coeso

connecting research and society

COLLABORATIVE ENGAGEMENT ON SOCIETAL ISSUES

WP2 – Pilots implementation and Open call

Report on the technical and legal framework for sharing confidential data

date 30.03.2022

COESO has received funding from the EU Horizon 2020 Research and Innovation Programme (2014-2020) SwafS-27-2020 - Hands-on citizen science and frugal innovation, under Grant Agreement No.101006325

Deliverable 2.9

Grant Agreement number	:	101006325
Project acronym	:	COESO
Project title	:	Collaborative Engagement on Societal Issues
Funding Scheme	:	H2020-EU.5. - SCIENCE WITH AND FOR SOCIETY
Topic	:	SwafS-27-2020 - Hands-on citizen science and frugal innovation
Project's coordinator Organization	:	EHESS-OpenEdition
E-mail address	:	pierre.mounier@openedition.org, alessia.smaniotto@openedition.org
Website	:	https://coeso.hypotheses.org

WP and tasks contributing	:	WP2 – Pilots implementation and Open call
WP leader	:	CRIA
Task leader	:	IRPI (Task 2.7)
Dissemination level	:	Public
Due date	:	31 March 2022
Delivery date	:	30 March 2022
Author	:	Michele Riccardi (Crime&tech)
Contributors	:	Luca Rinaldi (IRPI), Lorenzo Bagnoli (IRPI)
Reviewers	:	Prof. Massimiliano Carpino (Università Cattolica del Sacro Cuore), Arnaud Gingold (AMU-OpenEdition)

Contents

I. Introduction

Aim of this report

Pilot 4 – *Tools and databases to increase the impact of investigative journalism* – is aimed at creating a collaborative space between researchers (namely, the Crime&tech spin-off of Università Cattolica del Sacro Cuore) and civil society (namely, the investigative journalists at IRPI) with the aim to (a) improve journalistic investigations on corruption, collusion and financial crime; (b) improve the development of IT tools and (c) setting a sustainable framework for sharing sensitive data. In doing so, the project builds on previous projects which entailed a collaboration between the two entities, in particular on the EU co-funded project DATACROS.

The activity of Pilot 4 – but in general any collaboration between researchers and investigative journalists, and more specifically any collaboration in the field of crime investigation – lives a constant opposition and (re)composition between three poles, which are three sets of fundamental rights:

- On the one side, the need to **safeguard personal data and sensitive information** (e.g. those which are crucial to carry out a safe and effective investigation), in line with Articles 6, 7 and 8 of the Charter of Fundamental rights of the European Union;
- On the other side, the need to guarantee the **right of access to and freedom of information**, in line with Article 11 of the above mentioned Charter;
- On a third front, the push (fostered by the European Commission) of **'FAIR-ification',** i.e. the need to produce information which could be findable, openly accessible, interoperable and re-usable for research purposes, in line with Article 13 of the Charter.

This constant opposition/(re)composition poses important challenges both from the **legal and technical point of view.** This report (Deliverable D2.9), building on the specific collaboration experienced by IRPI and Crime&tech in the COESO and DATACROS projects (and in related initiatives) aims at **discussing them in-depth, in the light of paving the way for future partnerships between researchers and investigative journalists**, especially in the field of **investigation of (potentially) criminal behavior,** improve transparency and prevent inequality and illicit activities.

Background: the tool and the data employed

Understanding the nature of the tool and the data employed by the two groups of users is crucial for contextualizing the discussion of the legal and technical challenges. As said, for the purpose of COESO, IRPI has been employing a tool and a set of data which

build on what was developed previously under **project DATACROS** (hereinafter 'DATACROS tool prototype').

The DATACROS tool prototype was designed to **detect anomalies in firms' ownership structure that can flag high risks of collusion, corruption and money laundering** within the European Union. In particular, the tool is able to potentially **rate any single company (or group of companies)** within the EU28 countries in terms of the risk they can be involved in financial crime schemes.

The tool employs a wide set of information, including:

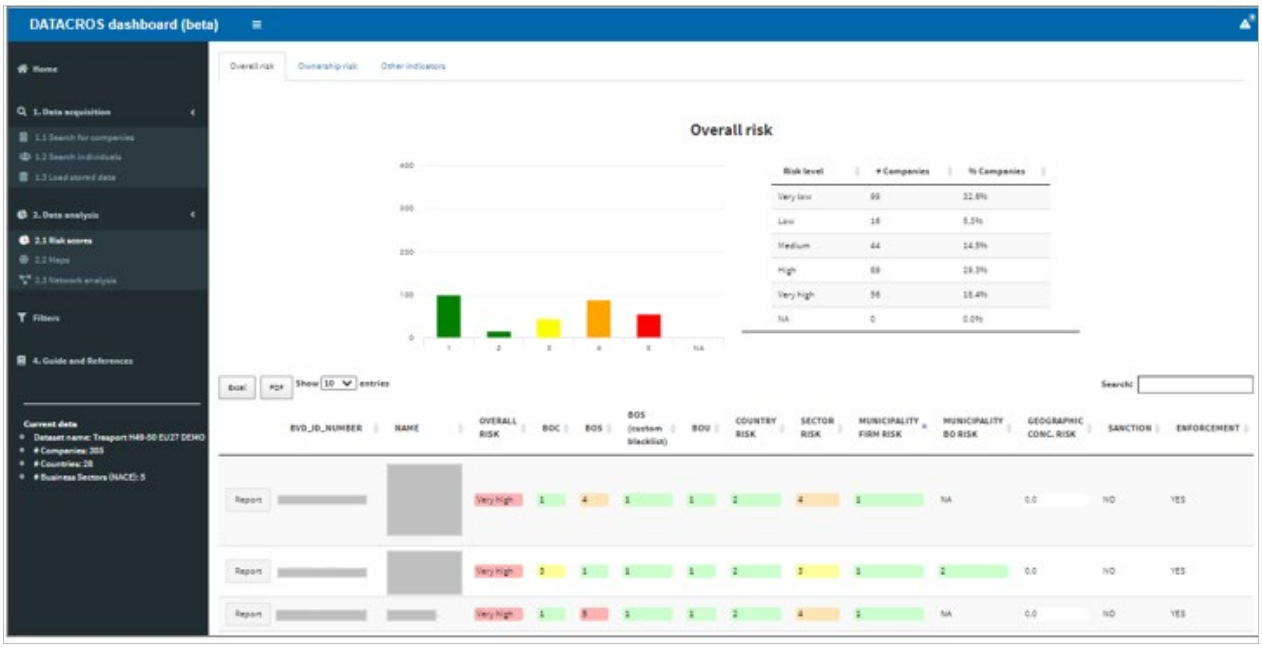
- Business ownership data on individuals (e.g. name of owners/shareholders, beneficial owners, directors, etc.);
- Business ownership data on companies (e.g. financials, territory and sector of activity, etc.);
- Data on politically exposed persons (PEPs) and local political administrators;
- Data on countries registered in official blacklists/greylists in the anti-money laundering (AML) and fiscal domain;
- Occasionally, data on individuals and entities included in official sanction or enforcement lists (e.g. Office Foreign Asset Control - OFAC, United Nations or EU sanctioned entities/individuals).

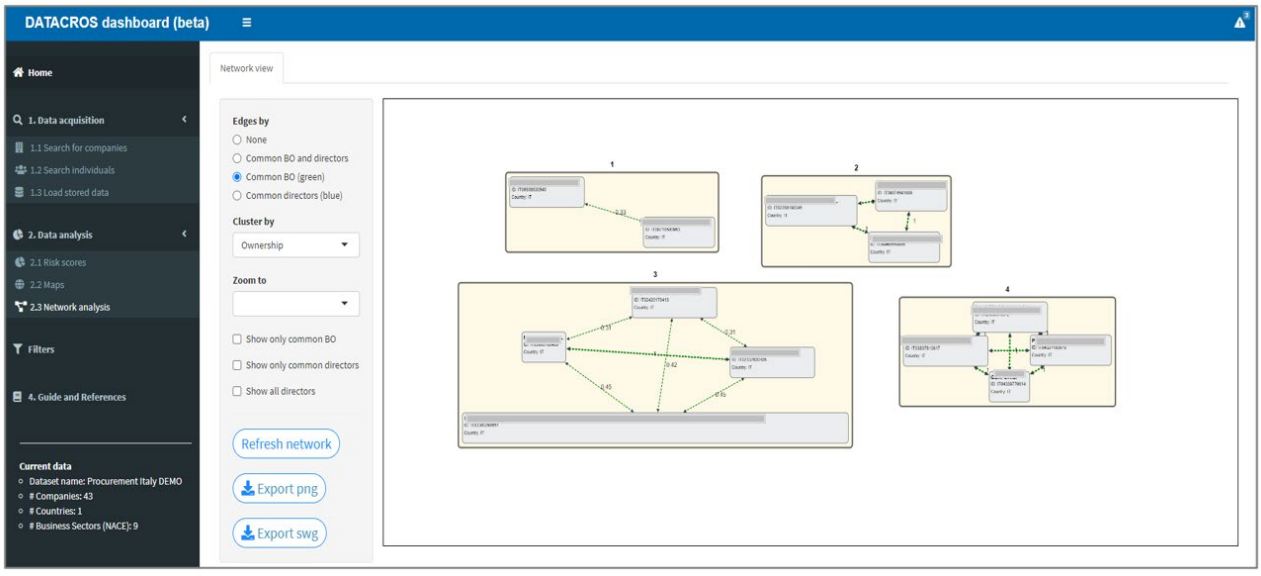
It is important to stress that the data employed is **not obtained directly from data subjects**, but it rather stems from **few identified public official sources and world-class data providers**. Generally speaking, this is the rule in journalistic investigations (at least in this field), as it will be discussed below.

The tool processes and combines this information and makes it available in the tool's User interface (UI) through a set of **data analytics and data visualization services**, in particular, a (a) risk scoring dashboard, a (b) ownership network visualizer and (c) a geo-mapping service.

Within COESO, IRPI is employing this tool for the analysis of the risks in two specific domains: (i) the **real estate sector**, with particular focus on Italy and (ii) the **maritime industry**, and in particular the illicit trafficking facilitated by legitimate ports and maritime companies in the Mediterranean.

Figure 1 – The DATACROS tool prototype: (a) risk scoring dashboard, a (b) ownership network visualizer





II. Legal framework and challenges

While an analysis of the legal framework can address a number of regulatory issues, focus here is posed on personal data protection, and more specifically on the challenges related to finding a balance between the employment of novel investigative tools by journalists and the need to safeguard individuals' privacy.

The legal basis

As mentioned, the processing purpose of the tool employed by IRPI is to early-detect (and rate) the risk, associated to a company or a group of companies, of being involved in financial crime schemes (e.g. corruption, collusion, money laundering, etc). For doing so, the tool processes some personal data (e.g. name of owners or directors of a firm). IRPI has been, together with the other DATACROS end-users, appointed as **joint controller** in the use of these tools (see DATACROS information notice pursuant to article 14 (5) (b) of GDPR).

The legal basis making the processing lawful is the **legitimate interest as per article 6, paragraph 1, letter (f) of the GDPR:** *"(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"* (Regulation 2016/679/EC, Art.6 (1)(f)).

In particular, the processing purposes is legitimate because DATACROS has been awarded by the **European Commission, DG Migration and Home Affairs**, whose specific objective is to ensure that all activities necessary and beneficial to the economic, cultural and social growth of the EU may develop in a **stable, lawful and secure environment** in particular by (a) fighting terrorism and organised crime, (b) promoting police cooperation and (c) preparing to swiftly respond to emerging crisis (see DG HOME website). Specifically, the call under which DATACROS was funded is the ISFP (Internal Security Fund Police)–2017-CORRUPT which had the specific objective of *"pursuing the public interest by fighting crime, and in particular corruption and money laundering, within the European Union"* (European Commission, 2017).

Public interest, freedom of information and personal data protection

The question is whether this tool and the background data – and the associated legitimate basis which has been just described - could be employed also outside an EU co-funded project in this area, i.e. in a **'ordinary' journalistic investigation**. While an

extended discussion of the relationship between freedom of information and personal data protection goes beyond the scope of this report (see instead Caruso, De Miguel Beriain & Pérez Campillo, 2020 for an in-depth discussion) it is useful to highlight certain fundamental issues which help setting the boundaries of the legal challenges that journalists have to face when carrying out investigations, at least in the crime domain. Most of these challenges are shared also by researchers in this field.

- Investigative journalists often carry out – practically speaking – the same kind of investigation that could be performed by law enforcement agencies (LEAs) or other competent authorities; but they **cannot benefit from the same regulatory framework** in which LEAs move, and which sets certain exemptions in their personal data processing. For example, Directive (EU) 2016/680 has contributed to discipline the processing of personal data for *"prevention, investigation and prosecution of criminal offences"* – which however does not apply for non-competent authorities (for a commentary, see Carpino, 2020).

- At the same time, journalistic investigations in the financial crime realm **do not usually rely on information collected directly from the data subjects** – who may be the target of the same investigation. This means that, of course, informed consents cannot be requested to the data subjects while, on the contrary, these latter should know the least as possible about the on-going investigation so as not to affect (a) the sensitivity and relevance of the journalistic investigation and (b) the security of the journalists themselves (on this, see below).

- Similarly, journalists cannot benefit from **clauses in contracts and pre-contracts** which instead are broadly employed in the private sector for conducting certain investigations on individuals. For example, in the anti-money laundering (AML) or anti-fraud domain, banks and other financial institutions may ask informed consents to clients so as to be authorized to collect and process some personal data related to them (including *special categories* of personal data, e.g. previous enforcement measures or judicial penalties) for due diligence purposes – in line with what is requested by the relevant regulation (e.g. AML) and in any case as bound by relevant regulations and opinions (see e.g. the limits set by Opinion 12/2021 of the European Data Protection Supervisor on AML/CFT).

- While a specific article – Art. 85 – is included in the GDPR to address the tension between **personal data processing and freedom of expression and information**, it is very broadly and vaguely designed, eventually leaving to EU Member States the possibility to exempt those who can exercise freedom of information (e.g. through journalistic activity) from certain GDPR provisions and obligations (Bitiukova, 2020). Even Recital 153 of the GDPR does not fully help to clarify the conditions for application of the derogations of journalists from GDPR. Consequently, a wide variety of interpretations and experiences have been observed across EU MS, which also generated harsh discussions and cases in

front of national data protection authorities and courts (Caruso et al. 2020, for a review).[1]

- Main reference therefore becomes the **current jurisprudence** of both the **European Court of Justice (CJEU) and the European Court of Human Rights (ECtHR)**. In summary, the case-law suggests that a case-by-case assessment of the balance between freedom of information and personal data protection shall be carried out. In this balance, several elements appear to be important – albeit not necessarily easy to be operationalized or interpreted in practice:

    - The **general public interest** addressed by the journalistic investigation (or broadly speaking by the 'freedom of information'-related activity);
    - The **level of intrusion** into an individual's privacy entailed by the investigation;
    - The **potential harm** which could be caused to individuals;
    - The possibility to achieve the same objective of public interest in a **less intrusive manner**.

- Key in this assessment is how the **notion of public interest** may be conceptualized and interpreted. Both CJEU and ECtHR historically avoided to define in detail what 'public interest' means, leaving margins for interpretation according to the circumstance. However, as outlined by Bitiukova (2020, p. 21), they provided some guidelines: *"the ECtHR [...] recognized this notion to cover the public, political and historic debate, issues related to the politicians, behavior of the public servants, large corporations, governments, crime-related matters".* In this light, 'public interest' shall not be interpreted as simply the public curiosity and gossip about details of the personal life of certain (public) persons, but it shall entail a tangible value in terms of knowledge on how the public sphere works. Or, as phrased by Council of Europe (2019, 12): *"Areas considered to be of public interest include - yet are not limited to -* ***misuse of public office, improper use of public money, protection of public health,*** *safety and environment, protection of national security, crime and social behaviour and similar political and socioeconomic topics"*.

- Similarly, the **notion of 'public person'** should not be interpreted strictly as persons who are already known to the public (or known as vested of a public role), but *"what matters is whether the person has entered the public arena by participating in a public debate, by being active in a field of public concern or in public debate"* (Council of Europe, 2019, p. 20).

- In summary, while neither the regulation, nor the jurisprudence, clarify in a

[1] See for example the case of RISE project in Romania and the Romanian data protection authority, reported by Caruso et al., 2020.

univocal manner the conditions under which personal data shall or may be processed in journalism – including journalistic investigations in the field of financial crime - it is clear that the **principles of proportionality and necessity** – which inspire the whole EU personal data protection regulatory framework, and are aligned with the so-called **'data minimization' principle** – still play a key role. As far as the 'public interest' is satisfied by investigative journalists in using certain tools or data, and the processing is proportionate (and its level of intrusion is, *ceteris paribus,* minimized), the employment of personal data may be, generally speaking, **lawful and object of a legitimate interest**.

- This is particularly true for **journalistic investigations in the financial crime** domain, and more specifically – such as in DATACROS or COESO – in the realm of anti-corruption and anti-money laundering given that, as stated by the Council of Europe, "***misuse of public office, improper use of public money"*** are explicitly mentioned as areas of 'public interest'.

Freedom of information and the protection of journalists' personal data and fundamental rights

On the other side, freedom of information may have unintended effects on the privacy (and fundamental rights) of the same researchers and journalists. This paradox has been highlighted already in several circumstances by media officers at EU and national level. In particular, it has been stressed that the request of information to a public administration by a journalist according to **Freedom of Information (FOI)** laws (or access to information laws) may lead the administration to **inform the same subject of the inquiry** about the information request. This may obviously not only expose the journalistic investigation at risk, but the same journalists to be violated in their privacy and fundamental rights – including suffering threat to their life.

The most known example is what happened to the **Slovak journalist Jan Kuciak**, who was likely killed on February, 2018, as a result of his work as an investigative journalist and in particular after his FOI requests were passed to the data subject under investigation (OCCRP, 2022). Jan Kuciak had requested information from various public agencies, including Slovakia's Agricultural Paying Agency, which handles the EU subsidies, the public prosecutor's office in Trebisov, east of Bratislava, the regional court in Bratislava, and SEPAS, the Slovak energy agency. All his requests were accompanied by his personal details (as requested), such as the home address. In some instances, all this information was passed to the companies which were under his scrutiny and eventually, dramatically, to those who hired the hitmen who killed him.

IRPI journalists – coordinator of this pilot – faced the same difficulty several times. In one of these cases, an IRPI journalist, who was working on an **illicit waste trafficking case**, filed a FOI request to three regions about the waste transportation operations

conducted by a broker and two companies operating with the public administration in the field of waste disposal; after this request, the enquired administrations passed the information about the FOI request to the same broker and the involved companies, **without concealing the personal data of the IRPI journalist** (name, date of birth, residence, telephone and email contact), and the reason behind the request. As a consequence, the IRPI journalist was contacted personally by the broker; who then also appealed so as to impede the FOI request. Eventually, the same administration refused the appeal and released the requested data to the journalist (Rinaldi, 2019).

As a consequence of Jan Kuciak's murder, and of these many other instances of unintended consequences of FOIA, a number of NGOs and civil society organisations asked for a **revision of access-to-information regulations.** For example, it was suggested to create a body or entity (at national or supranational level) acting as layer which could collect the FOI requests by the journalists, and then disseminate them to the relevant public administrations without disclosing the personal details of the single journalist. Similarly, a group of 61 civil society organisations sent a letter in 2018 to all the 751 members of the European Parliament to take urgent action to ensure strong protections for the safety and integrity of journalists' rights (Access Info, 2018).

In any case, given the problems that are generated even by a regulated framework such as FOI law, it is not surprising that journalists seek continuously **new ways and tools to increase their set of information through third-party data providers and tools** – such as DATACROS one – without the need to file formal request to public administration.

III. Technical framework and challenges

The technical challenges which have to be faced in researchers-journalists' cooperation, with specific regard to financial crime investigations, directly stem from the legal challenges above illustrated. In particular, they reflect the need to preserve **(i) personal data protection** (of both data subjects and journalists), **(ii) sensitivity** of the information, **(iii) integrity and quality** of the information and **(iv) accessibility of information** (for both journalists and readers). These are the same technical challenges which have been faced when designing the DATACROS tool and deploying it during the activity of investigative journalists. They are discussed in-depth below.

Technical ways to ensure data minimization

As already stressed, researchers and journalists need to demonstrate that the **proportionality and necessity principles** are satisfied when performing an investigation. This means first of all that the personal data employed should be limited to the minimum necessary in order to achieve the desired objective. This **'data minimization'** target could be reached also by designing technologies which, by default, allow to access only selected information, and do not allow indiscriminate collection and processing of massive information and protect this data.

The DATACROS tool prototype was technically designed in order to comply with this principle. In particular, some of the functions which have been envisaged are listed here below:

- The **names and details of the natural persons** related to the firms under analysis (i.e. shareholders, beneficial owners, directors) are not immediately exposed, as the output is first a list of firms (and associated risk scores) and not a list of individuals.
- A **maximum number of firms to be searched/assessed in a single query** has been set: the user could upload and risk score at most 500 firms, while it is not possible to analyze in a single query a higher number of companies. This is to avoid large-scale screening of firms (and related individuals).
- The collection of ***special categories*** **of personal data** (first of all, previous sanctions and enforcement measures on owners, beneficial owners, directors) is not automatically carried out when performing the query of firms, but shall be authorized in a second stage by the user, who can then decide if to (a) not execute the collection of special categories of personal data (and therefore limit the risk scoring to non-special category of data) or (b) execute it only for a subset of the firms originally uploaded.

Technical ways to protect the sensitivity of the data

The protection of the **sensitivity of data** is also a key measure in order to preserve the quality of research and investigations – and, as seen, the safety of researchers and journalists. This has been achieved via the DATACROS tool prototype in various ways:

- First, by setting up an IT infrastructure based on **secure servers**, both **GDPR compliant and ISO 27001** compliant, further reinforced by VPN and certain gateways which make it hard for intruders to penetrate the system. In order to further guarantee the security of the tool, it has been subject to a **Vulnerability Assessment/Penetration Test (VA/PT)**, executed by a third-party consulting company. The test served to identify potential loopholes which could be patched by specific IT or procedural interventions.

- Second, by setting up an IT infrastructure which allows registration of the **access logs** of the user, but not of their **query logs.** In other words, the DATACROS tool backend (and therefore their developers/managers) is able to record and displays whether and when a certain account has logged into the tool, but not what firms or names were searched. This functionality, which was developed for the sake of security of competent authorities which use the instrument (which of course required it for preserving the sensitivity of their investigations) has become useful for journalists, too.

- Third, by allowing users to **record previous queries** (e.g. names or list of firms previously searched), but by not allowing other users of the tool to access the same names/lists, nor notifying them that a firm had been already searched by another user.

Technical ways to maximize and preserve the integrity and quality of the data

This is one of the most difficult challenges, as 'quality' may be interpreted in very different meanings according to the individual research and investigation needs. For a thorough discussion of this problem, see **COESO Deliverable 2.8** (*Report on accessibility to sensitive and privately-owned databases*). However, an important sub-category of this challenge, with a crucial implication in terms of technical development, is related to: (i) the **level of coverage** of the data and (ii) the **level of historical depth** of the data (i.e. the availability and accessibility to historical data).

In terms of **data coverage**, some considerations – rather obvious, but still crucial – shall be done:

- Wider amount of data means greater technical challenges, as an investigative tool

- like the DATACROS one – should develop a **higher number of connectors to data sources**, take into account and face the possible wide variety in terms of format (e.g. .pdf, .csv, .json, .txt, .png, etc), accessibility, variability, frequency of update, etc.

- Wider coverage may also mean taking into account a potential wider **variety of conditions for accessing and employing the data**: some sources may pose certain constraints (from a technical, legal, privacy, commercial perspective) which other existing sources do not entail. This means, technically speaking, that the tool should be able to cope with all this diversity.

- Similarly, more sources mean also possible different levels of **sensitivity of the data in terms of personal data protection**. This then reflects in legal challenges which a proper data protection impact assessment shall address, and which an appropriate technical framework should embed.

- Finally, higher coverage also poses problems in terms of **entity reconciliation**. For instance, if, through the tool, a journalist or a researcher can access two documents related to a presumably same entity (e.g. two individuals with a similar or identical name), to what extent is the user able to check and demonstrate that the two are *in fact* the same entity? This has heavy implications in terms of minimizing the risk of generating or managing false positives. Various entity reconciliation techniques exist, also based on **artificial intelligence**, which allow, for example, to reconcile names written in a slightly different manner, or to transliterate them from various alphabets; but at the same time, even when the name is the same, there is the **risk of homonymity** which could be solved only through a cross-check of a variety of information (e.g. if applicable, date of birth, place of birth, ID). However, this latter is heavily dependent on data availability.

Secondly, in terms of **access to historical data**, this may mean, technically speaking, two things:

- First, **storage of data** in a way that then, in due course, it is not possible that this data could change or be altered in its integrity. For example, if through the DATACROS tool a journalist searches for the list of owners of a company, then the tool should make it possible that: (i) the journalist preserves this information and can access it back after in the longer term in a secure way, and (ii) the tool informs the user that the information has in the meantime changed and needs to be updated (e.g. because the company has changed its owners). In other words, it is necessary that each bit of information is associated with a certain time-stamp which becomes, therefore, unalterable.

- Second, typically a journalist (but also a researcher, and a law enforcement

investigator) should be able to search for **historical data** – for example, the list of owners of a certain company in, for example, 2003. This poses various technical problems. First, the possibility to collect data not available anymore, as many providers do not allow for this query; second, the possibility to store historical information, and this is challenging from both a mere technical perspective (due to storage problems of vast amount of information) and from a legal perspective (for example, GDPR requires personal data to be cancelled after a certain period of time or in any case if the activity for which it was used has ended).

Technical ways to improve accessibility and usability

Another technical challenge which researchers and journalists have to face when employing investigative tools is related to their **usability and accessibility**. This should be read in two manners:

- First, in terms of the **possibility for non-technical users** (as journalists often are), to use the tool for their activity. This means, for the DATACROS tool, the possibility to search for firms or individuals in an easy and user-friendly manner, without the need for programming or coding, nor going through lengthy pages of instructions.

- Second, in terms of the possibility for journalists to then **employ the outputs of the tool as evidence** to be included in their (online or offline) media coverage, in the form of picture, chart, graph or visual.

Project DATACROS has tried to face this difficulty from the very beginning, by **involving the journalists themselves in the design of the user-interface** and by collecting inputs upon which to define the tool outputs and export options. In other words, the research-journalist cooperation was also deployed not only in terms of content, but also in terms of IT development. However, this is a never-ending road, in the sense that the usability of a tool could be constantly improved and is constantly evolving due to the changes in users' habits, needs – and thanks to technology developments.

IV. Conclusion and the road forward

The work carried out by IRPI and Crime&tech within the COESO project, which built on what produced by the previous EU co-funded DATACROS project, has contributed not only to improve the analysis of financial crime risks in certain business sectors of the European Union; but, first of all, to **deepen the thinking and the discussion** over how these two poles – research and journalism – can cooperate to improve the investigation of financial crime, the development of investigative tools and the exchange of sensitive data.

Some lessons have been learnt and may be translated into recommendations for the future work of these actors in this field:

a) Investigative journalists (and researchers) often carry out the same activity of competent authorities, but without having an equally framed mandate and without benefiting from the same set of legislative exemptions and derogations. This holds in particular for the domains of **(i) personal data protection**, and **(ii) investigation secrecy**. This does not mean that for these actors it is not possible to process personal data nor keep the secrecy over their sensitive information. The two could be preserved by adopting appropriate – and fully lawful - **organizational and technical measures**.

b) In the personal data protection domain, researchers and journalists should first look at the principles of **proportionality and necessity** not as a constraint, but as a way to better circumscribe their action field. By leveraging on the relevant regulation – first of all the GDPR and the national laws – and guidelines (e.g. those issued by the Council of Europe), it is possible for these actors to understand to what extent their activity falls under a legitimate interest and, more specifically, may correspond to a public interest.

c) The protection of personal data may be achieved also through **technical and organizational measures,** both aimed at ensuring 'data-minimization' and the preservation of integrity and sensitivity of the data. Several examples entailed by project DATACROS have been illustrated in this sense.

d) While **personal data protection**, on the one side, and **cyber risks**, on the other, are often seen as complex issues by non-technical experts, they are two crucial issues which both journalists and researchers have to take into account, especially when involved in financial crime investigation. For this reason, it would be useful to foresee:

a. Practical guidelines with concise and operational tips on how to deal with them;
b. Specific training courses for these actors;
c. Future research projects addressing this issue. While several initiatives exist (e.g. Horizon2020 project PANELFIT), they do not seem to be focusing specifically on the cooperation research-journalism, and therefore dedicated project may be envisaged.

V. References

- Access Info, 2018, Letter to European Parliament with Statement on killing of Jan Kuciak, available at https://www.access-info.org/2018-03-13/call-on-eu-to-protect-those-who-exercise-the-right-of-access-to-information/

- Bitiukova N., 2020, Journalistic exemption under the European data protection law, Vilnius Institute for Policy Analysis, available at https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf.

- Caruso F., de Miguel Beriain, I., and Pérez Campillo L., Data protection in journalism: a practical handbook, European Data Journalism Network, available at https://bookdown.org/fede_caruso/bookdown/

- Carpino M., 2020, Personal data processing by law enforcement: finding a route between investigation opportunities and regulatory fragmentation, Milano: Università Cattolica – Transcrime, available at: https://www.transcrime.it/wp-content/uploads/2020/08/Personal-data-processing-by-Law-enforcement_Transcrime.pdf

- Council of Europe, 2019, Guidelines on safeguarding privacy in the media, Bruxelles: Council of Europe, available at https://edoc.coe.int/en/media/7772-guidelines-on-safeguarding-privacy-in-the-media.html

- European Commission, 2017, Call for Proposals for Projects on Corruption, Internal Security Fund – Police - Internal Security Fund – Police - ISFP-2017-AG-CORRUPT, available at https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2017-ag-corrupt_en.pdf

- European Data Protection Supervisor, 2021, Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, Bruxelles: EDPS, available at https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf

- Organized Crime and Corruption Reporting Project, 2020, “Freedom of information law: Reporter’s Best Friend or Killer?”, OCCRP, available at https://www.occrp.org/en/amurderedjournalistslastinvestigation/freedom-of-information-law-reporters-best-friend-or-killer

- Rinaldi L., 2019, “Come il Foia (Freedom of information Act) può migliorare l'informazione verso i cittadini e il lavoro dei giornalisti”, Presentation held at the Ordine dei Giornalisti, Roma on the 21 maggio 2019