European Review of Digital Administration & Law - Erdal
2024, Volume 5, Issue 1, pp. 237-256
ISSN 2724-5969 – ISBN 979-12-218-1507-8 – DOI 10.53136/9791221815078 18

*Law Enforcement or Administrative Duty? Decoding Legal Dimensions of Fraud Profiling in Public Administration**

Lena Enqvist
(Associate Professor in Law, specialising in administrative law, Umeå University, Sweden)

Markus Naarttijärvi
(Full professor in Law, specialising in constitutional law, Umeå University, Sweden)

ABSTRACT This article examines the integration of data analytics and automated fraud-detection systems within welfare sectors, focusing on the evolving legal landscape in Europe. Throughout Europe, the use of advanced technologies to monitor welfare payments has intensified. However, large-scale data profiling raises significant legal challenges, exemplified by the judicial scrutiny of the Dutch SyRI system, which was found to violate the European Convention on Human Rights and the General Data Protection Regulation (GDPR). This study addresses a pivotal question: whether the use of such systems under EU law constitutes law-enforcement activities or routine administrative operations. This classification impacts the legal framework—GDPR or the Law Enforcement Directive (LED)—governing data processing practices, and influences obligations under the forthcoming EU Artificial Intelligence Act. Through an analysis of European law, including GDPR, LED, the EU Charter of Fundamental Rights, and relevant case law, this article highlights the complexities of this legal demarcation and the potential for conflicting regulatory incentives. Swedish examples are used to illustrate how different legal and institutional setups affect these issues, offering insights into the broader implications for the legality and governance of fraud detection systems.

KEYWORDS: Fraud detection – Artificial Intelligence Act – GDPR – Law Enforcement Directive – Automated decision-making

1. *Introduction*

In an era marked by rapid technological advancements and concerns over benefits fraud, the use of data analytics and profiling through automated fraud-detection systems has in many countries emerged as a prioritised measure. The implementation of fraud-prevention and detection systems is visible across welfare sectors, partly driven by new and emerging forms of fraudulent activities and partly by new and enhanced tools of detection.[1] These developments have also acted as drivers to centralise or pool welfare data to allow for further analytics, where states leverage advanced technologies and implement automation and data analytics to centrally monitor payments originating from welfare systems via IT-based methods, representing the growing public-sector belief in the ability of technological-fraud detection. Examples include the new Swedish Payment authority [Utbetalningsmyndigheten], which commenced its operations in 2024, the Danish Payment authority [Udbetalning Danmark] which has been in operation since 2015, and the risk assessments performed by the Department of Work and Pensions in the United Kingdom.[2]

While these authorities are indicators of a larger trend towards centralisation of detection

* Article submitted to double-blind peer review.
This work was supported by the Swedish Research Council under Grant number 2020-02278.

[1] See S. Ranchordás and Y. Schuurmans, *Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations*, in *European Journal of Comparative Law and Governance*, vol. 7, no. 1, 2020, 5-42; M. Zaiko, *Automated government benefits and welfare surveillance*, in *Surveillance and Society*, vol. 21, no. 3, 2023, 246-258.

[2] See Swedish Government bill 2022/23:34 *Utbetalningsmyndigheten*, 2022; Swedish Government Enquiry (SOU) 2020:35 *Kontroll för ökad tilltro - en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen*, 2020, 213–214. See also Swedish Government Enquiry (SOU) 2023:52 *Ett stärkt och samlat skydd av välfärdssystemen*, 2023, 204-205.

systems, similar detection systems have already existed in specific administrative sectors such as taxation and social welfare, sectors where deployed systems have already indicated the potential risks involved with large-scale data analytics and profiling of citizens.

Instances where the legality of fraud-detection systems have come under scrutiny can be found in the case of the so-called SyRI system. This profiling system, employed by the Dutch government, was subject to judicial review by a national court, which found the authorising legislation to conflict with Article 8 of the European Convention on Human Rights (ECHR) and the right to private life. The system was also scrutinised by the national data-protection authority, which fined the administration for discriminatory profiling in breach of Article 6(1) of the General Data Protection Regulation (GDPR),[3] as well as the lawfulness and transparency principles under Article 5(1)(a). The system was further, based on a separate assessment, found to be in breach of the principle of fairness as expressed in Article 5(1)(a) GDPR.[4] While neither the EU Charter of Fundamental Rights (the Charter)[5] or the European Convention of Human Rights (ECHR)[6] impose a blanket ban on profiling systems for fraud detection, they underscore the sensitive and intricate legal challenges associated with such systems. The same holds true for data-protection regulations like the GDPR and the Law Enforcement Directive (LED).[7]

While there appears to be a clear trend towards implementing fraud-detection systems, there is also significant diversity possible in the approach to such systems. They can employ various techniques, operational logics, and involve diverse types and volumes of personal-data processing. These systems can also conduct a variety of different profiling activities, displaying differences in their recommendations and attributed functions within the organisational setting of the deploying authority. They can serve broader purposes beyond mere fraud detection, such as internally alerting authorities to cases that warrant further investigation. Additionally, they may be employed in situations where the responsible authorities have mandates akin to criminal investigators. Consequently, depending on their legal, organisational, and technical setup, profiling systems used for fraud detection may encounter or conflict with national or European legal frameworks in different ways.[8]

This article will focus on one pivotal question affecting the regulatory framework for such systems: Whether their use should be categorised – under EU law – as a law-enforcement practice or as an element of routine administrative-agency operations. The answer to this question carries consequences for whether the conditions for processing personal data required for profiling practises should be evaluated within the framework of the GDPR or the LED (which serves as *lex specialis* in relation to the GDPR within its area of application). The answer to this question also carries implications for the obligations and restrictions on such systems imposed by the EU Artificial Intelligence Act (AIA).[9] Our analysis will focus on one context

[3] 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) [2016] OJ L 119/1.

[4] S. Barros Vale and G. Zanfir-Fortuna, *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, Future of Privacy Forum 11 at https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf, accessed 26 June 2024.

[5] Charter of Fundamental Rights of the European Union, 2000, OJ C 364.

[6] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended), 1950.

[7] 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.

[8] The article cannot offer a comprehensive overview of the various types of profiling systems currently employed for fraud-detection purposes by public authorities in EU Member States or globally. This is due to the diverse structures of these systems and the confidentiality or trade-secret rules that often obscure their exact mechanisms from external viewers, as exemplified in, for example *Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations,* cit., 5-42; *Automated government benefits and welfare surveillance,* cit., 246-258.; E. Degrave, *The Use of Secret Algorithms to Combat Social Fraud in Belgium*, in *European Review of Digital Administration & Law*, vol. 1, no. 1-2, 2020, 167-178; M. van Bekkum and F. Z. Borgesius, *Digital welfare fraud detection and the Dutch SyRI judgment*, in *European Journal of Social Security*, vol. 23, no. 4, 2021, 323-340, and section 2.

[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending regulations

illustrating the challenges and effects of making this distinction, namely in situations where entities like social security authorities employ profiling technologies which process personal data for the specific objective of detecting fraud. Through this analysis, we aim to highlight the complexities surrounding the demarcation criteria determining the relevant legal framework for such systems, and how these demarcations may lead to somewhat conflicting logics and incentives. In particular, we identify drivers that could incentivise national legislators or implementing authorities to position such profiling practices under the regulatory framework that governs the law-enforcement domain and the implications this may carry for the lawfulness of processing. We will approach these issues through an analysis of European law, primarily the EU data-protection regulation in the GDPR, the LED and the Charter, as well as the AIA, and the case law from the CJEU interpreting each instrument. As the ECHR forms a lowest acceptable level for the protection of fundamental rights in the EU context, we will also analyse relevant case law from the European Court of Human Rights (ECtHR). To illustrate the demarcation issues, we will primarily draw examples from the Swedish administrative context. The aim of these examples is not to provide a complete assessment of their legal implications, but rather to show how different legal and institutional setups can impact the overall demarcation issues we study.

Before beginning our analysis, we will just briefly address the choice of terminology, specifically 'fraud detection'. Using 'fraud detection' as part of the overall description of these systems may indicate that what the systems detect is actually fraud, which is not necessarily true. While the term implies a connection to criminal-law definitions of fraud (which may vary from jurisdictional context), it is important to note that fraud-detection systems are not necessarily aimed solely at such activities, but rather at identifying erroneous applications or payments, or benefit claims carrying a higher-than-normal risk of errors. These may in some cases be the result of intentional fraud (from minor distortions of the truth, to more elaborate schemes),[10] but can also be caused by honest mistakes, misunderstandings, or be based on inaccurate information provided by the authorities themselves. Furthermore, the systems may of course indicate faults or risks that do not in fact exist, with potentially grave consequences for targeted individuals.[11] As such, we use the term *fraud-detection systems* here to refer to profiling systems for a wide range of fraud-detection purposes, mindful of these complexities rather than as a normative statement accepting the presupposed function of these systems.

2. *The Legal pertinence of typical fraud-detection-system characteristics*

In essence, fraud detection is intricately linked to the broader framework of crime prevention and prosecution – a range of activities that have grown in relevance for social-welfare agencies in the face of a general trend of criminalisation of welfare-related issues, and the development of what has been described as the welfare-surveillance state.[12] However, the extent to which the role of fraud-detection systems extends beyond mere identification of cases in need of further scrutiny, and the extent to which the 'flags' raised by the systems within the authority are seen as standalone investigations capable of determining the occurrence of fraud, may vary.[13]

Furthermore, profiling practices within these systems generally necessitate the processing of personal data, and in some instances, sensitive and special-category data. Although the GDPR has a broad material scope, it does not apply in all settings that personal data are processed. Of interest here is that those public activities which qualify as law-enforcement activities under the LED render the GDPR inapplicable.[14] Notably, the LED (despite its popular name) does not define nor make any explicit references to 'law enforcement'. Decisive for the assessment are instead two cumulative

(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).

[10] *Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigations,* cit., 10–11.
[11] See, for example, *Automated government benefits and welfare surveillance,* cit., 253–254.
[12] See K. Gustafson and S. Kaaryn, *Cheating Welfare: Public Assistance and the Criminalization of Poverty*, New York, New York University Press, 2011; *Automated government benefits and welfare surveillance,* cit., 249–251.
[13] See, for example, *The Use of Secret Algorithms to Combat Social Fraud in Belgium,* cit., 167-178.
[14] Recital 19 GDPR and Articles 1, 2 and 9 LED.

criteria. The personal data must be processed by an authority which qualifies as competent under the LED, for purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.[15] Whether an authority's use of a fraud-detection system relates to the GDPR or LED impacts the legal conditions for processing personal data for fraud-detection purposes, where generally the LED tends to take a more permissive stance to processing personal data for law-enforcement purposes.[16]

Confidentiality rules and trade secrets often apply to aspects of how a profiling system used for fraud detection by public authorities, such as social-security agencies, operates. In such cases, this results in intransparency and difficulties in establishing the detailed workings of these systems.[17] Consequently, it can be challenging for outsiders to determine whether these technologies involve AI technologies or employ machine-learning techniques. However, this article will proceed on the assumption that such systems may rely on technologies classified as AI, as well as sometimes including those based on machine learning. These systems typically operate by drawing inferences from the analysis of large datasets to make specific predictions or categorisations.[18] While there are different conceptions of 'artificial intelligence', our assumption also holds that the operational logic and technology in many cases align with the legal definition of AI established in the AIA, according to which an 'AI system' is a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'.[19]

Just as within the realm of data processing, however, the AIA provides different internal regulatory-governance schemes contingent upon whether the regulated activity is categorised as law enforcement or falls outside such a classification. A difference is that the applicability of the AIA is not dependent on the designation of an activity or system as 'law enforcement', but rather on which specific conditionalities and exceptions within the AIA will become applicable. Contrary to the LED, the AIA does provide separate definitions for both 'law enforcement authority' and 'law enforcement'. The first definition is actor-oriented and defines law-enforcement authorities as any public authority competent for 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; or any other body or entity entrusted by Member-State law to exercise public authority and public powers for these purposes.[20] The second definition is task-oriented and defines as 'law enforcement' activities carried out by law-enforcement authorities for 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.[21] The attentive reader will here note that the LED definition of 'competent authority' corresponds verbatim to the AIA's definition of 'law enforcement authority', implying a common delineation but also raising questions regarding the functional intertwinement between the two instruments for AI systems utilised for fraud-detection purposes.

As per usual, EU law definitions of law enforcement, competent authority, criminal offence *etcetera*, are autonomous and must be interpreted independently of any national understanding of these terms.[22] The national

[15] Articles 1(1) and 2(1) LED. It may also be noted that the application scope of the LED is also delimited by Article 2(3) as it does not cover processing operations that fall outside the scope of EU law, and by EU institutions, bodies, offices and agencies.

[16] N. Purtova, *Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships,* in *International Data Privacy Law*, vol. 52, no. 8, 2018, 59; P. de Hert and V. Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive: A First Analysis,* in *New Journal of European Criminal Law*, vol. 7, no. 1, 2016.

[17] See, for example, *The Use of Secret Algorithms to Combat Social Fraud in Belgiu*m, cit., 167-178; *Digital welfare fraud detection and the Dutch SyRI judgment,* cit., 323-340.

[18] See, for example, *The Use of Secret Algorithms to Combat Social Fraud in Belgium,* cit., 167-178

[19] Article 3(1) AIA.

[20] Article 3(45) AIA.

[21] Article 3(46) AIA.

[22] It is settled case-law that the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its

conception of what tasks are to be considered as law-enforcement tasks or what agencies are to be considered as law-enforcement authorities or competent to prevent or investigate criminal offences is therefore not decisive for whether this also corresponds to the EU conception.[23] Member States cannot at their own discretion choose whether the utilisation of a fraud-detection system by public authorities such as social-security agencies qualifies as a law-enforcement task performed by a competent authority. Both the LED and the AIA define the tasks and purposes of law enforcement broadly and in corresponding ways – and open for possibly also including fraud-detection systems used by public authorities not commonly associated with law-enforcement tasks, such as social-security agencies. These corresponding definitions suggest an intention to synchronise the applicability of the LED and certain high-risk designations of the AIA with regards to law-enforcement systems. As the classification will impact the lawful deployment and the protective regulations applicable to such systems during their training and utilisation, the following two sections will explore these effects in more detail, before we turn to discuss more closely how the demarcation of the applicability between the different instruments is to be determined. In other words, we will intentionally address the question of applicability *after* discussing some of the implications of each framework, in order to frame this discussion within a clearer understanding of the effects of this applicability for profiling systems used for fraud-detection purposes.

3. *The GDPR and the LED as two distinctive data-protection frameworks*

3.1. *It is either the GDPR or the LED – profiling practises rarely escape EU data protection*

Through the GDPR and the LED, the current EU data-protection legal framework has developed to recognise two distinct regimes of data protection that could potentially apply to profiling practises for fraud-detection purposes when performed by administrative authorities such as social-security agencies.[24]

As the LED is *lex specialis* and an exception to the GDPR, a suitable starting point is to clarify that the GDPR should in principle always apply when such authorities use a fraud-detection system in their activities (unless the LED becomes applicable). As fraud-detection systems which operate through profiling often process case-related data of transactional and individual nature, they typically rely on the processing of data classified as personal data under the GDPR.[25] The GDPR uses identifiability as the primary demarcation criterion for personal data, rather than the information alone having qualities that allow the data subject to be identified, the concept of personal data thus has the potential for expanding through a very wide range of data. This is especially true in so-called big data settings such as profiling practices – where large sets of data are combined to make inferences. Consequently, it does not matter whether the purpose of the system is to result in identification; what matters is whether the data can be combined in ways that allow identification.[26] Our assumption is therefore that fraud-detection systems based on profiling techniques rarely, and only in very limited circumstances, escape the applicability of data-protection rules.

meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union, see Case C-439/19*,* *Latvijas Republikas Saeima,* EU:C:2021:504, 81; C-595/20, *ShareWood Switzerland*, EU:C:2022:86, paragraph 21; Case C-300/21, *Österreichische Post AG,* ECLI:EU:C:2023:370, 29.

[23] See Case C-439/19, *Proceedings brought by B*, Judgment of the Court (Grand Chamber) of 22 June 2021, ECLI:EU:C:2021:504, 84.

[24] See *Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships,* cit., 59.

[25] The GDPR defines personal data very broadly in Article 4(1), as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[26] See for example, Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, EU:C:2016:779; Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, EU:C:2017:994; 'Are Personal Data Always Personal? Case T-557/20 SRB v. EDPS or When the Qualification of Data Depends on Who Holds Them' (*European Law Blog*, 7 November 2023) at https://europeanlawblog.eu/2023/11/07/are-personal-data-always-personal-case-t-557-20-srb-v-edps-or-when-the-qualification-of-data-depends-on-who-holds-them/, accessed 26 June 2024.

3.2. *Legal basis*

While the reasoning above forms the basis for a broad applicability of the GDPR in relation to profiling practices, the basic legality of such personal-data processing, however, hinges on it having a lawful basis under the GDPR.[27] To be lawful, the processing must be based on at least one of the explicit bases for lawful processing in Article 6 GDPR, where especially 6(1)(c) stating that the processing is necessary for compliance with a legal obligation, or 6(1)(e), that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, are possible bases for authorities' profiling practises for fraud-detection purposes.[28] Of note is that Article 6(3) GDPR for both bases requires that there is a further basis for this processing laid down in Union or Member-State law, thus emphasising that such processing must be limited to what is necessary to perform lawfully recognised practises. Here, Article 6(1)(c) requires such further basis for the obligation to process personal data and 6(1)(e) that the task of public interest have such a basis. The reference to a further basis in Union or Member-State law should, however, not be taken as implying an unfettered discretion for the Member States to impose regulatory duties or tasks on public administrations such as social-security agencies for allowing the processing of personal data to the extent they see fit. Any national legislation invoked under these opening clauses of the articles 6(1)(c) or (e) cannot undermine the content and objectives of that regulation, as well as have to respect the GDPR requirements of articles 5 and 6 (where Article 5 GDPR outlines the principles for processing personal data, emphasising lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality, while Article 6 entails the above-mentioned lawful bases for processing personal data).[29] The precise delimitation of Articles 6(1)(c) and (e), the terms of the data-processing practices they can accommodate, as well as the precise scope these provisions leave to national legislators to create possibilities for personal-data processing, are, however, all outside the scope of this article.

While there are at least two, rather wide legal bases relevant to fraud-detection systems under the GDPR, the LED only has one. It defines this legal basis in Article 8(1) solely with regard to the necessity of the processing for the performance of a task carried out by a competent authority for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, including safeguarding against and prevention of threats to public security. This clear connection between necessity and the specific law-enforcement aims can potentially create some complexities for fraud-detection systems falling under the LED, if they fulfil additional functions beyond the context of preventing, investigating or detecting crimes. All data that might be relevant for assessing eligibility for benefits may not be relevant for the tasks relating to law enforcement, and the test of necessity employed by the CJEU tends to be strict.[30]

Through Article 8(2), the LED sets up some minimum requirements for Member-State law regulating the processing under the directive, stating it needs to 'specify at least the objectives of processing, the personal data to be processed and the purposes of the processing'. Recital 33 of the LED connects this to the need for clear and precise legal rules, with their application foreseeable for those subject to it, 'as required by the case-law of the Court of Justice and the European Court of Human Rights'. Indeed, the principle of legality as enshrined in the Charter and the ECHR, as well as in the provision on lawfulness in the GDPR and LED, highlights the need for a clear, specific, transparent, and

[27] Article 5(1)(a) GDPR.

[28] See L. Enqvist, *Rule-based versus AI-driven benefits allocation: GDPR and AIA legal implications and challenges for automation in public social security administration*, in *Information & Communications Technology Law*, vol. 33, no. 2, 2024, 7–8.

[29] Case C-34/21, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums*, EU:C:2023:270, p. 59; Case C-319/20, *Meta Platforms Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, EU:C:2022:322, 60; *Rule-based versus AI-driven benefits allocation: GDPR and AIA legal implications and challenges for automation in public social security,* cit., 5 ff.; V. Gantchev, *Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?* in *European Journal of Social Security*, vol. 21, no. 1, 2019, 9 ff.

[30] See M. Tzanou, *Article 8 – lawfulness of processing*, in Costa & Boehm (ed.) *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, Incorporated, 2024, 202.

precise, legal basis with sufficient safeguards to protect against abuse, for the processing of personal data, especially in the context of automated processing.[31] As these cases are based on the Charter and the ECHR, these requirements apply independently of whether the processing takes place under the GDPR or the LED.

In sum, we can thus see that finding a legal basis for fraud-detection systems is likely not a problem under either framework. However, we can also see that the legal basis under the LED is more tightly connected to the necessity of the processing for the specific law-enforcement task. We can further see that there is need for a clear legal mandate to process personal data for fraud-detection purposes under both the GDPR and the LED. This need for a clear legal mandate is even greater as we move to the question of special-category data.

3.3. *Special-category data*

So far, our discussion has considered only the general requirements of lawful bases for processing personal data as outlined in Article 6 of the GDPR. For profiling systems, however, one additional factor to consider is that such systems are likely to process data that have been afforded special protection under both the GDPR and the LED.

Firstly, such systems are likely to process data which qualify as special-category data under Article 9 GDPR (meaning data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic, and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation). If this is the case, processing according to the article is prohibited unless one of the article's enlisted derogations apply. Similarly to the emphasis on 'identifiability' as determinate for what type of data constitute personal data under the GDPR, the CJEU has also stressed a functional approach to delineating special-category data. In *OT v Vyriausioji tarnybinės etikos komisija*, for example, the court stated that data capable of leading to inferences about special categories through intellectual operations such as deduction or cross-referencing, fall under the purview of special-category data as outlined in Article 9.[32] In this context, it should be noted that profiling systems for detecting social-security fraud typically require processing vast amounts of data, which increases the likelihood of enabling inferences about special-category data relating to natural persons.[33] Whether this is the aim of the system is not determinate.[34]

Since many profiling systems used for fraud-detection purposes thus will involve personal-data processing covered by the main prohibition rule of Article 9, it becomes relevant to examine the possible derogations from this prohibition allowed by the article. Here, Article 9(2)(g) contains the most relevant derogation, as it allows for processing necessary for reasons of substantial public interest, on the basis of Union or Member-State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Recital 52 expressly mentions social-protection law including pensions and health security as domains of public interest that may specifically allow for derogation from the prohibition of processing special-categories of personal data. Of note is, however, that this derogation hinges on there being a further basis for the specific processing in Union or Member-State law, thus emphasising that the processing must be limited to what is necessary to perform lawfully recognised practises. Any such legislation must also be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[35] In other words, careful consideration is needed at the legislative level (which in the case of the social-security domain remains under the purview of the Member States) to design a legal framework including a protective regime (safeguards) that

[31] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, EU:C:2014:238, 54 –55; Joined cases C- 203/ 15 and C- 698/ 15, *Tele2*, EU:C:2016:970, p. 117; Case C-623/17, *Privacy International*, EU:C:2020:790, 68.

[32] Case C-184/20, *OT v Vyriausioji tarnybinės etikos komisija*, EU:C:2022:601, 123.

[33] See A. Simonofski, T. Tombal, C. De Terwangne, P. Willem, B. Frenay, and M. Janssen, *Balancing fraud analytics with legal requirements: Governance practices and trade-offs in public administrations*, in *Data & Policy*, vol. 4, no.14, 2022, 13.

[34] EDPB guidelines on profiling, 15.

[35] Article 9(2)(g) GDPR.

is GDPR compliant when processing special-category data.

Secondly, to the extent that profiling systems for fraud-detection purposes will also process data relating to criminal convictions and offences or security measures, compliance with the protective regime for these data, as prescribed in Article 10 GDPR, must also be ensured. The article's function must be read in relation to the LED, as it applies to processing by private bodies and public bodies that are not competent authorities under Article 3(7) LED, or made for the purposes listed in Article 2(2)(d) and Article 1(1) LED. It thus seeks to ensure that criminal-data processing adheres to the GDPR's principles and includes appropriate safeguards in those cases when the LED is not applicable. Of note is that Article 10 lays down a subjective restriction on who may process data on criminal offences rather than setting out the purposes for which such data may be processed.[36] Unlike Article 9, Article 10 thus does not set out any main rule prohibiting the processing of data relating to criminal convictions and offences or security measures. The article instead holds that the processing of such data is only lawful when carried out under the control of an official authority (or when authorised by relevant Union or Member-State laws with safeguards). The article also holds that any comprehensive criminal-conviction registers must be under official authority's control.

While the main restriction in Article 10 GDPR is subjective, the CJEU has emphasised that it aims to ensure enhanced protection because of the particular sensitivity of the data at issue (which is liable to constitute a particularly serious interference with the fundamental rights to respect private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter).[37] The court has also stressed that the legislation allowing for processing of data as protected under Article 10 must be justified, and in particular proportionate, for the purpose of achieving the objectives pursued.[38] It further emphasised that the term 'criminal offence' has an autonomous meaning within EU law. The classification given by the Member State of an offence, such as an administrative rather than criminal offence, is not therefore conclusive for determining the applicability of Article 10 as the classification may vary from one country to another. The settled criteria include the legal classification of the offence under national law, the intrinsic nature of the offence, and the degree of severity of the penalty that the person concerned is liable to incur.[39] This fairly broad conception of criminal offences suggests that Article 10 is relevant to profiling practices for fraud detection not only when data related to criminal offenses are processed, but also when the intent behind the profiling (fraud detection) may bring the data within the applicational scope of the article. The French Supreme Administrative Court, *the Conseil d'Etat* has, for example, held that personal data relating to criminal offenses in addition to data on the offenses as such also cover data which are processed with the sole objective of establishing the existence or preventing the commission of offenses.[40] One could at least argue that when profiling leads to outcomes raising suspicions of fraud specific enough that the authorities must address them, that this context would bring the data processed under the purview of Article 10. As Article 10 predominantly restricts who may process data related to criminal offenses – an official authority or an actor authorised by Union or Member-State law providing for appropriate safeguards for the rights and freedoms of data subjects – this limitation has minimal impact in public social-security context of interest here. However, it does suggest the need for legislation to establish higher standards and safeguards for processing data concerning criminal convictions and offenses under the GDPR.

While the GDPR contains a main rule prohibiting the processing of special-categories of data, with certain exceptions, the LED – as it takes aim at specific actors – instead allows it through Article 10 LED, but subjects the processing to a strict necessity test, contingent upon appropriate safeguards for the rights and freedoms of the data subject. Furthermore, processing of such data needs to

[36] Opinion of Advocate General Campos Sánchez-Bordona delivered on 25 May 2023 in Case C-667/21, *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts,* Request for a preliminary ruling from the Bundesarbeitsgericht, EU:C:2023:433, 56.
[37] Case C-439/19, cit., 74 ff.
[38] *Ibid*., 106.
[39] *Ibid*., 87 and referenced case law.
[40] CE, 11 May 2015, 375669, Rec. Lebon; On this, see W. Maxwell, *The GDPR and Private Sector Measures to Detect Criminal Activity*, 1 March 2021, 17 ff., at https://papers.ssrn.com/abstract=3964066 accessed 29 May 2024.

be authorised by Union or Member State law; be processed to protect the vital interests of the data subject or of another natural person; or relate to data which are manifestly made public by the data subject. For some time, it was uncertain how this strict necessity requirement for the processing of special categories of data under the LED was to be interpreted, given that the CJEU, based on the Charter, had gradually begun imposing a strict necessity test for processing non-sensitive personal data.[41] In January of 2023, the CJEU clarified this in the case of *Criminal proceedings against V.S.* concerning the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution.[42] The court here found that the term 'only where strictly necessary' in Article 10 LED underlined that 'the processing of special categories of data, within the meaning of Article 10 [LED], will be capable of being regarded as necessary solely in a limited number of cases. Second, the fact that the necessity for processing such data is an 'absolute' one [('absolue')] signifies that that necessity is to be assessed with particular rigour'.[43] For fraud-detection systems, this ruling contains a few interesting findings. Firstly, that this level of necessity will only be reached in a limited number of cases and cannot be a standard operating procedure. Secondly, that that this level of necessity entails particularly strict checking that the requirement of data minimisation under the LED has been met. Finally, the court found that consideration must be given to the nature of the objective pursued, connecting the processing to 'the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats'.[44] While this case relates to biometric and genetic data, which can arguably be said to be very sensitive, the statements of the CJEU concern the strict necessity test relating to all types of special-category data. It highlights that the use of sensitive-category data in fraud-detection systems falling under the LED would need to be an exception, rather than the norm, and that the absolute necessity of that data needs to be closely monitored.

As we can see, the need for a clear legal basis becomes even stronger for special-category data and data relating to criminal offences. However, beyond this, we can also see that the discussions relating to the *proportionality* of processing special-category data in the law-enforcement context suggests a very strict assessment of this processing. While the use of special category data in the regular assessment of eligibility for benefits should be relatively common within welfare agencies, it is worth noting that processing of such data in the fraud-detection context may be viewed with significantly more stringency. There is a sliding scale between systems that assess the eligibility of individuals for benefits, and those that try to identify fraudulent applications. It is also worth noting that as a system slides further towards fraud detection, and consequently towards law enforcement, the strictness in the required specificity of the legal basis for processing special category data, as well as the strictness in the proportionality assessment of processing such data, is likely to increase significantly. In a system that falls under the LED, recent CJEU case law suggests that a strict, individual, proportionality assessment is needed in each case, to ensure that such processing becomes the exception, rather than the norm.

3.4. *Profiling and automated decision-making*

As seen so far, the GDPR imposes a number of requirements for safeguards to be observed when personal data are processed under Article 6, as well as where applicable also under Articles 9 and 10. As also seen, the GDPR in these cases imposes requirements for additional legal support for the processing through a legal obligation or established public task in Union or Member-State law. While this implies rather high-set requirements for processing data in the context of profiling for fraud-detection purposes, the regulation does contain possibilities to establish a legal basis for such processing. The fact that the particular processing of interest here is 'profiling', also raises the question of whether the regulations

[41] See M. Naarttijärvi, *AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity*, in E. Gill-Pedro, A. Moberg (eds.) YSEC Yearbook of Socio-Economic Constitutions, Springer, Cham, 2023.
[42] Case C-205/21, *Criminal proceedings against VS*, EU:C:2023:49.
[43] *Ibid*., 118.
[44] *Ibid*., 73.

applicable to fully automated decision-making should be considered applicable. This is because Article 22 is the only article in the GDPR that expressly refers to profiling, stating that the data subject 'shall have the right not to be subject to a decision based solely on automated processing, including profiling'. It has been established through case law that the article should be read as entailing a main rule of prohibiting *fully* automated decision-making.[45] If this prohibition were to apply to profiling practices for fraud-detection purposes in the public social-security domain, the applicability of the GDPR could effectively lead to a dead end for such practises (although, as we will see, the article also contains possible derogations from this prohibition). The scope and meaning of the article are thus of great importance for the prospective lawfulness of these practices.

The wording of Article 22 implies that a 'mere' profiling system, in the sense that it does not make any decisions related to its findings on suspected fraudulent activities, may also fall under the scope of the Article 22 prohibition.[46] However, because the definition of 'profiling' in Article 4(4) refers to 'any form of automated processing', and not just solely automated processing as in the case of Article 22, the GDPR can be said to recognise that decisions may be based on profiling without leading to a solely automated decision.[47]

To make sense of Article 22 in a context of profiling for fraud-detection purposes, one must start by determining whether the article applies at all. The applicability is contingent upon three cumulative criteria, that there must be a 'decision', that the decision must be 'based solely on automated processing, including profiling', and that it must produce legal effects concerning the interested party or similarly significantly affect him or her.[48] All of these criteria were elaborated by the CJEU in the 2023 *OQ v. Land Hessen* case. Here the court initially stated that while Article 22 lacks a definition of 'decision', it is apparent from the very wording of that provision that that the concept refers not only to acts which produce legal effects concerning the person at issue, but also to acts which similarly significantly affect him or her. As a result, the court found that it is not precluded that a result of a profiling exercise may count as a fully automated decision within the meaning of Article 22. The key issue in the case was whether Article 22(1) should be interpreted to mean that a credit-information agency automatically generating a probability score based on an individual's personal data to assess their future ability to meet payment commitments, constitutes 'automated individual decision-making'. The further context was also that a third party, which receives this probability score, relies heavily on that score to decide whether to establish, implement, or terminate a contractual relationship with the individual.

Against this background, the courtfound it to be apparent from the wording of Article 22, further emphasised in Recital 71, that the inclusion of acts which similarly significantly affect him or her expands the concept of a decision beyond merely those that produce legal effects concerning the person at issue.[49] The court therefore concluded that the concept is broad enough to encompass the result of calculating a person's creditworthiness in the form of a probability value concerning that person's ability to meet payment commitments in the future.[50] Regarding the second criteria, that the decision must be 'based solely on automated processing, including profiling', the court found that profiling practises that meet the definition of 'profiling' in Article 4(4) GDPR meet the criteria of being 'automated'.[51] Regarding the third criteria, that the decision must produce 'legal effects' concerning the person at issue or affect him or her 'similarly significantly', the court found that situations where a third party to whom the probability value is transmitted draws 'strongly' on that value, affect, at the very least, the data subject significantly.[52]

Through the judgement, the CJEU has emphasised the effect-oriented approach of Article 22 in determining whether the output of a profiling system should fall under its purview. The case therefore spurred some

[45] Case C-634/21, *OQ v Land Hessen*, EU:C:2023:957, 52.
[46] R. Binns and M. Veale, *Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR*, in *International Data Privacy Law*, vol. 11, 2021, 319.
[47] Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, 9.
[48] Case C-634/21, cit., 43.
[49] *Ibid*., 44.
[50] *Ibid*., 46.
[51] *Ibid*., 47.
[52] *Ibid*., 48-51.

discussions around whether specifically profiling practises for fraud-detection purposes now will fall under the Article 22 main rule of being a prohibited practise.[53] Our view is that the case does not give rise to the view that *any* profiling carried out in a social-security context for anti-fraud purposes should be considered to render the article (and its prohibition) applicable. Following the effect-oriented approach, the decisive factor should be the impact of the profiling on the individual. In cases where the findings of a profiling system directly lead to retributive actions by the authority—such as making a recovery decision or issuing a notification of suspected fraud intended to trigger a criminal investigation— the result of the profiling will likely be regarded as a decision which has been made fully automated under the article. Consequently, the general prohibition on such practices would apply. While there is no international or European overview over the use or technical configuration of systems used for profiling for fraud-detection purposes within social-security administration, it could, however, be assumed that such systems in most cases produce outputs which indicate risk of deviations, fault or fraud rather than establishing that fraud has occurred. It is therefore also likely more common that the results of profiling practices within authorities such as public social-security agencies lead to extended investigations within the authority rather than directly resulting in decisions regarding an individual's entitlement to benefits, including whether any fraudulent activities have occurred. Profiling practices that do not directly lead to such effects, but rather result in a case being flagged within the authority and investigated manually, or at least require human intervention before a decision is made, should therefore not be considered as falling under the prohibition.[54] However, the extent to which individual (human) decision-makers are organisationally and practically able to make independent and informed assessments rather than leaning too heavily on algorithmic predictions is a factor to consider in assessing compliance with Article 22 in this context.[55]

All in all, there is reason to assume that many profiling systems used for fraud-detection purposes within social-security administration will escape the application of Article 22 even considering the CJEU's clarification of the article's applicational scope in the *OQ v Land Hessen* case. However, the case does make clear these administrations will still need to assess thoroughly whether the specific use of a profiling system for these purposes includes a strong enough link between the profiling activity and significant effects on the individual whom the system has identified. Due to the lack of case law for these specific domains, which have different arrangements and characteristics from the credit scoring system examined by the CJEU in *OQ v Land Hessen*, this assessment is likely to be challenging. Note could be taken that in the initially mentioned *SyRi* case, where a fraud-detection system used by the Dutch Tax and Customs Administration was found to be in breach of Article 8 ECHR, the national Data Protection Authority, DPA, did not find that the system triggered the application of Article 22 GDPR.[56] Whether a system supports 'mere' profiling or rather is intricately linked with any decision-making is contingent upon how the assessment results of the profiling are leveraged. All in all, however, Article 22 does not aim at directly regulating profiling as a standalone practice within the GDPR, and 'mere' profiling does not trigger its application.

In those cases where the use of a profiling system by social security agencies does trigger Article 22, the article's (2)(b) provision contains a possible derogation from the

[53] T. Hartmann, *EU top court's ruling spells trouble for scoring algorithms*, in *Euroactiv*, 7 December 2023, www.euractiv.com/section/data-privacy/news/eu-top-courts-ruling-spill-trouble-for-scoring-algorithms (accessed 10 June 2024).

[54] *Rule-based versus AI-driven benefits allocation: GDPR and AIA legal implications and challenges for automation in public social security administration*, cit., 4 ff.

[55] See, P. Davis and S. F. Schwemer, *Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making*, in Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2023), held in conjunction with ICAIL 2023, June 19, 2023, available at SSRN: https://ssrn.com/abstract=4478107 or http://dx.doi.org/10.2139/ssrn.4478107; T. Enarsson, L. Enqvist and M. Naarttijärvi, *Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts,* in *Information & Communications Technology Law*, vol. 31, no. 1, 2022, 123.

[56] *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, cit.

prohibition of fully automated decision-making. However, the derogation comes with additional requirements for the lawful implementation of profiling practises in such cases. For one, the derogation only applies if there is further legal support under Union law or Member-State law which enables the practice. Furthermore, there must also be safeguards in place which are applied in addition to those required by other applicable GDPR articles. These requirements vary depending on the type of data used in profiling, such as special-category data, although the same type of safeguarding measure can satisfy multiple article-requirements simultaneously. In those cases where lawful profiling practises hinge on the (2)(b) derogation being applicable, an interesting aspect is that it is the automated processing, including the decision-making, that must be 'authorised' by Union or Member-State law. The CJEU in *OQ v Land Hessen* indicates that this legal authorisation cannot be too broadly defined to justify processing under (2)(b). If profiling for fraud-detection purposes is used in contexts where the outcomes directly affect individuals, national legislators may therefore need to review existing laws to ensure they are sufficiently precise to allow for an assessment of the authorisation's proportionality in relation to the intended goals of preventing or combating fraud. Ultimately, this could affect the degree to which the authorities' obligations to combat fraud are explicitly stated and emphasised.

Many points made above are relevant to understand Article 11 LED, which corresponds to Article 22 GDPR, as the terms and concepts relating to decision-making, profiling, and legal authorisation and safeguards are similar. Given the legal form of a directive, the LED, however, specifically instructs Member States to prohibit automated decision-making, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, unless authorised by union or Member-State law which provides the relevant safeguards – a prohibition that should apply without the need for actions or objections from the data subject.[57] The main additional substantive difference between the instruments is the focus within LED Article 11 on decisions, including profiling, 'which produces an *adverse* legal effect', unlike the GDPR where decisions need only produce legal effects. An adverse effect could include 'interferences with the rights and freedoms or the legitimate interests of the data subject'.[58] Article 11(3) LED contains a further explicit prohibition of profiling that results in discrimination against natural persons on the basis of special categories of data. However, fair criticism has been levelled by Gottschalk against the ability of Article 11 of the LED to protect against automated analysis that provides the mere grouping of persons based on special categories of data, but which escapes the profiling designation as long as it is not used to evaluate or predict characteristics or behaviour patterns of individual data subjects.[59]

Overall, we can see that the GDPR is more permissive towards automated decision-making than the LED. We can also see that the use of fraud-detection systems is unlikely to end up under the respective rules on automated decision-making, given the likely involvement of human decision-makers in later stages of the process before generating a decision (whether adverse, or not). Both frameworks, however, require a specific legal basis for automated decisions, including profiling, and the discussed case law in the GDPR context suggests a heightened emphasis on the specificity of national rules permitting such decision-making. Given the strictness of the proportionality assessment under the GDPR, the requirements ought to be even higher under the LED.

Thus, we can so far conclude that while both the GDPR and the LED permit the processing of personal data for profiling in fraud detection, they also impose several stringent requirements. These requirements necessitate, amongst other, clear legislative support for the practice within national law, as well as safeguards to ensure the lawful processing of personal data on which profiling depends. As our next section will show, the existence and structure of regulated mandates for fraud detection by authorities can also influence whether the GDPR or the LED applies to data processing. Additionally, we will show that it will impact the protective

[57] T. Gottschalk, *Article 11 – Automated individual decision-making*, in Costa & Boehm (ed.) *The EU Law Enforcement Directive (LED): A Commentary*, Oxford, Oxford University Press, 2024, 239.

[58] *Ibid*.

[59] *Ibid*., 237-239.

regime prescribed within the AIA for such practices. Therefore, we will now turn to examining the relevant factors to determine which of these legal frameworks will apply to profiling for fraud-detection purposes.

4. *Definitions of "law enforcement" in the data-protection and AI context and its relation to fraud-detection systems*

4.1. *Applicability and the LED as the exception to the GDPR*

As already mentioned, the LED provides derogations from the GDPR, meaning that the GDPR will apply unless the processing falls under the scope of the LED. To determine the application of the latter, two types of personal scopes of application need to be considered. The first is that the LED applies to a 'competent authority' in the strict sense, which takes aim at the traditional public-law enforcement agency. This classification is determined by whether an authority is tasked (by law) with preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties.[60] The second type of authority falling under the LED is 'any other body or entity entrusted by Member-State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safe-guarding against and the prevention of threats to public security'.[61] Again, we find that the actual tasks given to the authority will determine the scope of the LED, even though this section of the directive opens for outsourced data processing by private actors falling under the LED, which the first does not. In addition to being processed by a competent authority, processing activities also need to relate to law-enforcement purposes for the LED to apply.[62] In contrast, the GDPR applies to processing for law-enforcement purposes unless it is carried out by a competent authority.[63] The questions for us thus becomes; at what point does the tasking of specific control activities aimed at detecting or preventing crime such as fraud progress so far towards law enforcement as to make an authority a competent one under the LED, and the processing aimed at fulfilling law-enforcement purposes?

During the drafting and proposal phase of the current data-protection framework, both the European Data Protection Supervisor (EDPS) and Article 29 Data Protection Working Party (WP29) expressed worries regarding the potential broadening of the LED's scope to encompass authorities that would typically be governed by the GDPR. Their worries were that the second type of competent authority might encompass administrative or private entities not exclusively connected to criminal-justice concerns.[64] While the definition of competent authority is, as mentioned, an autonomous concept under EU-law and thus not open to reinterpretation by the national authorities, it does not imply that national authorities lack influence over the question of what legal rules regarding data protection apply to a specific type of fraud-detection system. Ultimately, applicability will depend on choices made by the national legislator with regard to the tasks and duties given to the authorities in question, something that challenges the harmonising effect of the directive.[65] But as we will see, institutional and internal organisational factors are important as well, which can create certain challenges in clearly delineating the applicability of the LED.

In one of the few cases relating to the delimitation of competent authority under the LED, the CJEU was asked through the preliminary-ruling procedure whether (among other things) data collection of a tax authority

[60] Article 3 - 7(a) LED.
[61] Article 3 - 7(b) LED.
[62] Article 2(1) LED.
[63] Article 2(2)(d) GDPR, see also M. Brewczyńska, *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation*, in E. Kosta, R. Leenes and I. Kamara (eds), *Research Handbook on EU Data Protection Law*, Cheltenham, Edward Elgar Publishing, 2022, 103-104.

[64] European Data Protection Supervisor, *Opinion 6/2015 A further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors*, 28 October 2015; Article 29 Data Protection Working Party, *Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, WP233, 01 December 2015.
[65] This was highlighted in the drafting process of the LED, see M. M. Caruana, *The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement*, in *International Review of Law, Computers & Technology*, vol. 33, no. 3, 2019, 253.

fell under the ambit of the GDPR or the LED. More specifically, the tax authority had requested the company running a web portal for the sale of vehicles to hand over data on the chassie-numbers of sold cars and the phone numbers of the sellers, to be able to collect tax and fight tax evasion. The CJEU, following the reasoning of the Advocate General, held that this was not a data collection that fell under the LED.[66] AG Bobek argued that even though the data processing of the tax authority 'might in some cases eventually result in the detection of a criminal offence in the form of a tax fraud, that is merely a hypothetical possibility at this stage'.[67] The CJEU developed this reasoning to take into account that even though the data could be used in criminal proceedings against individuals, the data was not collected for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law.[68] These findings are partly helpful in our attempt to analyse fraud-detection systems, but leaves a lot unanswered. The statements by the CJEU relate to the specific first-instance collection of data which are used by the authority for primary tasks other than fraud detection, rather than the further analysis of data within the authority for the specific purpose of detecting fraud. There are also clear indications that this dependency on the specific purpose of processing goes both ways. In a case relating to the processing of passenger name records from airlines under the PNR directive, the question was whether the analysis of such data performed by authorities normally falling outside the scope of EU law (and more specifically the LED), such as national security intelligence agencies, could be considered to take place within the scope of the LED or not.[69] AG Pitruzzella held that 'where a Member State entrusts its security and intelligence services with tasks in the fields listed in Article 3(7)(a) of the [LED], the data-processing operations carried out by those services in order to perform those tasks would fall within the scope of the [LED] […]'.[70] The grand chamber of the CJEU took a similar path and, leaning on the findings of the AG, held that the processing of PNR data was aimed at purposes defined in Article 3(7)(a) of the LED, and was performed by authorities that through their specific tasks could be considered competent under the LED. In contrast, the processing of data by air carriers, 'although they have a legal obligation to transfer PNR data, are neither in charge of exercising public authority nor entrusted with public powers by that directive, they cannot be regarded as being competent authorities within the meaning of Article 3(7) of [the LED]'.[71]

Both these cases support the conclusion that the applicability of the LED is conditioned on both the tasks entrusted to the authority in question, and the purpose of the specific processing operation. However, in the case of an authority vested with tasks falling both within and outside the law-enforcement tasks, the LED is supposed to cover, and where the processing also fulfils dual purposes, it is likely we need to look further, to the institutional and functional embedding of law-enforcement tasks within the authority.

4.2. *The importance of the institutional setup*

First, it appears clear that any tasking of a public authority that implies direct involvement in conducting traditional investigation of crimes in a pre-trial stage, intended to lead to prosecution of a specific individual, would imply that processing of personal data within the authority for that purpose would fall under the scope of the LED. While welfare agencies are not generally tasked with opening and conducting formal criminal investigations or collecting evidence intended specifically for prosecuting an individual, we can find examples of such mixed functions within the context of taxation. The Swedish tax authority, for

[66] Case C-175/20, *SIA 'SS' v Valsts ieņēmumu dienests*, EU:C:2022:124, 44-45.

[67] Opinion of Advocate General Bobek delivered on 2 September 2021 in Case C-175/20, *SIA 'SS' v. Valsts ieņēmumu dienests*, EU:C:2021:690, 40.

[68] Case C-175/20, cit., 44-45, with reference to Case C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*, EU:C:2017:725, 40.

[69] The activities of national-security agencies are often seen as excluded from the scope of EU law through art. 4(2) TEU, there are however ample examples of the CJEU finding that such activities fall under the scope of EU law, see M. Jaśkowski, *National Security and Essential Security Interests in CJEU Jurisprudence*, in J. Hillebrand Pohl et al. (eds.), *Weaponising Investments, Springer Studies*, in *Law & Geoeconomics*, 2024, 227–244.

[70] Opinion of Advocate General Pitruzzella delivered on 27 January 2022 in case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, EU:C:2022:65, 59.

[71] Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministres*, EU:C:2022:491, 81.

example, has long had specific units focusing on tax crime, with legal mandates to support prosecutors in preliminary investigations, but also to execute certain coercive investigative measures and independently investigate crimes without involvement of the prosecutor 'if the suspect can be assumed to plead guilty to the act'.[72] New legislative initiatives suggest that the tax authority's mandate to independently start and conduct preliminary investigations will be further expanded.[73] While the units focusing on tax-crime investigations have been organisationally (internally) separate from the ordinary administration of taxation cases, they are part of the same overall authority. Furthermore, there is a duty to internally transfer information to the crime-investigation units if the information can be connected to suspected criminal activity that is either systematic in nature or include crimes subject to a potential prison sentence of one year or more.[74] In other words, the tax authority must be seen as an authority competent for preventing, investigating and detecting criminal (tax) offences, a conclusion that is supported by the fact that the tax authority itself sees the LED as applicable to the processing of data within its crime investigation units.[75] The separation of such units does clarify the internal structure of tasks and the legal framework internally seen as governing each unit, but the question is whether such internal 'firewalls' would hold off the applicability of LED outside of units focusing on law-enforcement tasks. The use of fraud-detection systems that indicate criminal fraud may, in our example of the Swedish tax authority, trigger a responsibility to transfer indications to the criminal investigation units, as the intentional filing of incorrect tax information may be subject to a sentence of up to two years in prison.[76] In other words, fraud-detection systems are likely to become an integral part of an overall internal process that is characterised by the legally designated mandate to detect and prevent tax crimes, as well as investigate them. The processing of personal data within that fraud-detection system – in stages preceding the involvement of the crime-investigation unit – is thus likely to be processed for the purposes of detecting, preventing, or investigating crime, and thus be ruled by the LED.

To underscore this analysis, we can see that a similar separation between criminal investigations and overall information analysis exist within traditional law-enforcement agencies as well. Police organisations tend to have units focusing on criminal intelligence, with information processed not to support a specific criminal investigation, but rather to keep track of criminal developments and phenomena in society. This intelligence gathering can aid in the detection of criminal activity, in understanding existing and emerging criminal behaviour and environments, and in identifying individuals that warrant further scrutiny without reaching a specific level of suspicion in relation to a specific crime.[77] While personal data in this intelligence environment may or may not be fed into a specific criminal investigation, the processing of personal data in intelligence operations is still, overall, regulated by the LED as it serves to (among other purposes) detect criminal activity. In contrast, other tasks that may be performed by police organisations, which do not relate to the direct or indirect aim of detecting or preventing crime, or feed into potential criminal investigations, such as the issuing of passports or permits, are generally not governed by the LED, but by the GDPR, on account of Article 2(1) LED.

The situation becomes less clear-cut when the mandates of the authority in relation to the detection and prevention of crime are less clearly defined and where the investigation of criminal activity to a greater extent remains external, which is still the case for the Swedish Social Insurance Agency [Försäkringskassan]. While the instruction for the agency (issued as a government decree) includes a general task to ensure that faulty payments of benefits are not made, and to counteract welfare crimes,[78] the agency does not have the same legally designated mandates as the Swedish tax authority. Welfare fraud

[72] Act 1997:1024 om Skatteverkets brottsbekämpande verksamhet, §§ 2-5.
[73] Swedish government, Dir. 2023:143, Utökade befogenheter för Skatteverket inom brottsbekämpning och folkbokföring.
[74] Act 1997:1024 om Skatteverkets brottsbekämpande verksamhet, § 7.
[75] Swedish Tax Authority, Behandling av personuppgifter, at https://www.skatteverket.se/omoss/varverksamhet/behandlingavpersonuppgifter.4.18e1b10334ebe8bc80005971.html.
[76] Swedish tax crime act (1971:69), § 2.
[77] See S. D. Brown, *The Meaning of Criminal Intelligence*, in *International Journal of Police Science & Management*, vol. 9, no. 4, 2007, 336-340.
[78] Government ordinance (2009:1174) med instruktion för Försäkringskassan, § 2.

can lead to comparable and significant penalties as tax fraud, stretching up to six years imprisonment for severe cases.[79] However, where the tax authority has internal crime-investigation units, the Social Insurance Agency is instead mandated to file criminal complaints to the police authority if a welfare crime can be suspected.[80] While fraud-detection systems can be an important source of information that highlights cases or data that at some point ends up as part of a criminal investigation, the institutional setting of the fraud-detection system is less tightly connected to any legal mandate to detect, prevent, or investigate, criminal offences and would only result in the filing of a criminal complaint. In this case, the vague and limited mandate of the agency is likely to place the processing done within fraud-detection systems under the GDPR rather than the LED.

The legal and organisational aspects touched upon above can serve as indicators of a wider conclusion, that a tighter integration of law-enforcement tasks and welfare agencies is likely to bring larger parts of their internal fraud detection under the scope of the LED. The same goes for the expression of formal mandates for agencies that include detection, prevention, or investigation of (welfare) crimes. As we will show in the following, there may be secondary consequences from this analysis in relation to what obligations will apply to such systems under the AIA, as well as in relation to how the procedural-rights requirements under the ECtHR will affect the space for manoeuvre for national authorities to implement them.

5. *Fraud Detection, meet your new friend – the Artificial Intelligence Act*

5.1. *Applicability of AIA risk categories on fraud-detection systems*

As opposed to the EU legal framework for data protection, EU law does not entail separate legal frameworks for AI systems in general or within law enforcement. As far as of interest in this article, and as noted earlier, the AIA will regulate both domains. As previously mentioned, this article operates under the assumption that profiling systems used for fraud-detection purposes may utilise AI techniques, including those based on machine learning. Those systems will therefore likely qualify as AI-systems under the AIA, and trigger its application.[81] Even if the AIA applies, however, the act employs a risk-based approach that recognises different protection needs for different AI-use contexts – which in this article means that the act may prescribe different protective measures for the use of AI in fraud detection depending on whether it is utilised in routine activities by public authorities or within a law-enforcement context.

Since many of the AIA's substantive obligations are specifically reserved for systems qualifying as high risk according to the regulation, one first crucial question arises about whether the deployment of an AI system for fraud detection within public-sector domains like social-security administration will fall into this category. Here, Annex III 5(a) AIA classifies as high-risk those AI systems intended to be used by public authorities or on behalf of public authorities to *evaluate the eligibility* of natural persons for public-assistance benefits and services, as well as to *grant, reduce, revoke, or reclaim* such benefits and services. The wording makes it clear that the regulation attributes AI use in the context of eligibility evaluation to the high-risk domain. However, although profiling for purposes of fraud detection may lead to decisions on eligibility, revocation or reclamation of benefits, the profiling activity as such may typically not involve any direct decisions on eligibility. Instead, it may typically rather lead to administrations being alerted of irregularities or patterns which may prompt a further decision to investigate the matter more in depth. The answer to whether fraud detection systems will qualify as high-risk in the AIA will therefore depend on how narrow or extensive the delineation in Annex III 5(a) is to be construed, particularly regarding the degree of connection between the profiling practise and eligibility evaluation.[82] Of note is that Annex III 5 (b) lists AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score as high risk, but also expressly excludes 'AI systems used for the purpose of detecting financial fraud' from the high-risk classification. Even though the AI systems of

[79] 3 § Bidragsbrottslag (2007:612).
[80] 6 § Bidragsbrottslag (2007:612).
[81] See section 2.
[82] *Rule-Based versus AI-Driven Benefits Allocation: GDPR and AIA Legal Implications and Challenges for Automation in Public Social Security Administration*, cit., 20 ff.

interest in this article clearly will not fall under the 5(b) provision, a question could be raised whether it signals a lenient attitude in the AIA towards AI uses for fraud-detection purposes, and whether this should carry over into the assessment of whether a profiling system used for fraud detection should qualify as high risk under the 5(a) provision. We would argue that this should not be the case as there is no substantive link between the provisions. We also contend that profiling for fraud-detection purposes within the social-security domain involves assessing whether a claim is likely to be fraudulent or erroneous, or whether a payment is likely to be incorrect—thus directly affecting eligibility assessments. It is clear that the emphasis in the provision is on the evaluative element of benefits administration rather than decision-making itself. This is further supported by the fact that the second part of the provision, which begins with 'as well as' and lists actions such as granting, reducing, revoking, or reclaiming benefits and services, uses language that suggests expanding exemplification rather than limitation. Based on this, we argue that these systems fall under the high-risk category, even if the AI system does not make the final decisions. We will therefore proceed on the assumption that fraud-detection systems based on profiling practises which are used by public administrations in the social-security domain will qualify as high risk, even if they don't make any decisions (either in the meaning of Article 22 GDPR or in the sense of the Member States' administrative-law traditions).

What about AI systems used for law-enforcement purposes in the AIA then? As we have mentioned above, the definition of a law-enforcement authority under Article 3(45) of the AIA is identical to that of competent authorities under the LED. To the extent that AI systems, as defined under the AIA, are part of the fraud-detection systems that would, in terms of their data processing, fall under the LED, the AI system would also be subject to the requirements relating specifically to law-enforcement use of AI under the AIA. As we have also argued above, there is a clear possibility that AI-based fraud-detection systems (even without the applicability of the LED) would be deemed high-risk under the AIA as they would serve to evaluate the eligibility for public benefits. In addition to these effects of the AIA on AI-based fraud-detection systems within welfare agencies, the use of such systems when implemented by a competent authority under the identical definitions offered by the LED and the AIA would also fall under additional categories in Annex III, section 6(d-e), of the AIA which become relevant to ascertain the impact of the AIA on fraud-detection systems. These sections take on risk-assessment systems (6(d)) and profiling systems (6(e)). Both categories are relevant to fraud-detection systems in different ways. Category 6(d) systems assess the risk of a natural person offending or re-offending not solely based on profiling. If an AI system used in fraud detection is aimed at identifying individuals more likely to be engaged in fraud, or includes such an individualised risk-assessment in the overall determination of the risk of a specific benefit claim to be unfounded or fraudulent, the system is likely to fall under this category provided the agency can be considered a competent authority. Category 6(e) systems are focused on profiling 'in the course of detection, investigation or prosecution of criminal offences', which could become equally relevant if systems deploy profiling of natural persons as a means to detect criminal activity. The delineation between these categories can appear blurred, given that risk assessments tend to rely on profiling, but the wording of category 6(d) makes clear that risk assessments 'not based solely' on profiling (as defined by Article 3(4) of the LED) are included, as well as the assessment of personality traits and characteristics of past criminal behaviour of natural persons or groups. This could in other words also relate to the use of AI systems to identify previous patterns of criminal behaviour in large datasets to then apply to risk assessments relating to natural persons. Of note is however that recital 59 AIA excludes 'AI systems specifically intended to be used for administrative proceedings by tax and customs authorities' from the designation as 'high-risk AI systems used by law-enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offences'. There is no corresponding exception within the social-welfare domain.

As we have discussed, the purpose, but also the organisational structure surrounding a profiling system used in fraud detection is key to determining the applicable sections of the LED, and consequently, the AIA. While the legal rules of the AIA take as a point of

departure that AI systems fulfil a particular function,[83] we have continuously touched upon how fraud-detection systems exist on a sliding scale between assessing eligibility (or lack thereof) and assessing criminal liability or risk of future fraud. Given the more binary nature of assigning relevant sections of the AIA to a particular AI system, we would argue that the legal mandates and the organisational structure of the agency implementing fraud-detection systems, as discussed above in relation to the LED, will be key to clarifying which (among possible multiple) purposes should be the determining one for the AI system under the AIA. This brings us to the question of the implications that classifying a system as 'law enforcement' under the AIA will have.

5.2. *The impact of 'law enforcement' classification under the AIA*

Somewhat counterintuitively, the classification of AI systems used for fraud detection as belonging to the law-enforcement sections relating to high-risk systems rather than the high-risk sections relating to the assessing the eligibility for benefits, add few additional requirements. Instead, the AI system will primarily be subject to reduced transparency requirements and a different set of oversight mechanisms,[84] as well as possibilities for Member States to make further exceptions through national legislation. The AIA exceptions for law enforcement include, *inter alia,* the possibility to make exceptions to the requirement for separate verification by two natural persons in decision-making within the law-enforcement context (Article 14(5) AIA), an exception to the requirement to inform natural persons that they are subject to the use of a high-risk system (Article 26(11) AIA, by reference to the LED), and the registration of the high-risk system in a non-public section of the new EU AI database (Article 60(4)(c) AIA). In other words, the law-enforcement label in the AIA implies several exceptions to the general requirements of the act.

It is also worth mentioning that the harmonising effect of the AIA may be somewhat reduced in light of this possibility of Member States to independently control which national authorities should be competent authorities, by way of their tasking and designations. This, in combination with the definition of a competent authority in the LED, which in turn impacts the possible applicable exceptions in AIA, creates a situation where a largely identical fraud-detection system, used for that same overall purpose and with the same logic, would fall under different rules depending on the formal mandates and internal structure of the authority implementing them. This is in line with similar observations made regarding the LED.[85]

Counterintuitively, this would imply that a fraud-detection system implemented within a competent authority—where it is more clearly connected to the investigation of crimes and potential criminal sanctions—would be subject to less stringent rules. This is despite the fact that the risks and consequences for the individual would arguably be greater, as the system falls into two simultaneous high-risk categories, affecting both the determination of eligibility for benefits and potential criminal investigations.

6. *Conclusions*

Our discussion so far highlights the diverse legal issues that profiling systems for fraud detection purposes raise, even as we have focused on a limited set of issues connecting to applicability, basic legality of processing operations and AI-systems. This is indicative of the growing complexity of the legal landscape facing public administrative agencies in this context.

As we have shown, a number of interacting legal requirements flowing from the GDPR require a clear legal basis for the use of fraud-detection systems. The clarity required in turn requires explicit choices to be made regarding the closer functions and purposes of such systems. The explication of those purposes in the context of detecting and preventing fraud through profiling systems may in itself

[83] We do note that the AIA contains a definition of an AI-system, but not of a system as such. This begs the question of when an AI component in a bigger system is to be regarded as a system in itself, and when such a component makes the entire system an AI-system under the AIA.

[84] Oversight of law-enforcement use of AI is placed within the authorities exercising oversight of competent authorities processing of personal data under the LED, or data-protection supervisory authorities under the GDPR, rather than the specific authorities designated under the AIA in general, see Article 74(8) AIA.

[85] See *The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement*, cit., 253.

contribute to authorities being tasked (by law) with mandates that could bring their profiling practices (based on the processing of personal data) under the overall function-based definition of the LED, and consequently, the AIA. This, in turn, brings even further requirements of ensuring clear and specific legal rules supporting their data processing.

The regulation surrounding the use of profiling systems used for fraud detection is important. Legislative mandates can in themselves be determinative for whether the GDPR or LED will be applicable to profiling systems used in fraud detection by public welfare authorities such as social-security administrations, for example if they clearly state that relevant agencies have law-enforcement tasks or mandates. In cases where the legislative mandates are not that clear, the LED can still become applicable to the processing of personal data, given the relevance of the organisational factors we have discussed above. This implies that while the definition of competent authorities under the LED is autonomous and ultimately interpreted by the CJEU, Member States can influence the applicable legal framework by defining tasks and organisational structures of the relevant agencies.

In making that choice, which becomes necessary through the legality requirements surrounding the data processing, our study suggests that Member States need to consider a number of consequences relating to the use of profiling systems for fraud detection. The first is that CJEU case law relating to the fundamental right to data protection under the Charter, suggests a strict(er) proportionality assessment relating to the use of special categories of data in the law-enforcement context. Under the GDPR, special-category data may, to some extent, be routinely processed in the context of regular activities assessing the eligibility for social-security benefits, given their centrality to many such benefits and the legal tasks of relevant agencies. However, the CJEU case law on the LED has highlighted that the processing of special-category data is not supposed to be a routine part of law-enforcement activities, and thus subject to a very strict necessity and proportionality assessment.

The move towards using fraud-detection systems for purposes relating to law enforcement can also bring other fundamental rights-based effects. This can be exemplified by how fraud detection may rely on individuals providing data under obligation, with the possibility of sanctions for non-compliance. This also raise concerns under Article 6.1 of the European Convention on Human Rights (ECHR) regarding self-incrimination.[86] The ECtHR case law on using information obtained under the shadow of administrative sanctions in later criminal investigations is complex. The privilege against self-incrimination, essential to a fair trial under Article 6 ECHR,[87] applies when criminal proceedings are in place, as defined by the *Engel* criteria.[88] This includes considerations relating to the designation of a procedure under national law, but also the nature of the offense and the severity of possible sanctions.[89] Administrative sanctions with punitive aims may fall under Article 6, making fair-trial requirements and self-incrimination protections applicable in early stages of the process.[90] European case law highlights certain challenges in using coerced statements to impose criminal penalties, as authorities may be required to inform individuals at the data-collection stage of their right to remain silent to avoid interfering with the privilege against self-incrimination in future proceedings where the information is to be used.[91] As such, fraud-detection systems reliant on compelled information necessitates

[86] Consequently, in Sweden, some care has been taken to argue that activities aimed at detection and control of faulty applications or fraud should not, in fact, be seen as law-enforcement activities, see SOU 2023:100, 1032.

[87] ECtHR, *Saunders v. The United Kingdom* [GC] (19187/91), 1996, § 68.

[88] ECtHR, *Engel and others v. The Netherlands* [Plenary] (5100/71; 5101/71; 5102/71; 5354/72; 5370/72], 1976, most recently these criteria were reaffirmed in ECtHR, *Vegotex International S.A. v. Belgium* [GC] (49812/09), 2022.

[89] See ECtHR, *Ezeh and Connors v. the United Kingdom* [GC] (39665/98 & 40086/98), 2003, § 82.

[90] This was found in relation to administrative surcharges in the VAT tax context, see ECtHR, *Jussila v. Finland* [GC] (73053/01) 23 November 2006, §§ 29-39. In this case proceedings were labelled as fiscal, the penalties were minor, but the objective of those penalties were a punishment to deter reoffending, it was held to fall under the scope of Article 6 under the criminal heading. Do note that the ECtHR remarked that since tax surcharges 'differ from the hard core of criminal law, the guarantees of Article 6 do not necessarily apply with their full stringency', see *Jussila,* § 43, see also ECtHR, *Vegotex International S.A. v. Belgium* [GC] (49812/09), 2022, § 76.

[91] See A. de Vries, *Recent Developments Concerning the Right to Silence and Privilege Against Self-Incrimination Under the Charter of Fundamental Rights of the EU - A Critical Reflection on Case C-481/19 DB v Consob*, in *Review of European administrative law*, Vol. 15, no. 1, 2022, 40.

clear distinctions between eligibility analysis and criminal prevention to ensure compliance with fundamental rights. We would argue that this highlights the need for overarching assessments of information flows and secondary uses of data, focusing not only on the fundamental right to data protection.

Worth mentioning is also the new Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, where point 32 of the preamble states that 'All regular law-enforcement activities for the prevention, detection, investigation, and prosecution of crimes, including threats to public security, also remain within the scope of the Framework Convention if and insofar as the national-security interests of the Parties are not at stake'.

The corresponding definitions of competent authorities under the LED and 'law enforcement' under the AIA suggest that the case law of the CJEU interpreting this aspect of the LED should be relevant for our understanding of law enforcement under the AIA. However, the LED focuses on the actors and purposes underlying data processing, where aims and the specific data used can sometimes be fluid and *ad hoc* in the sense that they can be determined for specific processing operations. The AIA on the other hand, focuses on the purposes of a specific AI-system which is somewhat more tangible and potentially more long-term. An AI-system may however be designed to fulfil many different functions, that from the point of view of the administrative authority may be used for divergent tasks, and therefore also purposes, that fall under different data-protection rules. The problem here lies in how such mixed systems should be managed under the AIA. Given the understandable lack of guidance on this issue so far, our analysis of the LED suggests that the organisational context may be important to understand the applicable rules of such systems under the AIA.

While our analysis so far has mainly focused on the legislative level, we have repeatedly stressed the importance of the organisational aspects of fraud detection. These organisational aspects are to some extent determined on the level of administrative authorities themselves. For example, while the legally designated mandates are important in determining if an authority is a competent authority under the LED, the purpose underlying the processing is also relevant. Since the purpose of the specific processing is determined at the time the authority decides how to actually utilise their delegated authority, there is usually a discretionary space where administrative authorities themselves can influence the more detailed purpose of specific processing operations.

Ultimately, however, our analysis shows that the national legislative level is where crucial decisions are still made that influence the applicable EU data-protection rules. It is also the level that both the GDPR and the LED emphasise in relation to authorities' data-processing mandates. We have also shown how the decisions made by Member States in their regulatory approaches influence the relevant rules and exceptions that flow from the AIA, with a clear possibility for confusion arising at the intersection of the GDPR, LED, and the AIA. This highlights the need for clarity in the regulatory environment on the national level regarding the intended use of profiling systems for fraud-detection purposes. This clarity can also be said to be a clear requirement flowing from the case law of the CJEU. These considerations all highlight the significance of regulatory decisions on the Member-State level in shaping the landscape of data-protection and law-enforcement practices across jurisdictions.