Ariadna H. Ochnio, PhD
Gniewomir Wycichowski-Kuchta, PhD Candidate

Institute of Law Studies, Polish Academy of Sciences
Research project No. 2022/45/B/HS5/03080, National Science Centre (Poland)

Towards grassroots virtual justice: the role of NGOs and investigative journalism in 'open-source intelligence' for the purposes of investigations into corruption of politically exposed persons

Abstract

This paper examines the implications of cyberspace on criminal investigations, particularly regarding corruption involving politically exposed persons (PEPs). It highlights the challenges posed by the non-territorial nature of cyberspace, which complicates traditional concepts of jurisdiction and sovereignty. The study explores the growing significance of open-source intelligence and the roles of civilian actors, non-governmental organisations (NGOs) and investigative journalism, in achieving criminal justice purposes. It points out the lack of a regulatory framework for civilian OSINT in the European legal environment: the Budapest Convention on cybercrime and the EU e-evidence package. The authors argue that this evolving landscape necessitates the reevaluation of classic criminal investigations, advocating for public-private partnerships and outsourcing the tasks as a response to the challenges arising from the openness of cyberspace.

Keywords: cyberspace, e-evidence, open-source intelligence (OSINT), civilian criminal investigations, investigative journalism, EU e-evidence package, Budapest Convention, transparency, civil society

Introductory remarks

The realm of cyberspace is not defined by State borders and jurisdiction. Accordingly, it does not fit the classic concepts of national jurisdiction and territorial sovereignty. However, some attempts are being made to discuss the cyber reality in the context of well-established legal categorisations together with the challenges posed by the 'loss of location' encountered in cloud computing services.[1] It should also be remembered that even transborder gathering evidence of a less problematic character than electronic, for example under the European Investigation Order (EIO) mechanism, raised doubts on applicable law, the *forum regit actum* and the *locus regit actum.*[2]

Nevertheless, when it comes to e-evidence it is rather inevitable that we are heading to a point where cyberspace will be legally perceived as a universal phenomenon common to all humankind, primarily for the purposes of the fight against the most serious international criminal offences, which lies in the common interest of the international community.[3] Consequently, it can be expected that references to any 'place' ('location') will be gradually abandoned in legal discussions on interaction with this space for criminal justice purposes. Moreover, in the European legal environment, we have already reached this point as regards publicly accessible data, at least from the perspective of the Budapest Convention on cybercrime.[4] Notwithstanding that the EU e-evidence package is silent about the latter point, [5]

---

[1] See U. Sieber and C.-W. Neubert, 'Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty', 20(1) *Max Planck Yearbook of United Nations Law Online* (2017) 241-321, doi 10.1163/13894633_02001010. The CoE, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?', Discussion paper, 31 August 2010, https://rm.coe.int/16802fa3df (23.01.2025); C. Karagiannis and K. Vergidis, 'Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal', 12(5) *Information* (2021) 181, https://doi.org/10.3390/info12050181.

[2] In this context, see, e.g., M. Kusak, 'Mutual admissibility of evidence and the European investigation order: aspirations lost in reality', (19) *ERA Forum* 391–400 (2019), https://doi.org/10.1007/s12027-018-0537-0; *idem,* 'Mutual trust to obtain electronic evidence in the EU: is the bar low or high?', in A.H. Ochnio and H. Kuczyńska, eds, *Current Issues of EU Criminal Law* (Warsaw: Publishing House of ILS PAS, 2022), pp. 73-88, doi: 10.5281/zenodo.6856038.

[3] Cf. P. Wrange, 'Sovereignty, Belligerency and the New Normal in Cyberspace', in L.S. Bishai, ed., *Law, Security and the State of Perpetual Emergency* (Cham: Palgrave Macmillan, 2020), pp. 67-105, https://doi.org/10.1007/978-3-030-44959-9_4. R.A. Costello, 'International criminal law and the role of non-state actors in preserving open source evidence', 7(2) *Cambridge International Law Journal* (2018) 268-283.

[4] The CoE, Convention on Cybercrime, European Treaty Series No. 185, Budapest, 23 November 2001 (hereinafter: the Budapest Convention).

[5] See Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, OJ L 191, 28.7.2023, 181 (hereinafter: Directive 2023/1544); Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders f

it is crucial that almost all the EU MS (26 of the 27 MS) are parties to the Budapest Convention (Ireland is a signatory, with ratification ahead).

Cyberspace is characterised by a special kind of 'openness', as its users are, in principle, free to produce 'cyber content', on the one hand, and to access such content, on the other. Looking from a distance, one might say that one of the main features of cyberspace is the public availability of its open layer. This characteristic is not without consequences for the traditional way of thinking about criminal investigations when they reach into cyberspace. In particular, the open character prompts a redefinition of the classic role of the State actors. Two questions arise — who should be engaged in conducting such investigations, and should they be reserved exclusively to State authorities? These questions are particularly relevant when the purposes of criminal justice meet with the purposes of the public mission carried out by some civilian actors. Given that corruption is detrimental to the democratic processes and functioning of the State, its institutions, and communities, one such example is investigations concerning corruption involving politically exposed persons (PEPs) and related offences (e.g. money laundering), the purposes of which can be in the common interest of the triad of law enforcement authorities, investigative journalists and non-governmental organisations (NGOs).[6]

Corruption implies a strong bond between the persons engaged in it, based on mutual benefit. Thus, both the party transferring the assets and the beneficial owner are often hidden, or if present, usually not in a way visible to the wider public. All this supports an atmosphere of silence around criminal activities, including suspicious asset flows. The biggest challenges to dirty assets are publicity and transparency, and 'Sunlight is said to be the best of disinfectants'.[7] In modern times, the total concealment of asset flows on the Internet, as well as the identity of the parties to such transactions, has become increasingly difficult. Accordingly, here the door is open to civil actors, especially NGOs and investigative journalists, with the ability to freely conduct preliminary analysis of publicly available data in the virtual space, that can, at a later stage, be verified by investigative and judicial authorities through the use of their greater procedural powers (e.g. search, seizure, waiving banking secrecy, etc.). Especially when the State fails to function properly due to the corrupt practices of its political elites, the pursuit of prosecution by law enforcement authorities may be hampered, particularly when their political

---

or electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, 118 (hereinafter: Regulation 2023/1543).

[6] This paper concentrates on the involvement of civilian actors in investigations concerning corruption in the public sector, however, many other areas of crime may be identified where non-State actors may play a role in achieving the purposes of criminal justice, and the conclusions of this paper may be relevant.

[7] L.D. Brandeis, 'What Publicity Can Do', *Harper's Weekly* (20 December 1913) 10-13.

position is strongly influenced by executive power. At this point, a space unfolds for independent journalists and NGOs not officially connected with the State to step in.

Considering the open nature of cyberspace, it is difficult to defend the argument that exploring it for criminal justice purposes, at least at the level accessible to its civilian users performing a public mission on the same basis as to the law enforcement authorities, should be reserved only for the latter. All the more so, given that the State may profit from a public-civil partnership in this respect, starting from establishing the facts, identifying the perpetrators and victims, determining the harm done by a crime, and ending with preventing future crimes i.a. by informing the public about the outcomes of criminal proceedings.

In view of the above, the tasks of collecting and analysing open data seem to have the potential to be partially privatised, both to benefit the interest of civil society in being informed about suspicious practices of PEPs, and the interest of criminal justice in securing convictions of corrupt PEPs or securing seizure of their illicit assets. A public-private partnership in this respect may be beneficial in multiple dimensions. Engaging NGOs and investigative journalists in identifying the suspicious asset flows of PEPs is in line with their mission as intermediaries providing society with information about processes that are usually hidden from the general public. Furthermore, supporting civilian actors in performing the function of a 'watchdog' patrolling an 'open-source space' to detect the corrupt practices of PEPs may be valuable for the State, as the preliminary analysis delivered by these actors may ultimately result in freezing and confiscation of unexplained wealth, or launching criminal proceedings in corruption-related cases. Such pre-trial analysis by non-State actors may be perceived as a provisional investigation, '*quasi*-investigation', being the kind of 'screening proceedings' preceding official criminal proceedings or freezing and confiscation proceedings. Importantly, such initial analytical actions need not necessarily be conducted under the remit of the State. A concrete case may justify informing the public of suspicious practices by PEPs prior to informing law enforcement authorities, who may be reluctant to act if the results of the preliminary analysis concern the political establishment. In such cases, well-informed public opinion can apply pressure on authorities to follow through with investigations.

The concept of a public-private partnership in collecting e-evidence for the purposes of criminal justice is already employed in the EU e-evidence package, however, so far only in the field of co-operation between public authorities and service providers. Importantly, participation in this co-operation is mandatory for private entities. Conversely, it seems reasonable to frame the public-private partnership discussed in this paper, i.e. operating in the field of gathering open-

source evidence, around a voluntary alliance. The preliminary thesis is that gathering and analysing open-source evidence may be successfully performed by civilian actors who should be able to operate both on their own initiative, as is already taking place, and following outsourcing requests from public authorities. Accordingly, such co-operation should move beyond its current legal niche.

1.1. Research questions

The purpose of this paper is to answer the question of whether involving NGOs and investigative journalists in 'open-source intelligence' (OSINT) may support financial ('follow the money') investigations by law enforcement authorities in cases of corruption by PEPs and related offences. The second question goes in the opposite direction, asking how the State may support civilian actors in performing tasks in this field, the results of which may be used in criminal proceedings or freezing and confiscation proceedings. The considerations revolve around the opportunities for improving the EU regulatory framework in this respect.

Expanding the perspective, the paper attempts to answer the question of whether engaging civilian actors in performing tasks in the framework of virtual justice should become a strategic course of action for the EU MS in the fight against corruption in the public sector. Secondly, whether this should be promoted and invested in by the EU, as an element of the common strategy to strengthen the area of freedom, security and justice at the grassroots level.

1.2. Roadmap

This paper is structured as follows. Firstly, the terms 'open data' and 'open-source' are explained. Secondly, the concept of 'open-source intelligence' (OSINT) is explored and its suitability for 'follow the money' civilian criminal investigations. In the following subsections, the issue of the lack of a regulatory framework for civilian OSINT in the European legal environment is discussed, and the challenges that this may pose to the right to privacy. Further, the changing reality of criminal investigations in connection with the growing importance of representatives of civil society (NGOs, investigative journalists) is presented. This is evidenced by the experience of international criminal courts and the emergence of highly-specialised civilian actors conducting investigations for criminal justice purposes.

In the next section, the CJEU ruling in Joined Cases C 37/20 and C 601/20, *WM and Sovim SA,* concerning Luxembourg Business Registers is critically discussed. The CJEU decided on limited access by the general public to information on beneficial ownership. The main point

against the arguments presented by the CJEU is that civilian actors, either investigative journalists or NGOs, should also have the legal possibility to gather e-evidence concerning the corruption by PEPs when acting on their own, without any connections with formal criminal investigations.

In addition, a case concerning property acquisition transactions in London by PEPs from Kazakhstan is presented (*National Crime Agency v Baker and Others*, [2020] EWHC 822 (Admin)) as an example of revealing suspicious asset flows by the civilian actors, journalists and NGOs. The outcome of their cooperation resulted in unexplained wealth orders (UWOs) and interim freezing orders, issued on the basis of the Proceeds of Crime Act (POCA 2002). However, this case also shows that the results of civilian investigations may still be easily challenged before a court.

The paper ends with conclusions regarding the multiple benefits of public-private partnerships in gathering e-evidence from open sources. In addition, it poses some questions on the future of such cooperation.

2. Terminology issues: 'open data' and 'open-source'

The Budapest Convention in Article 32(a) uses both the terms 'publicly available' and 'open-source' concerning accessing 'stored computer data', though it does not explain them. In addition, the wording of Article 32(a) gives the impression that they are used interchangeably. Given that technically, the issue of 'open data' and 'open-source' is complex, explaining the meaning of these terms first would be helpful to determine the proper boundaries of handling freely accessible e-evidence, including by non-State actors, with a view to preserving their utility for the purposes of criminal justice. Likewise, the EU e-evidence law does not provide legal definitions of these terms. In the broader context, reference can be made to Directive (EU) 2019/1024 on open data and the re-use of public sector information,[8] stating that: 'Open data as a concept is generally understood to denote data in an open format that can be freely used, re-used and shared by anyone for any purpose' (Recital 16 of the Preamble). Notably, the official EU portal for European data refers to the principles of 'Open Definition' delivered by the Open Knowledge Foundation as regards 'open data' and 'open content'.[9] Simply put,

[8] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, 56, hereinafter the 'PSI Directive'.

[9] The EU, 'European data' (the official portal for European data), 'What is open data' https://data.europa.eu/en/dataeuropa-academy/what-open-data (27.01.2025).

according to the definition proposed by this foundation, the 'open' ('openness') means that 'anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)', in other words: '[o]pen data and content can be freely used, modified, and shared by anyone for any purpose'.[10]

However, at first glance, one can see that a similar approach, involving the free modification of data is highly questionable when gathering e-evidence, as it could challenge the intended utility of such evidence in criminal justice processes. Rather, it is reasonable to take the view that altering data exceeds the permissible boundaries of gathering 'e-evidence' for criminal justice purposes. *Ulrich Sieber* and *Carl-Wendelin Neubert* posed a question about the scope of the permitted 'access' to publicly available data under Article 32(a) of the Budapest Convention, and discussed the scope of the notion 'access', whether it permits only the viewing of data or maybe also copying, seizing, or altering of data.[11] Taking into account other provisions of the Budapest Convention[12], these Authors concluded that it distinguishes actions as 'identifying', 'materially obtaining' and 'controlling' data, with the aim of preventing data from 'alteration' or 'deletion', hence, the term 'access' does not include 'securing' or 'altering' the data.[13] However, bearing in mind the purpose of Article 32(a) of the Budapest Convention, consisting in using data as evidence without resorting to the mutual legal assistance mechanism, the cited Authors recognised that the term 'access' also covers the copying of data. In sum, under this legitimate view, the Convention term 'access' covers 'identifying', 'viewing', 'monitoring' and 'copying' data.[14]

Next, the differing referent objects of the terms 'data' and 'source' should be considered. The Oxford 'Dictionary of Computing' recognises broad and narrow meanings of 'data'. In a broad sense, this term means 'information, in any form, on which computer programs operate', whereas 'data' in the narrow sense is 'distinguished from other contrasting forms of information on which computers operate, such as text, graphics, speech, and image', and the 'distinguishing characteristic' is its organisation in a 'structured, repetitive, and often compressed way'.[15]

---

[10] The Open Knowledge Foundation, 'Open definition. Defining Open in Open Data, Open Content and Open Knowledge', https://opendefinition.org/ (27.01.2025).
[11] U. Sieber and C.-W. Neubert, *op. cit.,* p. 267.
[12] Article 19, 29, 31, and 32(b) of the Budapest Convention.
[13] U. Sieber and C.-W. Neubert, *op. cit*., p. 268.
[14] U. Sieber and C.-W. Neubert, *loc. cit*., p. 268.
[15] Oxford Reference, 'Data', https://www.oxfordreference.com/display/10.1093/oi/authority.20111005230343274 (27.01.2025), from J. Daintith and E. Wright, 'Data', in *idem*, *A Dictionary of Computing* (Oxford: Oxford University Press, 2008), https://doi.org/10.1093/acref/9780199234004.001.0001.

However, terminology issues should also be seen in the broader context of the 'DIKW hierarchy',[16] in which 'information' is not the equivalent of 'data'. The hierarchy is as follows: 1) data, 2) information, 3) knowledge, 3) wisdom.[17] Simply put, from this perspective, 'information' may be explained as a 'process of interpreting data based on possessed knowledge' or interpreted data, as clarified in the analysis of *Mariusz Grabowski* and *Agnieszka Zając*.[18]

Moving on to the next point, the definition of 'open-source' began to be developed in the nineties by *Bruce Perens* with the input of some participants of the Debian Project.[19] As originally envisaged, the term 'open-source' refers to 'software', not 'data' itself. Likewise, the current widespread 'Open Source Definition' (OSD) pertains not only to 'access to the source code', but also includes criteria determining the conditions of distribution of open-source software.[20] A deeper analysis in this respect exceeds the boundaries of this study, however, it is important to note that the term 'open source' is a separate concept from 'open-source intelligence'. It is generally agreed that OSINT does not refer to the 'open-source software movement'.[21] The key characteristic for OSINT is that it is targeted at freely available data, but it may also involve open-source software (applications).

Finally, it should be noted that the term 'open-source' is sometimes used to refer to applications which are not necessarily free of cost, contrary to how 'open data' is often associated with cost-free access.[22] However, there is a common view that 'open source intelligence', discussed in the next section, also includes paid access.

3. 'Open-source intelligence' and 'follow the money' investigations

[16] An acronym of 'data', 'information', 'knowledge', and 'wisdom'.
[17] M. Grabowski and A. Zajac, 'Dane, informacja, wiedza – próba definicji' ('Data, Information, Knowledge - an Attempt of Definitions'), 798 Zeszyty Naukowe, Uniwersytet Ekonomiczny w Krakowie (2009), 99-116.
[18] M. Grabowski and A. Zajac, *op. cit*., pp. 4-5.
[19] Debian, 'What is GNU/Linux. Welcome to Debian', https://www.debian.org/releases/bullseye/mips/ch01s02.en.html (27.01.2025). See also Free Software Foundation, GNU Operating System, 'The GNU Manifesto', https://www.gnu.org/gnu/manifesto.html.en (27.01.2025). Debian, 'The Debian Social Contract', version 1.2, ratified on 1st October 2022. https://www.debian.org/social_contract.en.html (27.01.2025). Debian, 'The Debian Free Software Guidelines' (DFSG), https://www.debian.org/social_contract.en.html (27.01.2025).
[20] See Open Source Initiative (OSI), 'The Open Source Definition' (7 July 2006, recently modified on 16 February 2024), https://opensource.org/osd (27.01.2025). Free Software Foundation (FSF), 'Free software is software that gives you the user the freedom to share, study and modify', https://www.fsf.org/about/what-is-free-software (27.01.2025).
[21] See J. Fruhlinger, A. Sharma, and J. Breeden, '15 top open-source intelligence tools' (15 August 2023), https://www.csoonline.com/article/567859/what-is-osint-top-open-source-intelligence-tools.html (02.02.2025).
[22] In this vein, e.g. GeeksforGeeks, 'Difference between Open Source and Open Data', https://www.geeksforgeeks.org/open-source-and-open-data/ (27.01.2025).

Commencing the explanation of the term 'open-source intelligence' (OSINT), somewhat perversely beginning from criticism that recently emerged in the subject literature, has merit in identifying its usefulness when looking through the prism of its special performers, i.e. civilian actors who, contrary to State actors, do not in principle have access to classified (non-open, closed, secret) data. However, it has been argued that the concept of OSINT, understood as intelligence from openly available sources, lacks coherence. One of the arguments raised is that sometimes OSINT cannot be distinguished from other types of INTs (human intelligence, imagery intelligence, etc.), and in fact may also cover classified content, for example in the aftermath of leakage of classified documents, like in the case of 'Wikileaks'.[23] The critical remarks in this respect raised by *Joseph M. Hatfield* revolve around the criteria for categorising OSINT as a distinct kind of intelligence and its historical context justifies seeing it as a relic of a 'transitionary stage' linked to the surge of 'unclassified information' that emerged in the nineties with the advent of the World Wide Web.[24] *Hatfield* questioned defining OSINT through a negative approach, i.e. that it pertains to 'information *not* under the control of governmental actors who may limit its production and distribution', accordingly, compared to other types of -INT and from the taxonomy viewpoint, it 'stands next to its brethren like a man wearing a clown costume in a police lineup'.[25]

While there is some validity to these arguments, at the same time it cannot be denied that the concept remains relevant when adopting the perspective of the involvement of non-State actors. Unlike State actors, they primarily rely on openly available (unclassified) sources or sources that have, in fact, lost their classified status due to leakage to the open layer, a distinction that warrants recognition.

Even though there is no single definition of the term 'open-source intelligence' in the literature, the essential elements are, in general, consistent. For instance, *Michael Bazzell* points out that OSINT may mean 'many things to many people', and answers the question 'What is OSINT?' in the following way: 'Officially, it is defined as any intelligence produced from publicly

[23] J.M. Hatfield, 'There is No Such Thing as Open Source Intelligence', (37) International Journal of Intelligence and CounterIntelligence (2024) 411.
[24] J.M. Hatfield, *op. cit.,* p. 397. See also B.H. Miller, 'Open Source Intelligence (OSINT): an Oxymoron?', 31(4) *International Journal of Intelligence and CounterIntelligence* (2018), 702-719, https://doi.org/10.1080/08850607.2018.1492826.
[25] J.M. Hatfield, *op. cit*., p. 399.

available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement'.[26]

According to *Clive Best*'s explanation, OSINT means the 'retrieval, extraction and analysis of information from publicly available sources', where currently the Internet represents the primary arena.[27] Sometimes this term also refers to the 'area of the security and intelligence industry, involving the collection of internet located open data from various sources, turning that data into actionable intelligence, which is reused where possible and relevant'.[28] The next example is defining OSINT as a 'process whereby police or other investigative agencies gather and analyse data that are in principle accessible to any organisation or individual'.[29] It can also be seen as a 'concept', referring to 'any publicly available data used to fulfill a specific need for information'.[30] OSINT can also be understood as the 'production of intelligence through the collection and enrichment of publicly available information', like in the definitional proposition of *Rae Baker* who uses the term publicly available 'information' interchangeably with 'data' in the sense of 'any data that is available for public access without the use of a secret clearance or intrusion into a system', including paid-access (e.g. newspaper subscriptions).[31] Importantly, under this view, OSINT is a 'purely passive method' not intended to using person's credentials to accessing or logging in to a database. According to *Baker*, active methods should be left to 'ethical hackers, penetration testers who have the legal authorisation to do so, or law enforcement who have prior authorisation and approved operational plans', as the idea is to make as little 'noise' as possible to avoid being detected.[32] However, it should also be noted that in the 'DIKW hierarchy',[33] 'information' is not the equivalent of 'data'. The hierarchy is as follows: 1) data, 2) information, 3) knowledge, 3) wisdom.[34] Simply put, 'information' may

[26] M. Bazzell, *Open Source Intelligence Techniques. Resources for Searching and Analysing Online Information* (Independently published: 2019) p. 6.
[27] C. Best, *op. cit.,* 331.
[28] S. Khan, and D. Wallom, 'A system for organising, collecting, and presenting open-source intelligence', (4) *Journal of Data, Information and Management* (2022), p. 107.
[29] D. Trottier, 'Open source intelligence, social media and law enforcement: Visions, constraints and critiques', 18(4-5) *European Journal of Cultural Studies* (2015) 530–531, https://doi.org/10.1177/1367549415577396.
[30] A. Qusef, and H. Alkilani, 'The effect of ISO/IEC 27001 standard over open-source intelligence', *PeerJ Computer Science* (2022) 2, 8:e810, https://doi.org/10.7717/peerj-cs.810.
[31] R. Baker, *Deep Dive. Exploring the Real-world Value of Open Source Intelligence* (Hoboken, New Jersey: John Wiley & Sons, Inc., 2023), p. 3.
[32] R. Baker, *op. cit*., p. 3.
[33] An acronym of 'data', 'information', 'knowledge', and 'wisdom'.
[34] M. Grabowski and A. Zajac, 'Dane, informacja, wiedza – próba definicji' ('Data, Information, Knowledge - an Attempt of Definitions'), 798 Zeszyty Naukowe, Uniwersytet Ekonomiczny w Krakowie (2009), 99-116.

be explained as a 'process of interpreting data based on possessed knowledge' or interpreted data, as clarified in the analysis of *Mariusz Grabowski* and *Agnieszka Zając*.[35]

In the Intelligence Community (IC) OSINT Strategy for 2024-2026, OSINT stands for 'intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps'.[36] Notably, alongside the development of the Internet and social media superseding traditional open sources, a distinction has been made between second- and third-generation OSINT. Second-generation OSINT was connected with the evolution of 'dynamic web pages' and 'user-generated content' (Web 2.0), whereas third-generation OSINT is connected with the evolution of the 'Semantic Web', especially 'machine processing of data', 'machine learning', and 'automated reasoning' (Web 3.0).[37]

It is also worth noting the existence of the related term 'open-source investigations', explained in the literature as investigations involving 'finding publicly available information sources, checking their accuracy, and piecing them together to build insights into events or situations'.[38]

As far as the relevance of OSINT in civilian investigations into corruption by PEPs and related offences is concerned, it may be used as a tool to reveal unexplained wealth, which may then be subject to an unexplained wealth order (UWO) not demanding criminal conviction, or subjected to deeper analysis in classic criminal investigations by law enforcement authorities with access to classified information. The Basel Institute of Governance Guide points out that 'follow the money' is a 'snappy way to say: investigate financial transactions and use them to extract information or evidence about a crime, suspect or criminal network'.[39] It helps in

---

[35] M. Grabowski and A. Zajac, *op. cit*., pp. 4-5.

[36] United States Intelligence Community, 'The IC OSINT Strategy 2024-2026. The INT of First Resort: Unlocking the Value of OSINT,' https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf (02.02.2025). It is also worth mentioning the definition of OSINT provided for in the Public Law 109–163 (109th Congress): 'Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement' (Section 931).

[37] H. J. Williams, I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (RAND Corporation: 2018), p. 39, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf (02.02.2025), referencing J. Markoff, 'Entrepreneurs See a Web Guided by Common Sense', *New York Times* (12 November 2006).

[38] H. Wilson, O. Samuel, and D. Plesch, 'Open Source Investigations in the Age of Google: How Digital Sleuths Can Strengthen Human Security', in H. Wilson, O. Samuel, and D. Plesch, eds, *Open Source Investigations in the Age of Google,* (London: World Scientific Publishing Europe Ltd., 2024) p. 5, https://doi.org/10.1142/9781800614079_0001.

[39] S. Ratcliffe, 'Following the money', Basel Institute of Governance, 15 *Quick Guide Series* (2020), p. 1, https://baselgovernance.org/sites/default/files/2020-08/qg15_following_the_money.pdf (02.02.2025). See also FATF Report 'Operational Issues Financial Investigations Guidance' (FATF/OECD: June 2012), https://www.fatf-

'tracking down' high-level criminals, their networks, and family members.[40] Accordingly, it may be recognised as a kind of investigative approach dedicated to acquisitive offences. In view of the definitions of OSINT, when considering its utility for civilian criminal investigations aimed at revealing illicit assets, it must exclude monitoring and examining confidential financial information (e.g. banking transactions). Instead, OSINT may be used to reveal how illicit assets have been laundered or hidden, for instance, based on information about registered goods, like immovable properties (e.g. plots, mansions), movables (e.g. motor vehicles, yachts and vessels, civil aircraft) or registered shares in companies. There are many paid and unpaid registers in which civilian criminal investigators may gain insight (e.g. company, association and foundation registers, beneficial ownership registers, land/real-estate registers, vehicles registers, etc.). When establishing links between PEPs and corrupt practices, suspected persons, or illicit assets, OSINT may also involve tracking aeroplanes and vessels through the use of such tools as 'Skyradar', 'VesselFinder' or 'MarineTraffic'. All other passive methods of collecting information can also be employed.[41] The main are 'data mining' (involving algorithmic processing),[42] 'web scraping' ('web extraction', 'harvesting')[43], and 'social media investigations'.[44] Nowadays OSINT involves manual and automatised techniques. *Denis Stodelov* and *Natalia Miloslavskaya* indicate the following basic set of OSINT tools: 'Shodan Search Engine', 'Domain Name Data' and 'ZoomEy'; 'Have I Been Pwned', 'Dehashed', 'Max Mind'; 'Abuse.ch', 'Alien Vault OTX' and 'Gray Noise', 'Wigle', 'Hunter', 'Master Name', 'Website Informer', 'Cert Spotter', 'Virus Total Public', and 'Spider Foot'.[45] However, the

gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf (02.02.2025).

[40] S. Ratcliffe, *op. cit.,* p. 1-2.

[41] See, e.g., M. Walkow and D. Pöhn, 'Systematically Searching for Identity-Related Information in the Internet with OSINT Tools', in, *Proceedings of the 9th International Conference on Information Systems Security and Privacy* (ICISSP 2023), pp. 402-409, https://doi.org/10.5220/0011644200003405.

[42] N. Memon and D.L. Hicks, 'Detecting Core Members in Terrorist Networks: A Case Study', in F. Fogelman-Soulié, D. Perrotta, J. Piskorski, and R. Steinberger, eds, *Mining Massive Data Sets for Security* (Amsterdam: IOS Press, 2008), p. 345.

[43] According to the Springer *Encyclopedia of Big Data,* 'web scraping' means a 'technique to extract data from the World Wide Web (WWW) and save it to a file system or database for later retrieval or analysis', in addition, 'current web scraping techniques have become customized from smaller ad hoc, human-aided procedures to the utilization of fully automated systems that are able to convert entire websites into well-organized data set', B. Zhao, 'Web Scraping', in L.A. Schintler, C.L. McNeely, eds, *Encyclopedia of Big Data* (Cham: Springer, 2022) pp. 951–953, https://doi.org/10.1007/978-3-319-32010-6_483.

[44] J. Golbeck (J.L. Klavans, Technical Editor), *Introduction to Social Media Investigation. A Hands-on Approach* (Waltham, MA: Syngress, imprint of Elsevier, 2015), p. 3.

[45] D. Stodelov and N. Miloslavskaya, 213 'Open Source INTelligence Tools' (2022), p. 87, https://doi.org/10.1016/j.procs.2022.11.041.

scientific literature has also identified many other OSINT tools[46] which are becoming increasingly sophisticated, though developments in this respect are fuelled primarily by security issues, not criminal justice purposes.

Given the huge volume of publicly available data and still evolving OSINT techniques, uncovering the corrupt practices of PEPs with its use requires advanced skills and specific knowledge of the methods of money laundering and obscuring the beneficial owners of assets. In this context, the State can play a role in training civilian investigators. Importantly, such knowledge sharing should not be limited to only entities accredited by State authorities, as investigating and exposing concrete corruption cases may require the involvement of independent 'digital vigilantes', operating outside formal legal frameworks, especially when unmasking the corrupt practices of PEPs in kleptocratic systems. It should also be remembered that OSINT has its own ethos, and the analysts distinguished the 'OSINT Community'. It is characterised by three features: 'the culture of transparency in their work', 'the presence of an adversarial mindset when conducting investigations', and 'collaboration among individuals with diverse motivations and backgrounds'.[47] In addition, the attempt has been made to define the 'social OSINT' (set of strategies supporting OSINT investigations).[48]

The approach advocated in this paper enters a more general vision of supporting civilian virtual justice, which means this area being shared between the State and civil society. In fact, we are facing a *fait accompli,* as reality has already proven that civil society representatives (NGOs, investigative journalists) can, and want to take matters into their own hands, as evidenced by numerous civilian criminal investigations. The law, being in principle secondary to the changing reality, must catch up with advances in this respect.

3.1. Legal niche

Gathering of e-evidence by civilian actors is currently outside the material scope of EU law on e-evidence. Regulation 2023/1543 pertains only to actions by State authorities and their cooperation with private service providers. Recital 6 of the Preamble refers to the Resolution

[46] See, e.g., the extensive analysis in this respect presented in the article authored by M.M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, and K. Muhammad, 'Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security', 10(12) *Mathematics* (2022), 2054, https://doi.org/10.3390/math10122054.
[47] Y. Belgith, S. Venkatagiri, and K. Luther, 'Compete, Collaborate, Investigate: Exploring the Social Structures of Open Source Intelligence Investigations' *CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, Article No. 129, pp. 14, https://doi.org/10.1145/3491102.3517526.
[48] Y. Belgith, S. Venkatagiri, and K. Luther, *op. cit.,* p. 15.

of the European Parliament of 3 October 2017 on the fight against cybercrime[49] underlining the importance of close cooperation between law enforcement authorities, third countries and service providers active on European territory. However, there is still no recognition of the importance of cooperation in this respect between public authorities and representatives of civil society. As far as the Budapest Convention is concerned, it deals with transborder access to stored computer data with consent or where publicly available. Nonetheless, it concerns accessing data by one Party without the authorisation of another Party (Article 32). Thus, the European legal environment is still lacking in legal frameworks for civilian gathering and analysing of open data for criminal justice purposes.

3.2. Privacy issues

The mere openness of data does not in itself mean that conducting OSINT is irrelevant to the right to privacy. Quite the contrary, targeting intelligence at concrete individuals with the use of OSINT tools, even if based on open sources, may trespass the area of their protected privacy. Accordingly, compliance of collecting e-evidence from open sources by non-State actors with privacy issues is the next area demanding minimum regulatory framework at the EU law level. The departure point in this respect should be Regulation (EU) 2016/679 of 27 of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).[50] When designing the legal framework for collecting e-evidence from open sources in line with the principles provided for in the GDPR, the following aspects of privacy protection should be taken into account: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability (Article 5). It should be remembered that 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, including the safeguarding against and the prevention of threats to public security' is outside the material scope of the GDPR (Article 2(2)(d)). However, it does not mean that classic criminal

[49] Resolution of the European Parliament of 3 October 2017 on the fight against cybercrime, OJ C 346, 27.9.2018, p. 29.
[50] 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), OJ L 119 4.5.2016, p. 1 (hereinafter: Regulation 2016/679).

investigations run by State actors do not raise any challenges regarding the right to privacy.[51] The situation is even more complex in the case of civilian criminal proceedings, where personal data is not processed by 'competent authorities', and where the GDPR is relevant. Privacy issues are also challenging in view of the emergence of 'online vigilante justice' and its 'digilantes' ('internet vigilantes')[52] operating outside the framework of legal authorisation.[53] Thus, they are also outside the procedures guaranteeing fundamental fair trial rights. Such a legal status quo, or rather the lack thereof, may pose unpredictable and disproportionate risks for individuals targeted using OSINT, and third persons as well. Nevertheless, given the purposes of such investigations, common to State and non-State authorities, the right of civilian users of cyberspace to trace e-evidence of crimes on the open layer deserves legal authorisation. Thus, the interests of civilian criminal investigations and the privacy interests should be reasonably balanced.

In this context, it is worth mentioning the constraints raised by *Bart Custers* and *Lonneke Stevens* regarding the processes of gathering and using data as criminal evidence and the procedural rights connected with these processes.[54] Based on the Dutch example, they remarked, i.a., that the 'right to digital privacy within criminal procedure is still in its infancy'.[55]

One of the additional solutions for protecting the right to privacy discussed in academic literature, apart from the need to establish regulatory framework, is securing it at the early stage of designing OSINT tools (so-called 'privacy by design').[56] Under this concept, privacy protection should be treated as an important system requirement, equal to any other functional requirement when developing IT systems.[57] *Bert-Jaap Koops, Jaap-Henk Hoepman,* and *Ronald E. Leenes* distinguished the following design principles: 'minimise', 'separate',

[51] E.g. in the context of Recitals 2, 6, 13-16, 34 and 40 of the Preamble to the GDPR. See also Article 1(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.
[52] See more about this phenomenon L. ten Hulsen, 'Open sourcing evidence from the Internet— the protection of privacy in civilian criminal investigations using OSINT (Open-Source Intelligence)', 12(1) *Amsterdam Law Forum* (2020), pp. 3, 5.
[53] See also Ch.M. McDermott and M.K. Miller, 8(3) 'Individual differences impact support for vigilante justice', *Journal of Aggression, Conflict and Peace Research*, (2016), pp. 188-189; P.H. Robinson, 'The Moral Vigilante and Her Cousins in the Shadows' (2015) *All Faculty Scholarship*, 506. https://illinoislawrev.web.illinois.edu/wp-content/ilr-content/articles/2015/2/Robinson.pdf (07.02.2025).

[56] B.-J. Koops, J.-H. Hoepman, R.E. Leenes, 'Open-source intelligence and privacy by design', 29(6) *Computer Law & Security Review* (2013), 676-688. https://doi.org/10.1016/j.clsr.2013.09.005.
[57] B.-J. Koops, J.-H. Hoepman, R.E. Leenes, *op. cit.,* p. 678.

'aggregate', 'hide', 'inform', 'control', 'enforce' and 'demonstrate'.[58] Based on Directive 95/46/EC (repealed by the GDPR)[59], these Authors identified the set of requirements for collecting and using personal data relevant to a 'techno-regulation approach'.[60] Importantly, collecting and using data intended to be used as criminal evidence should be in line with the requirements and procedures for collecting digital evidence to secure its admissibility and reliability in court.[61] It is also worth mentioning a concept proposed by *Jaap-Henk Hoepman* and *Bert-Jaap Koops* that is gaining recognition, which describes a 'digital home' that needs protection, just as with a traditional ('physical') home.[62] They analysed the theoretical basis for establishing 'home-equivalent' legal protection of private digital storage spaces (e.g. smartphones, private cloud storage accounts) resembling the storage spaces of 'private things'. Under this concept, our 'digital home' is wherever data is privately stored, and also needs protection, as with requirements for physical intrusion into private places. In view of the above, our new 'digital home' should gain legal protection compatible with the GDPR principles, and this also affects the protection of privacy in OSINT tools used by civilians.

4. How to 'legally catch-up' to the changing reality of criminal investigations?

The use of open-source evidence has been explored more by scholars in the context of proving crimes falling under the jurisdiction of the ICC,[63] as some mechanisms in this respect are already in operation. For instance, the International, Impartial and Independent Mechanism (IIIM) was introduced by the UN General Assembly in response to the situation in Syria (2018).[64] Next is the Investigative Team to Support Domestic Efforts to Hold the Islamic State in Iraq and the Levant Accountable for Its Actions in Iraq by the UN Security Council resolution

[58] B.-J. Koops, J.-H. Hoepman, R.E. Leenes, *op. cit*., p. 679.
[59] In the context of the GDPR, cf. S. Khan and D. Wallom, 'A system of organising, collecting, and presenting open-source intelligence', (4) *Journal of Data, Information and Management* (2022), p.116, https://doi.org/10.1007/s42488-022-00068-4.
[60] B.-J. Koops, J.-H. Hoepman, R.E. Leenes, *op. cit*., pp. 683-684. On 'techno-regulation' see, e.g., B.-J. Koops, 'The (In)flexibility of Techno-Regulation and the Case of Purpose-Binding', 5(2) *Legisprudence* (2011), 171-194, https://doi.org/10.5235/175214611797885701.
[61] B.-J. Koops, J.-H. Hoepman, R.E. Leenes, *loc. cit*., p. 684.
[62] J.-H. Hoepman and B.-J. Koops, 'Offering "Home" Protection to Private Digital Storage Spaces', 17(2) SCRIPTed (2020), 359-388, . See also L. ten Hulsen, *op. cit,* pp. 14, 30, and 41.
[63] E. White, 'Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations through the creation of a standing investigative mechanism', 37(1) *Leiden Journal of International Law* (2024) 228-250, doi:10.1017/S0922156523000444.
[64] L. Freeman, 'Digital evidence and war crimes prosecutions: the impact of digital technologies on international criminal investigations and trials', 41(2) *Fordham International Law Journal*, (2018) 283-336; The UN General Assembly resolution: International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011, A/RES/71/248.

2379 (2017).[65] Another example is the Independent Investigative Mechanism for Myanmar (IIMM) (2018).[66] Most recently, the Independent International Commission of Inquiry on Ukraine (2022).[67] The latter two were introduced by the UN Human Rights Council.[68] Experience gained dealing with open-source evidence for the purposes of investigations on grave crimes may be a valuable reference point for the EU when framing rules in this regard.

Furthermore, the ICC and the Office of the Prosecutor (OTP) developed the idea of outsourcing investigations to NGOs.[69] However, the receptiveness of the ICC to taking advantage of the capacities of external actors, for example acting under the aegis of the United Nations (UN) or civilian ones, to support investigations concerning atrocity crimes, seems to be a logical consequence of the specificity of the procedures applied. One explanation presented in the literature for such a course of action by the ICC is the 'absence of its own international police force'.[70] Similar arguments, however, are not equally pertinent to civilian investigations into corruption cases concerning PEPs, as in principle they are conducted by specialised law enforcement authorities, and even if a multidisciplinary team is established to this end, it is still acting under the remit of the State. In addition, the outcomes of such investigations are subsequently considered by national criminal courts under differing domestic criminal procedures. However, civilian criminal investigations also take place regarding corruption in the public sector.

It should be remembered that there are many private actors highly specialised in OSINT, like 'Bellingcat', which presents itself as the 'home of online investigations'.[71] Civilians operating therein also use crowdsourcing in their investigations.[72] Another example is the non-profit company 'Finance Uncovered' with the mission to 'improve the quantity and quality of investigative stories that are rooted in illicit finance or exploitation by training and supporting journalists and activists around the world'. They are particularly interested in working with

[65] Resolution 2379 (2017) adopted by the Security Council at its 8052nd meeting, on 21 September 2017, S/RES/2379 (2017).
[66] Resolution adopted by the Human Rights Council on 27 September 2018, A/HRC/RES/39/2.
[67] Resolution adopted by the Human Rights Council on 4 March 2022, A/HRC/RES/49/1; Resolution adopted by the Human Rights Council on 4 April 2023, A/HRC/RES/52/32.
[68] See more E. White, *op. cit.,* 236.
[69] See, e.g., E. Baylis, 'Outsourcing Investigations', 14(1) *UCLA Journal of International Law and Foreign Affairs* (2009) 121-147; E. White, *op. cit., passim;* R.A. Costello, 'International criminal law and the role of non-state actors in preserving open source evidence', 7(2) *Cambridge International Law Journal* (2018) 268-283. In more general context, see: K. Hiatt, 'Open Source Evidence on Trial', 125 *The Yale Law Journal* (2016) 323-330.
[70] E. Baylis, *op. cit.,* p. 121.
[71] See Bellingcat, 'Investigations', https://www.bellingcat.com/category/news/ (01.02.2025).
[72] L. ten Hulsen, *op. cit.,* p. 3. See also S.A. Stottlemyre, 'HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence', 28(3) *International Journal of Intelligence and CounterIntelligence*, (2015) 578–589, https://doi.org/10.1080/08850607.2015.992760.

'investigative centres and activists in kleptocracies and countries where Follow the Money journalism is hard to do'.[73] For instance, high-profile investigations concerning foreign PEPs locating assets in the UK have been conducted by British Broadcasting Corporation (BBC), including with cooperation with NGO partners.[74] The next example is 'Transparency International' with operations in more than 100 countries, which describes itself as 'independent, non-governmental, not-for-profit and work with like-minded partners across the world to end the injustice of corruption'; its mission is to 'stop corruption and promote transparency, accountability and integrity at all levels and across all sectors of society'.[75] According to the information provided on their website they 'have trained more than 1,250 journalists and activists from over 90 countries and contributed to well over 150 hard hitting investigations, including the GuptaLeaks, DubaiLeaks, LuandaLeaks and the Pandora Papers'.[76] It is also worth mentioning the Global Anti-Corruption Consortium carried out by Transparency International and the Organised Crime and Corruption Reporting Project to accelerate the 'fight against corruption by connecting hard-hitting investigative journalism to skillful civil society advocacy'.[77] A further example is the analysis by 'Global Witness' stressing the role of 'data-driven and digital approaches' in their operations. As indicated on their website: 'We use a range of techniques to scrape and analyse data from open source and leaked datasets, social media and other online sources'.[78] The next example is the Royal United Services Institute (RUSI), a think-thank whose areas of research cover 'Open Source Intelligence, AI and Disruptive Technologies'.[79] A similar example is the Institute for the Study of War (ISW), which sees its mission i.a. as conducting 'detailed, open-source intelligence analysis to provide the most accurate information on current conflicts and security threats', with operations characterised by researchers acting in conflicts zones which 'enhances their understanding of realities on the ground', in addition, the ISW's activity covers educating leaders from the military and civil sectors, reporters, and the public.[80]

[73] See Finance Uncovered, https://www.financeuncovered.org/about (01.02.2025).
[74] See, e.g., BBC News, D. Casciani, Ch. Eriksson, and S. Swann, 'Unexplained Wealth Order focuses on London mansion' (10 March 2020), https://www.bbc.com/news/uk-51809718 (01.02.2025).
[75] Transparency International, https://www.transparency.org/en/about (01.02.2025).
[76] Transparency International, *op. cit.*
[77] Global Anti-Corruption Consortium, https://gacc.occrp.org/ (01.20.2025).
[78] Global Witness, 'Pages tagged with Digital Investigations', https://www.globalwitness.org/tagged/digital-investigations/ (01.02.2025).
[79] RUSI, https://www.rusi.org/explore-our-research/topics/open-source-intelligence-ai-and-disruptive-technologies (01.02.2025).
[80] Institute for the Study of War (ISW), 'Our mission', https://www.understandingwar.org/who-we-are (07.02.2025). See also J.M. Hatfield, *loc. cit*., p. 409.

In view of the increasing role of non-State actors in performing OSINT, an important caveat should be made, engaging civilian actors in this task to support criminal investigations concerning corruption in the public sector should not be underpinned by questioning the capacity of professionals in this respect, like intelligence officers or policemen, or perceiving them as opponents. Accordingly, steps should be taken to avoid the caricature effect pointed out by *Hatfield* of dressing up civilian actors in the uniforms of professional investigators. Extending the quotation of *Braindeis:* 'Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman. And publicity has already played an important part in the struggle against the Money Trust'.[81]

The key issue is that the State apparatus, including the law enforcement authorities and analysts, is prone to take an opportunistic approach in examining corruption cases concerning political elites, especially when they are tied to the executive branch or create a risk of diplomatic tensions (e.g. in case of transnational placing or investing of corrupt assets). Accordingly, if State actors do not act *ex officio,* they may be forced to act by non-State actors performing OSINT and making their results public, at least partly, to generate additional pressure for investigations at the grassroots level. Therefore, even with the full awareness of the contested feature of the openness of sources that distinguishes OSINT, the engagement of non-State actors still makes sense in corruption cases involving PEPs, as it is in the interest of both, a State and society, to eradicate corruption from the public life, including by pointing to practices of transnational placing or investing corrupt assets.

5. The position of the CJEU in Joined Cases C 37/20 and C 601/20 *WM and Sovim SA* — free or limited access to information of beneficial ownership?

5.1. Transparency of Ultimate Beneficiary Ownership

One of the key resources that allows for the gathering of intel regarding financial links between companies and suspected individuals and makes it possible to trace illicit financial flows is the registry of Ultimate Beneficiary Ownership (the UBO registry). It plays a vital role in crime prevention since 'the availability of information about ownership of companies and trusts is frequently held out as an antidote to crime'.[82] The concept of an Ultimate Beneficiary

[81] L.D. Brandeis, *op. cit.,* p. 10.
[82] A. Moisenko, 'Value of Transparency: The Role of Beneficial Ownership Registers in Tackling Crime', in: S. Hufnagel, A. Moiseienko, ed., *Policing Transnational Crime. Law Enforcement of Criminal Flows* (London: Routledge, 2020) p. 183.

Owner (UBO) and the UBO registry emerged from the efforts of the Financial Action Task Force (FATF), which was the first international body to establish international standards on beneficial ownership in 2003 and refined them subsequently in 2012 and 2014.[83] In the aftermath of several high-profile fraud scandals, the most prominent being the 'Panama Papers', the FATF called on its members to ensure transparency concerning the provision of information on the beneficial ownership of legal entities.[84]

Those efforts resulted in an international Anti-Money Laundering (AML) legal framework, within which the key elements were initiatives of the European Union – the 4th and 5th AML Directives.[85] These two Directives introduced the concept of UBOs as persons who effectively control or enjoy the benefits of ownership of a legal entity, although the title or ownership is in another name. The definition of a UBO encompasses individuals who exercise control over an entity through direct or indirect ownership of a significant percentage of shares or voting rights, or an ownership interest in that entity. The threshold of shareholding of 25% plus one share, or an ownership interest of more than 25% in the customer held by a natural person, was established as an indicative of direct ownership (Article 3(6) of the 4th AML Directive). This has become an EU-wide benchmark for identifying the beneficial owner.

Simultaneously, the 4th AML Directive introduced to the EU legal system the UBO registry, obliging all the Member States to establish a central registry, which contains information about their legal owner as well as UBO (Article 30(1) and (4) of the 4th AML Directive) as a key element of the customer due diligence measures performed by the obliged institutions. This development was particularly significant in the context of the 5th AML Directive, which introduced a substantial advancement by ensuring the accessibility of the UBO registry to the general public (Article 30 (5) of the 4th AML Directive amended by Article 1 (15) of the 5th AML Directive). In this regard, EU legislators emphasised the significance of enhancing public access to the UBO registry, as articulated in the 5th AML Directive, underscoring the importance of this measure in fostering transparency and combatting financial crime: 'public access to

[83] See, FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012), p.117 and FATF Guidance on Transparency and Beneficial Ownership 2014, p. 8.
[84] J. Davila, M. Barron, T., Law, *Towards a Global Norm of Beneficial Ownership Transparency* (London: Adam Smith International, 2019), pp. 11-15.
[85] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter: 4th AML Directive) and 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 (hereinafter: 5th AML Directive).

beneficial ownership information allows greater scrutiny of information by civil society, including by the press or civil society organisations, contributes to preserving trust in the integrity of business transactions and of the financial system. It can contribute to combating the misuse of corporate and other legal entities and legal arrangements for the purposes of money laundering or terrorist financing, both by helping investigations and through reputational effects, given that anyone who could enter into transactions is aware of the identity of the beneficial owners' (Recital 30). This approach was also later emphasised in a European Public Sector Information Directive, which refers to beneficial ownership information as a high-value dataset that should be available free for access by the public.[86]

One can observe a strong 'Brussels Effect'[87] in the context of UBO registers, since as of now approximately 96 countries in the world have introduced their own UBO registry.[88] It is, however, worth noting that from the very beginning, there has been public discussion on the unrestricted openness of UBO registries, as this conflicts directly with the right to privacy and raises the question of the proportionality of such an approach, as was especially highlighted by business interests.[89]

5.2. The challenge to transparency

This legal landscape of far-reaching transparency and general access to the UBO registry was challenged by a preliminary question issued by the Luxembourg court, which considered that disclosing information contained in the UBO registry carried a disproportionate risk of interference with the fundamental rights of the UBO concerned. Therefore, questions of the validity of provisions of the 5th AML Directive regarding public access arose in the context of breaching the right to privacy guaranteed both by the GDPR[90] and Articles 7 and 8 of the Charter[91], and were referred to the Court of Justice of the European Union (CJEU) for

[86] See recital 66, Article 13(1) and Annex I of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-use of Public Sector Information.
[87] 'The Brussels Effect' is described as the external effects of the single market that allow the EU to influence the regulatory framework of other jurisdictions with which the EU interacts economically, thereby unilaterally regulating the global marketplace, see A. Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press 2019), pp. 1-4.
[88] See https://www.openownership.org/en/map/ (30.01.2025).
[89] J. Milaj, C. Kaiser, 'Retention of data in the new Anti-money Laundering Directive—"need to know" versus 'nice to know', 7(2) *International Data Privacy Law* (2017), p. 125, https://doi.org/10.1093/idpl/ipx002; D. Zigo, 'CJEU: WM and Sovim SA v. Luxembourg Business Registers (Joined Cases C-37/20 and C-601/20). Rethinking Transparency of Ultimate Beneficial Owners Register', 7(2) *Bratislava Law Review*, p. 228, https://doi.org/10.46282/blr.2023.7.2.725.
[90] 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 (hereinafter 'GDPR').
[91] Charter of Fundamental Rights of the European Union (hereinafter: the Charter).

preliminary ruling. This preliminary question resulted in the judgement of the CJEU's Grand Chamber of 22 November 2022 in Joined Cases C-37/20 and C-601/20 *WM and Sovim SA*.

The essential issue facing the CJEU was that of assessing whether the openness of UBO registries to the general public can be considered a necessary and proportional intrusion interference with the right to private life enshrined in Articles 7 and 8 of the Charter. Firstly, the CJEU had to trace whether transparency can be considered a value deriving from EU primary law, and whether it can serve as a legitimate objective in the general interest of the EU, in this case justifying interference with the right to private life, an undisputed individual right. The Court maintained that while transparency is a fundamental principle in democratic systems, it should pertain to activities of a public nature rather than to the identities of private individuals, as was the situation in the context of UBO registries (*WM and Sovim SA*, paras 60-62).

To assess the proportionality of the interference, the CJEU employed a well-established proportionality test regarding interference with personal data, used i.a. in the *Ligue des droits humains* case,[92] which established that any derogations from and limitations on the protection of personal data should apply only insofar as is strictly necessary, it being understood that where there is a choice between several measures appropriate to meeting the legitimate objectives pursued, recourse must be made to the least onerous. Thus, the determination of whether a restriction on the rights outlined in Articles 7 and 8 of the Charter is justifiable requires an evaluation of the severity of the interference caused by that restriction. Additionally, to meet the proportionality criteria, the relevant legislation must establish clear and detailed rules regarding the scope and application of the imposed measures, along with minimum safeguards. These safeguards should ensure that individuals have adequate protection for their personal data against potential interference (paras 63-66).

Initially, the CJEU found that the public's access to UBO registries and the interconnected increase in transparency were appropriate steps toward achieving the general interest objective, since they help create an environment less susceptible to money laundering and terrorist financing (paras 64-67). Next, the Court clarified that being strictly necessary means opting for the least burdensome measure when multiple appropriate avenues exist to achieve legitimate goals (para. 64). In this context, the Court scrutinised the amendment made by the 5th AML Directive, which broadened access to the registry beyond just those who can show a legitimate interest, and dismissed the Commission's claim that defining 'legitimate interest' posed

[92] Judgement of CJEU of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paras 115-117.

difficulties (paras 68-73). Moreover, the Court acknowledged that access to UBO information, motivated by the goals specified in Recital 30 of that Directive, constitutes a legitimate interest; however, this does not justify broader accessibility of the registry to the general public being strictly necessary (paras 74-76).

In examining the proportionality requirement, the Court evaluated whether the legislative measures that interfere with rights protected in Articles 7 and the other referenced article ensure 'clear and precise rules governing the scope and application' of these measures and provide minimum safeguards to protect data subjects from abuse (para. 64). The Court ultimately concluded that the rules governing public access to UBO information, particularly Article 30(5) of the 4th AML Directive, did not meet the standards of clarity and precision (paras 78-82). Additionally, when weighing the seriousness of the identified interference against the significance of the pursued general interest objective, the Court remarked that the realisation of AML policies primarily falls to competent public authorities and obligated entities, who already have access to UBO information irrespective of the amendments introduced by the 5th AML Directive (paras 83-84). Consequently, the Court did not see any added value in granting the general public access to UBO information, characterising this new measure as resulting in 'considerably more serious interference'. Finally, according to the Court, the exceptional provisions for limiting access to UBO registry information do not strike a proper balance between the pursued general interest and the rights involved, nor do they provide sufficient safeguards for individuals to effectively protect their personal data from potential abuse (para. 86).

It is worth emphasising that, as accurately highlighted by Maxime Lassalle, the CJEU did not make any reference to the Opinion of the Advocate General (AG), and dismissed the principle of transparency of UBO registries as neither strictly necessary nor proportionate.[93] In his Opinion, the AG did not replicate the CJEU's approach to rewriting the conditions regulating the public availability of the UBO registry, instead proposing a more nuanced approach.[94] Fundamentally from the logic of balancing transparency and privacy, the AG recognized that the principle of transparency in both EU law, as well as according to Member States' constitutional traditions, should prioritize transparency in public life, which can only be limited

[93] M. Lassalle, 'Who cares about financial privacy?: the Court of Justice in WM, Sovim SA v Luxembourg Business Registers, (C-37/20 and C-601/20)', *EULawLive*, 16 December 2022, https://eulawlive.com/op-ed-who-cares-about-financial-privacy-the-court-of-justice-in-wm-sovim-sa-v-luxembourg-business-registers-c-37-20-and-c-601-20-by-maxime-lassalle/ (30.01.2025).

[94] Opinion of AG Pitruzzella delivered on 20 January 2022, Joined Cases C-37/20 and C-601/20, *WM and Sovim SA*, EU:C:2022:43.

in exceptional cases. This, of course, contrasts with the confidentiality of the private sphere, protected by the right to privacy. However, the AG noted that there may be a public interest in certain aspects of an individual's private life. Consequently, the AG concluded that the transparency principle has been extended to financial market regulation to combat issues like corruption and terrorism - while transparency is connected mainly with the public sector, especially public officials, it can also apply to private entities when it impacts fundamental societal interests (AG Opinion, paras 38-48). While conducting the proportionality test, the AG observed that the data contained in UBO registries do not provide complete information about the individuals involved, as they refer only to a particular part of the person's assets, which means they do not directly or significantly interfere with the privacy of their personal lives (AG Opinion, paras 100-104). In light of these comments, the AG sought to find a more balanced approach between the transparency of UBO registries and the need to protect the right to privacy. The AG concluded that UBO registries should remain publicly accessible, however, Member States should not be allowed to broaden the range of data available to the public beyond that outlined in the 4th AML Directive, specifically in Article 30(5) subparagraphs 2 and 3, though they were given the discretion to do so in this provision (AG Opinion, paras 102-107). Furthermore, in the most interesting part of the Opinion, he emphasised the importance of ensuring that UBOs have adequate protections against potential misuse of their data – in order to achieve this, the AG stated that it is essential for Member States to know who is accessing these registries and to inform the beneficial owners about those individuals if doing so is necessary to uphold fundamental rights. To fulfil this goal, the AG suggested implementing measures such as requiring individuals to register before they can access the registry (as mentioned in AG Opinion, paras 195-208).

5.3. New balance or lack of balance?

The reasoning provided by the CJEU is rather unpersuasive in light of the more detailed and impactful arguments presented by the AG convicting. There is little doubt that the principle of total transparency interferes with fundamental tenets of data protection. However, calls for transparency regarding beneficial ownership information aim to empower the public, fostering transparency and accountability among corporate entities, which are constitutionally recognized values, as aptly noted by the AG. One must remember that privacy is not the only value in question. If one intends to limit transparency for the sake of privacy, the reasons for these limitations must be proportionate to both confronting values. Robert Alexy's work on the principle of proportionality provides a valuable framework in this context. Alexy argues that

proportionality, as the meta-principle that deals with legal principles, is an optimisation issue – legal principles co-exist limiting each other, so one has to decide which one to realise to a greater extent and find sufficient reason to do so.[95] Thus, every constitutional reasoning, such as the one conducted by the CJEU, requires finding a careful balance between competing rights or values to ensure that any limitation on rights is justified, necessary, and does not exceed what is required to achieve a legitimate aim, as Alexy briefly summarises: 'The greater the degree of non-satisfaction of, or detriment to, one principle, the greater the importance of satisfying the other'.[96] In the discussed case, the CJEU prioritised the right to privacy, thereby limiting transparency in public life and weakening market protections against potential abuses via illicit financial flows. There are alternative, persuasive arguments suggesting that transparency and market integrity are also fundamental values to be upheld alongside privacy.

In this context, it is important to note that the CJEU, in evaluating the right to privacy, has disregarded its limited scope in relation to certain individuals, particularly PEPs, under the European Convention on Human Rights[97] and European Court of Human Rights (ECHR) case law. This is although the referring court explicitly referred not only to the Charter but also to Article 8 of the Convention. Furthermore, the CJEU's own case law on data protection, as articulated in Article 52(3) of the Charter, underscores the necessary consistency between the rights enshrined within the Charter and the corresponding rights guaranteed by the Convention. Thus, the right to respect for private and family life, as enshrined in Article 7 of the Charter, corresponds to the right guaranteed by Article 8 of the ECHR, as they have the same meaning and scope[98]. It is, therefore, necessary to consider the ECHR's approach. Evidently, the right to privacy is not absolute and is subject to limitations, particularly in the context of individuals who are public figures (by definition including PEPs) or have direct and close relations with them.[99] The definition of 'public figures' is broad, encompassing not only politicians and celebrities but also individuals who play a significant role in the community, such as local priests.[100] As per the ECHR case law, this expansive definition serves as a compelling argument

[95] R. Alexy, 'On the Structure of Legal Principles', 13(3) *Ratio Juris* (2000), pp. 299–304, https://doi.org/10.1111/1467-9337.00157.
[96] R. Alexy, 'Constitutional Rights, Balancing, and Rationality' 16(2) *Ratio Juris* (2003), p. 136, https://doi.org/10.1111/1467-9337.00228.
[97] Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome, 4 November 1950 (hereinafter: the Convention).
[98] Judgement of CJEU of 18 June 2020, *Commission* v *Hungary (Transparency of associations)* (C-78/18, EU:C:2020:476, para. 122.
[99] Judgement of ECtHR of 19 November 2020, *Dupate v. Latvia*, ECHR:2020:1119JUD001806811, paras 54-57.
[100] Judgement of ECtHR of 14 October 2021, *M.L. v. Slovakia*, ECHR:2021:1014JUD003415917, para. 37

in favour of the transparency and openness of the financial register, particularly in the context of UBOs, which play a vital role in the contemporary economy.

Furthermore, the ECtHR has emphasised in its case law, both prior to and following the judgment in question, the significance of transparency and ensuring security as a legitimate interest that justifies the limitation of the right to privacy under Article 8 of the Convention. For instance, in the case of a lawyer obliged to provide information to the competent authorities about the suspicion of his client's unlawful money laundering activities, where such suspicions came to light outside the context of their defence role, no violation was found.[101] In the case of *L.B. v. Hungary*[102], which concerned the publication of information about tax defaulters, although it found an infringement of the right to privacy in the context of the specific case due to the defectiveness of the proceedings and potential stigma, it recognised the need for financial transparency (para. 113) and indicated a comprehensive framework for assessing whether a particular intrusion into private life was justified (summary in para. 128). It was determined that the assessment of necessity in a democratic society is contingent on various factors, including the scope, content, and nature of the information, as well as the manner in which it is disseminated (paras 115-123). It was acknowledged that the state retains considerable discretion in regulating this matter, and it was emphasised that consensus at the European level is imperative in determining the disclosure of data in the context under consideration (para 127). In the context of AML legislation, this would provide substantial support for the UBO registry's openness, given the data's scope and its non-stigmatising, objective nature. In this regard, considering the standards set by ECtHR case law would introduce a greater degree of nuance to the balance between transparency and security, on the one hand, and the right to privacy, on the other. The CJEU did not follow this path and explicitly prioritised the latter value.

Ultimately, this CJEU case highlights the rising importance of financial privacy from the CJEU perspective, raising crucial questions about its justifications and potential constraints. It also confirms the unyielding position of the CJEU, which can be derived from the 'Data Retention Saga'.[103] The decision also heavily impacts the role of civil society in ensuring financial

[101] Judgement of ECtHR of 6 December 2012, *Michaud v. France*, ECHR:2012:1206JUD001232311, paras 127-128.
[102] Judgement of ECtHR of 9 March 2023, *L.B. v. Hungary*, ECHR:2023:0309JUD003634516.
[103] The Data Retention Saga is a series of CJEU judgements and decisions issued since 2016, in which CJEU created the basic tenets of personal data protection and data retention, see G. Lasagni, 'Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the 'Data Retention Saga'', in L. Bachmaier Winter, F. Salimi, eds., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Oxford: Bloomsbury Publishing, 2024), pp. 30-38.

transparency and limits the options for civilian actors to act as support for public authorities in the fight against financial crime – a perspective which, again, was excluded entirely in the CJEU's judgement. UBO registries hold important information about UBOs, and this information may assist in gathering evidence regarding the location of illicit assets. While law enforcement agencies will still have access to this information to investigate criminal activity, the Judgement in question is a serious setback for all civil society actors, limiting their potential scope of engagement. The CJEU directly excluded the role of NGOs and non-public investigators in detecting and preventing corruption and money laundering, directly stating that it is the role of public authorities, not civil society, to target tainted money and illicit assets – thus, as considered in the commentaries on the Judgement,[104] it is a major setback for the development of grassroots activity by non-State actors.

6. The fall and rise of civilian actors and open sources: *National Crime Agency v Baker and Others* and *Viatcheslav Kantor*

The case of *NCA v. Baker* illustrates the complexities involved in tracing illicit financial flows and underscores the advantages of engaging civilian actors in this crucial process. This particular case revolved around assets belonging to the family of Rakhat Aliyev, which gained attention due to substantial allegations of corruption tied to their father's dealings. Notably, the initial investigation was prompted by detailed reports from non-governmental organisations (NGOs), such as Transparency International and Finance Uncovered, as well as BBC journalists. The reports highlighted suspicious financial activities, identified real estate and the actual owners, who were concealed behind shell companies, and advocated for scrutiny by the authorities.[105]

The official investigative task was undertaken by The National Crime Agency (NCA), a British institution tasked with combating serious and organised crime, which employs various legislative tools to tackle financial crime effectively. Among the most significant of these tools is Unexplained Wealth Orders (UWOs), introduced under the Criminal Finances Act 2017, an amendment to the POCA 2002. A UWO empowers the NCA to seize assets owned by PEPs when their wealth cannot be satisfactorily explained in relation to their publicly declared

[104] D. Haberly, T. Shipley, R. Barrington, *Corruption, shell companies and offshore financial secrecy: directions for anti-corruption policy*, (Brighton: Centre for the Study of Corruption, University of Sussex, 2023), pp. 24-25.
[105] Financial Times, 'London homes probe linked to former Kazakh ruler's family', https://www.ft.com/content/84d833ca-62d8-11ea-b3f3-fe4680ea68b5 (30.01.2025).

income. This mechanism is particularly pertinent in cases involving individuals with potential ties to corrupt practices.[106]

The *NCA v. Baker* case is particularly noteworthy as it was catalysed by reports from NGOs and journalists, especially by the fact that the properties about which questions were raised had been identified in an investigation by BBC News, Finance Uncovered and Transparency International. Utilising solely public sources, the civil investigators had established that the mansions in question were occupied by Nurali Aliyev, son of Rakhat Aliyev, his wife Aida Aliyeva, and Dariga Nazarbayeva, a prominent Kazakh politician and widow of Rakhat, despite the official ownership of the mansions being attributed to shell companies based in tax havens.[107] Moreover, the case was heavily reliant on a report published by Global Witness in 2015, which revealed significant involvement by Kazakh political elites in the London real estate market.[108]

In its submissions, the NCA incorporated a variety of evidence, including Rakhat Aliyev's memoir and relevant information derived from customer accounts at Harrods, a luxury department store. Additionally, the NCA included details about one of the registered owners and UBOs (Dariga Nazarbayeva and Nurali Aliyez, the ex-wife and son of Rakhat Aliyev, a deceased former senior Kazakh official) of the contested properties. Copies of LinkedIn profiles of the UBOs were included in the 'full and frank disclosure' section of its documentation, emphasising the role of open-source intelligence in financial investigations.[109] In May 2019, the National Crime Agency (NCA) secured UWOs along with interim freezing orders after convincing the court that several properties in London were acquired through money laundering. Various individuals and companies associated with the purchase or ownership of these properties were subjected to UWOs, and the prominent bank Barclays was linked to providing a mortgage for them,[110] however, the UWOs were challenged before the High Court.

---

[106] A. Moiseienko, 'The Limitations of Unexplained Wealth Orders' 3 *Criminal Law Review* (2022), pp. 231–234, http://dx.doi.org/10.2139/ssrn.4708025.

[107] Finance Uncovered, 'Unexplained Wealth Order focuses on London mansion', https://www.financeuncovered.org/stories/unexplained-wealth-order-focuses-on-london-mansion (30.01.2025).

[108] Global Witness report, 'Mystery on Baker Street', 2015, https://www.globalwitness.org/documents/18036/Mystery_on_baker_street_for_digital_use_FINAL.pdf (30.01.2025).

[109] Á. Clancy, 'Proving the Dough: National Crime Agency v Baker & Ors', 84 (1) *Modern Law Review* (2021), p. 173, https://doi.org/10.1111/1468-2230.12589.

[110] NCA, 'NCA secures Unexplained Wealth Orders for prime London property worth tens of millions', 2019 https://www.nationalcrimeagency.gov.uk/news/nca-secures-unexplained-wealth-orders-for-prime-london-property-worth-tens-of-millions?highlight=WyJ1bmV4cGxhaW5lZCIsIndlYWx0aCIsIm9yZGVycyIsIm9yZGVyIiwib3JkZXJlZCIsIm9

In their defence, the UBOs presented various pieces of evidence, including a comprehensive account from a Kazakhstani prosecutor regarding an investigation into Rakhat Aliyev and a witness statement from their legal representative. They also referenced a 2013 article published in Forbes Kazakhstan, alongside legal counsel provided by a lawyer based in Panama; this information was considered for its potential relevance. Despite the NCA's efforts to present a compelling case, the agency ultimately faced defeat in court. The judge assigned considerable weight to the evidence provided by the Kazakh defence, particularly emphasising the Kazakh prosecutor's narrative surrounding the investigation into Rakhat Aliyev. This prosecutor maintained that no unlawfully acquired funds had been transferred to Aliyev's wife as part of their divorce settlement, which played a pivotal role in shaping the court's conclusions (*NCA v. Baker*, paras 70-71). This ruling raised significant concerns, especially given the reliance on evidence from a country with notable rule of law challenges, effectively allowing a participant in the trial to shape the judicial narrative. Furthermore, the court expressed implicit criticism of the NCA's reliance on the Global Witness report concerning Aliyev's assets (*NCA v. Baker*, para. 87), displaying scepticism about the overall reliability of information sourced from NGOs. The court concluded that the NCA's UWO 'was flawed by inadequate investigation into some obvious lines of enquiry' (*NCA v. Baker*, para. 217). In summary, the *NCA v. Baker* case serves as a vital reference point for discussing the critical role of investigative work conducted by NGOs in financial crime cases. It exposes the challenges public institutions face in navigating complex legal frameworks while striving to combat financial crime and highlights the difficulties inherent in relying on international cooperation and evidence accumulation in such intricate matters. Ultimately, this case paints a rather pessimistic picture of judicial outcomes, particularly in light of the British court's stance on the presented evidence and the required standard of proof applied.

However, despite the rather reserved approach of the British court, one has to acknowledge the EU's latest positive development within the area in empowering the civilian actors and use of open sources regarding the - very recent ruling of the Court of the First Instance in *Kantor* case[111]. The Court, in the wake of the claim of Viatcheslav Kantor, a well-known Russian oligarch, to annul several Council decisions regarding sanctions placed on him and his enterprises, faced the issue of sufficient justification of restrictive measures targeted on a

yZGVyaW5nIiwidW5leHBsYWluZWQgd2VhbHRoIiwidW5leHBsYWluZWQgd2VhbHRoIG9yZGVycyIsIndlYWx0aCBvcmRlcnMiXQ== (30.01.2025).

[111] Judgement of the Court of First Instance of 15 January 2025, T-748/22, *Kantor v. Council of the EU*, ECLI:EU:T:2025:6.

particular individual. Kantor challenged the basis for the sanctions imposed, pointing out that the justifications and sources used by the EU Council are unreliable and biased, and in particular do not provide sufficient assurance, as they are publicly available websites such as Wikipedia, or media owned by a particular company that has an interest in providing biased information.

The Court rejected these claims, stating that since the EU authorities do not have investigative powers in third countries, their assessment must in fact be based on publicly available sources of information, reports, press articles as well as intelligence reports, especially in the context of Russia's aggression against Ukraine, where certain information is particularly difficult to obtain (para 108). In essence, the Court acknowledged in this fragment that, in the case of third countries, EU officials must use tools similar to NGOs and journalists, which underscores the role played by civilian actors in conducting international investigations into illicit financial flows. The Court also responded to claims about the unreliability of open-source information and press reports, stressing that it cannot be said that Wikipedia, by default, is not a sufficiently reliable source of information and has limited evidential value. This is because it can still corroborate information from other sources, so it can be used (para. 116). Similarly, the mere fact that evidence is taken from commercial websites is not sufficient to deprive it of any probative value because the fact that a particular company owns a media outlet does not automatically mean that the information presented there is not reliable (para. 112). This ruling confirms the role and power of investigative journalism and open-source intelligence techniques in the EU's decision-making process, which is certainly a very different position to that taken by the UK court in the Baker case. This is a positive sign for the emerging and growing role of civil society and its involvement in the promotion of the European area of freedom, security and justice, and perhaps a starting point for its redefinition.

Conclusions

Considering the open nature of cyberspace, it is difficult to defend the argument that exploring it for criminal justice purposes, at least on the level accessible to its civilian users on the same basis as to law enforcement authorities, should be reserved only for the latter. All the more so, given that the State may profit from a public-civil partnership in this respect, starting from establishing the facts, identifying the perpetrators and victims, determining the harm done by a crime, and ending with preventing future crimes i.a. by informing the public about the outcomes of criminal proceedings.

In view of the above, the tasks of collecting and analysing open data seem to have the potential to be partially privatised, both to benefit the interests of civil society and the interests of criminal justice. A public-private partnership in this respect may be beneficial in multiple dimensions. Engaging NGOs and investigative journalists in identifying the suspicious asset flows of PEPs is in line with their mission as intermediaries providing society with information about processes that are usually hidden from the general public. Furthermore, supporting civilian actors in performing the function of a 'watchdog' patrolling an 'open-source space' to detect the corrupt practices of PEPs may be valuable for the State, as the preliminary analysis delivered by these actors may ultimately result in freezing and confiscation of unexplained wealth, or launching criminal proceedings in corruption-related cases. Such pre-trial analysis by non-State actors may be perceived as a provisional investigation, '*quasi*-investigation', being the kind of 'screening proceedings' preceding official criminal proceedings or freezing and confiscation proceedings. Importantly, such initial analytical actions need not necessarily be conducted under the remit of the State. A concrete case may justify informing the public of suspicious practices by PEPs prior to informing law enforcement authorities, who may be reluctant to act if the results of the preliminary analysis concern the political establishment. In such cases, well-informed public opinion can apply pressure on authorities to follow through with investigations.

Ultimately, the State's resilience to corruption largely depends on the strength of its civil society. Thus, strengthening the representatives of civil society, like NGOs or investigative journalists performing anti-corruption tasks within their public mission, should not be overlooked in any corruption strategies, including the common strategy pursued by the EU.

Accordingly, this paper argues for increasing the capacity of civilian actors to perform OSINT in corruption-related cases through legislative and other measures. The legislative approach should involve establishing the EU legal framework for gathering publicly available e-evidence by State and non-State actors and their voluntary cooperation in this respect, including in the form of public-private partnerships and outsourcing the tasks. The regulatory framework should also give due regard to privacy protections. In addition, soft law recourse should be considered, especially establishing good practices of OSINT for criminal justice purposes. Implementing the concept of 'privacy by design' when creating OSINT tools may serve as an additional level of protection for privacy rights.[112]

[112] See B.-J. Koops, J.-H. Hoepman, and R.E. Leenes, *op. cit.,* pp. 676-688.

As far as non-legislative measures are concerned, there is room for the EU and MS to take action to promote professional knowledge-sharing about intelligence from open sources with civilian actors, providing training and delivering the necessary equipment. Establishing a network of highly trained NGOs cooperating with investigative journalists in each of the EU MS, with strong knowledge of the language and the domestic realities, would help when tracing corrupt practices of PEPs using publicly available sources. Creating a civilian anti-corruption network could be one of the goals of the EU's anti-corruption strategy, perhaps of greater importance than other actions addressed by the EU to the State authorities rather than directly to civil society.

However, there is also a less optimistic side to the issue under consideration. Increasing the capacities of private initiatives in the area of extracting intelligence from publicly available sources raises questions about the future role of State actors, as it cannot be ruled out that their role will be pushed to the margins, and entering into the public-private partnerships by States will turn out to not be a voluntary, but necessary, and indeed the only possible path. It can also not be excluded that terms and conditions of such agreements will be dictated by the private counterparts of the State actors (creating the risk for the State of moving civilian criminal investigations outside the area of legal authorisation). The risks and threats resulting from diminishing the role of the State should be subjected to discussion in academic and professional circles. Especially, given recurring leaks of classified documents to freely available layers, caused by leakers and whistleblowers acting in the public interest, a situation that States are evidently unable to counteract.