## Editorial: A trialogue on regulating data-driven criminal procedure

Galič, Maša; Stevens, Lonneke; Koops, Bert Jaap

***published in***
New Journal of European Criminal Law
2023

***DOI (link to publisher)***
10.1177/20322844231213484

***document version***
Publisher's PDF, also known as Version of record

*Editorial*

NJECL

New Journal of European Criminal Law
2023, Vol. 14(4) 423–433

DOI: 10.1177/20322844231213484
journals.sagepub.com/home/nje
Sage

# Editorial: A trialogue on regulating data-driven criminal procedure

**Maša Galič and Lonneke Stevens**
VU University Amsterdam, Netherlands

**Bert-Jaap Koops**
Tilburg University, Netherlands

## Abstract

This editorial introduces a special issue on the challenges of regulating data-driven criminal investigations, in light of the interplay – or rather, the lack thereof – between criminal procedure law and data protection law. The aim is to bring together scholars from both fields, to facilitate mutual understanding and to present ideas on better aligning these bodies of law to form a comprehensive normative framework. In data-driven investigations, police typically assemble large data sets to build an information position, followed by automated analysis to detect patterns and find evidence of potential crimes. The shift from traditional targeted, "case-seeks-evidence" investigations to data-driven untargeted, "evidence-seeks-case" investigations challenges the current normative framework. Discussing this challenge and the insights offered by the six contributions to this special issue, the authors identify multiple problems: people in criminal law lack knowledge of and therefore undervalue data protection law; data subject rights do not function well in the criminal procedure context; there may be an increasing emphasis on instrumentality in criminal law, at the cost of legal protection; criminal law strongly focuses on legal protection of suspects, particularly during trial, and does not cope well with investigations that never end up in court, nor with the protection of innocent citizens whose data are now also pervasively processed as by-catch in criminal investigations; and the law has relatively strong norms on data collection, but not on data analysis. The way forward lies in evolving towards a system that does not only protect suspects and victims but that systematically incorporates the rights of innocent thirds; developing an integrated and conclusive system of data processing rules in law enforcement, including data analysis and on-going reuse of data; and establishing a system of supervision that is adequately equipped to deal with the new reality of data-driven criminal procedure.

**Corresponding author:**
Bert-Jaap Koops, Tilburg University, Postbus 90153, Tilburg 5000 LE, Netherlands.
Email: e.j.koops@tilburguniversity.edu

**Keywords**
criminal investigation, criminal procedure, data protection law, privacy, legal protection, oversight, big data, algorithms

## Editorial

[Tuesday 15 August 2023, 12:39, café Zeezicht, Utrecht. Suspect has lunch appointment with C., who doesn't show up. He has lunch by himself, using various apps on his phone (see transcript XI.2 for log of phone activity). During that time, the microphone records a conversation in the background, apparently at the table next to suspect, which our system flagged as suspicious because of high-frequency occurrence of keywords "criminal", "police", "crypto", and "detecting". Three voices, one male (addressed as "BJ"), two female (addressed as "Lonneke" and "Masha" or "Martia"). Automated transcript, handcorrected by officer Berend van Baarle (BvB).]

BJ: … this special issue in the first place?

L: The idea was to bring together criminal lawyers and data protection lawyers. Bridge the gap between the two bodies of law, because experts in one field hardly understand the other field. As a criminal law scholar, all these papers about privacy and data protection are new to me. They're interesting, but I don't really know what to make of them. I do feel that it's somehow important to my work, seeing the changes in policing and criminal investigations.

M: You mean the fact that it's no longer about physical evidence, but all about data? Or that instead of targeted investigations of past crimes, police are increasingly collecting bulk data to be analysed later on in the hope of finding something interesting?

L: Both, actually – it's called the shift to data-driven investigations. I know that data protection is important in that respect, but I don't understand it, it looks so complex. What is it about? What kind of law is it?

BJ: I've always understood data protection law as a set of decency norms. Many people think that data protection is a negative type of law, with all kinds of restrictions and limitations. Privacy officer says no… But that's not true, you can process all kinds of data in all kinds of ways, as long as you do it properly. You can see it as a kind of new behavioural norms alongside the norms we've developed in human interactions. When you meet someone in person, you simply don't touch their private parts (well, unless that was the purpose of the meeting), and in a business conversation, you don't ask about someone's sex life (well, unless you're a sex therapist). Such norms on how you should interact with people have evolved over a long time. When computers entered society and started replaced certain human interactions, somewhere in the 1960s and 1970s, people realised it might help to develop some basic norms on how to deal with personal data, so that you treat persons decently when dealing with them not in person but in their informational representation.

L: How interesting! That's something I can relate to as a criminal lawyer. Decency, treating people fairly… I think that many people in criminal law practice and scholarship don't see it that way, though. Why does data protection have such a bad reputation?

BJ: Hm, perhaps because there are quite some people, also within the data protection community I'm afraid, who do tend to apply data protection law as primarily restrictive, blocking data collection and sharing that I think would be quite acceptable if only you have good procedures for it. What many people overlook is that the DPD [Detroit Police Department? no idea what they mean, BvB] and GDPR [General Data Protection Regulation, BvB] have always had a dual function: on the one hand, to offer legal protection by preventing harm from unfair or disproportionate data processing, and on the other hand, to facilitate the free flow of data within the EU, by ensuring a level playing

field of data norms. Even the LED [Law Enforcement Directive?, BvB] is officially called a directive "on the protection of natural persons with regard to the processing of personal data by competent authorities (…) and on the free movement of such data".

M: In that light you can also think of data protection as De Hert and Gutwirth explain it: privacy is an opacity tool while data protection is a transparency tool. Privacy shields things from sight, to keep something private; data protection allows things to be seen but ensures that people know their data are being processed and can complain if they feel they are being unjustly treated. In other words, that they have a certain level of control over the processing of data about them.

Male voice/waiter: Humus and grilled vegetable sandwich?

BJ: That 's for me, thanks.

Male voice/waiter: Lentil and sweet potato soup?

M: For me.

Male voice/waiter: And the goat cheese sandwich for you, then. Anything else to drink?

BJ/L/M: Eh, no, we 're fine.

L: Where were we? Oh, data protection as a transparency tool. That's interesting, because criminal investigation is shifting so much towards intelligence, which the traditional system of checks and balances in criminal procedure is not well-equipped for. Remember the crypto-communication cases Oerlemans and Royer write about: Sky ECC and Encrochat? These show that criminal investigation is nowadays more about "evidence-seeks-case" than about "case-seeks-evidence". The police are increasingly investing in data-driven policing, like the Dutch Refinery example in the paper by Te Molder and others, or the crime intelligence register Indicia discussed by Sunde. In many cases, this data-driven policing is not necessarily about bringing a particular suspect to justice; it is also and mainly about building an information position (you see: intelligence!), being able to prevent or stop certain crimes. But – and this is the crux, I think – the CCP [Code of Criminal Procedure?, BvB] is built on precisely this idea: a case against a suspect that is brought to trial. And the system of checks follows that idea: during an investigation into particular suspects, the police are supervised by a public prosecutor or an investigating judge, and at the end of the investigation by the trial court, which checks whether the evidence has been gathered by the book. In an intelligence type of investigation, however, all of this doesn't happen. [Small pause filled with biting and chewing sounds.]

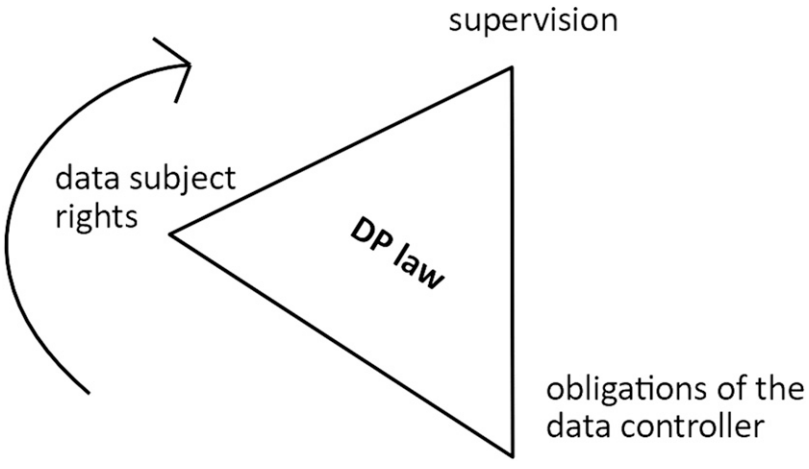
And I reckon there's another issue to be considered. The focus of data-driven policing is on data analysis. It's about generating more and better information by combining data. The CCP, on the other hand, is traditionally focused on collecting physical evidence and analogue data, aiming to limit the infringement that this causes on, say, privacy – think of the conditions for a house search. We, criminal lawyers, have never problematised the subsequent analysis of all the material that is legitimately found for evidential purposes. Well, maybe when it concerns expert evidence and reliability is at stake. But generally, further analysis of all information found is seen as a logical corollary of the collection of evidence. In their paper, Galič & Stevens quote a criminal lawyer who essentially says that processing all of the collected data is not just a necessity but a duty!

M: That's exactly where data protection law comes in. If we need additional rules on data analysis, then data protection law is our tool. Because data protection is essentially a set of rules on the design, management and operation of data processing systems. As you pointed out, Lonneke, this toolbox is indeed wide-ranging and very complex (Bygrave has called it Byzantine), which is why I like the simple yet powerful explanation of data protection law as a triangle by González Fuster. We can identify three cornerstones of data protection law. First, "data subject rights" (think of the right to be notified that your personal data are being processed and the right to access these data). Second, "obligations of the data controller" (for instance, the police or prosecution services in

charge of the processing are obliged to inform you of data processing and to implement security and privacy-by-design measures in their IT systems). These two are the main pillars, grounding the system. Third, on top you have "supervision by independent authorities" (Data Protection Authorities and other possible supervisory bodies). These three cornerstones are intrinsically connected. Controllers needs to comply with their obligations to allow individuals to control the processing of their personal data. For example, controllers need to actually allow access to the individuals' data being processed and fix any incorrect personal data. In this way, individuals help ensure that the controllers indeed comply with their obligations. And all of this activity falls under the supervision of an independent authority. For instance, if the controller doesn't secure the data well so that they are hacked, someone can complain to the Data Protection Authority, which can impose a fine and make the controller improve the information security.

L: But, Masha/Martia, this system clearly isn't suited for the law enforcement context. The criminal procedural system of checks and balances has some level of openness, in the sense that suspects should get to know that an investigation is taking place and what its results were, ideally during the investigation itself. But it doesn't make much sense to talk of a suspects' right to access and correct their personal data in the investigation file, for example. So, how would this body of law work in a criminal investigation?

M: Good point. Even though I said that data protection law's three cornerstones are intrinsically connected, they are also relatively autonomous. The emphasis depends on the context. In business-to-consumer relationships, data protection law is primarily based on data subject rights, allowing individuals to control the processing of their data. For example, they can give consent but they can also reject tracking cookies, or retract their consent later. But in the context of law enforcement, the specific needs of crime prevention and investigation imply that individuals cannot "control" the processing of their personal data. The LED itself severely limits data subject rights, so that in the end not much is left of them. So the triangle of data protection law tilts here: given the specific needs of law enforcement, only one cornerstone remains to ground data processing: the obligations of data controllers, with still some supervision of an independent authority on top. But the third cornerstone, of data subject rights, is left hanging in the air, losing its foundational function. Let me sketch this out for better illustration [sound of pencil on paper sketching and writing; our sound-writing detection algorithm reconstructs the following graphic, corrected by BvB on the basis of the description].



So, because we don't have that extra check of data subjects themselves, we really need to make sure that police and public prosecutor's office are processing the collected personal data in line with their obligations. Think of technical and organisational measures to prevent unjustified processing of personal data, timely deletion of irrelevant and superfluous data, the keeping of separate databases for different types of personal data, and general logging obligations to ensure that supervisory authorities can check compliance. As BJ already said, the idea isn't to prevent the police from processing personal data, the point is that they need to do this in a proper way, so that there's a balance between people's need to enjoy their fundamental rights and the need of law enforcement to investigate and prevent crime. And on top of that, we need to make sure that the supervisory authorities have sufficient access and resources to keep an eye on all of this.

L: Hm, interesting, but I don't think this is the case in practice... If I remember correctly, Galič and Stevens argue that this is partially because data protection authorities generally do not have enough staff and, perhaps, expertise, but also because the police and public prosecutor don't seem to have a good grasp on this body of law, so that they don't sufficiently feel the need to implement it in their practice. While we can't make funds appear, this second issue might well be improved, if the role and importance of data protection law in this particular context could be sufficiently clarified. Where there's a will, there's a way, don't you think?

BJ: I would hope so. But…

Male voice/waiter: Is everything all right here?

L/M/BJ: Yes, we're fine.

BJ: I was going to say, just articulating the importance of a set of decency norms to process data is probably not enough. Isn't there also an intrinsic tension between the transparency character of data protection law and the covertness of criminal investigations?

L: Yes, but only up to a point. Remember that the criminal procedural system of checks and balances assumes openness in the end. The premise is that during the process, the one who is being investigated (the suspect) becomes familiar with that investigation and can challenge its results. But you're right, BJ, what data-driven policing has in common with intelligence is that it's all done covertly. And I'm not just thinking of James Bond lurking in the bushes. With automated analysis of large data sets, there isn't any insight into what data is combined with which other data sets in exactly what way. There is so much going on there, and only a fraction of the results of the data analysis will end up in a criminal file as evidence against particular suspects. The method of analysis is generally not scrutinised in the trial, even when it's based on opaque and complex algorithmic analysis. On top of that, there are many cases with insufficient evidence, or the suspect lives in a country that does not extradite. And without a trial, there's no chance to challenge results or methods used.

M: And, of course, there's also the issue that while the criminal trial has checks and balances for the suspect, in investigations such as the bulk interception of crypto-communication services like SkyECC, data of many people are collected and analysed who never end up as suspects and can therefore also not benefit from oversight by the trial court. Consequently, data of large numbers of innocent citizens are processed as by-catch in criminal investigations, essentially falling out of the scope of criminal-law protection, which is still focused on suspects and defendants in the criminal trial. You really need the additional safeguards of data protection law to oversee the analysis of bulk data sets.

BJ: That's very insightful. It makes me think of what I said earlier about the dual function of data protection law, as both offering legal protection and facilitating the free flow of information. Isn't there an interesting parallel with the dual nature of criminal law that Foqué and 't Hart have

articulated? There is an intrinsic tension in criminal law between instrumentality – the need to catch criminals as much as possible – and legal protection, the need to protect innocent people from wrongful imprisonment or unnecessary intrusions into their private lives.

Maybe the problem is that while both fields of law have an intrinsic tension between facilitating information-gathering on the one hand and protecting people from undue interferences on the other, they have grown apart over time. My impression is that in criminal law, the emphasis over the past decades increasingly lies on instrumentality, and legal protection is seen as a nuisance – a necessary evil that distracts from the "real" purpose of criminal law. While data protection law seems to increasingly emphasise legal protection, disregarding the interest of the free flow of information. That could explain why data protection law is viewed with such suspicion and dislike by practitioners in law enforcement, and also by politicians and lawmakers who tend to call for ever more crime-fighting. Lovely sandwich, by the way. How's the soup?

M: Quite tasty, although I have a hard time detecting the sweet potato. But I disagree with what you just said. The development towards instrumentality in criminal procedure law very much depends on the country. Some countries and their criminal courts still take human rights protection in the context of criminal investigations very seriously. And concerning data protection law leaning towards the protection side of things, you might just as well say that the data protection community puts more emphasis on the legal protection side of data protection law because of the ever-increasing possibilities to process personal data through technological developments, and because there is a high level of non-compliance with data protection law in practice, both by private businesses and public institutions. That's one of the main reasons that the GDPR and the LED were adopted in the first place. Just think of the possibilities for mass surveillance that the use of facial recognition technology in public space by the police brings about, which Galič and Stevens discuss. One might suspect that the protections of criminal procedure law and general human rights law (especially Art. 8 ECHR [European Convention on Human Rights, BvB]) needs to be backed up by data protection law to improve the situation.

L: As a criminal law scholar I also think it's too simple to phrase it too much in terms of opposition between instrumentality and legal protection. At least, we still teach our students that criminal procedure is just as much about "policing the police". The way I see it is that with criminal procedure having to somehow incorporate data protection law, policing the police becomes more complicated because it has trade-offs within itself. Think of the interest of covert investigation in the early stages of criminal investigation, so as not to alert (potential) suspects and to prevent destruction of evidence. There's a strong incentive for secrecy in policing, shielding operational methods. However, when information is subsequently used as evidence, the right to a fair trial aims to guarantee data access and transparency for defendants, so that they can prepare their defence properly. This follows from the equality of arms, which is by the way, an abstract principle and not easy to interpret, as Oerlemans and Royer show. A big discussion in those crypto-communication cases is how this principle should be implemented when the evidence is extracted from huge datasets. Weaving data protection law into this system of criminal procedure is going to complicate that discussion.

BJ: Yes, but that doesn't mean it shouldn't be attempted. Perhaps we've been circling around the problem but not reached the heart of it. Isn't the underlying problem that the analysis of data collected for criminal investigation is underregulated? You were saying earlier, Lonneke, that criminal procedure law traditionally focuses on regulating evidence collection, and that it is assumed that using collected material subsequently is just a corollary. You could argue the same for data protection law. Although opinions differ on this, there's an argument to be made that data

protection law strongly emphasises regulating the initial stage of data processing. After all, its starting point is data minimisation. As Te Molder and colleagues discuss, the principles of purpose specification and use limitation imply that you should only collect data that serve a purpose that you have specified beforehand. There is an exception in the form of allowing secondary use, if this is not incompatible with the initial purpose, but this is supposed to be an exception. [Drinking sounds.]

Practice is different, of course. You hardly see data minimisation in the real world. Also, in the context of data-driven policing, law enforcement seems to strive for data maximisation rather than minimisation… This makes it all the more important to have rules on subsequent processing. There are such rules in data protection law, to be sure. For instance, article 4 of the LED says that data should be "relevant", "accurate", and processed in a manner that is "not incompatible" with the purpose for which they were collected. However, those are all open norms, which is understandable, but they offer very little guidance for the analysis stage of data-driven investigations.

L: Ha, so, it's not just criminal law, but also data protection law that could use additional and more concrete rules on data analysis! It's interesting that we took the initiative for this special issue assuming that the problem is a sort of disconnect between criminal procedure and data protection law, but we have now identified some four or five problems, I think. Let me try to summarize. First, practitioners (and scholars for that matter) in the field of criminal law lack knowledge of data protection law, and consequently do not appreciate its value. Second, the triangle of data protection law cornerstones is tilted in the criminal law context, with data subject rights hanging in the air. Third, there may be an increasing emphasis on instrumentality in criminal law, at the cost of legal protection. Fourth, criminal law has shifted from targeted "case-seeks-evidence" investigations to data-driven "evidence-seeks-case" investigations, implying that the exception – by-catch of data of third persons – has become the rule. Fifth, related to this, what legal protection there is in criminal law is strongly focused on suspects and defendants and on the trial as the place where it all comes together, not on innocent citizens whose data happen to be processed as by-catch in criminal investigations, nor on situations that never end up in court. And sixth, the law has relatively strong norms on data collection, but there is an under-regulation of data analysis, even where data protection law applies. It looks as if I should start mobilising my criminal law colleagues, since most of these problems lie within the criminal law domain…

BJ: Phew, six problems… They are interrelated, of course, but it would be useful if we could determine the core, underlying problem with regulating data-driven investigations. After all, it really matters how you frame a problem, because each frame carries with it an implicit suggestion where to find the solution. For instance, the lack of knowledge and appreciation of data protection law in the criminal law community calls for education programs. The lack of data subject rights calls for anchoring the interest of data subjects in another way, perhaps through ex-durante oversight by a supervisory body, as Fedorova and colleagues have argued. This might also help address the imbalance caused by the system of checks and balances being centred around the defendant, not around third parties. And the under-regulation of data analysis obviously invites creating more rules for the subsequent use of data after collection.

So what do you think is the core problem is and what do the authors in the special issue propose?

L: For me, the focus on suspects and the trial without bite and the emphasis on instrumentality seem fundamental. Earlier, I contradicted you, BJ, but I see you have a point. Criminal law practice is increasingly occupied with fighting organised crime. A serious and headache-causing problem for society, definitely, but, as a consequence, ever more digital data are being collected, and more and more powers are created to facilitate that. This also means that bulk interception and seizure of data is becoming daily practice, and with it the large-scale capture and storage of data of innocent third

parties. But the protection of third parties is almost forgotten in the criminal law system. The focus is on the suspect, and increasingly also on involving and respecting the victim in criminal procedure. Perhaps because of the latter, it is even more challenging to organise legal protection for third parties whose data are processed as a side-effect of data-driven investigations and who are not present in the criminal trial, nor anywhere else in the procedure for that matter.

M: I very much agree with your points, Lonneke, but I would approach the issue from a broader angle. In terms of the core or underlying problem, I wouldn't focus too much on the still relatively few cases of gathering bulk data sets in one go, such as the crypto-communication cases. If you regulate "bulk" investigations, which is not easy to define, it's pretty easy for law enforcement to circumvent this by interpreting "bulk" in a very narrow manner. For example, Dutch courts have not considered the very large collection of all the data of tens of thousands of individuals gathered in the EncroChat hacking operation as a bulk data set. Nowadays, almost every investigation delivers a larger or smaller data set, which can then be stored, combined, mined, and shared for the purposes of new investigations and – increasingly – the building of an information position. Without sufficiently concrete rules on data re-use, eventually anything can end up in bulk data sets. So, what we need to develop is adequate rules on the various ways of data re-use. Thinking about such rules, Te Molder and colleagues explore the potential role of the principle of purpose limitation, which delimits how personal data collected for a particular purpose can later be reused for another purpose. Unfortunately, as they make clear, this principle is completely without bite in the current understanding of the EU Court of Justice. But there is still very much a need for such limits. [Scraping sounds, presumably the last spoons-full of soup being delved from the bowl.]

This means that further analysis of already collected data is hardly limited, not just in practice but also in law. As such, I would put the main emphasis on further developing concrete rules for data analysis. The inspiration for such rules could be drawn from forensics, especially digital forensics. Digital forensics is already becoming an increasingly important tool in digital criminal investigations, but these norms for dealing with evidence might have to be formalised in law rather than in internal guidelines and standards, as is the case right now. As Sunde points out, good regulation of data analysis is necessary in order to protect existing data protection rules, as it further enables and promotes subsequent checks of compliance, both by data protection authorities and during trial.

L: We definitely need additional rules on data analysis, for which we should indeed look beyond both criminal procedure and data protection law. In this regard, Sunde actually proposes another way to delimit data re-use, by implementing a clear distinction between two types of data and how these can be re-used. She suggests that data analysis rules should rely on a strict distinction between "assessed digital information" and "excess data" whose contents is not known to police, a distinction which already exists in Norwegian criminal procedure, but is also found in rules regulating intelligence agencies. While assessed data could be stored for later re-use, excess data should immediately be deleted in order to prevent fishing expeditions.

BJ: Interesting, but I'm a bit sceptical whether you can define "excess data" with sufficient precision. Police practitioners will complain that potentially interesting data will be deleted without having been examined. And who knows, there might also be disculpatory evidence in the "excess" data-set. But it's still an interesting idea, which could be developed in line with the strong limitations on bulk data collection set in European case-law on data retention, which Flor and Panattoni mention.

M: Shall we have another round of coffee? … Good, I'll wave to a waiter when I see one.

So, based on our discussion, data protection clearly has an important role to play in the regulation of data-driven investigations. But it has also become clear that data protection law doesn't have all

the answers to all of the problems we've discussed. Flor and Panattoni make a good argument that besides data protection, also cybersecurity is a relevant interest, to protect the informational infrastructure on which people's lives increasingly depend. Now that police can lawfully hack into computers, the normative framework needs to consist not only of rules protecting data, but also of rules protecting the digital ecosystem as a whole, regardless of which specific personal data are collected.

Besides, I think that data protection is not only part of the solution, but also part of the problem. There are actually many layers of data protection law regulating specific contexts (even beyond the special regime of the LED) with lower levels of legal protection. This is most notably the case with the new regime for personal data processing by Europol. As Tas makes clear in her paper, this regime can be used to circumvent more restrictive national rules, both in data protection law and in criminal procedure, on data analysis and sharing personal data with other investigations or authorities. When countries send all data they've collected to Europol, with its much laxer rules on deletion and storage, Europol can subsequently share and analyse data sets in a much broader manner than would be possible for national investigative authorities.

L: That's very disillusioning… Still, some of the solution surely lies in making data protection law more forceful in criminal procedure, right?

M: Sure, particularly because I now clearly see that the core of the problem as we've discussed it is the under-regulation of the whole cycle of data (re-)use, which emerges with the shift of criminal procedure towards data-driven investigations. Data are collected from various sources and investigations, stored, combined, analysed, shared and used for other investigations or to build an information position. All of these parts of the cycle need to be adequately regulated in a coherent way.

L: Okay, but if we are looking for solutions then I think we must go back to the six problems we identified earlier. Perhaps one can say that, when thinking in solutions, we have three connected approaches? First, criminal procedural law must evolve towards a system that does not focus primarily on protecting suspects and victims. In most relationships this is not a good idea, but here I think a third party should be involved: the innocent citizen who, in digital times, is increasingly a bycatch by default. Perhaps we could even develop a new interpretation of the presumption of innocence, in the sense that, digitally, every citizen has the right not to encounter the police. Next to this, we need to explore how to arrive at an integrated and conclusive system of data processing rules in law enforcement. This should focus on the analysis phase and the constant reuse of data. And finally, we should look into a system of supervision that addresses the problem of secrecy in the criminal justice context, with the third cornerstone of the triangle hanging in the air, and the fact that criminal procedures are mainly focused on legal protection within the context of *a* case against *a* suspect. I realise these solutions are still rather academic and need to worked out on a case-by-case basis. But we should start somewhere…

BJ: Sounds like a good summary to me. But I just realised there's an important point we have overlooked so far, which has to do with poli[…]

[Note Berend van Baarle: At this point (14:16), the recording stopped, as suspect shut down his phone and left the café. Reading through the transcript, this intercepted conversation is probably not something to follow up on. It sounds like some intellectuals discussing privacy and law enforcement. It should interest people like me, but it's a bit over my head, I'm afraid. I recommend filing the transcript as D5, though, as it could perhaps be a cover-up of a conspiracy to set up a new cryptophone platform together with these Oerlemans and Royer types? If they are indeed intellectuals involved in privacy and criminal law, I hope they won't make things worse for us police

officers. We already have enough trouble with the Police Data Act and that new data protection officer. Let me just do my job, is what I always say.]

## Papers in this special issue

Roberto Flor and Beatrice Panattoni, 'Digital criminal investigations in Italy. The intersection between data protection and cybersecurity'

*Based on an analysis of the Italian regulation of data production orders and police hacking, the authors argue that the normative framework for digital criminal investigations should consist not only of privacy and data protection, but also of cybersecurity as a separate, vital interest.*

Maša Galič and Lonneke Stevens, 'Regulating police use of facial recognition technology in the Netherlands. The complex interplay between criminal procedural law and data protection law'

*Analysing the complex interplay between criminal procedure and data protection law in the Dutch regulation of police use of facial recognition technology, the authors highlight three main gaps in the system of checks and balances, stemming from differences in mindset, legal basis, and supervision.*

Jan Jaap Oerlemans and Sofie Royer, 'The future of data-driven investigations in light of the Sky ECC operation'

*The authors describe the Sky ECC operation (hacking and intercepting a platform for encrypted communications) and discuss the implication of data-driven investigations in "grey infrastructures" for the right to privacy and the right to a fair trial, based on European, Dutch, and Belgian case-law.*

Inger Marie Sunde, 'To have or have not. Limiting the data available for subsequent use by the police'

*Based on purpose limitation and purpose orientation, fairness, and regulation of intercepted communications in Norwegian law, the author argues that in police investigations involving bulk data, only data forensically analysed in the investigation at hand should be allowed to be re-used in other cases.*

Sarah Tas, 'The (challenging) increasing support of Europol in national criminal investigations. The *yin* to the *yang*'

*Analysing the 2022 amendments to the Europol Regulation, the upcoming Prüm II regime, and associated challenges to individuals' data protection, the author argues that while Europol plays an increasing role in national criminal investigations, it lacks sufficient safeguards and effective oversight.*

Ruben Te Molder, Masha Fedorova, Marieke Dubelaar and Sjarai Lestrade, 'The principle of purpose limitation in data-driven policing: a guiding light or an empty shell?'

*The authors discuss the challenges that the principle of purpose limitation in the EU Law Enforcement Directive poses to national law-makers when regulating data-driven policing and how these can be addressed, based on analysis of the Directive's legislative history and CJEU and ECtHR case-law.*

## Acknowledgements

This special issue is a follow-up of the international expert workshop on 'Bridging the regulatory disconnect between data collection and data analysis in criminal investigation' organised by Maša Galič and Juraj Sajfert at the VU University Amsterdam on 20 January 2023.

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## ORCID iDs

Maša Galič https://orcid.org/0000-0001-7119-5843
Bert-Jaap Koops https://orcid.org/0000-0002-2906-8215

## References

Bygrave Lee, 'The Byzantine Turn in EU Data Protection Law', in *The GDPR at Two: Expert Perspectives* (May 2020), https://iapp.org/resources/article/gdpr-at-two-expert-perspectives/

De Hert Paul & Gutwirth Serge, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', in Erik Claes, Antony Duff & Serge Gutwirth (eds), *Privacy and the criminal law* (Intersentia 2006)

Fedorova MI, te Molder RM, Dubelaar MJ, Lestrade SMA & Walree TF. *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*. STeR/WODC, 2022.

Foqué R & 't Hart AC, *Instrumentaliteit en rechtsbescherming. Grondslagen van een strafrechtelijke waardendiscussie* (Gouda Quint 1990)

González Fuster Gloria, '*Beyond the GDPR*, above the GDPR' [2015] *Internet Policy Review*, https://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385