **inherently high risk** to individuals' rights and freedoms. The preliminary risk assessment conducted in the first year of the project (September 2019) was inconclusive in terms of identifying "high risks[63]" in the processing operations involved in both the Public and Restricted Area of DATACROS. Nevertheless, it was decided to perform a DPIA to systematically address all the potential legal and ethical issues entailed in the Restricted Area[64] of DATACROS. The aims of the DPIA were:

- to precisely **identify** the risks involved in the proposed processing operation, taking into account the **nature of the data and the processing**, scope, context and purposes of the processing, as well as the sources of the risk – not only in normal circumstances, but also during special circumstances, and in the short-, medium- and long-term;
- to **evaluate** the identified (high) risk, particularly with respect to its origin, nature, and particularity, and both the likelihood and potential severity of the risk;
- to identify what **appropriate measures** can be taken to mitigate the (high) risks, in terms of the available technology and costs of implementation, and then propose such measures;
- to **record** the findings, evaluation and measures taken (or not taken, along with the reasons for not doing so), so as to be able to "**demonstrate compliance**" with the requirements of the GDPR under the "accountability" principle in relation to the assessed processing.

63. As defined by GDPR (Art. 35 paragraph 1).

64. The Public Area does not involve processing of any type of personal data, and thus it was excluded from the assessment.

A summary of both the contents and results from the DPIA are provided in the next section.

5.2.1 Purpose of processing

The **Restricted Area** of DATACROS is a **prototype tool** capable of detecting anomalies in firms' ownership structure that signal a high risk of collusion, corruption and money laundering within the EU, in order to support public authorities in their investigations of financial crime. The platform provides a set of services, which operate within a privacy and data protection environment that is configurable to local legal requirements.

The prototype tool allows for the early-detection of high-risk firms through identification of red flags in firm's characteristics and via the use of frontier machine learning algorithms. In particular, the tool:

- Identifies **firms' anomalies** and red flags, and then attributes them with a **risk score**
- Traces and reconstructs **cross-border ownership links**
- Detects **cartels and clusters of firms** which may signal collusive behaviour
- Assesses potential risks associated with protecting personal data, thus enabling the researchers to implement appropriate safeguards to mitigate such risks and technically enforce compliance with data protection law, to the fullest possible extent.

5.2.2 Types of data processed

The Restricted Area of DATACROS involves the processing of various types of information, including personal data. Specifically, we process the following types of data:

Non-Personal data

- **Data on companies' characteristics and ownership structure** (source: Bureau van Dijk): financials, territory, sector, and other general information;
- **Compliance List data on companies** (Source: LexisNexis WorldCompliance)
- **Country blacklists**: EU black and grey lists of non-cooperative jurisdictions for tax purposes (November, 2019), as well as FATF black and grey lists of non-cooperative jurisdictions in the global fight against money laundering and terrorist financing (October, 2019).

Personal Data

- **Data on companies' owners** (source: Bureau van Dijk): First name and surname, gender, date of birth (coverage: 10%), place of birth (coverage: 10%), country, BO distance, percentage of shareholding (direct and total) – includes *common categories of personal data*;
- **Compliance List data on individuals** - includes *special categories of personal data*:
  - o high-level PEPs (Source: LexisNexis World Compliance):
  - o local PEPs (ITA, FRA, ESP): - includes *special categories of personal data* (Sources: various sources[65] at the national level)

Information is retrieved by the DATACROS prototype tool only during users' sessions through API only for companies and related entities selected by end-users. In order to ensure "data minimisation", all the collected *personal data* are relevant and limited to the parameters deemed to be necessary for the purposes of the risk assessment. Details about the accuracy of the data, as well as how the data is updated based on the information given by data providers, are reported in the full version of the DPIA.

5.2.3 Data protection strategy

DATACROS was conceived and will continue to be carried out in accordance with **strict personal data and privacy protection obligations**. The strategy adopted to handle personal data is predicated on four pillars/ principles:

65. Italy (Source: Ministry of Interior), France (Source: Répertoir national des élus), Spain (Portal de Entitades Locales).

1. **Privacy-by-design concept**: the design of the DATACROS platform follows EU and MS' data protection rules (particularly those pertaining to the use of personal data by competent authorities, as stated below).
2. **Privacy-by-default concept**: the use of personal data is minimised unless strictly necessary, while in any case it is bound to existing rules governing their use (**data minimisation** principle)
3. **Systematic review of laws and guidelines**, at both the EU level and within each of the EU MS, with respect to the following domains (see full list of legal references in section 5.2.4):
   - o Use of personal data by LEAs and personal data protection;
   - o Use of risk profiling algorithms in investigations
   - o Criminal procedures, at both the EU and domestic level;
   - o AML/CFT and financial investigations.
4. The **implementation of logical and technical security safeguards** to preserve the integrity, availability and privacy of the processed data, as per ISO/IEC 27001:2013 standards (see section 5.2.5);

5.2.4 Key legislative references

The legal basis for making the processing lawful is the legitimate interest as per article 6, paragraph 1, letter f) of the GDPR. The following **key legislative references** constitute the parameters of the DATACROS prototype tool in terms of **personal data protection**:

- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of personal data (1981) – amended by Protocol CETS n° 223 and Protocol ETS n° 181;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance);
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April (European Parliament and Council of Europe 2016a) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ("LED"), and the MS' laws transposing the LED;
- Recommendation R(87)15 regulating the use of personal data in the police sector;
- Regulation (EU) 2016/794 of the European Parliament and of the Council on Europol;
- Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (EUROJUST);
- Guidelines on Automated individual decision-making and profiling for the purposes of GDPR (WP251) and the "Impact of GDPR on Artificial Intelligence";
- Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP 258, https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308;
- Flowcharts and Checklists on Data Protection by European Data Protection Supervisor (EDPS) issued on 6 July 2020;
- All national laws and guidelines issued by EU MS implementing and specifying the above listed legal acts.

5.2.5 Security safeguards

The following measures were implemented to preserve the integrity, availability and privacy of the processed data (e.g. individual accounts to authorised users; system of unalterable logs; secure environment), as per ISO/IEC 27001:2013 standards: 1) Data partitioning; 2) Logical access control; 3) Data minimisation; 4) Processing subcontracts; 5) Organisation measures; 6) Archiving; 7) Traceability; 8) Website security; 9) Hardware security; 10) Maintenance.

5.2.6 Information to be provided in the event that personal data was not obtained from the data subject

Data subjects are informed of the processing of their data via the privacy information notice published on the DATACROS website[66]. To exercise their rights concerning both data access and data portability, data subjects can contact Transcrime via email at: transcrime@unicatt.it, as reported in the privacy information notice.

5.2.7 Conclusions from DPIA

The DPIA highlighted that there were no significant risks to data subjects entailed in DATACROS. Therefore, the data processing related to DATACROS project can be implemented with no need of prior consultation with the Data Protection Authority, as envisaged by article 36 GDPR.

66. https://www.transcrime.it/datacros/wp-content/uploads/2021/03/DATACROS-Privacy-Policy.pdf

6. Conclusions and the way forward

6.1 Summary of findings

The opacity of corporate ownership has become a central issue in ongoing discussions around global financial crime patterns over the last 20 years. Several measures have been implemented worldwide in order to increase the transparency of firms and their owners, most notably, the establishment of BO registers. However, despite emergent interest in this issue, the empirical evidence-base and knowledge around this topic remains limited to handful of case-studies, with no large-scale analyses having been conducted. Moreover, the tools designed for risk assessment and risk monitoring of firms by public authorities (e.g., LEAs, FIUs, ACAs, TAs) are also lacking.

Project DATACROS has started addressing these gaps, by:

- **Proposing an innovative analytical approach** through which to measure the opacity of corporate ownership through a set of aggregate risk indicators at the macro level. The analysis conducted has mapped risk factors of ownership within legitimate businesses across EU countries, regions and business sectors. The results indicate that our knowledge of risky "hot-spots", both in terms of geographical areas and business sectors, remains limited. While most official blacklists (in both AML and tax domains) include developing countries and offshore jurisdictions, these data point out that **strong and stable economies**, including within the EU, also present certain vulnerabilities in terms of **corporate opacity and other red flags**.

- **Developing a prototype tool to support the investigation and risk assessment** of companies potentially involved in corruption, collusion or money laundering schemes. The survey conducted for the purposes of the project confirmed that **public authorities** in the EU declare a **strong need for technological solutions of this kind**. While the prototype is based on a database that was EU-limited in scope, it was successfully tested by project partners and was requested by a wider set of national and international LEAs and ACAs, all of whom provided highly promising feedback. The use of such tools can benefit a wide range of stakeholders in the EU and beyond, by:

  - Improving police investigations and judicial authorities' prosecution capabilities in cases of corruption and money laundering of its proceeds, especially cross-border cases;
  - Enhancing the ability of public authorities to detect cross-links between corruption, tax crime, organised crime, and fraud;
  - Increasing the effectiveness of cartel detection by competition authorities, especially within public procurement;
  - Allowing investigative journalists, NGOs and the entire civil society to check anomalous interactions between businesses, politics and public administration, and expose instances of corporate opacity;
  - Facilitating both national and EU authorities to map the role of entities from risky jurisdictions in public spending within the EU;
  - Enhancing the communication and data exchange between different public stakeholders (LEAs, ACAs, FIUs, CAs and TAs) and with civil society.

These findings lead us to offer the recommendations below.

6.2 Research recommendations

To improve knowledge of emerging illicit schemes

Further research efforts are required in order to advance knowledge on ownership opacity and increase the effectiveness of tools in this domain. In particular, it is important to increase the knowledge around the new – and underexamined - financial crime schemes that have emerged in relation to Covid-19. In fact, with the emergency of the global pandemic and the introduction of recovery plans by EU MS and by the European Union (e.g. *NextGenerationEU* instrument), criminal networks will seek further opportunities for draining public resources through the simultaneous use of corruption, fraud, tax crime and infiltration of public funds. Particular attention should be dedicated to investigating potential illicit conducts in public procurements procedures for accessing these public funds.

To improve mapping of risky areas/sectors

Future projects in this area should aim at advancing the understanding of *who are the owners* of EU companies, but also *how they exercise control*, to better understand *which companies* may be at risk of being misused to cover financial crime and other illicit schemes. New risk indicators in this domain should be developed, and a specific attention should be dedicated to analyzing the causes behind hotspots anomalous businesses identified in European territories or business sectors.

6.3 Policy recommendations

To facilitate integration of business registers across EU MS

The analysis conducted in project DATACROS shows a high level of interconnection between businesses in the European Union. Therefore, results support efforts and interventions by EU governments and the European Commission for facilitating the integration of business registers in the EU (e.g. the *Business Registers Interconnection System infrastructure - BRIS*[67], and the *Beneficial Ownership Registers Interconnection - BORIS*).

To reduce asymmetries in terms of opacity of businesses. and improve monitoring of risky situations.

The analysis conducted highlights great differences across business sectors and geographic areas in terms of concentration of companies with anomalous ownership characteristics. It is likely that criminals exploit asymmetries across EU MSs in terms of transparency requirements and set up businesses where concealing the identity of BOs is easier thanks to laxer regulation or controls. Therefore, the results of this project support the efforts by the European Union (e.g. 4th and 5th AMLD) to further **harmonise regulations** and promote business transparency in the EU.

Despite these regulatory efforts, criminals are still exploiting complex and opaque corporate ownership schemes for illicit goals. A number of scholars and practitioners are suggesting drastic regulatory measures such as limiting the lengths of ownership chains (Knobel 2021). However, these options have to be considered carefully, and one-size fits all solutions may create significant market distortions and generate additional costs on businesses, therefore hampering economic development and freedom of entrepreneurship. The results of this project rather suggest to **exploit available data analytics solutions and risk indicators** of anomaly to increase the effectiveness of monitoring, investigation and supervision of ownership opacity, without introducing new regulations and burdens on EU enterprises.

67.https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Business+Registers+Interconnection+System

To support public authorities with IT tools

We recommend that the EU supports the development and improvement of tools which respond to the needs by public authorities identified in Section 2.2 , to guarantee:

a. **More powerful risk assessment algorithms and richer data sources** with a wider geographical scope that extends beyond EU borders, in order to be able to detect global cross-border corruption schemes;

b. **The inclusion of a wider set of risk indicators and risk assessment algorithms** (e.g. covering financial red-flags, governance anomalies), also to tackle new illicit schemes that have emerged with the Covid-19 pandemic;

c. **A more integrated approach**, by extending the use of the tool to other stakeholders (e.g. FIUs, TAs and competition authorities), and strengthening the communication and exchange of expertise between them, LEAs, ACAs and civil society actors;

d. **Enhanced security**, both in terms of IT and personal data protection, so as to minimise the vulnerability to cyber-attacks, and with regard to guaranteeing EU citizens' privacy and rights.

To improve exchange and cooperation among public authorities

We recommend that the EU supports activities that promote communication, coordination and cooperation among the wide variety of stakeholders active in the fight of corruption, money laundering and other financial crimes (LEAs, ACAs, CAs, FIUs, Tax Agencies, Investigative journalists and civil society NGOs). The aim of these activities should be to:

a. **Exchange information** on crime schemes and anomaly indicators for detecting corruption and other financial crimes;

b. **Share best practices** on investigations and intelligence activities across EU MS;

c. **Provide requirements** and inputs for developing and improving risk assessment tools in this domain;

d. **Design integrated approaches** among stakeholders for early-detecting cross-links between corruption, collusion, bid-rigging, organised crime;

e. **Enhance communication** among public authorities and civil society.

References

Agence France-Presse. 2015. “Malaysian Taskforce Investigates Allegations $700m Paid to PM Najib.” The Guardian. July 6, 2015. http://www.theguardian.com/world/2015/jul/06/malaysian-task-force-investigates-allegations-700m-paid-to-pm-najib.

Andres Knobel. 2019. “More Beneficial Ownership Loopholes to Plug: Circular Ownership, Fragmented Control and Companies as Parties to the Trust.” Tax Justice Network. September 6, 2019. https://taxjustice.net/2019/09/06/more-beneficial-ownership-loopholes-to-plug-circular-ownership-control-with-little-ownership-and-companies-as-parties-to-the-trust/.

———. 2021. “Complex Ownership Structures. Addressing the Risks for Beneficial Ownership Transparency.” Tax Justice Newrok Working Paper, March.

Antonio Castaldo, Milena Gabanelli. 2020. “Covid, mafia e usura: chi sono gli sciacalli che speculano sull’epidemia.” Corriere della Sera. November 11, 2020. https://www.corriere.it/dataroom-milena-gabanelli/covid-mafia-usura-quante-carogne-campano-sulle-disgrazie/a71638de-2370-11eb-852a-fddf-3d627dac-va.shtml.

Aziani, Alberto, Joras Ferwerda, and Michele Riccardi. 2020. “Who Are Our Owners? Exploring the Cross-Border Ownership Links of European Businesses to Assess the Risk of Illicit Financial Flows.” European Journal of Criminology - in Course of Publication, no. 1: 43.

———. 2021. “Who Are Our Owners? Exploring the Ownership Links of Businesses to Identify Illicit Financial Flows.” European Journal of Criminology, January, 1477370820980368. https://doi.org/10.1177/1477370820980368.

Borselli, F. 2011. “Organised VAT Fraud: Features, Magnitude, Policy Perspective.” 106. Questioni Di Economia e Finanza. Roma: Banca D’Italia. http://www.bancaditalia.it/pubblicazioni/econo/temidi/td12/td868_12/en_td868/en_tema_868.pdf.

Charron, Nicholas, Carl Dahlström, Mihaly Fazekas, and Victor Lapuente. 2017. “Careers, Connections, and Corruption Risks: Investigating the Impact of Bureaucratic Meritocracy on Public Procurement Processes.” The Journal of Politics 79 (1): 89–104. https://doi.org/10.1086/687209.

Chong, Eshien, Michael Klien, and Stéphane Saussier. 2015. “The Quality of Governance and the Use of Negotiated Procurement Procedures: Evidence from the European Union.” Chaire Economie Des Partenariats Public-Privé Institut d’Administration Des Entreprises 3 (August). http://www.chaire-eppp.org/files_chaire/chong-klien-saussier-2015.pdf.

Conley, Timothy G., and Francesco Decarolis. 2016. “Detecting Bidders Groups in Collusive Auctions.” American Economic Journal: Microeconomics 8 (2): 1–38.

Council of Europe. 1981. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. European Treaty Series.

Daniel Haberly. 2020. “Mapping Politically Exposed Person (PEP)-Linked Shell Companies in the Panama and Paradise Papers.” Global Integrity Anti-Corruption Evidence. June 23, 2020. https://ace.globalintegrity.org/shellcompanies/.

DIA. 2016. “Relazione Del Ministero Dell’Interno Sull’attività Svolta e Sui Risultati Conseguiti Dalla Direzione Investigativa Antimafia. Primo Semestre 2016.” Ministero dell’Interno.

———. 2017. “Relazione Del Ministero Dell’Interno Sull’attività Svolta e Sui Risultati Conseguiti Dalla Direzione Investigativa Antimafia. Secondo Semestre 2017.” Ministero dell’Interno.

———. 2019. “Relazione Semestrale Sull’attività Svolta e Sui Risultati Conseguiti Dalla Direzione Investigativa Antimafia - Secondo Semestre 2019.” Ministero dell’Interno.

Does de Willebois, Emile van der, Emiliy Halter M., Robert. A. Harrison, Ji Won Park, and J.C. Sharman. 2011. The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. The World Bank. http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8894-5.

Does de Willebois, Van der, Emile, Emiliy Halter M., Robert. A. Harrison, Ji Won Park, and J.C. Sharman. 2011. The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It. The World Bank. http://elibrary.worldbank.org/doi/book/10.1596/978-0-8213-8894-5.

Duyne, Petrus C. van, and T. J. van Koningsveld. 2017a. "The Offshore World: Nebolous Finance." In The Many Faces of Crime for Profit and Ways of Tackling It.

———. 2017b. "The Offshore World: Nebolous Finance." In The Many Faces of Crime for Profit and Ways of Tackling It.

EFECC. 2020. "Enterprising Criminals – Europe's Fight against the Global Networks of Financial and Economic Crime." https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime.

European Commission. 2017. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Making Public Procurement Work in and for Europe." Strasbourg: European Commission. https://ec.europa.eu/docsroom/documents/25612.

———. 2019a. "Report from the Commission to the European Parliament and the Council on the Assessment of the Risk of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-Border Activities." Brussels.

———. 2019b. "Evolution of the EU List of Tax Havens." Https://Ec.Europa.Eu/. November 8, 2019. https://ec.europa.eu/taxation_customs/sites/taxation/files/eu_list_update_08_11_2019_en.pdf.

———. 2020a. "Taxation: EU List of Non-Cooperative Jurisdictions." 2020. https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/.

———. 2020b. "Methodology for Identifying High-Risk Third Countries under Directive (EU) 2015/849." https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf.

———. 2020c. "2020 Rule of Law Report - Country Chapter on the Rule of Law Situation in Malta." COMMISSION STAFF WORKING DOCUMENT. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0317&from=EN.

European Parliament, and Council of Europe. 2016a. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

———. 2016b. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance); Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Parliament and Council of the European Union. 2015. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015. Official Journal of the European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

———. 2018. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

Europol. 2018. “EU-Wide VAT Fraud Organised Crime Group Busted.” Europol. 2018. https://www.europol.europa.eu/newsroom/news/eu-wide-vat-fraud-organised-crime-group-busted.

———. 2019. “Parallel Investigations Bring down Sexual Exploitation Network and Freeze Criminal Profits in 12 Counties.” 2019. https://www.europol.europa.eu/newsroom/news/parallel-investigations-bring-down-sexual-exploitation-network-and-freeze-criminal-profits-in-12-counties.

FATF. 2006. “The Misuse of Corporate Vehicles, Including Trust and Company Service Providers.” Paris: The Financial Action Task Force. http://www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf.

———. 2010a. “Money Laundering Using Trust and Company Service Providers.” Paris: Financial Action Task Force - Organization for Economic Cooperation and Development. http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf.

———. 2010b. “Money Laundering Using Trust and Company Service Providers.” Paris: Financial Action Task Force - Organization for Economic Cooperation and Development. http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf.

———. 2012. “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations.” Paris, France: The Financial Action Task Force.

———. 2013a. “FATF Guidance - Politically Exposed Persons (Recommendations 12 and 22).”

———. 2013b. “FATF Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems.” Financial Action Task Force. https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

———. 2014. “FATF Guidelines on Transparency and Beneficial Ownership.” Paris: Financial Action Task Force - Organization for Economic Cooperation and Development. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

———. 2017. “Topic: High-Risk and Non-Cooperative Jurisdictions.” Financial Action Task Force. http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate).

———. 2018. “Financial Flows from Human Trafficking.” Financial Action Task Force. https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.

———. 2019a. “Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations.” Financial Action Task Force. https://www.fatf-gafi.org/publications/mutualevaluations/documents/4th-round-procedures.html.

———. 2019b. “Improving Global AML/CFT Compliance: On-Going Process - 18 October 2019.” October 2019. http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-october-2019.html.

———. 2020. “COVID-19-Related Money Laundering and Terrorist Financing Risks and Policy Responses.” https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf.

Fazekas, Mihály, and Gábor Kocsis. 2020. “Uncovering High-Level Corruption: Cross-National Objective Corruption Risk Indicators Using Public Procurement Data.” British Journal of Political Science 50 (1): 155–64. https://doi.org/10.1017/S0007123417000461.

Fazekas, Mihály, István János Tóth, and Lawrence Peter King. 2013a. “Anatomy of Grand Corruption: A Composite Corruption Risk Index Based on Objective Data.” Social Science Research Network 2: 1–46.

———. 2013b. “Corruption Manual for Beginners: ‘Corruption Techniques’ in Public Procurement with Examples from Hungary.” SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2333354.

Ferwerda, Joras, and R. Edward Kleemans. 2018. “Estimating Money Laundering Risks: An Application to Business Sectors in the Netherlands.” European Journal of Criminal Policy and Research.

Garcia-Bernardo, Javier, Jan Fichtner, Frank W. Takes, and Eelke Heemskerk. 2017a. “Uncovering Offshore Financial Centers: Conduits and Sinks in the Global Corporate Ownership Network | Scientific Reports.” Nature Scientific Reportsvolume 7, Article number: 6246 (2017). https://www.nature.com/articles/s41598-017-06322-9.

———. 2017b. “Uncovering Offshore Financial Centers: Conduits and Sinks in the Global Corporate Ownership Network | Scientific Reports.” Nature Scientific Reportsvolume 7, Article number: 6246 (2017). https://www.nature.com/articles/s41598-017-06322-9.

Gdf. 2015. “Operazione Gambling - Eseguite 41 Ordinanze Di Custodia Cautelare.” July 22, 2015. http://www.gdf.gov.it/stampa/ultime-notizie/anno-2015/luglio-2015/operazione-gambling-eseguite-41-ordinanze-di-custodia-cautelare.

Global Witness. 2020. “Patchy Progress in Setting Up Public Beneficial Ownership Registers in the EU.” Global Witness. March 20, 2020. https:///en/campaigns/corruption-and-money-laundering/anonymous-company-owners/5amld-patchy-progress/.

Halliday, Terence, Michael Levi, and Peter Reuter. 2014. “Global Surveillance of Dirty Money: Assessing Assessments of Regimes To Control Money-Laundering and Combat the Financing of Terrorism.” Chicago: American Bar Foundation. http://www.lexglobal.org/files/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf.

Hangacova, Natalia, and Tomas Stremy. 2018. “Value Added Tax and Carousel Fraud Schemes in the European Union and the Slovak Republik.” European Journal of Crime, Criminal Law and Criminal Justice. https://doi.org/10.1163/15718174-02602005.

HM Revenue & Customs. 2010. “Anti-Money Laundering Guidance for Trust or Company Service Providers.” London: HM Revenue & Customs. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/372271/mlr8_tcsp.pdf.

IADB and OECD. 2019. A Beneficial Ownership Implementation Toolkit. Inter-American Development Bank and OECD. https://doi.org/10.18235/0001711.

ICIJ. 2016. “The Panama Papers: Exposing the Rogue Offshore Finance Industry - ICIJ.” 2016. https://www.icij.org/investigations/panama-papers/.

———. 2017. “Paradise Papers Exposes Donald Trump-Russia Links and Piggy Banks of the Wealthiest 1 Percent.” ICIJ. November 5, 2017. https://www.icij.org/investigations/paradise-papers/paradise-papers-exposes-donald-trump-russia-links-and-piggy-banks-of-the-wealthiest-1-percent/.

Imhof, David, and Yavuz Karagok. 2017. “Screening for Bid-Rigging – Does It Work?” CRESE Working Papers No 2017-09.

King, Colin, Clive Walker, and Jimmy Gurulé, eds. 2018. The Palgrave Handbook of Criminal and Terrorism Financing Law. Vol. II. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64498-1.

Knobel, Andres. 2019. “Beneficial Ownership in the Investment Industry: A Strategy to Roll Back Anonymous Capital.” SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3470358.

Law, Jonathan. 2009. Trust. Oxford University Press. https://doi.org/10.1093/acref/9780199234899.013.6562.

Le Parisien. 2009. “Les parrains du Vieux-Port avaient bâti un empire mafieux.” Le Parisien, 2009. http://www.leparisien.fr/faits-divers/les-parrains-du-vieux-port-avaient-bati-un-empire-mafieux-05-10-2009-662406.php.

Levi, Michael, Peter Reuter, and Terence Halliday. 2018. “Can the AML System Be Evaluated without Better Data?” Crime, Law and Social Change 69 (2): 307–28. https://doi.org/10.1007/s10611-017-9757-4.

Moneyval. 2019. “Anti-Money Laundering and Counter-Terrorist Financing Measures - Malta.” Fifth Round Mutual Evaluation Report.

Mungiu-Pippidi, Alina. 2016. “The Good, the Bad and the Ugly: Controlling Corruption in the European Union.” Berlin: Hertie School of Governance. http://www.againstcorruption.eu/reports/the-good-the-bad-and-the-ugly-controlling-corruption-in-the-european-union/.

Natrella, Giuseppe. 2018. “Appalti: Corigliano Calabro, 50 imprese controllate da una persona – Lamezia oggi.” Lamezia Oggi, July 12, 2018. https://www.lameziaoggi.it/cronaca/2018/07/12/appalti-corigliano-calabro-50-imprese-controllate-da-una-persona/.

Netherlands Chamber of Commerce - KVK. 2020. “Foundation - Stichting.” Business.Gov.Nl. 2020. https://business.gov.nl/starting-your-business/choosing-a-business-structure/foundation/.

OCCRP. 2019. “The Troika Laundromat.” The Organized Crime and Corruption Reporting Project. March 4, 2019. https://www.occrp.org/en/troikalaundromat/.

OECD. 2001. “Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes.” Paris: Organisation for Economic Co-operation and Development. http://www.oecd.org/daf/ca/behindthecorporateveilusingcorporateentitiesforillicitpurposes.htm.

———. 2019a. “Global Forum on Transparency and Exchange of Information for Tax Purposes: The Netherlands 2019 (Second Round).” Global Forum on Transparency and Exchange of Information for Tax Purposes: Peer Reviews. https://www.oecd.org/tax/transparency/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-the-netherlands-2019-second-round-fdce8e7f-en.htm.

———. 2019b. “Peer Review Report on the Exchange of Intormation on Request.” Global Forum on Transparency and Exchange of Information for Tax Purposes - Organisation for Economic Co-operation and Development. https://www.oecd.org/tax/transparency/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-the-netherlands-2019-second-round-fdce8e7f-en.htm.

OLAF. 2017. “Fraud in Public Procurement - A Collection of Red Flags and Best Practices.” European Anti-Fraud Office. https://ec.europa.eu/sfc/sites/sfc2014/files/sfc-files/Fraud%20in%20Public%20Procurement_final%2020.12.2017%20ARES%282017%296254403.pdf.

Rajwani, Tazeeb, and Tahiru Azaaviele Liedong. 2015. “Political Activity and Firm Performance within Nonmarket Research: A Review and International Comparative Assessment.” Journal of World Business 50 (2): 273–83. https://doi.org/10.1016/j.jwb.2014.10.004.

Riccardi, Michele. 2020. Beyond Blacklists: An Alternative Approach to Identifying Countries at High-Risk of Money Laundering and Illicit Financial Flows - Working Paper.

Riccardi, Michele, Riccardo Milani, and Diana Camerini. 2018a. “Assessing Money Laundering Risk across Regions. An Application in Italy.” European Journal of Criminal Policy and Research.

———. 2018b. “Assessing Money Laundering Risk across Regions. An Application in Italy.” European Journal of Criminal Policy and Research.

Riccardi, Michele, and Ernesto U. Savona, eds. 2013. Final Report of Project BOWNET - Identifying the Beneficial Owner of Legal Entities in the Fight against Money Laundering Networks. Trento: Transcrime - Università degli Studi di Trento. http://www.bownet.eu/materials/BOWNET.pdf.

Rose-Ackerman, Susan, and Bonnie J. Palifka. 2016. Corruption and Government: Causes, Consequences, and Reform. Second edition. New York, NY: Cambridge University Press.

Savona, Ernesto U., and Michele Riccardi, eds. 2017. Assessing the Risk of Money Laundering in Europe - Final Report of Project IARM. Milano: Transcrime - Università Cattolica Sacro Cuore. www.transcrime.it/iarm.

———. 2018. Mapping the Risk of Organised Crime Infiltration in European Businesses - Final Report of Project MORE. Università Cattolica del Sacro Cuore. MIlano. In course of publication.

Savona, Ernesto U., Michele Riccardi, and Giulia Berlusconi, eds. 2016. Organised Crime in European Businesses. Abingdon: Routledge.

Soreide, Tina. 2002. Corruption in Public Procurement Causes, Consequences and Cures. Bergen: Chr. Michelsen institute (CMI).

Tavares, Rui. 2013. “Relationship between Money Laundering, Tax Evasion and Tax Havens.” Thematic Paper on Money Laundering. Bruxelles: European Parliament - Special Committee on Organised Crime, Corruption and Money Laundering. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dv/tavares_ml_/tavares_ml_en.pdf.

Tax Justice Network. 2015. “Financial Secrecy Index - 2015 Methodology.” Chesham: Tax Justice Network. http://www.financialsecrecyindex.com/PDF/FSI-Methodology.pdf.

———. 2018. “Financial Secrecy Index - 2018 Results.” Tax Justice Network. https://www.financialsecrecyindex.com/introduction/fsi-2018-results.

———. 2020. “Financial Secrecy Index 2020 - Methodology.” Chesham: Tax Justice Network. https://fsi.taxjustice.net/PDF/FSI-Methodology.pdf.

Transcrime, ed. 2018. Mapping the Risk of Serious and Organised Crime Infiltration in Europe - Final Report of the MORE Project. Milano: Università Cattolica del Sacro Cuore. www.transcrime.it/more.

Tribunal de Marseille. 2009. Ordonnance de non-lieu partiel et de renvoi devant le Tribunal Correctionnel. Tribunal de Grande Instance de Marseille.

UNODC. 2020. “Covid-19 Vaccines & Corruption Risks: Preventing Corruption In The Manufacture, Allocation And Distribution Of Vaccines.” COVID-19 POLICY PAPER.

World Bank. 2011. “The World Bank Risk Assessment Methodology.” The World Bank. http://www.fatf-gafi.org/media/fatf/documents/reports/risk_assessment_world_bank.pdf.