Universiteit
Leiden
The Netherlands

Data-driven investigations in a cross-border setting: experiences from the Netherlands

de Jonge, B.; Vries, B. de

Citation
De Jonge, B., & Vries, B. de. (2025). Data-driven investigations in a cross-border setting: experiences from the Netherlands. *Eucrim - The European Criminal Law Associations' Forum*, *2024*(3), 214-221. doi:10.30709/eucrim-2024-020

Version:	Publisher's Version
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/4208979

Note: To cite this publication please use the final published version (if applicable).

Georg Roebling
Head of Unit "Intelligence & Operational Analysis", European Anti-Fraud Office (OLAF)

Bogdan Necula
Deputy Head of Unit "Intelligence & Operational Analysis", European Anti-Fraud Office (OLAF)

ficial intelligence and amending certain Regulations and Directives (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.
4 See D. Hadwick, "'Error 404 – Match not found' – Tax Enforcement and Law Enforcement in the EU Artificial Intelligence Act", (2023) *eucrim* 55–60.
5 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, 39.
6 See for example the 2024 Call for proposals for the Union Anti-Fraud Programme (EUAF), available at: <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/euaf/wp-call/2024/call-fiche_euaf-2024-ta_euaf-2024-trai_en.pdf> accessed 9 December 2024.
7 The financial transaction typically has a description field that, from a data perspective, is a free text field. It usually contains details of the transactions, in many cases with valuable insights such as invoice number, contract reference, explanation for the payment, etc.
8 See Recital 59 AI Act. For the concerns, see also D. Kafteranis, A. Sachoulidou, and U. Turksen, "Artificial Intelligence in Law Enforcement Settings – AI Solutions for Disrupting Illicit Money Flows", (2023) *eucrim*, 60–66, in particular Chapter IV.
9 See Recital 1 AI Act.
10 Art. 113(a) AI Act.
11 Art. 113 AI Act.
12 Art. 111(2) AI Act.
13 Art. 111(2) AI Act, last sentence.
14 Art. 2(8) AI Act.
15 See Art. 60(4) AI Act.
16 Art. 61(1) AI Act.
17 Art. 5(1)(d) AI Act.
18 See the legal definition in Art. 3(45) AI Act.
19 See Art. 49(4) AI Act.
20 Art. 2(7) AI Act.
21 *Op. cit.* (n. 5).
22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 199, 4.5.2016, 1.
23 See for example ECJ, 9 November 2023, Case C-319/22, *Autoteile-Handel,* para. 45 with reference to the earlier judgment of 19 October 2014, Case C-582/14, *Breyer*, paras. 43 *et seq.*
24 See Art. 2(1) Regulation 2018/1725.
25 See Art. 39 Regulation 2018/1725.
26 See European Data Protection Supervisor, "Data Protection Impact Assessment (DPIA)" <https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en> accessed 9 December 2024.
27 Art. 4(1)(a) Regulation 2018/1725.
28 Art. 5(1)(a) Regulation 2018/1725.
29 Art. 4(1)(c) Regulation 2018/1725.
30 Art. 4(1)(d) Regulation 2018/1725.
31 Art. 27(1) Regulation 2018/1725.

Data-Driven Investigations in a Cross-Border Setting

Experiences from the Netherlands

Boudewijn de Jonge and Barry de Vries*

Current technology enables drug traffickers and other criminals to live like digital nomads and direct global operations from any location in the world. That said, this surge of technology also provides law enforcement with new tools. Large datasets allow us to change the way we conduct investigations, making a data-driven law enforcement approach possible. No data-driven investigation can ignore the international dimension of organised crime. In this article, the authors analyse some of the challenges and achievements they see in cross-border data-driven investigations, in the light of the standards of the Law Enforcement Directive.

I. Introduction

Many have been suggesting that we are currently witnessing the advent of a totally new technological era. Our societies are changing due to the democratisation of technology and the incredible power of those technologies. In the individual Member States of the EU, many initiatives have been launched by law enforcement and the judicial sector to explore how technology can be exploited for fighting crime and administering justice. The police force of the Netherlands is no exception and strives to be amongst the most innovative forces in Europe, with data-driven policing being one of the four pillars of their multi-annual strategy.[1] In this article, we share some of our experiences with data-driven work in cross-border cases.

In section II, we explain and illustrate the data-driven investigation strategy that is being followed in the Netherlands. In section III, we look at some of the lessons learned in the Netherlands and relate those to European law, including the Law Enforcement Directive (LED).[2] The perspective of cross-border cooperation is the topic of section IV, from which we draw some conclusions for future practice in section V.

II. Data-Driven Investigations

In line with technology having become more widespread and powerful, criminal investigations have gained access to ever larger data sets. In the fight against child pornography, for example, the exchange and cross-border matching of large data sets has long been a cornerstone of investigative work.[3] Likewise, the seizure of darkweb servers, including servers of illegal marketplaces, has created dazzling amounts of data; in some instances, investigating one such seizure has resulted in as many as hundreds of criminal cases. Yet, the hacking of the encrypted communication services EncroChat and SkyECC has represented a turning point when it comes to assessing the necessity of and control over the use of such data sets. Along with the availability of large data sets, new ways of policing have been invented.

Data-driven work in the investigative police branch is now considered a crucial component of the strategy of the Dutch police. Data-driven methodologies provide new opportunities for tackling criminal activities more efficiently and effectively. This goes beyond the mere obtaining and analysing of a large data set.

This strategy is rooted in the notion of problem-oriented policing shaped by *Herman Goldstein* in the 1990s.[4] Building on that theory, the concept of intelligence-led policing was developed at the beginning of the 21st century. Another crucial step was to incorporate social network analysis into policing, one proponent being *Paul Duijn*.[5] This systematic approach and use of data has the potential to identify key actors and relationships, disrupt critical connections, unveil hidden structures, prioritize vulnerabilities and minimize collateral damage.[6] By using this systematic approach, police can focus their efforts on key elements within a network rather than applying broad or generalized approaches. Combining the problem-oriented approach with network analysis and adding large data sets and technology offers a comprehensive framework for modern policing. We now have the tools to analyse data sets, identify patterns, trends, and connections within criminal networks more quickly and accurately. Next to enabling more targeted interventions, this integration allows police to dismantle organisations as such and develop proactive strategies. The outlined strategy differs fundamentally from starting an investigation based on a single incident, such as the seizure of one drugs transport or intelligence about a single criminal organisation.

This can be illustrated by the SkyECC case, in which police revealed that messages from dozens of cocaine traffickers had been exchanged via the encrypted communication service SkyECC; the data obtained by hacking the service served as evidence of an industry that functions as an interconnected global network, supported by various enablers.[7] The authors witnessed the clever use of logistics chains, complex financial schemes, and the use of encrypted apps.[8] The higher echelons of drug trafficking organisations live like digital nomads and organise complex supply chains residing, for example, on the Mediterranean coast. The distribution of these drugs from a Western European port to the end users takes only days, sometimes hours.[9] In this fast-moving market, it is difficult for national law enforcement to make a lasting impact. A data-driven approach represents one attempt of formulating a response to that complex criminal industry.

As organised crime benefits from operating across borders and has characteristics of a global industry, a data-driven police approach must also address the challenges of cross-jurisdictional collaboration. Criminal organisations often exploit international boundaries to evade law enforcement, requiring a coordinated effort between local, national, and international agencies. By combining problem-oriented strategies with network analysis and leveraging big data, police forces can better anticipate and respond to transnational crime, targeting the key nodes and connections that sustain global criminal networks.

III. Some Lessons from the Netherlands

A data-driven approach to criminal investigations should result in admissible and understandable evidence in court. In a learning-by-doing process, three standards have been carved out to ensure reliable output that can be used in court: (1) clean data; (2) transparency, and (3) collaborative design. Whilst these standards primarily serve the admissibility and evidential value of the data in court, we will show how they align with the privacy standards of the LED.

1. Clean data

Clean data, which is accurate, consistent, and free from errors or duplicates, is crucial for drawing reliable conclusions and making informed decisions. Minor inaccuracies or biased selection of data can lead to significant misinterpretations. Therefore, ensuring data integrity and cleanliness is essential for law enforcement to effectively understand and act upon the insights derived from big data.

For example, it can occur that the timestamp of a message is inaccurate or a message is replicated for technical reasons. In order to easily read and correctly interpret the evidence, technical errors may be corrected in the data set. Yet, at all stages of processing this initial correction will have to be visible and traceable. Secondly, the reason for the correction is to be explained. By doing so, all parties to the trial and the court will be able to properly evaluate the evidence and the correction, and compare it to the original uncorrected data if requested.

Data-driven investigations are able to bring together data sets of different origins and quality. For example, travel data combined with encrypted communication might reveal logistical hotspots of criminal goods. Or the book-keeping of a criminal facilitator combined with an analysis of FIU information might reveal illicit money flows of his clients. Moreover, a large data set gathered in one case may later become relevant for another investigation. The combination of such datasets offers new insights.

In order to maintain data quality and ensure consistency, the Dutch police follows the CSAE model when handling large data sets. "CSAE" is a cycle and stands for the four phases of the process: **C**ollect, **S**tore, **A**nalyse, and **E**ngage.[10]

The *Collect* stage focuses on gathering data from various sources, such as crime scenes, former investigations, digital devices, and large data sets (e.g., encrypted communication). Next, the *Store* stage ensures that all collected information is securely stored in information management systems preserving it for further analysis. In the *Analyse* stage, forensic tools and techniques are used to examine the evidence, identifying patterns and connections between suspects, victims, and crime scenes. Lastly, in the *Engage* stage, interventions take shape. Interventions may range from searches and arrests within the framework of a criminal investigation, to enabling administrative authorities to act within their respective competences.

The output can be used as evidence in a criminal investigation or to disrupt criminal activities, for instance by taking a criminal marketplace offline. In particular with cross-border crime, criminal prosecution of foreign-based networks may be impossible and disruption of the crime may be a more realistic option.[11] The results of the interventions will be fed back into the loop in the form of new data, closing the cycle.[12]

So what role does the LED play in this context? Amongst others, it requires that the data processed are adequate, relevant, and accurate.[13] Whereas the significance of these principles seem indisputable, one may wonder how exactly they play out with large data sets. Initial, unedited data will include (technical) errors, mistakes, and inaccuracies. Yet the authentic, unedited copy is of tremendous importance for later verification of evidence by the parties to the trial. As to data minimization, storing only the "relevant" parts of a data set brings about the risk of eliminating exculpating evidence. Another problem with that principle arises in connection with the identification of (criminal) users of an anonymous communication network. It is hard to predict whether and when a positive identification can be made.

In the Netherlands, for example, the first large data set obtained by the police resulted from the decryption of communications on the Ennetcom network in 2016. It consisted of a few million messages obtained when a server was seized in Canada. Initially, only a small number of users could be identified. However, the data came back into focus when other providers of anonymous communication services were hacked, providing new leads for the identification of users of the Ennetcom service. Several murder cases involving Ennetcom users did only end in court very recently.[14] It was thus only after many years that accuracy and relevance of the data became clear, and the wider data set became of relevance to the defence to search for exculpating evidence. This example calls for caution against a too strict interpretation of the principles of Art. 4 of the LED. An original, unedited copy of the data may have to be kept for a very long time.

2. Transparency

Data-driven investigations ultimately serve justice. An accusation will have to be sustained in the courtroom, and the quality, reliability, and legality of the evidence presented may be tested there. Transparency on the basis of the collection of data, and logging of procedural decisions is thus crucial to sustain the subsequent penal or administrative actions. Accountability must be ensured during all steps of a data-driven investigation; this is essential for upholding legitimacy.

Yet the challenge is that hundreds or even thousands of court cases may follow from the collection of a single data set. Art. 4(2) of the LED permits the collected metadata of one criminal group to be further processed in new investigations.[15] Take the example of the metadata of one single, powerful organised crime group being intercepted while its members were communicating over the SkyECC platform. This metadata revealed insights not only into the group's own dealings, but also into their contacts with other criminals outside the group. When analysed further, this led to new groups being identified. In this new case, the defence was provided with the original interception warrant, but the court did not find it relevant for the defence to know which other contacts were identified.[16]

In other cases, it has been debated whether the defence ought to be given access to complete data sets, given that receiving only a copy of the data pertaining to the accused person alone might feel too restrictive.[17] In some cases, Dutch courts have allowed the defence to read other persons' communications, or provided a list of keywords to search the entire data set.

Restricted access to the original data for the defence has not been the only point of contention; it has been argued that the same tools should be made available as were available to law enforcement.[18] In the Netherlands, discovery by the defence is now facilitated by the very same tool that the police uses, tailored to the selection of data relevant to the case at hand. The platform *Hansken*, developed by the national forensic institute, enables the consultation of large data sets.[19] The defence may now be granted access to this data, both on site and remotely.

3. Collaborative design

The standard of transparency requires planning ahead, thinking of the ultimate test in court. It is key to involve all actors from an early stage, in this instance the prosecution service. In the EncroChat and SkyECC investigations, there was an intense collaboration between the police and public prosecution service to ensure the data could be used in court. This did not only help to ensure that innovation was developed in line with the classical rules of criminal procedure, it also ensured focus in the phase of analysis.

A data-driven law enforcement approach offers a new way of improving the efficiency of criminal justice[20] and of bringing about more impactful judicial interventions. Law enforcement analysis on SKYECC revealed, for instance, an essential element to the thousands of drug transactions: an underground banking system.[21] By searching the data – in conformity with the judicial warrants –, various global underground bankers were identified that had been processing transactions worth hundreds of millions of euros each.[22] In consequence, that analysis has inspired the public prosecution to dedicate more attention to the phenomenon of underground banking.

Another advantage of the involvement of the prosecution service in the early stages of data-driven investigations is that cases can be more properly selected. A criminal investigation traditionally starts from a position of suspicion, followed by a search for evidence, either incriminating of exculpatory. Conversely, today's abundance of data evidence allows us to select markets, subjects and regions. It allows us to decide to prosecute a single key player in an individual case, or to prosecute an entire network in a large-scale trial. These choices in the investigation have far-reaching effects on the way a trial is organised and – indeed – the capacity needed further down the chain. As this concerns prosecutorial strategies, these choices are usually made jointly by the prosecution and the police.

The study of the first deciphered messages from EncroChat brought about an important insight, which proved relevant for any work with the data in general. In most cases, it appeared very difficult to prove which one of numerous conversations on drug transactions did actually result in a deal or international drug transport. Yet, each conversation constituted an inchoate crime, i.e. that of making preparations for drug trafficking. This allowed the police to change their selection of cases, given the limited capacity of the police, prosecution service, and the criminal courts: the best way forward was to reason backwards. There was sufficient proof against the average EncroChat user for dozens of separate inchoate crimes. Yet, in most cases they were only accused of a limited number thereof; usually the more serious ones. The goal was to optimize the use of resources in order to achieve the best result. In this way, resources of the police could be conserved, case files limited in size, and trials shortened.

Clearly, these choices have only been possible because the Dutch criminal justice system allows for a wide prosecutorial discretion. However, another important element in this selection and prioritization process is the collaborative effort in the early phases of analysis. Proper guidance and insight into the capacity of the partners prevented the system from collapse.[23]

IV. International Cooperation in Data-Driven Investigations

Organised crime often takes place in a transnational setting. This international context poses additional challenges for a data-driven law enforcement approach when fighting organised crime. The following outlines these challenges.

1. Burden sharing and solidarity

It is general consensus that there is a necessity to respond to digitalised crime. However, in the context of large data sets, jurisdictional problems for police and judicial authorities arise. It is often unclear at the beginning of an investigation where exactly the users of a platform or service are based, and where most of the crimes have been committed. In some cases of transnational organised crime, international public law stipulates an obligation to investigate and cooperate on cross-border crime, such as Art. 11(2) of the Palermo Convention.[24] There are only a few pan-European agreements that include a fair distribution of cases.[25] Yet, in many more cases, it will depend on the personal motivation and solidarity of the involved law enforcement and judicial actors to work on cases that may initially have a very limited link to their own jurisdiction.

A praiseworthy example in this context is how certain German police and prosecution services have taken action against darkweb marketplaces. The direct link to their respective jurisdictions may have been relatively limited, but in the wider interest of disrupting drug trafficking they worked on identifying online drug traffickers.[26]

Similar questions regarding the limits of jurisdiction and responsibility are also relevant when it comes to mutual legal assistance requests. One example is offered by the numerous large data hosting companies that have been established in the Netherlands.[27] Frequently, the Dutch authorities receive requests to seize or intercept servers with suspect data, such as online platforms that spread illegal content. Often, the requesting authority is only interested in one particular account, but it appears not always technically possible to single out that particular account. When executing the request, Dutch authorities may need to seize very large volumes of data, and initial analyses often reveal that the seized data relates to crime all over the world. Hence, it is sometimes a challenge to determine who should obtain, process and act upon that data.

The example shows that solidarity is needed and the burden of work should be shared. Nevertheless, discussions on burden sharing are sometimes complex due to the differences in legal systems. For example, Dutch courts consider an extended conversation containing pictures or screenshots of money transfers sufficient evidence to convict a suspect of money laundering.[28] In other countries with different legal systems, the physical seizure of the money as well as the direct connection of that money with a crime is needed for conviction. Another example is the penalisation of inchoate crimes. The mere act of preparing a transport of cocaine is subject to a maximum sentence of six years in the Netherlands, whilst in other countries it is hardly worth being brought to court.[29]

It has been well-studied that significantly differing levels of penalties exist in EU Member States.[30] These stark differences in substantial criminal law limit the possibilities of sharing the burden of working together in cross-border crime in general, and data-driven investigations in particular.

2. Obligation to share data and how the data was acquired

The jurisdiction of the investigating national authorities is commonly limited to crime occurring on its national territory or with a link to its territory. Their powers and resources may not legitimately be used for crimes that lie beyond that. Yet, there are many obligations in international treaties and positive human rights obligations to act if a serious crime is detected in another country.[31] Cooperation should not be rooted in a one-sided, particular interest of one state. The recently adopted Directive on exchange of information between the law enforcement authorities of EU Member States[32] does not encompass a direct obligation to share relevant information with foreign counterparts. But the spirit of loyal cooperation between EU Member States itself should inspire states to show solidarity when they suspect a crime to have occurred in another state.

When sharing data across borders, the issue of admissibility of that data as evidence merits additional consideration and collaboration.[33] When the encrypted communication server Exclu was recently hacked, the Dutch authorities shared an extensive package of national court orders and official reports that explain how the data was obtained. Yet, the standards for interception, data-processing, re-

cord-keeping, and transparency may be different in the receiving country. To meet the objective of sharing data in a reliable manner, it is necessary that the receiving public prosecutor or investigating judge explain their national requirements up front. In its judgment in *EncroChat*, the ECJ upheld the non-inquiry principle, while at the same time requiring that evidence be excluded if a person is not in a position to comment effectively on that information.[34] The interpretation of that last sentence will be subject to debate in many national courts in the coming years.

3. International data needs international context

(Automated) processing of large data volumes is a necessary step to select relevant data. In their attempt to select and understand data, national authorities cross-reference it against their own national databases. Hence, potentially relevant names and phone numbers from surrounding countries may easily slip through the cracks. This national focus seriously limits the scope of the analysis. There is empirical evidence that crime spread over different jurisdictions indeed prevents detection.[35] The need to include foreign data in the analysis is therefore obvious.[36] While jurisdictions regularly collaborate to collect relevant evidence, collaboration on storing and analysis is less common:[37] data is generally stored in accordance with national standards and analysed against national databases only.

The problem becomes evident, for example, when we look at the process of matching data between different Financial Intelligence Units (FIUs) within the EU.[38] The automated analysis of cross-border transactions by a national FIU is at most partial when foreign information on the persons involved in reported suspicious transactions cannot be included.

In our experience, it has proven of added value on several occasions to invite foreign analysts to a scrum session and both work on the same data set. Whilst this could be done as part of a Joint Investigation Team, the analytical teamwork as such can also take place within the framework of police cooperation. The data shared during such a session can be made subject to any conditions, including those from the applicable judicial warrants.[39]

Another challenge when processing content data is language. Naturally, our own teams of investigators principally speak Dutch as their native language. Yet, by focusing mainly on Dutch speakers and Dutch citizens we create our own blind spot. While working on the EncroChat and SkyECC data sets, we therefore actively sought cooperation with relevant foreign authorities to mitigate this effect and to prevent the bias of language. In practice, this meant compiling top-ten lists of communication network users per nationality and actively approaching their respective country of origin with the aim of cooperation. This was a useful bottom-up approach, while the involvement of Europol had its advantages in distributing the analysis results.

The challenge to the selection and further processing of data is relevant also in the context of the principle of data minimisation. As already noted in relation to the national strategy on data-driven law enforcement (supra II), Art. 4(1)(c) of the LED requires that data only be processed in so far as it is relevant and not excessive. If the acquired data does not result in any matches, one may lightly conclude that the unmatched data is not relevant and may be deleted. Yet, if the data set has a strong cross-border component, that conclusion may only be reached once it has been sufficiently ensured that the legitimate interests of foreign jurisdictions have been met. Obviously, a data set of, for instance, participants in an online exchange of child pornography should not go undetected because the processing is limited to a particular jurisdiction. Likewise, a data set of internal communication of a foreign crime group may hold crucial evidence to solve serious crimes in another state.

4. Coordinating European criminal justice

A data-driven approach to tackling criminal networks is implemented effectively when trials against connected elements of the network can be carried out in various jurisdictions in a coordinated manner. The interest of justice is better served if the judicial authorities not only coordinate their initial efforts (who will prosecute?) but continue to stay in touch until the end of a trial.

For example, the conviction of a drug dealer/money launderer in Germany is likely to be relevant for the prosecution of the broker in the Netherlands. Likewise, a German judgment convicting an online drug trader who also sold drugs to Indonesia via the darkweb was later used in Dutch court proceedings as supporting evidence against the producer, in order to show the global distribution of his illicit products.[40]

Another example illustrating the need for coordination at the trial level are the EncroChat/SkyECC cases mentioned above. In the Netherlands, they have handed down well over 500 judgements to users of SkyECC and EncroChat to date.[41] Many of these judgements relate to conversations with criminals in other countries, or even include convictions for crimes committed abroad.[42] Whilst the EU framework calls for practitioners to contact each other when conflicts of jurisdiction arise, it is equally relevant to share milestones in related proceedings, including important statements, ac-

quittals, plea arrangements, and convictions. The sharing of the precise outcome of a court case can also be in the interest of the defence. An acquittal or different interpretation of the facts in one country should be known to the parties involved in related cases in other countries. Thus far it has proven difficult to be aware of relevant outcomes of EncroChat/SkyECC cases elsewhere in the EU. The automated exchange of criminal records through the ECRIS is insufficient: it is limited to final convictions,[43] whilst information on the earlier steps is equally relevant in practice.

V. Conclusion

The surge of large data sets opens up opportunities for law enforcement to combat organised crime more effectively. Data-driven investigations are one way of achieving that. This article outlined that this approach is still a very new way of thinking in law enforcement, breaking with some of the traditional ways of starting and conducting investigations and allocating resources.

In the authors' experience, the close collaboration between the police and prosecution service has proven key to ensuring that data-driven investigations get off the ground and operate within the law. The correct application of the EU's relevant data protection framework – the Law Enforcement Directive – is fundamental to that work, and it guarantees transparency to the defence and the court. However, some elements of the Law Enforcement Directive, such as the data minimisation principle and the requirement that only accurate data be processed, necessitate additional considerations when applied to large data sets.

We also demonstrated in this article that the cross-border nature of organised crime requires this data-driven work to be done in cooperation with international partners. As the criminals we investigate are digital nomads travelling the world, we have to foster a culture of digital cooperation as well. International law and solidarity require that data be shared proactively. Ideally, the burden of exploiting large data sets should be shared. And we must reflect on how to facilitate transparency and accountability at an early stage when we cooperate internationally on large data.

In addition, we have provided some insights into how the differences in substantial and procedural law within the EU make such conversations sometimes very complex. It will be interesting to further research the ratio of users versus convictions in the different EU Member States, and explore to what extent differences in substantive law play a role in the efficiency of criminal justice.

Boudewijn de Jonge
Senior public prosecutor at the National Public Prosecution Office of the Netherlands.
PhD candidate at the University of Leiden

Barry de Vries
Inspector at the National Police of the Netherlands

* The opinions in this article are strictly personal and do not necessarily reflect those of the organisations the authors work for. The authors thank Sarah Norman and Thomas Wahl of the eucrim team for their constructive comments on the earlier version of this article.

1 National Police of the Netherlands, Office of the Chief Commissioner, *Begroting en beheerplan 2024–2028* [Budget and management plan 2024–2028], 3 July 2023.

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

3 The first initiatives to automatically match images go back to the year 2000. A. Minnaar, "An examination of early international and national efforts to combat online child pornography and child sexual exploitation and abuse material on the Internet", (2023) 24(2) *Child Abuse Research in South Africa*.

4 H. Goldstein, *Problem-Oriented-Policing*, 1990.

5 P.A.C. Duijn, *Detecting and disrupting criminal networks: A data driven approach*, 2016, [PhD thesis for the University of Amsterdam].

6 An excellent illustration of the application of this concept to countering cannabis cultivation is described in this movie: <https://www.youtube.com/watch?v=Qhk9ciHlzzo> accessed 6 January 2025.

7 Interesting work is done by *Enderwick* who compared regular multinational enterprises to criminal organisations. P. Enderwick, "Understanding cross-border crime: the value of international business research" (2019) 15(2/3) *Critical perspectives on international business*, 119–138.

8 European Monitoring Centre for Drugs and Drug Addiction and Europol, *EU Drug Market: Drivers and facilitators,* 2024.

9 InSight Crime and the Global Initiative Against Transnational Organized Crime, *The cocaine pipeline to Europe,* 2021; Organized Crime and Corruption Reporting Project, *The Highway to Europe – Inside A*

Global Drug Collaboration, 2023, available at <https://www.occrp.org/en> accessed 6 January 2025.
10 See for a more detailed description: E. van de Sandt, A. van Bunningen, J. van Lenthe and J. Fokker, *Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest*, March 2021.
11 See for example: V. Harinam and B. Ariel, "The Role of Law Enforcement in the Regulation of Cryptomarkets (and the Limited Role of Deterrence)", in: *Law Enforcement Strategies for Disrupting Cryptomarkets: A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches,* 2024, pp. 49–83.
12 M. den Hengst, and O.L. Wijsman, "Datagedreven politiewerk: Een organisatorisch en juridisch perspectief", in: T. Snaphaan, W. Hardyns, A. J. van Dijk, R. Spithoven and R. Van Brakel (eds.), *Big data policing,* 2023, pp. 71–90.
13 Art. 4(1)(d) of the LED, *op. cit.* (n. 2).
14 For instance: Court of Amsterdam, 27 February 2024, ECLI:NL:RBAMS:2024:692.
15 The EU framework for forwarding of data to a new investigation depends on whether the data was (a) collected from telecom providers or (b) collected by the authorities (see also the conclusion in Case C-162/22 by Advocate General *Campos Sánchez-Bordona*, ECLI:EU:C:2023:266, paras. 41–45). In the first scenario, data may only be forwarded if the receiving investigation concerns a serious crime or serious threat to public security (ECJ, 7 September 2023, Case C-162/22, *Lietuvos Respublikos generalinė prokuratūra,* ECLI:EU:C:2023:631, summarized at *eucrim* 2/2023, 149–150). In the second scenario, data obtained legitimately may be processed for other criminal investigations, in accordance with national law.
16 Court of The Hague, 19 March 2021, ECLI:NL:RBDHA:2021:3224.
17 The ECtHR accepts that the defence counsel may be granted access to a limited data set, but must be granted full access to relevant material: ECtHR, 4 June 2019, *Sigurður Einarsson v Iceland,* Appl. no. 39757/15.
18 See on this matter, for instance: ECtHR, 25 July 2019, *Rook v Germany,* Appl. no. 1586/15.
19 See <www.hansken.nl/hansken-academy/hansken-courses/hansken-for-lawyers> accessed 6 January 2025. For an example on how the defense uses the system, see: Court of Amsterdam, 1 April 2021, ECLI:NL:RBAMS:2021:1507.
20 I. Helsloot, P. van Lochem, C. Kijne, "Slimme(re) Opsporing. Een verslag van de ontwikkeling en pogingen tot implementatie van een handreiking voor efficiënte opsporing door de politie", (2022) *Politiewetenschap,* 125.
21 For an explanation and overview of the efforts to counter underground banking, see: Annual Review Criminal Money Flows 2022, Public Prosecution Service of the Netherlands, 2 April 2023, available at: <https://www.prosecutionservice.nl> accessed 6 January 2025.
22 One example is the conviction of an underground banker who moved €246 million by the court of Rotterdam on the basis of SkyECC data: Court of Rotterdam, 5 September 2024, ECLI:NL:RBROT:2024:8533.
23 A system based on the legality principle may have to make different choices. The massive launch of large criminal cases due to EncroChat forced the government of Hamburg to assign 28 additional judges, prosecutors and judicial staff in 2021: Senat Hamburg, Press release of 1 June 2021, <https://www.hamburg.de/politik-und-verwaltung/behoerden/bjv/aktuelles/pressemeldungen/2021-06-01-bjv-encrochat-ermittlungen-232564> accessed 6 January 2025.
24 B. de Jonge, "Transnational Crime Without Transnational Prosecution: How Positive Obligations to Cooperate May Inspire National Judicial Authorities", (2023) 2(2) *Transnational Criminal Law Review*, 98–112.
25 The lack of such rules is particularly noticeable in the context of digitalized crime. See for instance: T. Beekhuis, "Executieve jurisdictie: het (grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?", (2022) *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 106–118.
26 Over the years, the German authorities have taken down dark-web marketplaces, such as Crimenetwork (2024), Nemesis (2024), Kingdom (2023), Hydra (2022) and Wall Street (2019). These marketplaces were used by hundreds of vendors and visited by thousands of buyers around the globe.
27 To avoid any misunderstandings: the reason why many companies host large datacenters in the Netherlands has to do with the proximity of transatlantic sea cables, availability of qualified staff, and general economic climate.
28 The decision of 12 July 2022 by the Court of The Hague, ECLI:NL:RBDHA:2022:6763, exemplifies Dutch case law. Here, the court found the combination of a picture of bank notes and the message that "it was 428" sufficient proof that the suspect was laundering €428,000.
29 Court of The Hague, 24 December 2021, ECLI:NL:RBDHA:2021:14242.
30 EMCDDA, *Drug trafficking penalties across the European Union a survey of expert opinion,* Lisbon 2017, *pp. 15–23.* For a critical overview of the efforts to harmonise sanctions within the EU, see for instance: K. Zoumpoulakis, "Approximation of criminal sanctions in the European Union: A wild goose chase?", (2022) 13(3) *New Journal of European Criminal Law*, 333–345.
31 Both treaty law (the crime control treaties) and human rights case law include multiple specific obligations to cooperate when authorities are faced with cross-border crime. See *supra* note 24.
32 Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, OJ L 134, 22.5.2023, 1.
33 The principle of non-inquiry may be a strong principle in several EU Member states, but its interpretation is subject to debate. See G. Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations" (2023) 14(3) *New Journal of European Criminal Law*, 273.
34 ECJ, 30 April 2024, Case C-670/22, *M.N. v. Staatsanwaltschaft Berlin (EncroChat),* summarised in *eucrim* 1/2024, 40–43.
35 M. Lammers and W. Bernasco, "Are mobile offenders less likely to be caught? The influence of the geographical dispersion of serial offenders' crime locations on their probability of arrest", (2013) 10(2) *European Journal of Criminology*, 168–186.
36 D. Skillicorn, *Cyberspace, data analytics, and policing*, 2022, p. 234.
37 As shown by Den Hengst, and Wijsman, *op. cit.* (n. 12), p. 27.
38 F. Mouzakiti, "Cooperation between financial intelligence units in the European Union: stuck in the middle between the general data protection regulation and the police data protection directive", (2020) 11(3) *New Journal of European Criminal Law*, 351–374.
39 Art. 3 lit. c) of Directive (EU) 2023/977, *op. cit.* (n. 32).
40 Court of Appeal of The Hague, 1 February 2022, ECLI:NL:GHDHA:2022:346.
41 This number is based on the judgements of first instance courts published on the official webpage of the Dutch judiciary: <www.rechtspraak.nl>. The real number should be higher, because there is no general obligation to publish every judgement.
42 Dutch law established broad extraterritorial jurisdiction over Dutch nationals committing crimes abroad, and over foreign nationals if they contribute to a criminal organisation that can be prosecuted in the Netherlands.
43 Art. 2 of Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, 23.