ARICA

Assessing risk indicators of child sexual abuse

White paper – current legal and policy challenges in open source CSAE investigations on the dark web

Date of initial publication: 23/04/2024

Updated to reflect the official publication of the AI act on 12 July 2024

Funded by the European Union

ARICA

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

This report was prepared as part of the ARICA project. The contents of this document are provided “AS IS”, and no guarantee or warranty is provided that the information is correct, representative, or fit for any particular purposes. Neither the Union institutions and bodies, nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The user, thereof, uses the information at its sole risk, responsibility and liability.

Copyright notice

Abbreviations and acronyms

AI	Artificial Intelligence
AIA/ AI Act	The EU's Artificial Intelligence Act
CSAE	Child sexual abuse and exploitation
DPIA	Data Protection Impact Assessment
EC	European Commission
EU	European Union
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
LE	Law Enforcement
LEA	Law Enforcement Agency
LEAs	Law Enforcement Agencies
LED	Law Enforcement Directive
OSINT	Open Source Intelligence

ARICA

Contents

ARICA

Executive summary

This paper discusses three of the main current legal challenges in open source investigations of CSAE on the dark web, common to LEAs across the EU. It is the result of an EU-wide legislation monitoring activity of the ARICA project.

The three challenges discussed in this paper are the following:

- **Challenge 1**: the **procedural legality** of the use of OSINT in CSAE investigations on the dark web;
- **Challenge 2**: the rules of the recently adopted **AI Act** and their impact on AI-driven OSINT tools to be used for CSAE investigations on the dark web;
- **Challenge 3**: the impact of the data protection rules of the **Law Enforcement Directive** (LED) on the use of OSINT tools in CSAE investigations on the dark web.

The purpose of this white paper is to explain the essence of these complex issues in concise terms, in order to raise awareness and facilitate further discussions and debate on the topic, as well as to propose some policy actions that may help to remedy the current problems.

With regards to **challenge 1**, the main finding of this white paper is that **the procedural framework for the use of OSINT as it currently stands is not satisfactory**. OSINT is usually based on general police powers to prevent, detect and investigate crime and to keep public order, which do not required any (judicial) authorization or judicial review, nor provide for specific safeguards. Such general powers can justify OSINT applications that have a limited impact on privacy ("low interference"), but more complex and impactful applications ("high interference"), while they may be needed in practice, are less easily justified used on this basis, if at all. The policy recommendation here is to address the current grey zone, which leads to LEAs either not using available, cost-effective OISNT tools, or may force them in a situation to use such tools in breach of fundamental rights guarantees, which may moreover lead to issues with the admissibility of the evidence obtained in this manner. Rather, **a clearer framework should be available to LEAs, providing clear conditions for higher interference OSINT use and safeguards**, including judicial authorization or authorization by an independent competent authority (with judicial review) for complex and privacy-intrusive OSINT applications.

In relation to **challenge 2**, the main finding is that **the AI Act will have a profound impact on the use of AI-driven OSINT applications in CSAE investigations on the dark web**. Many complex OSINT applications may qualify as a high-risk AI system and the AI Act imposes important obligations, not only on the developers ("providers") of such systems, but also on the LEAs merely using ("deploying") such tools. Moreover, LEAs that intend to substantially modify existing tools or modify their purpose must keep in mind that may result in them qualifying as a provider themselves, meaning the more stringent provider obligations would apply to them as well.

Given their role and responsibility, actions by LEAs using AI are inherently characterized by a significant degree of power imbalance vis-à-vis the people involved, which highlights the need for safeguards in relation to the use of AI in open source investigations on the dark web, also in situations where the AI Act perhaps does not regulate.

Appropriate human oversight, sufficient training and knowledge and a thorough understanding of potential fundamental rights impact, tradeoffs and necessary safeguards are important in this context. LEAs, like most other organizations, are not yet fully prepared for the impact of the AI Act. Hence, **awareness raising, knowledge building and training is going to be important in order to make sure LEAs will be able to meet their compliance requirements under the AI Act.**

The policy recommendation in relation to this challenge is therefore to **make sure that sufficient support is made available to LEAs** in order to raise awareness about the AIA and its obligations, provide training, and to provide resources, such as **guidance, checklists and templates** (including the form of tools or wizards to guide the user through the process), which are **ready to use, clearly explained and remain reasonable in terms of resource requirements**.

Concerning **challenge 3**, the main finding of this paper is that the **LED and its national transposition presents some challenges for the use of OSINT applications in CSAE investigations on the dark web**. In particular, there remain gaps in the national transposition of the LED, and these gaps have a negative impact on **the legality of personal data processing in OSINT use cases** under Article 8 LED (which requires a legal basis for data processing) and Article 10 LED (which requires a justification for the processing of special categories, and only when strictly necessary). In addition, the **national transposition is not always clear, complete, and accessible,** which may present issues for tool developers to adjust their design to be compatible with national transposition across the Member States. Lastly, attention to data protection and data protection knowledge has increased since the introduction of the LED, but still presents room for further improvement. **Further awareness raising and training is still needed, both on the LED and national implementation in general, and on specific topics**, such as the intersection of the LED with the AI Act, which will provide particular challenges for LEAs when using AI- and (big) data-driven OSINT tools for CSAE investigations on the dark web. Specifically for the national transposition, **it would be desirable to have a complete and detailed overview on the EU-level of national transposition and the application of such rules in practice**. This would greatly facilitate discussions on this topic easier, including whether further action is needed by certain Member States to reach the requirements of the LED. The policy recommendation for this challenge is to create such an overview as a basis for a further exploration of the actions needed to support a complete transposition and implementation of the LED, and to continue (and perhaps intensify) existing efforts on training and awareness, in particular adding specific training on new challenges such as the AI act.

The overall conclusion of the white paper is that in **open source CSAE investigations on the dark web, the amount of issues adds up**, leaving LEAs to navigate a complex, and at times uncertain and times unclear legal framework, in an area (the dark web) that is already at the very center of the tension between secure societies and privacy. **LEAs deserve more legal clarity** on the procedural framework for using OSINT, as well as continued (and perhaps intensified) **support** in terms of awareness raising, training and resources to support them in the concrete implementation of a growing body of (complex) regulation on the EU and Member State level.

Introduction

This paper has been written within the context of the ARICA project (https://aricaproject.eu/), which stands for “Assessing Risk Indicators of Child Sexual Abuse” and is a two-year project funded by the European Union's Internal Security Fund, which aims to support law enforcement agencies in their fight against child sexual abuse. It develops technologies that will enhance the LEAs’ capabilities in investigations on online child sexual abuse and exploitation (CSAE) and CSAE material. These technologies will remain free to use for LEA after the end of the project.

The focus of the ARICA project includes CSAE on the dark web and hence there is a need to explore the legal framework and the existing legal challenges faced by LEAs investigating CSAE on the dark web.

This paper is not an analysis of compliance aspects or capabilities of the tools developed in the ARICA project for the use by Law Enforcement. Nothing in this paper is meant to comment on the details of the tools, their capabilities or the requirements for their use in compliance with applicable law. Information on the ARICA project outcomes is and will be made available to the law enforcement community, for whom these outcomes are intended.

Rather, this paper is intended to highlight some specific challenges and to further the debate on this topic. As such, the ARICA project serves as a platform to further the on-going broader debate about police capabilities in the digital age and specifically their use of technology to combat crime on the dark web. Criminals, including those committing various crimes related to child sexual abuse and exploitation (CSAE), are quick to use and adapt technology to their advantage and it must be assessed how police can equally leverage the capacities of technology to fulfill their duties in this domain, namely to prevent, detect, investigate and prosecute criminal offences, taking into account their limited resources and the need to remain in compliance with national and European law, in particular fundamental rights like privacy, data protection and fair trial.

ARICA

ARICA aims to contribute to addressing the fight against CSAE, which is a priority on the EU level. It is a sad finding that, according to a recent annual report of the internet watch foundation,[1] 59% of reports of confirmed CSAE were hosted in an EU Member State. The European Commission presented its EU strategy for a more effective fight against child sexual abuse in 2020[2], covering the 2020-2025 period. As a part of this broader strategy, the EU has notably introduced an interim (temporary) derogation[3] from certain provisions of the ePrivacy Directive in order to allow (or rather create temporary legal certainty) around the voluntary use of CSAE material detection technologies by certain service providers (notably interpersonal communication services),[4] and introduced a proposal for a regulation to combat child sexual exploitation and abuse online, in particular by detecting and removing (new) CSAE material (commonly referred to as the CSAM regulation proposal),[5] meant to enable i.a. obligatory detection orders and mandatory reporting obligations for providers of interpersonal communication services and providers of hosting services in the EU.

In addition, in February 2024, the European Commission has also introduced a proposal to recast the CSA Directive,[6] with the aim to make sure that the existing rules of Directive 2011/93/EU[7] are completely and effectively implemented. In addition, the recast Directive proposes an expansion of offences and higher penalties for CSAE material in the EU. Moreover, it will also provide a firm legal basis for civil society hotlines to process reports of suspected CSAM and collaborate with law enforcement to remove such material. This includes

[1] Available at: https://annualreport2022.iwf.org.uk/.

[2] Communication from the commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 607 final, EU strategy for a more effective fight against child sexual abuse, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607 (last consulted 08/04/2024).

[3] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance), OJ L 274, 30.7.2021; the interim derogation was set to expire in August 2024, but has been extended until 3 April 2026 while waiting for a more permanent solution. The extension was agreed in February 2024 (see https://www.europarl.europa.eu/news/en/press-room/20240212IPR17636/child-sexual-abuse-online-agreement-on-extending-current-rules-until-april-2026) and more recently endorsed by the European Parliament in early April 2024 (see https://www.europarl.europa.eu/news/en/press-room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026).

[4] Regarding the legal framework of such voluntary efforts and their future within the EU, please refer to the whitepaper on this topic recently presented by Timelex. Available at https://www.timelex.eu/en/blog/future-voluntary-csam-detection-eu-primer.

[5] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN.

[6] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast), COM/2024/60, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A60%3AFIN. For more details on the recast, please see: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757790/EPRS_BRI(2024)757790_EN.pdf

[7] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011.

activities like receiving and analyzing reports, notifying law enforcement, collaborating across borders, and conducting proactive searches. The directive aims to reduce the workload for law enforcement, enhance cooperation between hotlines and law enforcement, and streamline the removal of illegal content from the internet.[8]

An explicit part of the EU strategy for a more effective fight against child sexual abuse is to make sure the EU has the right legal framework to protect children. Protecting children requires various angles of action, but certainly includes a law enforcement response to identify victims and to investigate suspects in order to identify perpetrators and have them prosecuted. This paper aims to contribute some elements to the discussion on the legal framework (and the interpretation of the existing legal framework) needed to present an effective law enforcement response to CSAE, in particular on the dark web (and using OSINT tools).

While it is justified that a lot of efforts are dedicated to the detection and the prevention of CSAE (including grooming) and CSAE material on the clear web, sufficient attention must also be devoted to the prevalence of CSAE material and the impact of CSAE communities on the dark web. The size of this problem is significant and the growth in recent years of these communities, in number and membership, extremely concerning.[9]

A specific characteristic of the dark web is a heightened level of anonymity, meaning that it is more difficult compared to the clear web to identify a perpetrator, as well as to find out where that perpetrator is physically located.[10] De-anonymizing efforts are significant, meaning that LEAs must be strategic in the use of their resources.

Within the setting of CSAE investigation on the darknet, the most relevant evolutions in recent years relate to the increasing capabilities and availability of tools leveraging the potential of Artificial Intelligence (AI) to assist LEAs in their work.

Of particular interest are tools that use openly or publicly available online sources to produce intelligence for law enforcement, evidence in an investigation, or to enrich already existing police data within a given context. Such tools, often referred to as OSINT (open source intelligence tools) are very useful to Law Enforcement, in particular on the dark web where direct identification of the perpetrator is difficult and resource intensive, to help LEAs in their tasks e.g. to perform lexical analysis or geo-spatial analysis to help victim identification and localization, or to prioritize targets. The essence of such tools is that they leverage information that is freely available to LE in practical terms (because it is publicly available on the internet).

However, the fact that information is freely available and can be accessed easily in technical terms, does not mean that this can be done without restriction. Rather, the use of OSINT tools,

[8] See for more details the analysis by INHOPE, a members' organization for hotlines in 51 countries, in the EU and globally: https://inhope.org/EN/articles/how-the-recast-eu-csam-directive-empowers-inhope-hotlines.

[9] See e.g. Gannon, Colm; Blokland, AAJ; Huikuri, S; Babchishin, KM; Lehmann, RJB (2023). Child sexual abuse material on the darknet. La Trobe. Journal contribution. https://doi.org/10.26181/24971157.v1.

[10] Which highlights the need for cooperation between LEAs, as otherwise many efforts would be wasted or duplicated, as many LEAs will spend time on the dark web investigation criminals that are not within their own jurisdiction.

in particular complex OSINT tools with a level of automation in data collection and/or use, raises questions in terms of privacy impact and procedural powers.

Not only privacy is relevant in this context. Since the use of AI tools in general, and OSINT tools in particular, often implies the use of personal data, the fundamental right to data protection must be considered as well. This right is enshrined in Article 8 of the EU Charter of Fundamental Rights,[11] and implemented in particular in the Law Enforcement Directive, which will be discussed further.[12] OSINT use may additionally also have an impact on other fundamental rights, including procedural fundamental rights such as the right to an effective remedy, the right to a fair trial, the right of defense, and the presumption of innocence.

Another topic of relevance is the permissibility of the use of AI tools in specific settings and use cases, especially those that may have a significant impact on the people involved and their fundamental rights. With the Artificial Intelligence Act,[13] the EU is introducing new rules to help ensure that AI is developed and deployed in a trustworthy manner, with the ultimate aim that society can benefit from the capabilities of AI, while staying true the Union's values.[14] The AI Act also applies to law enforcement and therefore is important to be considered here as well.

[11] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.
[13] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.
[14] See on this in particular the updated coordinated plan on AI (2021), available at: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review; for a basic overview of the policy context, please refer to https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

As such, the ARICA consortium selected the following current challenges as topics to be addressed in this paper:

- Challenge 1: the legality of the use of OSINT tools and access to publicly accessible sources online;
- Challenge 2: data protection under the law enforcement directive;
- Challenge 3: the use of AI during investigations on the dark web.

All three topics focus on the context of a CSAE investigation on the dark web, but will also provide some more generalized comments and observations. They are developed in more detail in the sections below.

In an attempt to gather some insights into the practical reality that exists within LEAs, the ARICA consortium has contacted representatives from LEAs as stakeholders to answer a questionnaire containing some specific questions on the 3 aforementioned topics/challenges. The questionnaire that was used is added in Annex A. The questionnaire will run throughout the project but so far 26 responses have been received from 15 countries. In order to have a realistic insight, extensive promises of confidentiality were made and answers were provided anonymously. No specific answers of respondents will be referenced, only high level findings. No claims are made as to these answers being correct, or being representative of the opinions of LEAs as a whole or of LEAs in the given country from which the respondents originate. Nonetheless, some clear indications can be drawn from the results. These findings will be presented in relevant part in the appropriate sections, but primarily in the policy statements.

ARICA

CHALLENGE 1: the legality of the use of OSINT tools and access to publicly accessible sources online

OSINT in law enforcement

Setting the scene – meaning of OSINT

While there is no universally accepted definition (which in itself hinders targeted discussion on the topic), Open source intelligence or "OSINT" in this paper refers to:

- The collection, processing, analysis, production, classification, and dissemination of information;
- Derived from or found at publicly available "open" sources;
- With the aim to either produce actionable intelligence or evidence.

Typical examples of such open sources include:

- Public Records;
- News media;
- Public profiles on social media platforms;
- Images, videos published on the internet on various openly accessible platforms;
- Publicly accessible websites;
- The dark web (in as far as the specific parts that are accessed are not private).

OSINT can be as simple as manually checking public records as part of an investigation, or to view the profile or public social media activity of a perpetrator or victim to acquire information. However, OSINT can also include more advanced and automated techniques. Certain tools will for example use web scrapers (also referred to as web crawlers) to automatically collect information (text, video, images) and then use AI to analyze, evaluate and present the data.

Open sources

Open sources is a broad concept, and can encompass many situations. Open sources also includes information for which LEAs must take additional steps to access it, such as making an account, or taking technical steps to access or collect the information. **However, LEAs must not circumvent technical security measures to take access to a source, even if this could easily be done**.

Whether or not a given source is publicly available or private can be subject of some discussion and may depend on national law (in particular also case law and interpretation). Generally for example, the requirement of an account does not render the information of the service requiring that account private in itself. Hence, registering an account, whether on social media or on a dark web hidden service, to gain access to the information accessible to any user of that

service is generally permissible. However, services, groups or networks requiring an invitation link that must be authorized by another member of the service, group or network, and that cannot be automatically generated upon mere request, would indicate that the source is in fact not open and publicly available. The same is true if there is an effective verification mechanism in place so that for example a realistic false identify must be assumed to gain access to a source. The importance of this element of open or closed source is mostly that it brings with it different implications in terms of fundamental rights, notably privacy.

Some elements that LEAs might want to consider when deciding whether a source is open or not include:

a) Registration requirements (i.e. to make an account or create a profile) and the broader circumstances of such registration (will any user name do or are there particular requirements to make it seem like a realistic profile?);

b) Identity and device verification steps (i.e. is there any type of procedure in place to check identify or that the user is authorized?);

c) Invitation only access (i.e. can the source only be accessed by individuals who have been personally invited?);

d) Obfuscation of access links (i.e. can the source only be accessed when its URL is already known specifically?);

e) Available data access mechanisms (e.g. is the source accessible to a public API which anyone can use?);

f) Communicated access conditions and intended target audience (e.g. do the terms and conditions of the source clearly stipulate certain uses or exclude certain uses?).

The above examples are by no means exhaustive and are simply illustrative of elements that may be at times construed as limiting who has access to the resource and therefore its open nature. Final evaluations depend on the factual circumstances and applicable national law.

OSINT vs. special investigative powers

For the purposes of a clear discussion on the topic, OSINT must be understood as another tool in the LE toolbox, in addition to but distinct from special powers of investigation, such as wiretap/interception, infiltration, systematic observation etc., which require special permissions under national law because of their inherent implications on fundamental rights. Such special investigative powers are normally very targeted, limited to specific persons and limited in duration.

OSINT tools may however, at least in data collection, be broader. Their use may be limited as well, or may also cover a broader range of situations. Those elements are discussed further under the subsection of “high vs. low interference”, as they have a bearing on the fundamental rights impact of such tools. This however does not mean that the use of OSINT tool excludes the use of special investigative powers together, but rather that they are distinct concepts, which may or may not overlap.

The two elements that are most relevant in determining whether OSINT tools are self-standing or whether they (should) involve the use of special procedural powers are the **presence or absence of a systematic and targeted observation** and the question of whether or not there is **any form of engagement of the target(s)** (which almost certainly includes some form of deception, assumption of a realistic false identify etc.).

For what concerns the **systematic nature of the observation,** it must be noted that specific procedural powers for this tend to be focused on systematic observations of specific persons. Investigative powers are usually intended for the physical world and may not necessarily translate immediately to an online context. Nonetheless, when an OSINT tool is used to systematically keep an eye on specific persons, there is likely a need for additional approvals under national law. However, an OSINT tool observing a specific environment in general, e.g. a specific website with known illegal activity, but without focusing on any specific individuals, will tend to be permissible absent specific authorization. In such cases in particular, the question must be raised what the privacy impact is of such tools. This is in the following section on the legal implications of OSINT.

The second element relates to whether the activity **involves some type of direct engagement of the person(s) of interest**. Typically, OSINT in Law Enforcement is passive, and avoids any type of communication with or engagement of the individuals who are subject to the information gathering, but mere observation of the information that is available. OSINT for intelligence may not even have any type of person of interest or target in mind.

Any type of active approach however, engaging with targets or subjects in some way or another, e.g. adding them as a friend, liking or commenting on their posts, messaging them, etc. in the environment of the open sources that are considered, is likely to trigger special investigative methods, such as infiltration, which require special authorization pursuant to national law. It is outside of the scope of this white paper to focus on the details of the special investigative methods under national law relevant to CSAE investigations, including for example the rules on entrapment and the use of real and AI-generated CSAE material to build trust with CSAE offenders on the darknet. Within the context of this discussion, the focus will be on passive forms of OSINT, where the purpose of the OSINT tool is to merely observe.

Types of OSINT and legal implications

Interference with fundamental rights

The mere fact that information processed by OSINT tools is publicly accessible online does not mean that there are no privacy implications.[15] Rather, OSINT must still comply, like any other investigative technique, with fundamental right concerns, namely a potential interference with, in particular the following rights:

- Article 8 ECHR: right to private and family life, home and correspondence;
- Article 7 EU Charter: right to privacy;
- Article 8 EU Charter: right to the protection of personal data.

Interference with these rights are permissible, but only if based in law, in order pursue a limited number of legitimate aims, and only in as far as this is necessary in a democratic society, i.e. limited to what is needed. In other words, the criteria to be met, as applied also consistently in the case law of the CJEU and the European Court of Human rights are the following:

1. **Lawfulness**: The interference must be **prescribed by law** and the law must be sufficiently **clear and precise rules** which determine the scope and the application of the intended measure and must impose minimum safeguards;[16]
2. **Legitimacy**: The interference must pursue a **legitimate aim,** pursuing an objective of general interest recognized by the Union or the need to protect the rights and freedoms of others. Legitimate aims include preventing crime and disorder, protecting public safety, national security;
3. **Proportionality**: The interference must be **proportionate** in relation to the goal pursued, meaning that the interference in fact **genuinely meets the legitimate objectives** that justify the interference, and that the **same result cannot be achieved by lesser means.**

[15] See for a starting point on the case law of the ECtHR on this point: Milaj-Weishaar, J., & Mifsud Bonnici, J. (2022). Stitching lacunas in open source intelligence – Using Ethics to fill up legal gaps. Illyrius - International Scientific Review , 18(1), 47-57, pages 51-52. For more details, please refer to the ECtHR's case law guide on Article 8 (https://www.echr.coe.int/documents/d/echr/guide_art_8_eng) and on data protection (https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG). It is clear from these sources that OSINT has privacy implications, even if the source is public, and even if the data was made public by the data subject themselves.

[16] This principle can be observed clearly in the case law of the European Court of Human Rights in ECHtR, H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, para. 62-63; Rotaru v. Romania, para. 57-59, and S. and Marper v. the United Kingdom, para. 99.

It should be noted here that in both the CJEU's data retention case law,[17] as well as case law related to the Passenger Name Records (PNR) Directive,[18] the CJEU has in principle accepted serious interferences with privacy and related fundamental rights for the purposes of law enforcement,[19] however always focusing on the specific balance struck in any given case, including the necessity of a given interference, the aims pursued (with the prevention of and fight against terrorism and serious crime, the latter typically including CSAE, being able to justify stronger interferences), how targeted the interference is in relation to the objectives pursued, the duration of the interference and taking into account the safeguards put in place.

Note that the use of OSINT in investigations may also impact other fundamental rights, in particular procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defense and the presumption of innocence. For this reason, any OSINT use should also be documented, follow appropriate standard operating procedures, and, when used for investigations, comply with applicable evidential standards and minimum requirements.

The potential impact on fundamental rights, in particular in this case privacy, is why special investigative techniques provide for both requirements and safeguards in relation to their use, which is typically very targeted , limited in duration, and subject to judicial authorization or authorization by an independent competent authority (with judicial review).

For OSINT however, typically, the only legal ground available in applicable national law are general powers for police to "detect crimes and gather evidence " and to perform their task of "upholding law and order ". In essence, these general legal bases will allow police forces to perform their tasks without the need to obtain a specific authorization from a judicial or other competent body. Use of OSINT can be part of these tasks, but since this is a broad and general legal base, the amount of interference with fundamental rights must be limited.

[17] See for example: CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238; CJEU, Joined Cases C-203/15 and C-698/15, *Tele2*, ECLI:EU:C:2016:970; CJEU, Case C-623/17, *Privacy International*, ECLI:EU:C:2020:790; CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, ECLI:EU:C:2020:791; CJEU, Joined Cases C-793/19 and C-794/19, *SpaceNet*, ECLI:EU:C:2022:702; CJEU, Case C-746/18, *Prokatuur,* ECLI:EU:C:2021:152; CJEU, Case C-140/20, *Commissioner of An Garda Síochána*, ECLI:EU:C:2022:258.

[18] CJEU, Case C-817/19, Ligue des droits humains ASBL v Conseil des ministers, ECLI:EU:C:2022:491.

[19] In the PNR case for example, the CJEU accepted the continuous, untargeted and systematic collection, including an automated assessment of the personal data of anyone using air transport services, without consideration of prior indications of unlawful activity, as long as there was a terrorist threat which is shown to be genuine and present or foreseeable (CJEU, Case C-817/19, Ligue des droits humains ASBL v Conseil des ministers, ECLI:EU:C:2022:491, para. 171 and following). In the data retention cases, the CJEU has also consistently accepted the indiscriminate retention of traffic and location data in specific high risk zones for example; there as well regular review and a limited duration is necessary, but this can be extended, which has lead in practice to several Member States maintaining such indiscriminate zones that cover most of the territory (see for a thorough analysis: Adam Juszczak, Elisa Sason, "Recalibrating Data Retention in the EU - The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?", eucrim 4/2021, pp. 238-266, available in open access at https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/).

Note that OSINT may at times also be used in use cases where special investigative power apply. However such powers, e.g. wiretap/interception, systematic observation, infiltration, access to non-content communications data, are usually by their nature under applicable national law aimed at a very targeted collection of data, related to specific, identified individual or set of individuals, whereas many OSINT applications, at least in terms of collection of data, often cover a broader scope of individuals and data in order to produce useful results. Hence, the fact that permissions for special investigative powers apply does not necessarily mean that the scope of OSINT use is changed significantly, and OSINT must still be assessed largely on the basis of general police powers, meaning that, absent a specific legislative framework, the interference must be limited to an acceptable level. Another element to consider is that, while in this discussion OSINT is regarded as separate tool compare to existing special investigative powers, certain OSINT uses meant to be covered under general powers may afterwards be construed as exercising special investigatory powers. LEAs should therefore always verify whether this could be the case, as such use cases would then require prior authorization from a competent body or judge.

In general, when considering whether the use of OSINT, LEAs should ask the following questions:

- Are the sources intended to be used really open?
- Is the intended OSINT use meant to support one of the limited legitimate aims, e.g. national security, public safety, for the prevention of disorder or crime?
- Does the OSINT use fit specifically within the general national legal basis available (based on that specific wording and taking into account that any interference must have a legal basis that is sufficiently clear and precise, meaning the interference can be expected on the basis of the legal text)?
- Is the OSINT use necessary to reach this goal and are there no less invasive alternatives or set-ups available that might also reach this goal?
- Does the OSINT use actually reach to this goal (is it effective)?

In essence **this means there must be a balancing between the right to privacy and the importance of the goals of policing set out in the national legislation**. Normally it is for the legislator to make the balancing exercise with regards to restrictions of fundamental rights. However, since general national police powers are often worded in a broad way, effectively LEAs have to consider whether or not an intended OSINT use is permissible or not, taking into account not only the importance of the goal and the necessity of the intended use of OSINT for those goals, but also the **extent of the privacy impact** and the presence or absence of **mitigating measures** that might diminish the privacy impact.

Note that in most national laws, there are competent bodies in charge of prosecution that may order police to take certain actions necessary for an investigation and OSINT uses may be sanctioned by them as well, helping police feel more confident in the use of certain OSINT applications or in setting up a given OSINT use case. Such authorization however only moves the responsibility, but does not address the core of the issue, namely that the use of OSINT

must be assessed for its privacy impact and whether this is permissible in the light of fundamental rights.

After all, **not all OSINT uses are the same in terms of impact.** In one of its most simple forms, OSINT can consist of checking the social media profile of a suspect or performing a quick search on a clear web search engine, which clearly has a different impact altogether compared to, for example, a hypothetical OSINT tool that indiscriminately scrapes information from the whole of the internet, systematically saves this in a database and runs various AI applications on this data to help police perform diverse (automated) operations to help them with whatever input they may need: intelligence, monitoring and surveillance, or for investigations. These examples are extremes, which serve to illustrate that OSINT tools have a different level of potential interference with the fundamental right to privacy. In the former example, the interference is virtually zero, as the OSINT tool does not add any further privacy interference to the situation of the suspect (who is, already undergoing an investigation that interferes with its privacy). In the latter example, the OSINT tool is indiscriminately collecting lots of information, on a high number of people most of whom have nothing to do with the use case at hand, from various different sources, almost certainly including sensitive information, and for a myriad of vaguely defined purposes. The latter example therefore illustrates an extremely high level of interference with privacy.

Most OSINT tools are based somewhere in between these extremes, and this is where the concepts of **"high" and "low" interference OSINT tools** and use cases become relevant. Given that OSINT most usually is based on general policing powers, interference should normally be on the low end of the spectrum, so "low" interference OSINT tools are generally permissible. High interference is more difficult to base on such general powers, given the high potential interference with fundamental rights and the complete absence of requirements, limitations and safeguards in the law. This is a challenge, as high(er) interference OSINT applications and use cases may at times be necessary for LEAs to perform their tasks, with the means available to them. Mitigation measures however may help reduce the potential impact.

High vs. low interference

In order to determine the interference level, it is important to consider the **intentionality** (i.e. the purposeful and deliberate targeting of a certain specific scope) of **both the data collection and the use of the OSINT tool** as important elements in the assessment. Generally, the more targeted the collection of data and the use of the OSINT tool, the smaller the potential negative impact on fundamental rights will be presented by its use.

Elements to consider the impact level of the interference with fundamental rights include:

- The **relevance and necessity of the data collection** (indiscriminate collection of data vs. collection based on pre-defined parameters clearly linked to the goals pursued, e.g. specific offender websites);

- The **scope of the data collection**: amount of data, sources (even when arguments exist for broad data collection, a large scope may present stronger privacy interference);
- The (expected) presence of **sensitive data (special categories)** in the data to be collected and the necessity of collecting those elements;
- Whether OSINT data collected is meant to be **linked with other data** (enriching data sets);
- The **degree of automation and targeted nature of the use of the tool**: targeted manual searches based on reasonable suspicions or prior intel vs. automated searches (which may lead to "fishing expeditions" and arguments of mass surveillance);
- The **duration** of the use of the tool in relation to particular environments and especially in relation to specific targets (different privacy impact when the tools is used to collect data on certain websites vs. observe specific persons);
- Any **measures used to limit interference** (e.g. scrubbing).

Based on these elements, LEAs must make an assessment of whether the use of a particular OSINT application is permissible or not.

An important note has to be made here regarding the automated nature of the data collection and analysis by OSINT tools, as compared to the question of the systematic and automated nature of their use to perform searches. Most OSINT tools, by their nature, require automated data collection to function. Even simple OSINT "tools", such as using a search engine requires the automated indexing of websites to be functional. To an extent, to remain readily available, such automated collection must also be continuous, i.e. systematic. The same is true for more complex OSINT tools, made for specific purposes, that require the scraping of publicly available data as input. For them to be functional, data collection and processing must be automated. For them to be available to LEAs, practically speaking, this process must be continuous and automated to ensure the tools are ready to be used when necessary.

It is therefore not the automated nature of the data collection in itself that is the most important, but rather the scope of the data collection and the circumstances surrounding the use of the tool to perform searches and whether the scope of the collection (e.g. only known offender environments) and use (e.g. specific manual searches vs. automated systematic searchers) is sufficiently targeted.

The Clearview AI example can serve to illustrate what happens if data collection is not targeted. Clearview.AI is a company that has a database of 30 billion facial images from global public web sources, obtained through web scraping. Its AI-powered search service creates profiles from biometric data extracted from these images, enriched with additional information like tags, geolocation, and source web pages, in particular (but not exclusively) targeting Law

Enforcement users to help them with facial recognition for investigative and intelligence purposes.[20] This is a good example of "OSINT data collection "gone wrong", with Clearview AI scraping the internet indiscriminately, interfering with privacy and moreover, in violation of several data protection principles such as:

- A lack of lawfulness, fairness, and transparency in processing, given the lack of information to data subjects, and a completely disproportionate intrusion into privacy compared to Clearview AI's commercial interests;
- Processing for a different purpose than the original publication of personal data, without strong arguments for compatible use, and without obtaining additional consent from data subjects;
- Breach of the data minimization and storage principles through indiscriminate collection and permanent storage;
- Processing of special categories of personal data without proper justification.

Moreover, the use of facial recognition as a technique in itself raises serious concerns about fundamental rights and questions regarding the legal basis in national law for LEAs to use such software. In addition, LEAs must question whether they can use a third party service provider (moreover based outside the EEA) under national law in general, and in particular given that Clearview AI collects and processes police data as part of their service. Hence LEAs lose control over police data regarding a very sensitive type of processing. As a consequence, many data protection authorities took action.[21] In addition to the massive data collection and the reliance on a private sector third party by LEAs using the tool, there were issues regarding the lack of a legal basis under the LED to process data and in particular special categories like biometric data, in this manner. In the near future, the AI act will prohibit this type of extreme OSINT use (see further).

In the Clearview AI example, LEAs should conclude that the data collection is very clearly not targeted enough, given its extremely broad and indiscriminate nature. Such a finding should lead to the conclusion that the tool should not be considered for use, even before considering the nature of running searches on the tool, and whether this meets the criterion of intentionality, i.e. whether the tool allowed to perform searches in a sufficiently targeted manner. **In that sense, OSINT tool use must be considered as a two-step test: both the data collection and the use of the tool should be sufficiently targeted given the purpose(s) pursued**. If either step clearly fails, the interference level of the tool is too high to be used in compliance with fundamental rights.

[20] See https://www.clearview.ai/.
[21] For an overview, please see https://edri.org/our-work/we-need-to-talk-about-clearview-ai/.

Legality of OSINT use by LEAs: policy statement

The preceding section has described the elements to determine the level of fundamental rights interference that an OSINT tool presents. Interference exists on a spectrum, and the terms of "low interference" and "high interference" are used merely to categorize OSINT tools used for CSAE investigations on the dark web to some extent, according to their potential impact on fundamental rights.

As stated before, the fact that data is freely available does not mean that it is not protected, but simply that it is easily available to law enforcement practically speaking and does not come from other official sources or is the result of using specific powers of investigation (e.g. seizing of a device, seizing of data, orders to transmit data, cover investigations, infiltration, wiretap/interception etc.) which provides for a clear legal framework of obtaining and using such information in compliance with fundamental rights. OSINT tools however, do not benefit from such a clear legal framework, but are rather based on general policing powers. The questionnaire submitted to LEAs in the context of ARICA very clearly confirmed this reality.

Under the current legal framework then, only low interference OSINT is really clearly permissible under most national laws given the fact that the use of LEAs of such technologies must be based on a broad and often vague general power of policing, which does not provide for any safeguards, such as the need for authorization by an independent body or judicial authorization or review of such measures. Consequently, in accordance with the arguments presented above, high interference uses based on such powers are legally problematic in terms of fundamental rights concerns and may lead to inadmissible evidence.

Interestingly, in the questionnaire the ARICA project sent out to a selection of LEAs, all of the respondents indicated that the use of high interference OSINT tools were permissible in their jurisdiction, with the vast majority indicating that such tools could be used for both investigations (i.e. under the general power for police to investigate crime) and for intelligence (i.e. under the general power for police to keep public order and monitor the public space to that extent). Those results may of course be based on a misunderstanding of the meaning of high vs. low interference (which are in themselves vague concepts), but since some explanations were provided to this extent in the questionnaire, it is nonetheless a relevant finding. This result may be an indication that high interference OSINT is used in practice, or at least that many LEAs may consider it permissible and necessary to use such tools in practice. The questionnaire did not address whether or not the respondents used high interference OSINT tools in their own practice but rather whether they thought such tools to be permissible under their national legal framework.

Another interesting finding from the questionnaire is that LEAs had quite different views on what constitutes high or low interference OSINT. This is a logical consequence of having no clear legal framework for the use of open sources by Law Enforcement. Various actors, even within the same country and working on the basis of the same (national) legal framework will make divergent assessments of what is permissible and what is not. This creates a lack of legal certainty, which may easily lead to divergent protections within the EU and even within Member States or regions of the same Member State. Inherently, legal rules and in particular

a legal basis for interference with fundamental rights should be sufficiently clear and precise, and general policing powers will struggle to meet that criterion in relation to OSINT tools, which covers a vast array of different tools and applications, with strongly varying levels of impact on and (potential) interference with fundamental rights. This will likely lead to the following two outcomes with regards to CSAE investigations on the dark web, neither of which are desirable:

- Certain LEAs may use certain OSINT tools in breach of fundamental rights guarantees; and
- Certain LEAs may avoid the use of certain OSINT tools for fear of such breach, leaving valuable options on the table for intelligence and/or investigations, since OSINT tools are often very capable and cost-effective.

In addition, the lack of a clear legal framework makes it difficult for tool providers to know the legal requirements for the tools they are developing.

An appropriate legal framework would consider as main elements the nature of the data collection, which must be targeted and proportionate to the purpose pursued, and the nature of the use of such tools. There are as well, searches performed with OSINT must be targeted and justified, so that neither data collection nor use leads to mass surveillance and fishing expeditions on the open internet. However, at times, high(er) interference may be permitted, provided that there are safeguards in the law, including but not limited to judicial authorization or authorization by an independent competent authority (with judicial review).

Parallels can be drawn to the on-going data retention debate in the EU.[22] The debate concerns the extent to which electronic communications service providers should be obliged to retain non-content data (e.g. location, traffic) data from mobile devices for the purposes of potential law enforcement use for intelligence and investigations. In this context as well, a balance must be struck between privacy interference and avoiding mass surveillance on the on hand, while, on the other hand, being realistic in the needs of internal security practitioners and LEAs in particular in order for these actors to remain able to perform their tasks in society. In this context as well, since there is no EU level framework since the invalidation of the data retention Directive, Member States have maintained very different approaches (some of which, arguably, are at odds with the CJEU case law on the topic).[23] Such a situation leads to different levels of protection of fundamental rights within the EU, which is at odds with EU values and therefore hard to justify and maintain. This is true for OSINT as well, which moreover concerns

[22] See on this in particular the EC's non-paper, i.e. a document prepared by staff but no approved as an official position), available at https://cdn.netzpolitik.org/wp-upload/2021/07/wk07294.en211.pdf . This is also covered in the work of the High-Level Expert Group on access to data for effective law enforcement, see in particular the scoping paper, available at https://data.consilium.europa.eu/doc/document/ST-8281-2023-INIT/en/pdf.

[23] See for example the 'Study on the retention of electronic communications non-content data for law enforcement purposes (HOME/2016/FW/LECO/0001)', available at https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1. For an overview of the CJEU case law on the topic, see: Adam Juszczak, Elisa Sason, "Recalibrating Data Retention in the EU - The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?", eucrim 4/2021, pp. 238-266, available in open access at https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu.

open sources across borders (or sometimes not localized). **It would therefore be desirable for the Commission to take the lead on further exploring this topic and the potential routes to support clearer regulation on this topic (whether specific to CSAE or more generalized), within the limits set by the treaties, coherent across Member States, which strikes an appropriate balance between law enforcement needs and respect for fundamental rights**.

Synergies may be possible with, or inspiration may be drawn from the work done in the High-Level Group on access to data for effective law enforcement,[24] which deals with the challenge for LEAs to get appropriate access to data in transit, data at rest on a user's device and data at rest in a provider's system. While in OSINT application the access to the open source data is not technically a challenge, some of the legal considerations and challenges overlap, in particular when talking about dark web CSAE investigations, where access to data issues and challenges related to anonymization are very real, and are a part of the reason why OSINT tools, potentially sometimes including high interference OSINT applications; are a necessary part of the toolbox so LEAs can continue to maintain effective law enforcement across the Union, safeguarding public security and preventing, detecting, investigating and prosecuting crime effectively, thereby meeting legitimate expectations of society at large, and victims in particular.

[24] For more information, see https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en.

ARICA

CHALLENGE 2: the use of AI during investigations in the dark web

The second challenge related to the use of OSINT tools on the dark web is the use of Artificial Intelligence. More complex use cases and tools for OSINT utilize web scrapers to collect data and AI technology to process such data and visualize outcome. Many different types of applications exist.

Allowed and forbidden applications of AI by Law Enforcement under the AI Act

Using AI in a Law Enforcement context, including in OSINT applications, has the potential to interfere with fundamental rights of individuals, and hence the Artificial Intelligence Act (further referred to as the AI act or AIA),[25] which adopts a risk-based approach to AI systems based on their implications for safety, health and fundamental rights, regulates several Law Enforcement uses of AI that have strong potential to interfere with fundamental rights, namely:

- **Forbidden** are (Article 5 of the AIA):
    - AI systems that **create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage**, which is to be understood in the light of the Clearview AI scandal. Clearview AI used open source images from the whole internet to create an enormous database, and scraped this completely indiscriminately, which led to enforcement action by several Data Protection Authorities;
    - AI systems intended to **individually categorize natural persons based on their biometric data** to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. There is however an exception for LE (see further under high-risk);
    - AI systems that **make risk assessments** about natural persons**, assessing or predicting the predict the risk** for that person **to commit a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics.**

      Note that the prohibition does not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity. The reasoning behind this is that, in line with the presumption of innocence, natural persons in the EU should always be judged on their actual behavior “to assess the risk of them offending or for predicting the occurrence of an actual or potential criminal offence”, not solely AI-predicated behavior,

[25] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

"without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof". However, AI systems that do not solely use such techniques are permissible, but present a high-risk use case (see further).

- AI systems that use **'real-time' remote biometric identification systems, in publicly accessible spaces for the purpose of law enforcement**. The most common example of this is live facial recognition software. There are 3 exceptions to this rule, namely if strictly necessary for:
  - "The **targeted search** for specific **victims** of abduction, trafficking in human beings and **sexual exploitation of human beings** [which includes CSAE] as well as search for missing persons";
  - "The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack"; and
  - "The **localization or identification of a person suspected of having committed a criminal offence**, for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty" for certain serious offences listed in the AIA **(including CSAE and CSAE material**), where the Member State concerned punishes this offence by a custodial sentence or a detention order for a maximum period of at least four years.

The above exceptions will still present high-risk and hence must be subject to the requirements of high-risk systems.

The AIA clarifies that these systems can in any case only be used to confirm the specifically targeted individual's identity and must perform a type of balancing act between:

- ⇨ "The nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system"; and
- ⇨ "The consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences […]".

Moreover, **the exceptions only apply to the extent that Members States decide to partially or fully authorize them to the extent allowed by the AIA**. This means that they can decide to only grant some of the three exceptions and not others, and/or that they can limit the list of offences referred to in the third exception. Hence, certain Member States could decide to not include CSAE and CSAE material offences in the third exception, or could simply not allow for

the exceptions (in particular 1 and 3 for the setting of CSAE investigations) to start with.

If Member States do allow the exceptions, they can only do so subject to the requirement of prior authorization granted by a judicial authority or an independent administrative authority, whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request (with some specific exceptions for situations of urgency). Member State must provide for detailed rules regarding the request, issuance and exercise of, as well as supervision and reporting relating to such authorizations. This must include "necessary and proportionate safeguards and conditions in relation to the use [of such systems] […] "in particular as regards the temporal, geographic and personal limitations."

Note however that the exceptions concern **publicly accessible spaces,** which the AIA defines as "any publicly or privately owned **physical place** accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions". This leaves some leeway for online spaces, even though the most likely biometric AI applications in that setting would not be "live" but "post", i.e. on images, video etc. that has already been recorded.

- **Allowed,** but only **under certain compliance conditions** of the AIA, **are** the following **high-risk use cases by Law Enforcement** (Article 6 and Annex III of the AIA):
    - **Real-time' remote biometric identification systems**, in as far as allowed by Member State Law, and under the specific stringent conditions set by that law. In addition however, such use is subject to the rules for high-risk AI systems as well, because remote biometric identification systems are generally a high-risk use (see Annex III, point 1, a) AIA) unless the system is solely "intended to be used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be", which does not apply in real-time use cases;
    - **Post remote biometric identification systems**: use by LEAs of post remote systems (including online or based on online only collected data sets) is generally a high risk use, again subject to the limited exception mentioned above.

      The AIA notes that "considering the intrusive nature of post remote biometric identification systems, the use of post remote biometric identification systems shall be subject to safeguards. Post biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus **targeted**, in terms of the **individuals** to be identified, the **location, temporal scope** and based on a **closed dataset** of **legally acquired** video footage." The use of such systems by LEAs must not lead to indiscriminate

surveillance or to circumvent the prohibition and strictly defined exceptions for real-time remote biometric identification.

In addition the AIA defines several requirements for LEAs using ("deploying") **post remote biometric identification systems**:

- ⇨ LEAs must perform **a fundamental rights impact assessment prior to first use of the system** in accordance with the minimum requirements set by the AIA;
- ⇨ Any **specific use** of/ use case for the system is **subject to an authorization**, prior to the use, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, unless when the system is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. If the authorization is not granted the use must be stopped with immediate effect and data used must be deleted;
- ⇨ Each use must in any case be **strictly limited to what is necessary for the investigation of a specific criminal offence (i.e. be targeted).** It cannot be used "in an untargeted way, without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence or the search for a specific missing person";
- ⇨ The system's outputs **cannot be the sole source for LEAs to take a decision** that produces an adverse legal effect on a person, and regardless of the purposes, each use of such systems shall be **documented** in the relevant **police file.** In addition, LEAs deploying such systems must prepare **annual reports** on their use of post-remote biometric identification systems. Both the police file and the report is to be made available to the market surveillance authority under the AIA and the national data protection authorities, however excluding the disclosure of LEA's sensitive operational data.

- o Systems intended to be used to **label or filter lawfully acquired biometric datasets**, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement. The AIA makes an exception to the prohibition for LE purposes, but this also remains a high-risk category;
- o Systems intended to be used by or on behalf of LEAs or by Union institutions, agencies, offices or bodies in support of LEAs or on their behalf, **to assess the risk** of a natural person **to become a victim** of criminal offences;
- o Systems intended to be used by or on behalf of LEAs or by Union institutions, agencies, offices or bodies in support of LEAs, to act **as polygraphs and similar tools**;

- Systems intended to be used by or on behalf of LEAs or by Union institutions, agencies, offices or bodies in support of LEAs, **to evaluate the reliability of evidence** in the course of investigation or prosecution of criminal offences;
- Systems intended to be used by or on behalf of LEAs or by Union institutions, agencies, offices or bodies in support of LEAs, **for assessing the risk** of a natural person **of offending or re-offending, not based solely on profiling** of natural persons (with reference to the meaning of this term under Article 3(4) of the Law Enforcement Directive)**, or based on assessing personality traits and characteristics or past criminal behavior of natural persons or groups**;
- Systems intended to be used by or on behalf of LEAs or by Union institutions, agencies, offices or bodies in support of LEAs, **for profiling of natural persons in the course of detection, investigation or prosecution of criminal offences.**

Other use case of AI that are not high risk or prohibited are in principle allowed and not regulated by the AI Act (with the exception of some specific requirements for AI systems that directly interact with natural persons e.g. deepfakes and requirements for General Purpose AI Systems).

Moreover, there are some limited exceptions to systems that are normally considered high risk (Article 6(3) AIA). This may be the case when the AI system is intended to:

- "Perform a narrow procedural task";
- "Improve the result of a previously completed human activity";
- "Detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review";
- "Perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III" of the AIA, which include the above mentioned high-risk Law Enforcement uses.

However, AI systems that perform profiling of natural persons cannot benefit from this exception, which significantly limits its use in a law enforcement context. In any case it is for the provider/developer of the system to make the argument and document why a system they have developed is not high-risk. LEAs who are only using/deploying the system must in principle not make this assessment themselves.

Notably however, these criteria may change in time, as the AIA empowers the Commission to adopt delegated acts to amend these criteria. Moreover, Article 6 of the AIA also requires the Commission to provide a "comprehensive list of practical examples of high risk and non-high risk use cases on AI systems", at the latest 18 months after the entry into force of the AIA (so no later than 2 February 2026, concretely).

ARICA

OSINT tools and the AI Act

There are many complex OSINT tools that may be envisioned that could qualify as high-risk AI systems under the AIA, in particular in relation to evaluation of the reliability of evidence and risk assessments of victimization and (re-) offending through profiling and related techniques, or other uses of profiling for the purposes of detection, investigation or prosecution of criminal offences. For all these uses, open source information that LEAs did not yet possess but can be found online could feature into AI applications, either purely based on OSINT or to enrich existing data. In addition, also biometric identification systems may be based on OSINT and on openly available sources.

The AIA explains the reasoning for why many Law Enforcement uses of AI (potentially including OSINT applications) are considered high-risk as follows in recital 59:

"Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterized by a ***significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights*** *guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a* ***discriminatory or otherwise incorrect or unjust manner****. Furthermore, the exercise of important procedural fundamental rights, such as the* ***right to an effective remedy and to a fair trial as well as the right of defense and the presumption of innocence****, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as* ***high-risk,*** *insofar as their use is permitted under relevant Union and national law, a number of AI systems intended to be used in the law enforcement context* ***where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress****".*

It is clear that expectations are high for LE use of AI. Hence, LEAs developing or deploying (i.e. using) such systems, or considering their use, should become familiar with the obligations the AIA will impose upon them in the future. Given the important role of LE in society, LEAs may even reasonably be assumed to take certain accountability measures for the use of AI even outside of the high-risk situations directly regulated by the AIA (more details on this below).

The main provisions concerning high-risk systems appliable to Law Enforcement will apply as of 24 months after the after the entry into force of the AIA. Prohibited uses will already become applicable 6 months after the entry into force. The AI act was published on 12 July 2024 and consequently entered into force on 1 August 2024 (20 days after publication). Hence, the main rules will apply from 2 August 2026, but chapters I and II, including prohibited uses will already apply as of 2 February 2025.

For existing OSINT tools (i.e. OSINT tools developed before the AIA becomes applicable) to be used by LEAs, which qualify as a high-risk AI system, the AIA foresees that both providers and deployers of those systems have six years after the entry into force (i.e. 4 years after the entry into application) of the AIA to comply with their new obligations. In practice this means 2 August 2030. However, if OSINT tools are subject to significant changes in their design after the AIA applies, i.e. after 2 August 2026, then the AIA will apply to the changed tool. Significant updates of existing tools and software may qualify as such a change, if it impacts the compliance aspects of the tool/software.

Note that the AIA does not apply to uses of AI that are solely for research, so for LEAs testing tools in a research setting, e.g. as part of a research project funded by the Eu or on the national level, there are no AIA obligations.

Obligations in relation to high-risk AI applications in OSINT

Different roles exist under the AIA. The two most relevant roles for LEAs are the following:

- **Providers** are the most regulated stakeholders, because of the decisive role they have in the design and development of an AI system. Providers are the natural or legal persons, public authority, agency or other body that ***develops or has developed*** an AI system and *places them on the market* or ***puts them into service*** under their own name or trademark, whether for payment or free of charge;
- **Deployers** are the natural or legal persons, public authority, agency or other body **using** an AI system under their authority, except when the AI system is used in the course of a non-professional activity.

Based on the role a LEA performs in relation to an AI-driven OSINT application, different obligations will apply. In most circumstances, LEAs will obtain AI-driven OSINT tools from a third party provider, which may be a commercial provider or solutions provided to LEAs for free, e.g. through Europol's Innovation lab, EACTDA, etc. **Hence, in most cases LEAs will act as a deployer of the AI system.** Nonetheless, it is important to understand some of the main obligations of the providers as well, before focusing on the deployer obligations as the most likely set of obligations for LEAs. This is in particular important because roles regarding the AI system may in limited circumstances be subject to change, namely a deployer may become a provider (with the more extensive obligations applying) when:

Notably, roles in relation to high risk AI systems may change in practice. The AIA foresees certain situations in which any distributor, importer, deployer or other third-party may become requalified as a provider of a high risk AI system, and thus become subject to the more extensive provider obligations of the AIA, namely when:

- They put their **name** or trademark on a high-risk AI system that has already been placed on the market or put into service;
- They make a **substantial modification** to a high-risk AI system that has already been placed on the market or put into service in a way that is remains high-risk;

- They **modify the intended purpose** of an AI system, including a general purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such manner that the AI system becomes a high risk AI system.

LEAs should take care not to accidentally cross these lines. In particular the modification of the purpose of a general purpose AI systems for Law Enforcement purposes could present such risk.

Obligations of providers of AI-driven OSINT tools under the AI Act

Providers have the most extensive obligations under the AIA to assess, manage and mitigate the risk of AI, namely they must provide for:

- The establishment of a **risk management system** that deals in particular with the known and the reasonably foreseeable risks related to the use of the system, as well as reasonably foreseeable misuse and proposes risk management and mitigation measures and must include a feedback loop based on the input from the market and deployers (who may identify additional risks);
- The implementation of **appropriate data management and data governance practices**, namely in relation to
    - The relevant design choices made;
    - The data collection processes and origin of data, and for personal data, the original purpose of the data collection;
    - The relevant data preparation processing operations (e.g., annotation, labelling, cleaning, etc.);
    - The formulation of assumptions;
    - An assessment of the availability, quantity, and suitability of the needed datasets;
    - An examination in view of possible biases that are likely to negatively affect human health, safety, and fundamental rights, or lead to discrimination;
    - Appropriate measures to identify and prevent such biases, using special categories of data in as far as strictly needed for bias detection and correction subject to specific additional safeguards;
    - The identification of relevant data gaps or shortcomings that prevent compliance with the AIA, and measures to address those issues;
    - Ensuring data quality standards: data must be relevant, sufficiently representative, free of error and complete in view of the intended purpose (to the best extent possible), and have appropriate statistical properties. The datasets must also take into account the features that are specific to the environment, i.e. the

geographical, contextual, behavioural, or functional setting within which the AI system is intended to be used.

- The **creation and maintenance of technical documentation** on the high-risk AI system;
- The **incorporation of automatic record-keeping/logging capabilities** within the high-risk AI system;
- High-risk AI systems to be designed and developed in a way that is **sufficiently transparent for deployers to interpret it correctly**, providing information to this extent (i.e., to enable understanding and provide clear instructions of use);
- The **effective possibility for humans to oversee** the high-risk AI system while it is being used;
- High-risk AI systems to be designed and developed in a way that they achieve **an appropriate level of accuracy, robustness, and cybersecurity and perform consistently in those respects** throughout their lifecycle.

Whereas the abovementioned obligations generally concern the development and design of the high-risk AI system, there are **additional obligations aimed at providers demonstrating compliance with the AIA**. These obligations notably include the following actions:

- Providers must identify the high-risk AI system, notably by putting their name or trademark on them;
- Providers must ensure that the high-risk AI system undergoes a conformity assessment, draw up an EU declaration of conformity and affix the CE marking to the AIS to indicate compliance with the AIA;
- Providers must maintain proper documentation for at least 10 years after the system was placed on the market or put into service;
- Providers must in place a quality management system, from which several additional requirements stem;
- Providers must keep the logs that are automatically generated by the system;
- Provider must register the high-risk AI system in a specific EU database set up for this purpose;
- Providers must create a post-market monitoring system in a manner that is proportional to the nature and risk of the AI used, to help them evaluate the continuous compliance of AI systems. As an example such a system would ensure that any newly identified risks by reported by or identified on the basis of reports of deployers are made part of the risk management system;
- Providers must notify the competent authority if their high-risk AI system presents a risk to the safety, health, or fundamental rights of humans, and take the necessary corrective actions;

- Providers must report serious incidents to the market surveillance authorities set up under the AIA;
- Providers must cooperate with the competent authorities and upon request demonstrate the conformity of the high-risk AI system with the AIA;
- Providers located outside of the Union must appoint an authorized representative which is established in the Union.

Specific exceptions exist for sensitive operational data of law enforcement where the provider is in Law Enforcement.

One of the main outcomes of the provider obligations for high-risk AI systems is that **a conformity check is performed, an EU declaration of conformity drawn up and CE marking** is affixed before the system is put on the market, so that anyone, but in particular deployers can easily be assured that the AI system complies with the AI act. Strong sanctions help ensure that providers will not take this obligation lightly, although Member States retain the right to decide on the types of sanctions applicable to public bodies, including LEAs that would be classified as a provider.

Importantly, the conformity assessment must not always be carried out by a third party, but is in most instances based on internal control of the provider. The AIA defines in which cases third party assessment is needed. In relation to the regulated LE uses, only biometrics (including remote biometric identification systems) are currently subject the third party assessment (unless common standards exist and the provider has followed them, then they have the choice for third party assessment or internal control). This may change, as the AIA allows the European Commission to adopt delegated acts in the future to extend the types of high-risk AI systems that must be subjected to third party assessments, taking into account that those third party capacities must also be developed. For now however, most high-risk AI systems will be assessed internally by the provider. While internal assessment is not necessarily less stringent than a third party assessment, it is important for LEAs deploying a high-risk AI system to consider this element as part of their own accountability exercise and when implementing their deployer obligations.

Other provider obligations that should be noted are those for providers of AI systems that directly interact with natural persons (Title IV of the AIA, with exceptions for the LE context) and for providers of certain General Purpose AI models, where transparency obligations apply.

This section serves to illustrate the extent to which providers are regulated under the AIA. Luckily, most LEAs will only act as deployers and therefore will not be faced with these extensive obligations. Nonetheless, LEAs must take care not to end up in as situation where they might be requalified as a provider (see above). Moreover, LEAs should take care to understand the provider role, also when they purely act as a deployer. This will help them ask the right questions and provide appropriate scrutiny toward the providers, whether this is a commercial third party, or a partner in the LE sphere (e.g. when obtaining tools through Europol's innovation lab, EACTDA, etc.).

Obligations of deployers of AI-driven OSINT tools under the AI Act

In the scenarios where the AIA applies to LEAs using OSINT tools, they are most likely to use a system/tool developed by a third party, and are therefore to be qualified as a deployer. **Notably, deployers have their own obligations under the AIA to be aware of, and these apply to LEAs as well.**

Most deployer obligations related to high-risk AI systems, namely deployers of such systems, including **LEAs using high-risk law enforcement AI systems must**, for example:

- Take **appropriate technical and organisational measures** to ensure they **use such systems in accordance with the instructions** of use accompanying the systems;
- Assign **human oversight** to natural persons who have the **necessary competence, training and authority**, as well as the necessary support; in particular when the deployer exercises control over the high-risk system;
- Ensure, to the extent that they can exercise control over the input data, that **the input data used is relevant and sufficiently representative** in view of the intended purpose of the high-risk AI system;
- Monitor the operation of the high-risk AI system on the basis of the instructions of use and when relevant, inform providers of issues, as well as others (depending on the case: the distributor, importer or the market authority) in cases of serious risks and serious incidents, unless this concerns sensitive operational data of LEAs;
- Register their use of high risk systems in a EU database set up for this purpose. For LEAs, the registration is done in a secure non-public section of the EU database and only contains a subset of the information that must normally be registered to respect the LE context; moreover when they find as part of registration that the system they intend to use has not yet been registered by provider they shall inform the provider or the distributor;
- Keep the logs automatically generated by the high-risk AI system to the extent such logs are under their control for a period appropriate to the intended purpose of the high-risk AI system, of at least six months;
- When required by applicable data protection law (i.e. the Law Enforcement Directive), **carry out a Data Protection Impact Assessment (DPIA),** using information provided to them by the provider under its transparency obligation;
- **Inform natural persons of the fact that they are subject to the use of the high-risk AI system** in cases covered by Annex III (which includes the LE uses discussed), where the system make decisions or assists in making decisions related to natural persons. However, the AIA here refers to Art. 13 of the Law Enforcement Directive, which allows for a more limited or delayed form of information to respect LE purposes;
- To cooperate with national competent authorities to implement the AIA;

- In relation to post remote biometric identification systems: respect the conditions already described above, as present in national law, including in particular the need to request and receive authorization, from a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for each specific and targeted use of such a system, in accordance with national law requirements. Each use must be document in the police file and annual reports on the general use of post remote biometric identification systems must be prepared.

The AIA also foresees deployer obligations in terms of transparency, including in relation to **systems directly interacting with natural persons** (Title IV of the AIA), for deployers of **emotion recognition** systems, **biometric categorisation** systems, systems that generates or manipulates image, audio or video content constituting a **deep fake**, or systems that **generate or manipulate text**, which is published **with the purpose of informing the public on matters of public interest**. In all those circumstances however, **specific exceptions exist to allow for the LE context**, namely where the use of such systems is authorized by law in order to detect, prevent, investigate and prosecute criminal offences. Hence, LEAs must assess whether they can benefit from this exception under national law and under what conditions.

While deployer obligations are clearly less demanding than the obligations of the provider, the obligations of the deployer will still require a great deal from LEAs that intend to use high-risk AI systems. Many complex OSINT tools may fall within this category, and hence further clarification will be needed to really understand the scope of application and when these obligations will apply.

The AIA however providers for the Commission to provide guidance on many mattes of practical implementation, including the prohibited practices, the practical implementation of the provisions related to substantial modification (which might requalify a LEA from deployer to provider), as well as a "**comprehensive list of practical examples of high risk and non-high risk use cases on AI systems**", as already mentioned above. This latter list must be produced latest 18 months after the entry into force of the AIA, i.e. no later than 2 February 2026. Knowing that the AIA obligations on high risk systems in LE will only as of 2 August 2026, this means that for at least six months in between, more guidance will have been available. Nonetheless, it would certainly be advisable for LEAs as deployers to start preparing well before that time (more details on this are provided in the next section).

A last obligation for LEAs as a deployer relates specifically to the potential impact of LEA's use of AI systems on the fundamental rights of the public at large in general, and the persons concerned in particular (whether as a victim, witness or suspect). The AIA provides for a specific subset of deployers, in particular public bodies including **LEAs, that they must carry out a fundamental rights impact assessment (FRIA) prior to their first use of a high-risk AI system.**

As such, LEAs considering to start using a complex OSINT tool that would qualify as a high-risk AI system, should perform an assessment of the impact on fundamental rights that may be produced as a result of using the system within their organisation. **The fundamental rights impact assessment (FRIA) should include the following elements:**

- A description of the LEA's processes in which the high-risk AI system will be used, taking into account the system's intended purpose;
- A description of the duration (period of time) and frequency of the intended use;
- A description of the categories of natural persons and groups likely to be affected by the system's use in the specific context;
- A description of the specific risks of harm that are likely to have an impact on the categories of persons or groups identified to likely be affected, taking into account the information made available to the LEA by the provider of the system;
- A description of the measures implemented by the LEA using the system, in accordance with the instructions of use made available by the provider, to ensure human oversight;
- A description of the risk management measures in place to deal with any risk that would materialize in reality, including the arrangements made for handling of complaints and internal governance.

Updates to this assessment must be performed when any of the elements has changed or is no longer up to date, meaning that LEAs must have some procedure in place to periodically review the status of the FRIA. LEAs can however, for similar systems, rely on previously conducted FRIAs, and may also leverage existing impact assessments made available by the provider of the high-risk AI system.

In addition, the AIA explicitly mentions that elements of a DPIA under the Law Enforcement Directive may be used for the FRIA. As such, both Impact Assessments are meant to completement each other and together cover all elements required by both the AIA and the Law Enforcement Directive (for more details on DPIAs, see further under challenge 3).

In principle the assessment must be made available to the market surveillance authority that Member States must create under the AIA, with some limited exceptions where a high risk AI system can be put into use and deployed by LEAs without the FRIA and without a conformity assessment by the provider. The AIA allows this only for exceptional reasons, with the most relevant for LEAs being public security and the protection of life and health of persons. Moreover, there must be an element of urgency that justifies the derogation.

In order to help deployers covered by the FRIA obligation, the AIA explicitly mentions that the AI Office (which is the body within the European Commission that will support the AIA's implementation in a practical manner) must develop a template to conduct such an assessment in a simplified manner, including through an automated tool. This is good news for LEAs in principle, although the AIA does not provide with a strict deadline for this, as it does with other elements of further guidance, implementation and support for developers and deployers. Moreover, it remains to be seen whether such a template and tool will be specific enough to the LE context (since the FRIA obligation applies to all public bodies).

LEA obligations, FRIA, and accountability measures in current practice

This section aims to explore what LEAs may already do today in order to deal with the potential impact of their use of AI, in particular in this case through using OSINT tools. This can be seen both as preparation for the future obligations of the AIA, as well as an accountability measure for the use of AI by law enforcement in general.

The reason that this bears relevance, is that even in cases of AI-driven OSINT use that do not present high-risk use case under the AIA, the use of AI in LE in general, and in OSINT tools in particular, may raise legal and ethical concerns, relating i.a. to the privacy impact, data protection law compliance, and the potential impact on other fundamental rights, such as right to an effective remedy and the right to a fair trial, including the right of defence and the presumption of innocence.

As such, **a proactive assessment of the fundamental rights impacts of the use of a tool should therefore be considered good practice for every AI-driven OSINT tool** before a LEA takes such a tool into use, whether categorized under the AIA as high-risk or not. There's two reasons for this:

- First, the fact that the AIA does not categorize an AI use as inherently risky by marking it as high-risk, does not mean that such a use case does not or cannot present high risk. The AIA's approach is to regulate only certain types of use cases, but this does not prevent high risk from arising in other situations. Hence, LEAs should for reasons other than the AIA (including data protection and principles/legal obligations of good governance by LEAs) likely implement a more generalized type of impact assessment when considering to use AI systems in the implementation of their tasks.
- Second, the AIA is explicit in acknowledging that the list of LE uses targeted by the AI act as high-risk may be amended over time, which means use cases can be added, modified or deleted under certain conditions. This means that the scope of the obligation is subject to change, and LEAs that voluntarily implement a standard process to assess all types of AI will have a much easier time in dealing with such changes.

Best practice and **good governance is in particular relevant in an OSINT context**, given that **OSINT is usually based on general policing powers,** which, as described above, is **a tense situation vis-à-vis fundamental rights to start with**, in the absence of more specific legislation on this topic to provide LEAs with clearer procedural powers in this regard. Given that reality, some type of (voluntary) Fundamental Rights Impact Assessment prior to the use of AI-driven OSINT tools can work as a strong accountability measure, even where such an assessment is not (yet) mandated under the AIA, as well as for high-risk applications intended to be used before the AIA's date of application. Such an exercise will help LEAs to ensure that the actual risks of an AI-driven OSINT tool intended to be used is acceptable.

Well before the AI Act proposal already, there was an awareness of the risks of AI to fundamental rights and freedoms, ethical rules and more generally the values of the Union. As such, **guidance, methodologies and frameworks already exist to help LEAs** out in this regard. The following couple of examples provide some good starting points:

- **The Assessment List for Trustworthy Artificial Intelligence** (2020),[26] based on the Ethics guidelines for trustworthy AI (2019)[27] developed by the High-Level Expert Group on AI, a group of experts appointed by the European Commission to provide advice on the EU's AI strategy. This list is not specific to LE, but provides a good basic understanding of some of the ethical challenges, including basic of fundamental rights impact assessment;
- The **Fundamental Rights and Algorithms Impact Assessment template ("FRAIA"),** which was developed by the Dutch Ministry of the Interior and Kingdom Relations.[28] This methodology is again not LE specific, but was developed for use by Dutch public authorities in general. The FRAIA template is a comprehensive impact assessment, which focuses on fundamental rights impact of AI systems, considering a very broad list of potential fundamental rights (and provides examples and subsets of the main rights). This large list of rights that must be considered and assessed for each high-risk AI system, combined with the elaborate methodology means it is a valuable input for LE (as it will likely be for the AI office). However, this methodology is perhaps too board and extensive for LEAs only deploying an AI system.
- A specific methodology for LEAs as deployers has been developed in the EU-funded ALIGNER project (https://aligner-h2020.eu/about/). **The ALIGNER Fundamental Rights Impact Assessment (AFRIA)**[29] covers specifically the following rights that are of main importance to LEAs deploying AI systems: presumption of innocence, right to an effective remedy, right to a fair trial, right to equality and non-discrimination, right to freedom of expression and information, right to respect for private and family life (privacy), and right to protection of personal data. It also provides an AI system governance template, covering the main categories of the ALTAI/HLEG guidance. It provides an approach for LEAs that are deployers that is reasonable in terms of complexity.
- Another methodology specific for LEAs is **AP4AI, which stands for Accountability Principles for AI**.[30] This tool, available to LEAs and the methodology on which it is based, was developed within the AP4AI Project, jointly conducted by CENTRIC[31] and Europol Innovation Lab and supported by several EU actors, such as Eurojust, the EU Agency for Asylum (EUAA), the EU Agency for Law Enforcement Training (CEPOL) and the EU Agency for Fundamental Rights (FRA), in the framework of the EU Innovation Hub for Internal Security. The AP4AI methodology includes principles of importance that are more specific to the LE context, such as a legality of use of an AI

[26] Available as a list and a web-based tool at https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.
[27] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[28] Available at https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms.
[29] Available at https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/.
[30] Available at https://www.ap4ai.eu/.
[31] CENTRIC stands for Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research, and is a multi-disciplinary and end-user focused centre of excellence, located within Sheffield Hallam University in the UK.

system in a criminal justice context, or commitment to robust evidence. Moreover, there's detailed information available on how the methodology was built.[32]

- Importantly, the AP4AI project is also working on implementing the rules of the AIA, the result of which will be made available as the **CC4AI tool**. With this tool, available free of charge to internal security practitioners, LEAs will, citing to the AP4AI website, "be able to assess compliance of their AI systems with the requirements of the AI Act. This will allow users [of the tool] to evaluate whether, existing or future applications, meet the criteria set by the new regulatory framework."[33] LEAs can get access to the tool through the Europol Innovation Lab.

In addition to the above, for LEAs intending to develop/provide an AI based tool, a methodology of interest could be **CapAI**,[34] which is a rather comprehensive methodology, which aims at providing organizations (not just LEAs, more general), with practical guidance on how high-level rules relating to ethical and trustworthy use of AI can be translated into verifiable criteria, to help shape the design, development, deployment and use of AI systems. Its purpose is to act as a governance tool to ensure and demonstrate compliance with the AIA, specifically in relation to the conformity assessment that providers must carry out. While the AIA defines two separate types of conformity assessment (the one provided for in Annex VI of the AIA based on internal control and the one provided for in Annex VII of the AIA based on a third party assessment), it does not provide a concrete and comprehensive methodology. In particular on the internal conformity assessment, the AIA is rather succinct. **The CapAI methodology aims to fill that gap by providing a detailed methodology for such conformity assessments**. As such it is a valuable resource for LEAs that will qualify as a provider of a high risk AI system. CapAI may also be used optionally by LEAs acting as providers of AI systems that are not high-risk. At the time of writing, the publicly available version of Cap4AI dates from mid-2022 and is hence based on an earlier draft of the AI act. This does not necessarily detract from its value, but LEAs considering its use might enquire whether a more recent version is available to them prior to launching this exercise.

[32] Available at: https://www.ap4ai.eu/reports/2022/02/ap4ai-framework-blueprint.
[33] https://www.ap4ai.eu/cc4ai-tool.
[34] Floridi L., Holweg M.,Taddeo M., Amaya J., Mökander J., and Wen Y., "capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act" (2022). Available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091.

AI-driven OSINT by LEAs and the AI Act: policy statement

With the recently published AI Act, LEAs using AI-driven tools, including OSINT tools for CSAE investigations on the dark web, will have a **set of additional obligations to comply with, which will put an additional strain on their resources.**

From the results of the questionnaire, it is clear that AI compliance is not something that LEAs are already very familiar with:

- About 10% of respondents already knew the existing methodologies for AI ethical and legal compliance described in this paper;
- About one third of the respondents indicated to have already conducted a human rights or fundamental rights impact assessment before using a tool (AI or otherwise).

This is confirmed by the self-assessment questions, where respondents were asked to rate the level of their own organization on a scale of 1 to 5 (1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent). The results were as follows:

- On average, respondents rated the technical knowledge about AI and AI literacy of their organization at roughly 2.5 out of 5 (in between “fair” and “good”);
- On average, respondents rated the knowledge of their organization of the AIA and the requirements applicable to high-risk systems to be used by LEAs at roughly 2 out of 5 (“fair”);
- On average, respondents rated the preparedness for the AI Act of their organization at roughly 2 out of 5 (“fair”).

In addition, only one third of the respondents indicated to have deployed AI before, mostly very recently. A couple of respondents indicated that AI is present in the software and tools they use. In fact, given the very broad definition of AI under the AIA, it is quite likely that most, if not all, of the respondents have already utilized AI in the sense of the AIA in some way or another in pursuit of their tasks, as AI functionalities have been on the market for years, both in commercial solutions and free open source software available to LEAs. However, software and functionalities are not often branded or highlighted as AI-driven, and AI features may silently be integrated as updates into existing tools and software (suites) used by LEAs. As a concept, “deploying AI” may instinctively refer more readily to a conscious choice to use AI, rather than the use of (hidden) AI functionalities in a given tool or software (suite), as part of the regular use of that tool or software, without a conscious choice by the LEA to start using or deploying AI. This reality may help explain the answer of two third of the respondents that they have not deployed AI in the past, meaning that they have not actively and consciously chosen to use specific AI systems or applications up until now.

While the questionnaire results are not necessarily representative of all LEAs, they do show quite clearly that **awareness raising, knowledge building and training will be important in order to make sure LEAs will be able to meet their compliance requirements under the AI Act.**

It is therefore essential that sufficient support is made available to LEAs in order to raise awareness about the AIA and its obligations, provide training, and to provide resources, such as guidance, checklists and templates (including the form of tools or wizards to guide the user through the process), which are ready to use, clearly explained and remain reasonable in the light of the Law Enforcement reality in terms of resources.

Existing efforts e.g. by CEPOL, or under the auspices of Europol's Data Protection Experts Network (EDEN), to discuss and educate should be valued and continued, but more may be needed in the future.

In particular, the European Artificial Intelligence Board, the European Commission and the AI Office should make sure to take into account the specificities of Law Enforcement in their upcoming work regarding the (practical) implementation of the AI Act. When developing a template for the fundamental rights impact assessment (FRIA) required to be performed by LEAs using high-risk AI systems, for example, it would be recommendable to provide a specific template (and tool) for this context.

CHALLENGE 3: data protection under the law enforcement directive (LED)

Relevance of data protection and introduction to the LED

OSINT tools use data in order to provide their functionalities. Quite often this will involve personal data, including sensitive attributes of individuals. Hence, the third major important legal consideration regarding the use of OSINT tools for CSAE investigations on the dark web is the element of data protection. Where under challenge 1 above the question was asked to what extent LEAs can legally take access to an open source based on procedural powers under national law, **the topic covered in this section is the data protection rules that apply to the use of the data collected from such sources**, in particular through AI- and data- driven OSINT tools, and therefore also to the requirements that such tools and LEAs using such tools must meet to be in compliance with the law.

Data protection, while related to privacy, is a separate self-standing fundamental right, which is practically implemented in the EU in three major pieces of legislation: the General Data Protection Regulation (GDPR),[35] the Law Enforcement Directive (LED),[36] and the Regulation 2018/1725, sometimes referred to as the EUI-GDPR.[37] The GDPR is the general regime, while the LED and EUI-GDPR provide specific regimes for Law Enforcement and the EU's institutions, bodies and agencies respectively. **The GDPR is undoubtedly the most well-known, which can be a challenge, as it is often mentioned and referred to in a law enforcement context where it does not in fact apply**. Of course the GDPR does apply to LEAs as well, but only for processes that are outside the scope of their main tasks related to 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**"**.[38] **For the core "law enforcement" purposes of a LEA, the LED applies**. Hence, in relation to the use of OSINT tools, in particular AI- and (big) data-driven OSINT tools, used in relation to the power of LEAs to keep order (intelligence and monitoring of public space purpose) and investigate crimes (investigation purpose) the LED will be the applicable framework, and will hence be explored further in this section. For Union bodies, offices and

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

[36] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

[37] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance), OJ L 295, 21.11.2018, p. 39–98.

[38] Article 1(1) LED and Article 2(2), d) of the GDPR. In its Article 9, the LED sets out some specific situations with an explicit mention that the GDPR applies in those cases, namely where a LEA processes LE data for other purposes specifically provided for by law, or where LEAs have been entrusted by Member State law to perform other than LE tasks, such as archiving, research or statistics.

agencies carrying out activities which fall within the remit of judicial cooperation in criminal matters and police cooperation under the TFEU[39], chapter IX of the EUI-GDPR provides an exceptional regime akin to the LED.

The distinction between the LED and the GDPR is important, at least for two main reasons:

- First, the LED provides for a **specific exceptional regime to the GDPR**, with **significantly different rules** to allow for the specific circumstances of a Law Enforcement context. The LED provides for both less stringent and more stringent rules compared to the GDPR, depending on the topic.

  Examples of **less stringent rules** include a different criterion for how much data can be collected for a specific purpose, with LEAs being allowed to err on the side of caution in terms of data collection, as long as it is "not excessive", compared to a much stricter rule under the GDPR, where data collected needs to be "necessary". Another example is the right to information for the data subject, which is more restricted under the LED so as to avoid hindering LEAs in their core tasks, e.g. where information would obstruct or prejudice an investigation.

  At the same time however, the LED also provides **for stricter or more specific rules** compared to the GDPR. This includes the need for a specific legal basis for any processing, describing what LEAs can do under Article 8 LED (compared to six broader legal grounds under the GDPR), more limited exceptions for the use of special categories,[40] additional obligations to distinguish between categories of data subjects (witness, suspect, victims, other parties) and between data based on facts vs. data based on opinions,[41] specific time limits for storage and/or periodic reviews of necessity of further storage of data set in national law (compare to the controller being in charge of this under the GDPR)[42], specific logging obligations,[43] and more detailed obligations related to the technical security of processing.[44]

- **Second, the LED is a Directive from the EU, meaning it must be transposed in national law to take effect.** While Regulations, including the GDPR often leave some leeway for Member States to introduce exceptions or make certain choices, a Directive presents a different level of national implementation, **to an extent allowing for, and in practice typically leading to more divergent national rules** compared to a regulation. In addition, the LED allows in a general fashion (i.e. not restricted to specific obligations) for Member States to introduce stricter rules.[45] The LED must be

[39] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, part III, title V, chapters 4 and 5.
[40] Article 10 LED.
[41] Article 6 and 7 LED.
[42] Article 5 LED.
[43] Article 25 LED.
[44] Article 29 LED.
[45] Article 1(3) LED.

understood as providing the minimum level to be met (minimum harmonization of national laws).

In the following sections, some of the elements of the LED's regime will be explored and applied to OSINT tools in CSAE investigations, in particular AI- and (big) data-driven OSINT tools. The focus will be on the LED's EU-wide minimum rules, with slight excursions into national implementation.

Generally however, the national law of Member States in this field is particularly important to understand the conditions for the use of AI- and (big) data-driven OSINT tools. The fact that this law is rather inaccessible, is a **challenge for tool developers in EU-wide projects to collect data protection requirements** in order to make sure the tool is suitable for use by LEAs across the Union. Accessibility (in a broad sense) is a general issue in relation to national implementation of EU law, for various reasons, including:

- **Language barriers**: legislation and case law is only often accessible in the official language(s) of the Member State concerned;
- **Practical difficulties in accessing sources**: researchers from other countries may not know where to look, may not have access to paid sources for literature and case law (not all case law is always publicly available online);
- **Lack of case law**: this is often an issue, rendering it necessary to rely on national experts and experiences to understand the interpretation of the law, which invites misunderstandings;
- **Complexity of the national legal landscape**, including the number of legal instruments implied in creating a comprehensive overview of the national legal situation. This may include several instruments such as instructions from ministries, and other forms of guidance that are not easily identifiable or even publicly accessible;
- **Reliance on and issues with expert knowledge**: often expert knowledge is needed, meaning that the understanding of a legal system is (partially) based on statements or explanations from a third party (rather than a primary source of law). Expert knowledge may come from publications or presentations or may be specifically and proactively procured through questionnaires, interviews, etc. Reliance on expert knowledge is an uneasy situation to start with, as it is much less transparent than having access to primary sources explaining all details of a legal question. Moreover, expert knowledge is often difficult to identify or procure. Practitioners may know the practical implications of the rules for their work but not have a view on the broader legal picture and legal questions and concerns. Legal experts (e.g. lawyers, researchers) may often be limited to analyzing the legislation (and some case law, if present), while not knowing the (finer) details of the situation on the ground. In addition experts may not be able or willing to engage (e.g. supervisory authorities or high-level national experts may be well placed but not have the practical resources available) and experts may in addition differ in their understanding of or opinions about certain rules, meaning one expert opinion is hardly enough to be considered conclusive;

- **Lack of familiarity with the legal system** to adequately interpret and understand information that is collected (either desktop, from interview, from an expert analysis);
- **Restraints in terms of time and resources** to create a good overview.

All of these challenges are certainly present in the context of the national implementation of the LED, which is a complex field of law, often with many different elements being present to putting together an overview of the national legal landscape.[46]

This is important to understand for what follows, as existing sources provide an incomplete overview of national requirements, and while the reasons for this are well understood, this does somewhat hinder the analysis. **Two reports providing an overview of the LED's national implementation** are of main importance here, namely:

- The European Commission's first report, pursuant to Article 62(1) LED, on the application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')[47]: this report covers on a high level the transposition of the LED and some first lessons learned from the situation in the Member States (July 2022);
- A study requested by the LIBE Committee of the European Parliament, providing an "Assessment of the implementation of the Law Enforcement Directive"[48] (December 2022).

Both of these reports are incredibly valuable to understand the lay of the land of national laws throughout the EU. **However, tool developers wanting to gather requirements in order to make their tools easily accessible to LEAs from any Member State will struggle to get the necessary actionable information on the basis of these overviews.** This lack of clarity may hurt in particular the EU-wide and EU-funded efforts to make new tools available to LEAs, as clarity on the legal situation is a prerequisite for designing tools in a manner that they are legally compliant, ideally in all Member States.

Some requirements may be circumvented without understanding in detail the specific situation in the different national laws, such as specific time limits for storage. Tool developers could simply allow for a process of review and erasure and allow LEAs to set the timeline based on their national law. Other elements however, are not so easily circumvented, since they may influence the design of the tool, such as the types of legal bases that exist in national laws for processing certain types of data in certain specific contexts, e.g. in relation to specific types of

[46] A good illustration of this complexity can be found in a Dutch study that aimed to compare the implementation of the LED in 5 countries, trying to gather input from the transposition of the LED and approach to data protection in policing in other Member States to solve the challenges in the Dutch situation. Available online, including a summary in English at: https://repository.wodc.nl/handle/20.500.12832/3025.

[47] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, available at: https://commission.europa.eu/publications/first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016680-led_en.

[48] Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, available online at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740209.

serious crime such as CSAE (Article 8 LED), or whether, for tools processing special categories of data, a legal basis exists in national law to process such data in the specific context in which the tool is meant to operate (Article 10 LED). The precise wording and extent of such legal bases is important to understand what is legally permissible and what types of tools LEAs can use. Hence, such information is important to make strategic design choices in order to optimize the design of the tool, especially when they are developed with public funds, to benefit LEAs in as many Member States as possible.

OSINT and lawful processing

This section explores some of the main elements to ensure that processing of data by OSINT tools is lawful under the LED.

It covers the following elements:

- General lawfulness under Article 8 LED;
- Lawfulness of the use of special categories of data under Article 10 LED (if applicable);
- Lawfulness of automated decision-making under Article 11 LED (if applicable).

Lawfulness of processing

Article 8 LED provides that processing by LEAs of personal data 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, shall be lawful only when such processing is necessary for the performance of those tasks and based on EU or national law. **Member states must provide for specific legal bases and must specify "at least the objectives of processing, the personal data to be processed and the purposes of the processing**". Hence, other than under the GDPR, it is not LEAs as controllers who determine what legal basis they use (as there is only one, namely a basis in law), or what objectives they pursue and what data to use for that. Member States enjoy a margin of discretion in determining such elements, but must of course remain within the limits set by fundamental rights (which links the question of lawfulness of the processing, to the legality of OSINT use mentioned in challenge 1).

Merely repeating the rule of Article 8 LED in national law is therefore not enough, rather specific legal bases must be foreseen for processing regulating the processing by competent authorities, specifying specific tasks, which authorities are competent for these, and the personal data needed for such tasks and purposes.[49] The first report of the Commission on the application and functioning of the LED mentions that some national transposition indeed merely repeat Article 8 LED without specific further legal bases, omitted certain elements of Article 8 or did not transpose the requirement of Article 8(2) LED that the data to be processed and the purposes of processing should be made explicit in law.[50] In addition, it mentions that

[49] Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, p. 41 and following.
[50] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 14.

some national transposing laws refer to consent as a legal basis for processing of personal data, including special categories of data. While consent can be an additional and even mandatory safeguard in some situations, if national law provides for this, this is never the legal basis in itself. Hence, arguments along the lines of disallowing OSINT because open sources do not imply consent of the data subject (which is true), cannot hold unless this is a mandatory requirement under applicable national law.

For OSINT tools' processing of personal data to be lawful, in principle then there needs to be a legal basis that covers OSINT. When such **a legal basis is missing, or it is too focused**, e.g. related to specific investigative powers rather than allowing open source collection for general policing powers, **there may be questions as to the legality under the LED of OSINT processing of personal data**. There is some evidence to suggest that at least in some countries this may be the case.[51]

Special categories of data

OSINT tools used in a context of CSAE investigations on the dark web are very likely to collect special categories of data. Even if such data categories would not be part of the intended scope of the collection, it is unlikely that their collection can be completely avoided, in particular when data collection is automated to a certain extent.

For lawful processing of such data it must be a) strictly necessary for the purpose, b) subject to appropriate safeguards[52] and c) based on one the following grounds:

- The processing is authorised by EU of Member State law (in particular the legal base required under Article 8 LED);
- The data is strictly necessary to protect the vital interest of the data subject or a third person;
- The data has been manifestly made public by the data subject.[53]

While the text of the LED seems to provide a legal basis as one of the options to authorize the use of special categories, both the Commission and the WP29 have in the past taken the point of view that a legal basis must be present in any case,[54] meaning the legal basis under Article 8 GDPR must provide specifically for the authorization to use special categories. The CJEU

[51] Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, p. 42-43.
[52] Recital 37 LED provides some examples: "the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities".
[53] To be interpreted narrowly (Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 10).
[54] Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, p. 47 and references there.

had an opportunity to look at this matter in case C-205/21[55] but only found that, where a legal basis under Article 10 LED exists, it must be sufficiently clear and precise and an erroneous reference to the GDPR rather than LED did not, in and of itself, call into question the existence or validity of the legal basis/authorisation to use special categories. The text of the LED however, does not very clearly support such an interpretation, and moreover it has become clear from the first report of the Commission on the application and functioning of the LED that most Member States follow the structure of 3 legal grounds for the use of special categories, with some Member States adding additional legal grounds related to the protection of life and persons.[56] In some Member States, the main transposing law does not provide for safeguards, which must then be provided in sectoral laws.[57]

As such, it seems that there is leeway to argue that special categories of data can be collected by OSINT tools absent a specific authorization in national law, when this data is strictly necessary in order to protect the vital interest of the data subject or another person (e.g. the victim) or when strictly necessary for the purposes pursued and the data has manifestly been made public by the data subject. The mere fact that something is available online or open source however does not constitute in and of itself that the data has been "manifestly made public". As the A29 WP highlighted back in 2017, this has to be interpreted to imply that the data subject was aware that the respective data will be publicly available to everyone including authorities, and that the data subject has voluntarily given up the special protection for sensitive data by making them available to the public including authorities.[58] In case of doubt, a narrow interpretation should be applied. Moreover, it should not be forgotten that many pieces of information in open sources may have been published by other parties than the data subject itself, limiting the application of this ground. When relying on the ground of a legal basis, this legal basis must be sufficiently precise as to allow the use of special categories.

For all three cases, strict necessity in relation to the purpose pursued is required by the LED. There is some discussion about the language here, as the French version seems to require an "absolute" necessity. In any case the necessity criterion seems to be quite rigorous. According to the first report of the Commission on the application and functioning of the LED, most, but not all, Member States require strict necessity as a prerequisite of processing as per the LED.

Hence, **LEAs using OSINT tools that will or may involve the collection of special categories, must make an assessment under their national law of the permissibility of such collection and use**. Both one of the three grounds under Article 10 LED must apply, and there must be a strict necessity for that data to be processed in relation to the purpose pursued by the OSINT use. Significant differences may exist between national laws.

[55] CJEU, Case C-205/21, V.S., ECLI:EU:C:2023:49.
[56] Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, p. 46-49; European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 14.
[57] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 14.
[58] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, 29 November 2017, p. 10.

ARICA

Automated decision-making

OSINT tools that are AI-driven may often include a form of profiling. In as far as such profiling constitutes automated processing, which leads to decisions that produce an adverse legal effect concerning the data subject or significantly affects him or her, Article 11 LED requires a specific legal basis in/authorization by Union or Member State law, which must moreover provide for appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention. In case the automated decision-making involves special categories, additional suitable safeguards must be put in place. Any form of profiling that results in discrimination against natural persons on the basis of sensitive elements covered in the special categories, is forbidden without exception.

According to the first report of the EC on the implementation of the LED, while all Member States provide for the prohibition unless the automated-decision making is provided for by law, not all (but most) require that such decisions not be made on the basis of special categories, unless there are suitable safeguards.[59] In addition, not all Member States provide for suitable safeguards and not all Member States provide for the right to obtain human intervention. Hence again, national differences may exist.

The main question however is whether an OSINT tool constitutes automated-decision making in the sense of Article 11 LED. Whether there is any form of decision will depend on the automated nature of the use of such tools rather than the data collection. OSINT tools that function on the basis of targeted searches by LEAs, should be able to avoid such a qualification. For OSINT tools automatically running searches (on the basis of set parameters), the element of human oversight and involvement in the process will be of primary importance to show that the tool does not take automated decisions. The element of adverse legal effect or significantly affecting the person concerned is another threshold that must be considered in order to determine whether Article 11 LED applies. Given that wording of the LED is different from the GDPR, it is unclear whether the existing guidance on those terms under Article 22 GDPR can apply.[60]

National interpretations on these terms may be relevant for LEAs to consider. **However, most OSINT-tools, even AI- and (big) data-driven OSINT tools should not reach this threshold, not in the least because of the challenges explained above relating to a legal basis for OSINT**. Such automation would be a very high interference into fundamental rights and therefore not permissible under general policing powers.

Note that AI- and (big) data-driven OSINT tools that involve profiling are typically covered by

[59] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 14-15.

[60] The LED talks about "adverse legal effect" or "significantly affects [the data subject]", where the GDPR refers to "legal effects" and "similarly significantly affects [the data subject]". Hence it is unclear of the guidance of the A29 WP (Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), p. 21-22) can apply under the LED.

the AIA as high-risk use cases, also when they do not reach the level of Article 11 LED. The references in the AIA related to the general definition of profiling under the LED in Article 3(4) LED as a form of automated processing of personal data and not to Article 11 LED, which covers specific cases of automated processing that lead to automated decision-making and therefore have a very different impact. The terms and their consequences should not be confused, as many OSINT tools may involve profiling, but not automated decision-making.

OSINT and LED controller requirements

LEAs using OSINT tools will qualify as the controller in relation to the processing covered by those tools. Hence it is important to consider the controller obligations imposed by the LED, which must hence be requirements for LEAs in such cases to:

- **Implement appropriate technical and organisational measures to ensure that processing complies with the LED** (**Article 19 LED**): this is a general obligation that links to ensuring within the organization of the LEA that all rules of the LED are complied with. In particular, this include the principles covered in **Article 4 LED**, namely that processing of personal data (in the context of OSINT tools):
    - Is fair and lawful (**lawfulness and fairness**): this requires legality under the LED under Article 8 LED, as well as 10 LED, but also a broader legality of the processing, meaning the lawfulness of OSINT tools as such under procedural powers is covered here as well; This requirement also considers whether the use can be considered fair towards the data subjects (which includes often not only suspects, but many third parties, often unrelated to the enquiry). Safeguards have an impact on fairness.
    - Is only ”collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes” (**purpose limitation**): for OSINT this consideration includes whether data can be re-used and data can be linked with other data sets, when allowed by Member State Law.
    - Is “adequate, relevant and not excessive in relation to the purposes for which they are processed” (**data minimisation**): the LED allows LEAs to err on the side of caution, at least to an extent when it comes to data collection, as long as it is “not excessive” for the purposes. This is supportive in principle of OSINT applications.
    - Is accurate and kept up to date (**accuracy**): in relation to OSINT, this obligation may be read as a reason for LEAs to have in place measures for accuracy, such as reliability testing i.e. a post-hoc assessment of OSINT tool outcomes in terms of reliability and accuracy of the data and findings, the sources used, and the outcomes being validated by staff.
    - Is performed on data, “which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed” (**storage limitation**): for OSINT this relates to rules surrounding how long the data is kept in

identifiable form, data retention and storage limits in national law and the national rules on regular reviews on whether data is kept or not, but can also be relevant in relation to measures like scrubbing or pseudonymization that may be used within OSINT tools to prevent identification until it is necessary;

- Is processed "in a manner that ensures appropriate security" (**security, integrity, confidentiality**): see for more details Article 29 LED below.

- **Implementing data protection by design and by default measures** (**Article 20 LED**): this article requires LEAs to consider data protection elements throughout the process. Hence, a LEA considering the use of new tool should consider and question the data protection compliance aspects of such a tool, and to take appropriate measures (or to not use a tool, if the data protection compliance under national law is too problematic).

- **Respect obligations regarding the use of processors** (**Article 22 LED**): this Article sets out the conditions for LEAs to utilize third party processors (themselves LE or commercial third parties). This may be relevant for certain OSINT tools, if they are hosted by a third party. When the OSINT tool and code is available to LEAs as such, LEAs may run it on their own premises or outsource this. However, at all times security requirements of Article 29 LED must be respected (see further). Moreover, as the LED is minimum harmonization, some national laws explicitly prohibit for LE data to be accessed by external service providers (so also the provider of a hypothetical OSINT tool). LEAs have to assess whether they are allowed under national law to rely on processors, and what conditions, if any, apply. Moreover, if allowed, LEAs should take care to verify contractual arrangements and their compliance with the LED, any localization requirements that may exist under Member State law (to keep the data within their own jurisdiction, or to only leave it subject to specific condition, or to avoid hosting in third countries), and should in any case perform some vendor due diligence, which may of course be facilitated through existing organizations and networks.

- **Implement logging measures** (**Article 25 LED**): this Article provides for specific accountability obligation which is quite extensive in relation to the logging of various operations in automated systems, namely collection, alteration, consultation, disclosure including transfers, combination and erasure of data. The logs must contain "justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data". The logs are meant amongst other things for LEAs to verify the lawfulness of their operations and self-monitor. overlaps with logging requirements under the AIA. Logging helps to ensure legality, security, and avoids misuse. This means that OSINT tools must allow for extensive logging to facilitate LEA's compliance with this obligation, also where an AI-driven OSINT tool is not high-risk under the AIA.

- **Carry out a data protection impact assessment** when the processing is likely to result in a high risk to the rights and freedoms of natural persons**,** in particular when using new technologies (**Article 27 LED**): this requirement will tend to apply to AI- and

(big) data-driven OSINT tools, both because of the use of new technology (which may present non-obvious negative effects that must be considered and counteracted with safeguards), because of the potential scale of data collection of some tools, because of the potential, processing of sensitive data and because of the potential fundamental rights impact, already described in challenges 1 and 2 above.

- **Implement appropriate measures to guarantee a level of security appropriate to the risk, in particular for special categories** (**Article 29 LED**): this article provides an overview of measures to be considered for the security of the processing, from a technical and operational point of view, taking into account nature, scope, context and purposes of the processing, the risks posed and the state of the art and costs of implementation. The LED, other than the GDPR provides for a list of measures to be implemented by controller or processor, following an evaluation of the risks, namely measures:
    - To deny unauthorised persons access to processing equipment (**'equipment access control'**);
    - To prevent the unauthorised reading, copying, modification or removal of data media (**'data media control'**);
    - To prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (**'storage control'**);
    - To prevent the use of automated processing systems by unauthorised persons using data communication equipment (**'user control'**);
    - To ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (**'data access control'**);
    - To ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (**'communication control'**);
    - To ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('**input control'**);
    - To prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('**transport control'**);
    - To ensure that installed systems may, in the case of interruption, be restored (**'recovery'**);
    - To ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system (**'integrity'**).

LEAs must take into account all these elements when considering the use of OSINT tools.

OSINT databases and LED checklist for OSINT

A last topic for OSINT tools, especially AI and (big) data-driven OSINT tools, are some specific requirements of the LED that are particularly relevant to the database and data management aspects, also in relation to OSINT tools. In addition to elements already discussed above, the LED contains the following specific obligations that are of importance:

- **Time-limits for storage and review** (Article 5 LED): this Article requires Member States to set clear limits by law for personal data to be erased or for a periodic review of the need to store the data in question. Instead of controllers having to determine such limits, as is the case under the GDPR, under the LED national law should provide for legal obligations to review or limit the continued storage of personal data.[61] Combined with Article 20 LED, the argument can be made that OSINT databases should allow for automated erasure of data after the applicable time limit has passed. Different time limits may be set for different purposes, i.e. including differentiation for example on the basis of the types of data subjects involved, the types of crimes, the types of procedural powers utilized, or the types of databases that are created. Significant discretion is left to Member States, and it seems that varying regimes have been set up, with certain Members State providing for very specific time limits, while others, arguably against the wording of the law, leave considerable discretion to the LEAs.[62] In addition, many Member States have yet to pass more sectoral legislation in addition to transposing the general rule of Article 5 LED. For OSINT databases, any applicable national rules must be followed in their creation and management, including (automated) erasure measures.
- **Distinction between different categories of data subject** (Article 6 LED): this Article requires LEAs to clearly distinguish between suspects, convicted persons, victims and other parties such as witnesses, however only “where applicable and as far as possible”. OSINT applications aimed specifically at victim identification for example may be able to satisfy the requirement. For other applications, it is likely that different

[61] The CJEU has recently reviewed national rules under Article 5 LED for the first time and found that Bulgarian legislation, which provided for the storage of personal data by police, including biometric and genetic data, of persons convicted by final judgment of an intentional criminal offence subject to public prosecution, until their death was not compatible with the LED. According to the CJEU, while “until the death of the data subject” may in principle constitute a time limit, such a time limit cannot be regarded as appropriate where it is applicable generally and indiscriminately to any person convicted by final judgment. Moreover, since Bulgarian legislation did not provide for periodic reviews by the LEA-controller, to assess whether such storage was still necessary and to erase data in case it was not, the legislation in question was in breach of the LED’s principles of data minimisation and storage limitation. See CJEU, Case C-118/22, NG, ECLI:EU:C:2024:97.

[62] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (‘LED’), COM(2022) 364, p. 13; Vogiatzoglou, P., & Marquenie, T. (2022), Assessment of the implementation of the Law Enforcement Directive. European Union Publications Office, p. 38-39.

categories or roles become involved, and it may be difficult or impossible for the system to differentiate between them.

- **Distinction between personal data and verification of quality of personal data** (Article 7 LED): this Article requires " as far as possible" for LEAs to distinguish between data based on facts and data based on personal opinions. In the context of OSINT tools, doing this in open source environments may prove impossible, or very difficult (likely with a high error rate if trying to automate such an assessment). Article 7 however also imposes quality verification, in particular when they are transmitted or made available. In relation to OSINT, this is quite relevant. This taken together with the general accuracy requirement could be read as a reason for LEAs to have in place measures for accuracy, such as reliability testing i.e. a post-hoc assessment of OSINT tool outcomes in terms of reliability and accuracy of the data and findings, the sources used, and the outcomes being validated by staff, in particular before such information is transmitted.

In addition, it should be noted that several Member States have specific requirements in their legislation for the creation of certain police databases, that may cover the creation of an OSINT database by LEAs, which may include a review by or notification to the competent data protection authority, as confirmed in the questionnaire sent out to LEAs in the context of the ARICA project.

As such, bringing together all the elements that were discussed, **a LEA, acting as a controller under the LED, setting up a database (or using a database provided by the tool provider as processor) in relation to the (planned) use of an OSINT tool, must consider** the following elements:

- The legality of the data collection under Article 8 LED, Article 4(1), a) LED and national law implementing the LED (clear legal basis, fair and lawful processing);
- The legality of the data collection relating to special categories under Article 10 LED and national law implementing the LED, and where there is no basis, whether such collection can be avoided;
- The implementation in the set-up of Article 6 LED and national law implementing the LED on distinguishing between different categories of data subject, if possible;
- The implementation within the database set-up of Article 7 LED and national law implementing the LED on making a distinction between data based on facts and data based on opinions through data categorization and labeling, if possible;
- The implementation in relation to the OSINT tool, its use and data(base) management of the data accuracy principle under Article 4(1), d) LED, and Article 7 LED relating to verification of quality of personal data, as well as Article national law implementing the LED;
- The implementation within the database set-up of Article 5 LED, and national law implementing the LED relating to specific time limits and/or specific limits for review,

where possible in accordance with Article 20 LED and national law implementing the LED using automated means to guarantee;

- The implementation of the storage limitation principle under Article 4(1), e) LED and national law implementing the LED, including the initial need for identification, considering measures pseudonymous and anonymous options or variations, including measures to scrub data;
- The implementation of the data minimization principle under Article 4(1), c) LED and national law implementing the LED in relation to the OSINT data collection not being excessive, meaning that it is sufficient targeted and not excessive in relation to the purpose of the OSINT tool (see intentionality above under the discussion of legality of the use of OSINT);
- The implementation of the purpose limitation principle under Article 4(1), b) LED and national law implementing the LED, in particular in relation to linking databases and leveraging existing police resources in relation to an OSINT application, as well as the use and re-use of OSINT data, including the re-use of intelligence data for investigations, which may or may not be permissible under national law and may have certain conditions attached;
- The implementation of security requirements as foreseen in Article 4(1), f) LED and Article 29 LED, as well as the logging obligation under Article 25 LED and national law implementing the LED, in particular the measures mentioned in Article 29(2) LED, which include for example role-based and “need-to-know” access to the tool and database, input control on the database, access control to working stations where the tool is available, and logging of all operations, including the justification, timestamps for the use of the tool and operations in the database, as well as the identity of the persons who carried out this operation, and where possible the intended recipients of any data that was disclosed/exported;
- In cases where the database is hosted by the OSINT tool provider, or the LEA would like to host the database on the Cloud, whether this is permissible under national law and, if so, ensuring the conditions of Article 22 LED, and national law implementing the LED are met. This includes: verifying contractual requirements, due diligence, analyzing any data localization measures (including national hosting or a prohibition to host outside the EEA) that may be applicable, authorization that may need to be obtained and other requirements that maybe be applicable;
- The need to carry out a Data Protection Impact Assessment (DPIA) should be verified, prior to any use of the tool or database, under Article 27 LED and national law implementing the LED, and, if required, a DPIA must be carried out containing at least the elements required by the LED and national law. OSINT tools that involve AI and automated collection or processing of (big) data most likely need a DPIA. Where the AIA will apply (or as best practice also outside those situations and prior to the entry into force of the AIA), the DPIA process should be linked to the Fundamental Rights Impact Assessment (FRIA) for deployers of AI tools, so as to not unnecessarily

duplicate efforts. For both processes, it is advisable to leverage existing documentation made available by the OSINT tool provider, keeping in mind however, that merely copying information is not sufficient. LEAs must make their own assessment, as required by law. LEAs may also leverage their own prior assessment of similar tools and databases;

- The need to implement any other measures to satisfy the requirements of data protection by design and default in accordance with Article 20 LED and national law implementing the LED. An example of this could be the automated deletion of OSINT data from the database after the time limit under national law has passed. This may be different for data that is purely for intelligence purposes vs. data that is being used in an active investigation. Such data should be labeled as such, or be stored separately altogether, and benefit from a different retention policy given the different purposes pursued in their processing;
- The need under national law, in as far as not covered in any of the points above, to comply with requirements in relation to the creation of a specific police database, such as authorization and/or notification requirements.

OSINT and the LED: policy statement

As is clear from the first report on the implementation of the LED, the introduction of the LED itself, and its requirement to appoint a Data Protection Officer (DPO) as a data protection expert to support LEAs in their implementation of the Directive, has had and continues to have a major impact on LEAs' awareness of and focus on the importance of data protection, and supervisory authorities have helped out by providing guidance and training.[63] Other initiatives have helped too, such as national DPO networks, the network for the Data Protection Officers of competent authorities, Justice and Home Affairs agencies and the European Public Prosecutor's Office, the Europol Data Protection Experts Network (EDEN), and the efforts by CEPOL in providing data protection training.[64]

As part of the questionnaire submitted to LEAs in the ARICA project, respondents were asked a couple of self-assessment questions in relation to data protection and the LED. Respondents were asked to rate the level of their own organization on a scale of 1 to 5 (1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent). The results were as follows:

- In relation to the level of understanding of the distinction between the GDPR and the LED, and the distinct scenarios in which these legal instruments apply, respondents on average scored their organizations a 3 out of 5 ("good");
- In relation to the level of understanding of the LED itself (i.e. the rules on the EU level), respondents on average scored their organizations roughly a 2.8 out of 5 (between "fair" and "good", but closer to "good");
- In relation to the level of understanding of their national framework implementing the LED, respondents on average scored their organizations a 3 out of 5 ("good").

These results highlight that, at least in the ARICA sample, the level of awareness among LEAs and understanding of the relevant legal framework in relation to data protection is at an acceptable level, but that there is still room for improvement. In particular the distinction between the GDPR and the LED is often not well understood in practice, despite its relevance, given that both instruments differ significantly in terms of content.

Hence, **further awareness raising and training is still needed, both on the LED and national implementation in general, and on specific topics, such as the intersection of the LED with the AI Act**, which will provide particular challenges for LEAs when using AI- and (big) data-driven OSINT tools for CSAE investigations on the dark web. Both the EU bodies

[63] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 18.
[64] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 19; for CEPOL's activities, please see https://www.cepol.europa.eu/, in particular https://www.cepol.europa.eu/thematic-areas/fundamental-rights-and-data-protection.

and agencies and the Member States should continue efforts in this regard and perhaps intensify them.

Moreover, in order to support LEAs in such an understanding, as well as tool developers, law makers (to compare their approach with other Member States) and civil society in general**, it would be advisable for the EU to request further studies on, or otherwise further explore, the topic of the national transposition and implementation in the Member States**, in addition to the future actions already identified in the first report on the implementation of the LED.[65] Such a further exploration, whether through a study or a dedicated EU-funded project, should cover not only the national legal framework in great detail (and providing a matrix of the rules for comparison), but also how that framework is interpreted and applied in practice, of course without revealing tradecraft. Insight into the national situation in the Member States to this extent would greatly enhance the level of detail of the discussion on this topic, including to what extent further action is needed by certain Member States to reach a complete and satisfactory transposition of the LED, and could easily feed into the second report on the evaluation and review of the implementation of the LED, which, under Article 62(1) LED, should be produced by the Commission in 2026.

[65] European Commission, Communication from the Commission to the European Parliament and the Council, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364, p. 34 and following.

Conclusions

This paper has addressed three major current (and future) legal challenges for LEAs intending to use AI- and data-driven OSINT tools in their CSAE investigations on the dark web, namely the legality of OSINT under procedural powers, the legal and ethical compliance of AI in such tools, and the data protection compliance of processing of personal data (including special categories) with OSINT tools.

The use of such tools, even high interference OSINT tools, may at times be necessary in practice. The signal from the ARICA questionnaire is clear that the power of OSINT, as effective and cost-effective tools, should be harnessed. This is not an argument for untargeted surveillance and fishing expeditions by LEAs, but rather a reason to create **a clear procedural framework to allow for OSINT use, in limited and targeted circumstances and providing appropriate safeguards**. The current situation however, with OSINT being based on general policing powers, may lead to LEAs avoiding tools that are available to them or conversely, to LEAs using tools in breach of fundamental rights guarantees. Neither situation is desirable. Moreover, in particular the use of high interference OSINT tools may lead to inadmissible evidence. Hence, a clear legal framework of procedural powers related to the use of open sources and publicly available information is important to enable LEAs to utilize OSINT tools available to them to fight CSAE on the dark web in a situation of legal certainty and in compliance with fundamental rights.

The recently published **AI Act will present LEAs using certain OSINT tools in their investigations to CSAE on the dark web with a specific additional challenge**. Many such OSINT tools will be AI-driven and contain techniques (e.g. profiling) that may qualify them as high-risk AI systems. As such, LEAs using ("deploying") such tools and software will need to comply with deployer obligations under the AI Act. While certainly less extensive than the obligations imposed on the developer ("provider") of the AI system, these obligations nonetheless require substantial efforts, knowledge and preparation from LEAs, including the conclusion of a fundamental rights impact assessment before any new AI-driven OSINT tool can be used. LEAs should be supported in such efforts and with AI Act compliance in general, with specific guidance, training and templates, that are reasonable in terms of the effort required.

Last, but not least, **data protection compliance** is the third major topic of importance. Data protection in OSINT presents several specific challenges, including the need for a legal basis to process personal data in an OSINT use case, with specific additional requirements for special categories of data, which are most likely included in any OSINT application, which is missing or incomplete in many Member States. National transposition of the LED has not been without difficulties and a better overview of the details of the legal situation in the Member States is needed to enable informed discussions, better regulation and better insights for LEAs, tool developers, legislators and civil society alike. While the LED has been a catalyst for a greater focus on data protection in law enforcement and has helped the level of knowledge, awareness and preparedness of LEAs, work remains to be done. A continued focus on awareness raising, training and support of LEAs will be needed to ensure that open source CSAE investigations on the dark web remain in compliance with applicable data protection law, as well as more broadly, with the intentions of the Law Enforcement Directive and the fundamental right to data protection, given the sometimes incomplete national transposition.

The purpose of this paper was to explain the abovementioned issues in some detail **to enable a common understanding, necessary for further debate**. Moreover, for each topic, a policy statement was formulated with some policy recommendations.

However, these issues are not specific to CSAE investigations on the dark web. In general, Europe needs to perform a balancing exercise in relation to effective Law Enforcement in an age of new and rapidly evolving technologies, in particular between privacy and security (of society, in a broad sense). This is the issue at stake in many areas discussed in this paper: the proposed CSAM regulation and the interim derogation to the ePrivacy Directive, the proposed ePrivacy Regulation, the data retention debate, the Passenger Name Record Directive, the regulation of facial recognition in the AI Act, etc. Privacy, including confidentiality of communications, is important, but there is a tradeoff with security and effective law enforcement if information and evidence is not available or not accessible to LEAs, in particular where this is not a technical or organizational challenge, but purely for legal reasons or as a consequence of legal rules (e.g. limited data retention, where data is erased that is later needed for an investigation). Criminals are always quick to adopt new technologies and do not shy away from abusing its potential. LEAs should justifiably be held to a higher standard, and the desire for a safe society should not be an argument to justify a "big brother" approach, where mass surveillance and other forms of unacceptable interference with fundamental rights is commonplace. However, practical ways forward should be defined that prevent law enforcement from "going dark" (i.e. not having (legal) access to the information necessary to perform their tasks) or more generally being forced to fight crime with significantly unequal weapons, putting them and secure societies with them in a losing position from the start. This intent is clearly included in the mission statement of the HLG on access to data for effective law enforcement, which is a good initial step in the direction of defining common solutions for this difficult balancing act between privacy and security.

In the case of open source CSAE investigations on the dark web, the challenges add up: an unclear procedural framework, relatively complex new AI regulation and a significant set of data protection rules, with lacking national transposition. The position of LEAs in this regard is not easy. They must navigate a complex, uncertain and unclear legal framework, in an area (the dark web) that is already at the very center of the tension between secure societies and privacy.

LEAs deserve more legal clarity on the procedural framework for using OSINT, as well as continued (and perhaps intensified) **support** in terms of awareness raising, training and resources to support them in the concrete implementation of a growing body of (complex) regulation on the EU and Member State level. **Without such attention, to allow LEAs to meet the challenges posed by technology, we are putting at risk either the effective performance of the tasks imposed upon them, or compliance with fundamental rights.**

ARICA

Annex A – Questionnaire answered by LEA respondents

Introduction

As part of the ARICA project we are producing a white paper on some of the legal challenges of CSA investigations on the darknet and the use of tools like ARICA in this context.

We would like to better understand concerns from practitioners to inform our work in this regard, hence this survey.

We have chosen to focus on three main topics:

- The legality of the use of OSINT tools
- The use of AI in law enforcement and the AI Act
- The use of personal data in investigations (law enforcement directive)

We would highly appreciate your input by filling in the following questionnaire.

All answers will be treated with complete confidentiality. We only ask for your country (no organizations and certainly no names or other direct identifiers) and **will not identify you or your answers.**

Your answers will be processed by ARICA project partners only and will not be shared onwards. By processing your answers we mean we will read them and try to draw conclusions from them in order to give further direction to the topics discussed in our white paper. **We will not reference any specific answer or set of answers**, but may present very general conclusions, e.g. if all or most respondents note a similar issue, we may mention that issue in general terms.

Some practical details:

- The questionnaire can be filled out in around **10 minutes**
- Most of the questions are quick multiple choice or yes/no questions, others are open questions or fields where more information may be provided
- Depending on your level of detail you may spend a bit more time, which we would greatly appreciate
- You can leave questions open if for example you do not know the answer

We are grateful for your time and for any input you may be able to share with us. This will help us to identify the topics where we need to try and influence policy.

For further information on our activities or for any questions you may have, you can contact us via the contact form at aricaproject.eu.

General questions:

- What country are you based in?

OSINT questions

Introduction

OSINT (open source intelligence) tools use data that is freely accessible on the internet to provide insights. Law enforcement can use such tools for both intelligence activities as well as to collect data in the context of an investigation. When used for investigations, some may argue that this is no longer proper OSINT, as it is not used for intelligence but to support an investigation or to produce evidence.

OSINT typically does not have such a specific regulation under national laws and is usually justified based on general competences of policing especially for the intelligence goals (protecting security, public safety, maintaining order) and investigative general powers related to the duty to detect, prevent and investigate crime for the purpose of investigations.

When specific procedural powers/legal grounds are missing, it is important to remain in compliance with fundamental rights (privacy, data protection). Therefore, OSINT tools should only be used where this is justified, i.e. the use of the tools is necessary in a democratic society (balancing the privacy infringement against the interests that are aimed to be protected), actually contributes to/reaches the goals for which it is used, and there are no less invasive alternatives. OSINT tools that are automated and systematically carry out searches are classified as “high interference” and are not so easily justified. OSINT tools that only involve non-systematic and targeted manual searches are classified as “low interference” and are more easily justified.

Not only the purpose of the tool may be relevant, also the extent of the data utilized in the tool. OSINT tools that use the whole internet as a basis for searches, comparisons and analysis may have higher interference than tools looking at closed networks, and preselected sources (e.g. offender website, darknet forums) because the selection is a safeguard, even if the data is freely accessible.

Questions

- What is your organization’s definition of OSINT? (open question)
- Would you consider a tool like ARICA to qualify as OSINT? (yes/no)
    - Why (not)? (open field)
- If you consider ARICA an OSINT tool, do you think its functions are high interference (e.g. systematic automated monitoring) or low interference (e.g. targeted searches)? (choice: high interference/low interference)
    - Why is this? (open field)
- Generally, is the use of low interference OSINT tools allowed in your jurisdiction in the CSA/CSAM domain, for intelligence, investigations or both? (multiple choice: allowed for intelligence, allowed for investigation, allowed for both, not allowed for either)

- Generally, is the use of high interference OSINT tools allowed in your jurisdiction in the CSA/CSAM domain for intelligence, investigations or both? (multiple choice: allowed for intelligence, allowed for investigation, allowed for both, not allowed for either)
- What is the legal basis used for using OSINT tools if allowed? If more than one option exists, please list them (open question)
- If OSINT tools can be used, are there specific requirements for the use of OSINT tools (high or low interference)? (yes/no)
    - Which are these? (open field)
- Can information gathered with OSINT tools be admitted as evidence? (yes/no)
    - Are there conditions that must be fulfilled? (yes/no)
    - What are those conditions? (open field)
- If evidence gathered with OSINT tools is questioned in court for lack of compliance with procedure or for exceeding competence, does it always become in admissible or is it only inadmissible if it reaches the level of infringing on fair trial (or other fundamental rights like privacy)? (choice: always inadmissible/only inadmissible for infringements of fundamental rights like fair trial)
    - Do you have further comments on this to clarify the situation in your country? (open field)
- When creating a specific database through/for the use of OSINT tools, do specific national requirements apply? (yes/no)
    - What are these requirements? (open field)

AI questions

Introduction

The EU legislator is currently in the process of finalizing the EU AI act. This piece of legislation will have significant implications for Law Enforcement. Tools like ARICA also use various forms of AI for their functionality.

Questions

- Have you deployed AI within your organization before? (yes/no)
    - If yes how often and since when? (open field)
- How do you rate your technical knowledge about AI tools/AI literacy level? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)
- How well do you feel you and your organization know the AI act and the specific requirements that will be applicable to high-risk AI systems used by police (e.g. human oversight, monitoring, fundamental rights impact assessment, where applicable control over input data)? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)

- Do you and your organization feel prepared to implement the AI act's requirements? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)
- Are you and your organization familiar with existing methodologies for ethical AI, such as ALTAI, AP4AI or capAI? (yes/no)
- If you are familiar with any of these methodologies, have you used any of these? (yes/no)
    - If you did, did you feel this covered your needs? (yes/no)
    - Why (not)? (open question)
- Have you and your organization in the past ever conducted a human rights or fundamental rights impact assessment before starting to use a tool? Perhaps as part of a DPIA? (yes/no)

LED questions

Introduction

Tools like ARICA, and most tools used in an investigation will deal with personal data, even if there are no direct identifiers or further steps have to be taken to actually identify a person. Personal data is protected in the law enforcement context by the GDPR and the Law Enforcement Directive (LED). Confusion often exists about when the GDPR applies and when the LED (and national implementation of the LED) applies.

Questions

- In your organization, how would you rate the level of understanding of the distinction between the GDPR and the LED and the distinct scenarios in which these legal instruments apply? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)
- How would you rate the knowledge level of your organization regarding the LED as such, i.e. the rules on the EU level? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)
- How would you rate the knowledge level of your organization regarding the national implementation of the LED? (multiple choice for scoring 1-5 ; 1 = Poor · 2 = Fair · 3 = Good · 4 = Very Good · 5 = Excellent)
- Are you as a LEA allowed under your national law to use third party processors of personal data (e.g. a tool that processes data, a cloud storage provider, etc.) for operational law enforcement purposes e.g. an investigation tool? (yes/no)
    - If yes, what conditions apply to such use? (open question)
- Does it matter if the third party processor is also law enforcement? (yes/no)
    - In what way does this make a difference? (open question)

- How long can data be stored if used in an active investigation (active preservation)? If there are different regimes applicable to different situations, please elaborate (open question)
- How long can data be stored if not used in an active investigation (passive preservation)? If there are different regimes applicable to different situations, please elaborate (open question)
- If data is stored passively (intelligence data for example), can it be used in an active investigation or to start an investigation? (yes/no)
- If you would need to create a specific technical database to run ARICA at your premises, are there national legal requirements to be fulfilled in order to do this? (yes/no)
    - If yes, what are these requirements? (open field)
- Could data collection with OSINT tools be considered excessive in your opinion (breaching the LED principle of data necessity/data minimization)? (yes/no)
    - If yes, does this only apply when the tool entails systematic operations? (yes/no)

End of survey