Digital investigation powers and privacy

Hirsch Ballin, Marianne; Gali, Maša

published in
Boom Strafblad
2021

DOI (link to publisher)
10.5553/BSb/266669012021002004007

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

citation for published version (APA)
Hirsch Ballin, M., & Gali, M. (2021). Digital investigation powers and privacy: Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure. *Boom Strafblad*, *2*(4), 148-159. [2021/4]. https://doi.org/10.5553/BSb/266669012021002004007

Article

Digital investigation powers and privacy

Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure

Prof. mr. M.F.H. (Marianne) Hirsch Ballin and dr. mr. M. (Maša) Galič*

1. Introduction

Technological advances in the past thirty years have significantly increased the array of tools for investigating and prosecuting crimes, providing law enforcement with almost endless possibilities for electronic surveillance.[1] The police can now not only search the data on a suspect's computer and all of its connected networks or intercept his communications, it can also track a suspect anywhere on earth using GPS or stealth SMS, and even hack his or her computer. This increasing sophistication of digital investigation techniques leads to more efficient and effective investigation and prosecution of crimes. In fact, it is necessary to benefit from the possibilities of digital investigative techniques in order to keep pace with suspects' use of technology, especially in the context of serious organised crime. At the same time, the potential high degree of intrusiveness of such techniques seriously interferes with fundamental rights, particularly the right to privacy.[2]

Many legal systems – including the Netherlands – are still struggling with the regulation of these digital powers.[3] Digital methods of investigation oftentimes remain unregulated by statutory law, or are regulated in a makeshift manner by already existing provisions developed for analogue investigation methods, such as searching and seizing physical documents. In view of this lack of legislative regulation, courts have played a key role in the regulation of digital investigation powers.[4] This led to a type of *ad hoc* regulation, which is neither very consistent nor comprehensive.

In the Netherlands, this situation is about to change with the proposed modernisation of criminal procedure, representing a big step forward. An important element of the new draft Code of Criminal Procedure concerns the manner in which digital investigation powers have been embedded in the regulation of criminal investigation. Based on the advice of the Committee 'modernising criminal investigation in the digital era' (Committee-Koops), the investigation of data has obtained a central position in the draft law, with the criterion of systematicness (*stelselmatigheid*) playing a key normative role.[5] Some specific techniques in the digital context

* Marianne Hirsch Ballin is professor of Criminal Law and Criminal Procedure at Vrije Univeristeit Amsterdam and member of the editorial board of this journal. Maša Galič is assistant professor Criminal Law and Criminal Procedure at Vrije Universiteit Amsterdam.

1. G. Di Paolo, 'Judicial investigations and gathering of evidence in a digital online context', *International Review of Penal Law* (80) 2009/1, p. 201.
2. See *e.g.*, J.A.E. Vervaele, 'Surveillance and criminal investigation: blurring the thresholds and boundaries in the criminal justice system?', in: S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection*, Dordrecht: Springer 2014; Di Paolo 2009.
3. See *e.g.*, Report of the Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie-Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, June 2018.
4. Di Paolo, 2009, p. 202. In the Dutch context, see *e.g.*, B.J. Koops en J.J. Oerlemans (eds.), *Strafrecht en ICT*, Den Haag: SDU Uitgevers 2019, p. 207; W.Ph. Stol, 'Essenties van politiewerk en digitalisering', *Strafblad* 2019/1. In regard to the search of a smartphone see L. Stevens, 'Onderzoek in een smartphone. Zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing', *AA* 2017, 730.
5. Report of the Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie-Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, June 2018.

doi: 10.5553/BSb/266669012021002004007

will also be given a specific statutory basis for the first time, such as the search of data carriers, open-source investigations and network searches.[6]

Nevertheless, it remains important to pay attention to the jurisprudence of the European Court of Human Rights (ECtHR or Court),[7] which continues to set minimum safeguards for the interference with private life in the digital context. Whereas the Court of Justice of the European Union has not yet ruled on the specific subject of digital investigation powers, the ECtHR is no stranger to its regulation, particularly in regard to Article 8 ECHR.[8] The ECtHR has oftentimes acknowledged that there is a need for vigilance in the light of increasingly sophisticated technology, where 'advances in technology present increasing threats to the private life of the individual'.[9] The Strasbourg Court has made it very clear that any state, which claims a pioneer role in the development of new investigatory technologies, also bears *special responsibility* for striking the right balance between the public interest in the prevention and prosecution of crime and the protection of a person's private life.[10] Considering that the Dutch state certainly stands at the forefront of the development and deployment of novel investigation technologies,[11] there is a need to take particular care when it comes to its regulation.

While the ECtHR has not yet ruled on the most recent investigation techniques such as hacking, open-source investigation or predictive policing, it has nevertheless set minimum safeguards in relation to other investigatory developments, such as digital search and seizure, location tracking and bulk interception of communications. In this article, we conduct a brief overview of recent ECtHR jurisprudence concerning several types of digital investigation powers.[12] In our overview, we place particular – although not exclusive – focus on post-2010 case law and organise it in relation to the five types of digital powers on which the Court has recently ruled: the creation of police databases, digital search and seizure, location tracking, the collection and processing of traffic data, and bulk interception of communications. A notable omission in our examination is case law concerning targeted interception of communications by the police. This is due to the fact that most recent ECtHR case law focuses on 'bulk' interception of communications conducted by intelligence agencies, rather than 'targeted' interception conducted by the police. Considering the increasing importance of specialised police units that are employing preventive and bulk investigation techniques for the purpose of gathering *police intelligence*,[13] we find it important to present the newly expanded safeguards concerning mass surveillance as well.

The goal of this article is twofold. First of all, we aim to provide a broad overview of the current state of ECtHR jurisprudence concerning five types of digital investigation powers. Such an overview is needed because it explicates the ECtHR-requirements for regulating these powers; something that is relevant for all European countries that are in the process of developing adequate legal bases for new digital powers.[14] Furthermore, such an overview enables scholars and regulators to draw conclusions for the regulation of other digital investigation powers, including those that are yet to come. In the first part of this article, we therefore examine recent ECtHR case law concerning: (1) databases and personal data, (2) digital search and seizure, (3) location tracking, (4) traffic data and (5) bulk interception of communications.

The second goal of this article is to draw conclusions from this case law for the upcoming regulation of digital investigation powers in the Netherlands. The draft new Code of Criminal Procedure (draft CCP) namely provides for specific regulation of digital investigation (with some exceptions[15]) for the first time. In general, the draft CCP is founded upon the requirements stemming

6. Draft Explanatory note new CCP (version July 2020), available at: https://www.rijksoverheid.nl/onderwerpen/nieuwe-wetboek-van-strafvordering/documenten/publicaties/2020/07/30/ambtelijke-versie-juli-2020-memorie-van-toelichting-wetboek-van-strafvordering (last visited on 10 July 2021), pp. 32-33; see 'Advies van de Commissie Implementatie nieuw Wetboek van Strafvordering (Commissie-Letschert)', bijlage bij *Kamerstukken II* 29 279, nr. 637, p. 3.
7. Of course, the same applies to the jurisprudence of the Court of Justice of the European Union (CJEU) in relation to the right to respect for the private and family life and the right to protection of personal data (Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union). However, in this article we focus on the jurisprudence of the ECtHR, because the CJEU has – as yet – not examined digital investigation powers in particular. It has addressed the matter only indirectly, in relation to data retention obligations (*e.g.*, *Digital Rights Ireland Ltd*, C-293/12 and C-594/12 and *Prokuratuur*, C-746/18). Moreover, the CJEU must take account of the jurisprudence of the ECtHR regarding corresponding rights protected in the ECHR (see *e.g.*, CJEU 2 February 2021, C-481/19, ECLI:EU:C:2021:84 (*Consob*)). See M.G. Pascuel, 'A European Standard of Human Rights Protection?', p. 58 and E. Brouwer, 'Private Life and Data Protection in the Area of Freedom, Security and Justice, p. 375 in S.I. Sanchez and M.G. Pascuel (eds.), *Fundamental Rights in the EU Area of Freedom, Security and Justice*, Cambridge University Press 2021.
8. See *e.g.*, T. Murphy and G. Ó Cuinn, 'Works in Progress: New Technologies and the European Court of Human Rights', *Human Rights Law Review* 2010/4.
9. B. Rainey, E. Wicks and C. Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights*, Oxford: Oxford University Press 2017, p. 410.
10. ECtHR Case 4 December 2008, ECLI:CE:ECHR:2008:1204JUD003056204, appl. nos. 30562/04 and 30566/04 (*S. and Marper v. United Kingdom*), para. 112.
11. See *e.g.*, C. Driessen and J. Meeus, 'Unieke hack van EncroChat leidt tot veel lastige juridische vraagstukken', *NRC*, 9 June 2021.
12. In order to compose a list of recent ECtHR case law concerning various types of digital investigation powers, we first consulted case law included in ECtHR factsheets concerning 'new technologies', 'personal data protection' and 'mass surveillance' (all from May 2021). We then searched the HUDOC database concerning Art. 8 cases with terms: 'digital investigation', 'electronic data', 'computer data', 'digital search', 'digital access', 'GPS surveillance', 'location tracking', 'communications data', 'traffic data', 'mass surveillance' and 'secret surveillance'. This resulted in a narrowed-down list of sixty judgments, from which we then excluded cases concerning targeted interception of communications.
13. See *e.g.*, M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States* (diss. Utrecht), The Hague: Springer 2012, p. 26 and 184; Vervaele 2014, p. 122.
14. For this reason, we have also decided to write this paper in English.
15. *E.g.*, the authority to hack computers, Art. 126nba CCP.

from Article 8 ECHR.[16] However, the draft explanatory note does not include any concrete assessment against the background of recent ECtHR case law regarding digital investigation. In the second part of this article, we therefore examine the manner in which three types of digital investigation powers – the investigation of data, open-source investigations and location tracking – have been regulated in the draft law, and whether this implementation has been done in accordance with ECtHR case law. Our analysis of the draft provisions regarding digital investigation does not aim to be comprehensive. On the contrary, the aim is to draw attention to those aspects that stand out on the basis of ECtHR case law, including the specificity of the legal basis, the need of end-to-end safeguards and the importance of ex ante safeguards. We conclude by emphasising the urgency of *specific* regulation of digital investigation powers – and the modernisation of the CCP in general – and by highlighting the most notable implications from ECtHR case law from which the modernisation process would further benefit.

2. ECtHR jurisprudence concerning digital investigation powers

2.1 Databases and personal data

There is longstanding ECtHR case law concerning the processing of personal data for the purpose of detection and prevention of crime. The ECtHR has made it very clear that when an individual's personal data are retained by the police, data protection principles and rights need to be in place. This includes minimum safeguards concerning, inter alia, duration, storage, use, access by third parties, procedures for preserving the integrity and confidentiality of data, as well as procedures for its destruction.[17]

According to the Court's case law, the mere collection and retention of personal data – including fingerprints, palm prints, photographs, physical descriptions, DNA profiles and cell samples – in a police database constitutes an interference with the right to private life.[18] When considering whether the interference was legitimate, the Court commonly focuses on the 'necessary in a democratic society' requirement. For this purpose, the Court assesses the proportionality of the collection and retention of personal data, placing particular emphasis on safeguards such as the nature and gravity of the offence(s) in question, whether the person was eventually convicted or not, and whether there was a time-limit and an independent review concerning the retention of data.[19] These safeguards need not only be present in the law, the Court also checks whether they were effective for the applicant in practice.[20]

Another element t the Court considers in its assessment of the proportionality of the measure is the level of actual interference with private life. This does not mean that when it comes to personal data, which are in principle less privacy-sensitive (*e.g.*, fingerprints and photographs), the identified safeguards need not be implemented.[21] Quite the contrary. In view of rapid advances in digital technology and the ever-expanding desire of law enforcement to store as much personal data as possible, the need for safeguards is high, even when it comes to data that are less privacy-sensitive. In Gaughran v. UK, for instance, the Court dealt with the situation, in which the (indefinite) retention of photographs in a police database was coupled with the real possibility to search the database with facial recognition technology. Due to the likely use of such sophisticated technology, the risk for interference with private life and for abuse is much higher than it would otherwise be, and must be accompanied with a high level of safeguards.[22] The Court nicely summed it up in Aycaguer v. France:

> '[T]he Court observes at the outset that it fully realises that in order to protect their population as required, the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences, including the most serious types of crime … However, such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept. Indeed, without respect for the requisite proportionality vis-à-vis the legitimate aims assigned to such mechanisms, their advantages would be outweighed by the serious

16. Draft Explanatory note new CCP (version July 2020), p. 29.
17. ECtHR Case 11 June 2020, ECLI:CE:ECHR:2020:0611JUD007444017, appl. no. 74440/17 (P.N. v. Germany), para. 62; see also S. and Marper v. United Kingdom; ECtHR Case 4 May 2000, ECLI:CE:ECHR:2000:0504JUD002834195, appl. no. 28341/95 (Rotaru v. Romania).
18. See *e.g.*, P.N. v. Germany; ECtHR Case 13 February 2020, ECLI:CE:ECHR:2020:0213JUD004524515, appl. no. 45245/15 (Gaughran v. United Kingdom); ECtHR Case 24 January 2019, ECLI:CE:ECHR:2019:0124JUD004351415, appl. no. 43514/15 (Catt v. United Kingdom); ECtHR Case 22 June 2017, ECLI:CE:ECHR:2017:0622JUD000880612, appl. no. 8806/12 (Aycaguer v. France); ECtHR Case 18 April 2013, ECLI:CE:ECHR:2013:0418JUD001952209, appl. no. 19522/09 (M.K. v. France); S. and Marper v. United Kingdom.
19. These elements include: (1) whether and how domestic authorities had taken into account the nature and gravity of the offences in question in their decision to retain data; (2) whether the person concerned was (subsequently) convicted in the criminal proceedings or not; (3) the level of actual interference with the right to respect for private life; (4) whether there was a time limit for the retention of data, and the length of this time limit; (5) whether there was an independent review of the necessity to further retain the data in question, allowing the deletion in practice of the data if they were no longer needed for the purpose for which they had been obtained; and (6) whether in the light of ECtHR case law, there were sufficient safeguards against abuse (*e.g.*, unauthorised access, dissemination). See *e.g.*, P.N. v. Germany, para. 74; see also Catt v. United Kingdom; S. and Marper v. United Kingdom; ECtHR Case 4 June 2013, ECLI:CE:ECHR:2013:0604DEC000784108, appl. nos. 7841/08 and 57900/12 (Peruzzo and Martens M.K. v. France, para. 41.
20. See *e.g.*, Gaughran v. United Kingdom, para. 94; M.K. v. France, para. 41.
21. S. and Marper v. United Kingdom, para. 120.
22. Gaughran v. United Kingdom, para. 86; see also Catt v. United Kingdom, para. 114; S. and Marper v. United Kingdom, para. 71.

doi: 10.5553/BSb/266669012021002004007

breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction.'[23]

2.2 Digital search and seizure

The ECtHR has also dealt with several cases concerning digital search and seizure, by which we mean access to and seizure of electronic data stored in various forms (*e.g.*, on a smartphone, laptop or hard drive). Most of these cases (also) concern data protected by the legal professional privilege (LPP), but not all. In this section, we will first examine both search and seizure of electronic data in general, followed by an examination of search and seizure of electronic data protected by LPP in particular.

According to the ECtHR, traditional or physical search and seizure represent 'a serious interference with private life, home and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear and detailed rules on the subject'.[24] Recent ECtHR case law has made it clear that the same applies when it comes to digital searches and seizures.[25]

Just as with databases, the Court usually focuses on the question, whether the digital search and seizure were 'necessary in a democratic society', when assessing the legitimacy of the interference. For this purpose, the Court employs the same criteria as when it considers 'traditional' searches and seizures:

1. the severity of the relevant offence;
2. whether the search was based on a warrant issued by a judge and based on reasonable suspicion;
3. whether the scope of the warrant was reasonably limited; and
4. in cases where the search of a lawyer's office is concerned, whether the search was carried out in the presence of an independent observer in order to ensure that materials subject to LPP were not removed.[26]

A warrant issued by a judge is thus a general requirement when it comes to digital search and seizure. Notably, the Court does not seem to distinguish between more or less intrusive searches, which would not require such a warrant.[27] Delimiting the scope of the warrant is an important ex ante safeguard meant to limit the intrusion into private life.[28] Furthermore, the Court looks not only at the manner in which the warrant was drafted, but also the manner in which the search and seizure were actually executed.[29] In Robathin v. Austria, the Court considered that a search warrant, which led to the copying of all of the applicant's electronic data in practice, could not be considered 'reasonably limited'.[30]

Deficiencies in the limitation of the scope of the warrant – or even a complete lack of a warrant – can nevertheless be offset by ex post judicial review. However, in order for this review to be an effective safeguard against abuse, it needs to be quite rigorous. In Robathin, the Court noted that the reviewing domestic court

> 'gave only very brief and rather general reasons when [approving] the search of all the electronic data from the applicant's law office [as authorised by the investigatory judge in the warrant]. In particular, it did not address the question whether it would be sufficient to search only those discs which contained data relating to "R." and "G.". Nor did it give any specific reasons for its finding that a search of all of the applicant's data was necessary for the investigation. Thus, the way in which the Review Chamber exercised its supervision in the present case does not enable the Court to establish that the search of all of the applicant's electronic data was proportionate in the circumstances.'[31]

When data protected by LPP are concerned, the ECtHR requires much higher safeguards and much more concrete rules.[32] After all, professional secrecy forms the basis of the relationship of trust between a lawyer and her client, and the corollary of the right of a lawyer's client not to incriminate him- or herself.[33] It is important to note that stricter rules govern not only cases of digital searches and seizures in a lawyer's office, but also cases in which privileged information is likely to be found on the smartphone or computer of a lawyer's client.

23. Aycaguer v. France, para. 34. The Court repeated the last part of the paragraph in Gaughran v. United Kingdom, para. 93; see also S. and Marper v. United Kingdom, para. 112.
24. ECtHR Case 27 September 2005, ECLI:CE:ECHR:2005:0927JUD005088299, appl. no. 50882/99 (Petri Sallinen and others v. Finland), para. 90.
25. See *e.g.*, Petri Sallinen and others v. Finland, para. 90 and ECtHR Case 17 December 2020, ECLI:CE:ECHR:2020:1217JUD000045918, appl. no. 459/18 (Saber v. Norway).
26. See *e.g.*, ECtHR Case 3 July 2012, ECLI:CE:ECHR:2012:0703JUD003045706, appl. no. 30457/06 (Robathin v. Austria), para. 45-7; ECtHR Case 22 May 2008, ECLI:CE:ECHR:2008:0522JUD006575501, appl. no. 5755/01 (Iliya Stefanov v. Bulgaria), para. 38; ECtHR Case 16 October 2007, ECLI:CE:ECHR:2007:1016JUD007433601, appl. no. 74336/01 (Wieser and Bicos Beteiligungen GmbH), paras. 57-60.
27. However, the Court has not yet ruled on a case concerning the search of a smartphone incident to arrest and whether a warrant is required in that case as well. For a comparative perspective on this topic see B.J. Koops, B.C. Newell and I. Škorvánek, 'Location Tracking by Police: The Regulation of "Tireless and Absolute Surveillance"', UC Irvine Law Review, 2019/3.
28. ECtHR Case 30 September 2014, ECLI:CE:ECHR:2014:0930JUD000842905, appl. no. 8429/05 (Prezhdarovi v. Bulgaria), para. 49; Robahtin v. Austria, para. 47.
29. See *e.g.*, Iliya Stefanov v. Bulgaria, para. 38; Robahtin v. Austria, para. 47.
30. 'While limiting the search and seizure of files to those concerning R. and G., [the warrant] authorised in a general and unlimited manner the search and seizure of documents, personal computers and discs, savings books, bank documents and deeds of gift and wills in favour of the applicant'; Robathin v. Austria, para. 47.
31. *Robathin v. Austria*, para. 51; see also ECtHR Case 3 December 2019, ECLI:CE:ECHR:2019:1203JUD001470412, appl. no. 14704/12 (*Kırdök and others v. Turkey*), para. 53; *Prezhdarovi v. Bulgaria*, para. 49; *Iliya Stefanov v. Bulgaria*, para. 38.
32. For an in-depth discussion of this topic, see L. Stevens & M. Galič, 'Bescherming van het professionele verschoningsrecht in geval van doorzoeking van een smartphone: het EHRM eist een concrete basis en een praktische procedurele regeling in het recht' (forthcoming *Ars aequi*).
33. *Saber v. Norway*, para. 51.

When it comes to search and seizure, which might involve privileged electronic data, the Court demands very clear and precise rules set out in advance in the law, preferably in statutory law.[34] In recent case law, the Court noted that general procedural rules regarding searches and seizures concerning physical places and documents oftentimes include numerous provisions in several laws. This situation can quickly lead to unclarity and diverging views on the extent of the protection afforded to privileged material in the context of digital devices.[35] This was the case in *Saber v. Norway*, in which the Court emphasised the absence of any express and specific procedural guarantees, which could safeguard LPP from being compromised by the digital search. It noted in particular, that there was no indication of how to go about the filtering of privileged information from the smartphone in practical terms, that is, who may conduct the filtering and according to which procedural rules and safeguards?[36] When it comes to digital searches in the context of privileged information, the Court thus places greater emphasis on *ex ante* safeguards than on *ex post* (judicial) review.

2.3 Location tracking

Location data is a valuable piece of information in criminal investigations as it can pin down a suspect to a crime scene or provide them with an alibi. While such data can be gathered as a type of data about a communication (see discussion on traffic data in section 2.4), it can also be gathered beyond the context of communications, for instance through GPS tracking or automated number plate recognition. There are two notable cases in which the ECtHR has considered the interference of GPS surveillance[37] with the right to private life: *Uzun v. Germany*[38] and the more recent case of *Ben Faiza v. France*.[39]

The ECtHR considers the gathering of location data (in public space) through GPS surveillance a limited intrusion into a person's private life. This means that the legal framework governing the use of GPS surveillance does not need to be as strict and precise as in the case of interception of communications or visual observation.[40] Nevertheless, the legal framework governing GPS surveillance still needs to satisfy the Court's general principles on adequate protection against arbitrary interference with Article 8 ECHR, requiring a consideration of the scope and duration of the measure, the grounds for ordering it, the authorities competent to authorise and carry it out, and the remedies provided by the law.[41]

Based on these general principles, non-systematic GPS surveillance does not always require a warrant issued by a judge. However, cases of systematic GPS surveillance (*e.g.*, lasting more than a month) *in principle* do require such authorisation.[42] In *Uzun*, the Court also noted that authorities need to consider the 'aggregation of surveillance measures' when determining the intrusion into private life.[43] While GPS surveillance *in itself* might be a limited intrusion into privacy, the aggregation of surveillance measures can lead to an extensive observation of a person's conduct and, thus, a more serious interference with their private life, requiring a higher level of safeguards.[44]

Furthermore, the Court has recently made clear that even in the case of a limited intrusion into private life, such as with (non-systematic) GPS surveillance, a very general legal basis will likely not satisfy the requirements of Article 8 ECHR. In *Ben Faiza*, the relevant French provision at the time referred merely to a very general notion, allowing the police to conduct all 'acts of information deemed useful for establishing the truth'.[45] Even though the provision designated the investigatory judge (*juge d'instruction*) as the authority carrying out such measures, the Court considered that it did not indicate with sufficient clarity to what extent and how this authority was entitled to use its discretionary power,[46] finding a violation of Article 8 ECHR.

2.4 Traffic data

Traffic data refer to data that provide information *about* a communication, for example a text message, email or phone call. They can reveal the origin, destination, route, time, date, size and duration of the communication,[47] but they do not reveal its content. As such, the gathering of traffic data is oftentimes considered as amounting to a lesser intrusion into a person's private life than the gathering of content data.[48]

34. See *e.g.*, *Saber v. Norway*, paras. 55-56; *Petri Sallinen and others v. Finland*, paras. 91-92.
35. *Ibid*.
36. *Saber v. Norway*, paras. 52-56.
37. GPS is a radio navigation system that works with the help of satellites which allows for the continuous location of objects equipped with a GPS receiver (*e.g.*, a smartphone or a car with a GPS tracker) anywhere on earth.
38. ECtHR Case 2 September 2010, ECLI:CE:ECHR:2010:0902 JUD003562305, appl. no. 35623/05 (*Uzun v. Germany*).
39. ECtHR Case 3 February 2018, ECLI:CE:ECHR:2018:0208 JUD003144612, appl. no. 31446/12 (*Ben Faiza v. France*).
40. *Uzun v. Germany*, para. 66.
41. A full list of these general principles includes: (1) the nature, scope and duration of the possible measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out and supervise them; and (4) the kind of remedy provided by national law; *Uzun v. Germany*, para. 63.
42. In *Uzun v. Germany*, the Court nevertheless found in that *ex post* judicial review of GPS surveillance and the possibility to exclude evidence thereby is a sufficient safeguard against abuse (paras. 71-72).
43. *Uzun v. Germany*, para. 79; *Ben Faiza v. France*, para. 58.
44. *Uzun v. Germany*, para. 80.
45. Art. 81 Code Pénal: «Le juge d'instruction procède, conformèment à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vèritè. Il instruit à charge et à dècharge. … »; as referred to in *Ben Faiza v. France*, paras. 58-60.
46. *Ben Faiza v. France*, paras. 58-60.
47. See *e.g.*, Art. 1(d) of the Cybercrime Convention (Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest).
48. See *e.g.*, the argumentation of the Dutch government, acting as an intervening government in the *Big Brother Watch and others v. United Kingdom* judgment, stating that it is 'still relevant to distinguish between content and communications data, as the content of communications [is] likely to be more sensitive than communications data' (Big Brother and others v. UK, para. 231).

doi: 10.5553/BSb/266669012021002004007

The collection and processing of traffic data has garnered particular attention in ECtHR jurisprudence in the context of mass surveillance cases in the past fifteen years (discussed in section. 2.5). However, the Court dealt with traffic data already in 1984 in *Malone v. the United Kingdo*m.[49] In this case, the Court determined that 'metering' – a process, which registers the numbers dialled on a telephone and the time and duration of each call – processes data, which are an integral element in the communications made via the telephone.[50] Releasing metering information to the police therefore entails an interference with the right to private life and requires an adequate legal framework in place.[51]

Two important questions arise here: how serious is the interference with privacy in the case of traffic data and what kind of legal framework is required? These questions received an answer in recent mass surveillance cases, at least in regard to bulk interception. In the two mass surveillance cases from 2021,[52] the ECtHR has made clear that traffic data can indeed reveal a great deal of personal information, such as the identities and geographic location of the sender or recipient, and the equipment through which the communication was transmitted.[53] The Court thus makes clear that the interference with privacy through traffic data is not as minor as is oftentimes assumed. Moreover, when traffic data are obtained in bulk, the intrusion is magnified,

> 'since [traffic data] are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with'.[54]

At least in the context of bulk interception, the ECtHR concluded that the acquisition of traffic data is 'not necessarily less intrusive than the acquisition of content'.[55] This means that the collection, retention and processing of (bulk) traffic data should in principle be governed by the same rules and safeguards as those applicable to content data.[56] While the Court noted that this does not mean that the legal provisions governing traffic data need to be 'identical in every respect' to those governing content data, the space for discretion seems to be rather narrow.[57]

2.5 Bulk interception and mass surveillance

In May 2021, the ECtHR ruled in two landmark mass surveillance cases and set stricter standards for bulk interception of communications by intelligence agencies: *Big Brother Watch and others v. United Kingdom* and *Centrum för rättvisa v. Sweden*.

Until now, the ECtHR has been routinely applying the six minimum safeguards developed for targeted interception of communications in criminal investigations[58] to cases concerning mass surveillance – that is, non-targeted or 'bulk' interception of communications for intelligence gathering.[59] However, in the two new judgments the Court notes quantitative and qualitative differences between targeted and bulk interception, which demand different standards of assessment. Considering the enhanced dangers for abuse stemming from bulk interception, the Court notes that such a regime requires *end-to-end safeguards*. This means that: (a) an assessment should be made at each stage of the process of the necessity and proportionality of the measures; (b) bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and (c) the operation should be subject to supervision and independent *ex post facto* review.[60] The Court also acknowledged that bulk interception is a gradual process in which the degree of interference with individuals' Article 8-rights increases as the process progresses and begins to target individuals. Nevertheless, the Court makes clear that the requirements of Article 8 ECHR apply to *all* of the stages of the interception process.[61]

Based on these general considerations, the Court sets out a new and expanded list of eight criteria that need to be taken into account when it comes to bulk interception of communications:

49. ECtHR Case 2 August 1984, ECLI:CE:ECHR:1984:0802JUD000869179, appl. no. 8691/79 (*Malone v. United Kingdom*).
50. *Ibid*., para. 84.
51. *Ibid*., para. 87.
52. ECtHR Case 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, appl. nos. 58170/13, 62322/14 and 24960/15 (*Big Brother Watch and others v. United Kingdom*) and ECtHR Case 25 May 2021, ECLI:CE:ECHR:2021:0525JUD003525208, appl. no. 35252/08 (*Centrum för rättvisa v. Sweden*).
53. *Big Brother and others v. United Kingdom*, para. 342; *Centrum för rättvisa v. Sweden*, para. 256.
54. *Big Brother Watch and others v. United Kingdom*, para. 342; *Centrum för rättvisa v. Sweden*, para. 256.
55. *Big Brother Watch and others v. United Kingdom*, para. 364.
56. *Big Brother Watch and others v. United Kingdom*, para. 364.
57. In the case of *Big Brother Watch and others v. United Kingdom*, the UK regime concerning traffic data was generally the same as for content data, but it did differ in two respects. The Court examined whether the difference was justified and whether the safeguards were sufficiently robust (para. 421). In the *Centrum för rättvisa v. Sweden*, the rules governing traffic data were the same as for content data.
58. These minimum safeguards developed in 1990s ECtHR case law are: (1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed; see *e.g.*, ECtHR case 24 April 1990, ECLI:CE:ECHR:1990:0424JUD001110584, appl. no. 11105/84 (*Huvig v. France*) and ECtHR Case 24 April 1990, ECLI:CE:ECHR:1990:0424JUD001180185, appl. no. 11801/85 (*Kruslin v. France*).
59. See *e.g.*, ECtHR Case 1 July 2008, ECLI:CE:ECHR:2008:0701JUD005824300, appl. no. 58243/00 (*Liberty and others v. United Kingdom*); ECtHR Case 29 June 2006, ECLI:CE:ECHR:2006:0629DEC005493400, appl. no. 54934/00 (*Weber and Saravia v. Germany*).
60. *Big Brother Watch and others v. United Kingdom*, paras. 350, 357 and 359.
61. *Ibid*., para. 330.

1. the grounds for authorisation;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure for granting authorisation;
4. the procedures for selecting, examining and using intercepted material;
5. the precautions when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercepted material and the circumstances for erasure and destruction of the material;
7. the procedures and modalities of supervision by an independent authority and its powers to address non-compliance; and
8. the procedures for independent *ex post facto* review of such compliance and the powers of the competent body in addressing instances of non-compliance.[62]

Considering the British and Swedish intelligence regimes, the Court placed particular focus on the third, fourth, fifth and eighth criterion, emphasising both *ex ante* and *ex post* safeguards when it comes to intelligence gathering.

According to the third criterion, authorisation of bulk interception needs to be granted by a body independent of the executive. Moreover, the authorisation process needs to include *ex ante* oversight of the choice and application of selectors and query terms (*e.g.*, keywords, IP or email addresses with which the initial automated search of bulk data is done), or at least the categories of selectors.[63] When it comes to 'strong selectors' such as email addresses, which enable specific individuals to be targeted, enhanced safeguards are required.

The fourth criterion requires that the material resulting from the initial searches through selectors – the stage at which the process begins to target individuals through strong selectors – is described in a sufficiently precise manner in the warrant, so as to provide meaningful restriction. For instance, 'material providing intelligence on terrorism as defined in the Terrorism Act 2000' was seen as insufficiently precise by the Court.[64] In order to facilitate the supervision of the bulk interception process, this criterion also requires that logs and detailed records of each step in the bulk interception operation, including all of the selectors used, are kept and set out in domestic law.[65]

The fifth criterion applies when making a decision about intelligence sharing, especially with foreign agencies. It requires that prior to the sharing consideration is given to the privacy interests of the individual concerned, and that this consideration is also provided for in a law.[66]

Finally, the eighth criterion requires that *ex post* review by an independent body is available to anyone suspecting that their communications have been intercepted by intelligence services. The review needs to guarantee insofar as possible an adversarial process, which means that its decisions also need to be reasoned and legally binding.[67] A review, which would only inform the complainant that an investigation has been carried out, without any reference as to the content, would thus not meet this requirement. As the Court put it, reasoned decisions are needed in order to provide 'sufficient basis for public confidence that abuses, if they occur, will be unveiled and remedied'.[68]

2.6 Conclusion: insights stemming from ECtHR case law

The above brief examination of recent ECtHR case law concerning five types of digital investigation powers that have been examined by the Court, offers several insights relevant for the regulation of digital investigation powers. For the purpose of examining the Dutch modernisation of criminal procedure law in light of this ECtHR case law, we single out five insights in particular:

- the importance of adopting specific and concrete provisions concerning digital investigatory powers, which lead to clarity and foreseeability of the law;
- the requirement for a sufficiently specific legal basis even in the case of powers, which in principle represent a limited intrusion into private life, such as GPS surveillance;
- the need for end-to-end safeguards when it comes to the collection and processing of large amounts of traffic data (particularly in the context of bulk interception), as such processing also amounts to a significant privacy intrusion;
- the absence of a distinction between more or less intrusive digital searches (all searches and seizures are considered a serious interference with private life), where the requirement of a warrant issued by a judge is an important safeguard; and
- the prerequisite of *ex ante* safeguards (preferably in statutory law), when it comes to serious interferences with private life or other rights and principles, such as cases concerning the LPP-data and bulk interception of communications (for less privacy-intrusive digital powers, *ex post* judicial review may be sufficient, but this review will need to be quite rigorous in order to satisfy the requirements of Article 8 ECHR).

In the following section we will apply these insights concerning the regulation of digital investigation powers to the modernisation of the CCP.

62. *Big Brother Watch and others v. United Kingdom*, para. 361; *Centrum för rättvisa v. Sweden*, para. 275.
63. *Big Brother Watch and others v. United Kingdom*, para. 383.
64. *Ibid.*, para. 386.
65. *Centrum för rättvisa v. Sweden*, para. 311.
66. *Ibid.*, para. 330.
67. *Ibid.*, paras. 361-362.
68. *Ibid.*, para. 361.

doi: 10.5553/BSb/266669012021002004007

3. The implications of ECtHR case law on the modernisation of the Code of Criminal Procedure

The draft Book 2 of the new Code of Criminal Procedure (CCP)[69] provides for a restructured and partly novel regulation of criminal investigation. An important change compared to the current Code of Criminal Procedure is the adoption of specific provisions that deal with (aspects of) digital investigation, such as the investigation of data and covert investigatory powers, which are found in Chapters 7 and 8.

The modernisation is a big step forward from the current situation in which most of the regulation still needs to be found in provisions developed for analogue investigative powers and, especially, case law. Based on the examined ECtHR jurisprudence, it is safe to say that the adoption of specific provisions dealing with digital investigation powers is urgent. An adequate legal basis offering clarity regarding the applicable safeguards for digital investigation is essential if both law enforcement and society are to benefit from the sophisticated technological developments when confronted by serious organised crime. After all, society needs to know under what circumstances and in what manner the government may employ such intrusive techniques.

In this section, we start by briefly explaining the main assumptions of the proposed new regulatory framework for digital investigation powers and the key role of the criterion of systematicness (3.1). We then focus on three new powers in the draft CCP: the investigation of data, open-source investigations and location tracking. Considering these three new powers, we then examine those aspects of the draft CCP that – based on the main insights stemming from our analysis of ECtHR case law – might require additional attention (3.2.1-3.2.3).

3.1 The key role of the criterion of systematicness

Book 2 of the draft CCP is founded upon two main regulatory assumptions,[70] which not only underpin the regulation of criminal investigatory powers in general, but have an important impact on the regulation of *digital* investigatory powers, particularly through the criterion of systematicness.[71]

The first regulatory assumption concerns the authority, which may authorise (or apply) a specific investigatory power. When the power concerned is considered more intrusive, a higher level and different nature of authority is required, ranging from the investigative (police) officer, the public prosecutor and, finally, to the investigatory judge. The second assumption concerns the required level of precision of the statutory provision determining the conditions under which an investigatory power may be employed. The more intrusive the power, the more detail is required in statutory regulation. There is a normative relation between the two assumptions: the higher the level of intrusiveness of the power, the higher the level of authority that will need to authorise it and the more precise its regulation in the law will need to be.[72]

Due to this normative relation between the two regulatory assumptions – and based on the recommendations of the Committee-Koops – the criterion of systematicness (*stelselmatigheid*) has come to play a key role in the regulation of digital investigation powers. What these investigative powers have in common is that, because of their digital – and infinitely scalable – character, their application may result in severe intrusions into one's private life, depending on factors such as the automated character of application, the amount of data searched and conclusions that can be drawn on the basis of data aggregation and analysis. New digital investigation powers, such as the investigation of data (Title 7.3, Chapter 7),[73] open-source investigations (Art. 2.8.8) and systematic location tracking (Art. 2.8.18),[74] are thus not only regulated by the specific conditions set out in statutory provisions, but also regulated by the general criterion of systematicness.[75]

What does the use of the criterion of systematicness mean in more concrete terms? It means that when the above investigatory powers are considered to result in a limited interference with private life, they may be based on the general power to investigate (draft Art. 2.1.8), and may be conducted by investigative officers without higher authorisation. As an example of a limited interference, the explanatory note mentions scrolling

69. Draft Book II 'The Criminal Investigation' (version July 2020), available at: https://www.rijksoverheid.nl/onderwerpen/nieuwe-wetboek-van-strafvordering/documenten/publicaties/2020/12/11/ambtelijke-versie-juli-2020-wetsvoorstel-wetboek-van-strafvordering-boek-2 (last visited on 10 July 2021).
70. Draft Book II, Arts. 2.1.2-2.1.4. These two regulatory assumptions are not completely new – they form the basis of the regulation of investigatory powers already in the current CCP.
71. Draft Explanatory note new CCP (version July 2020), p. 230-231. The draft Book 2 also includes the codification of certain general principles that have to be taken into account when employing criminal investigation powers: proportionality and subsidiarity, purpose limitation (investigative powers should be exercised 'in the interest of the investigation') and the prohibition of provocation (*instigatieverbod*). These general principles have regulatory influence in addition to the specific conditions set out in the statutory provisions. See Draft Explanatory note new CCP (version July 2020), p. 247-252.
72. The normative relation between the two regulatory assumptions has already been recognised by the Supreme Court in cases dealing with digital investigation, such as search and seizure of smartphones (see *e.g.*, HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017, 229) and open-source investigations (Gerechtshof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (approved by the Supreme Court, HR 24 maart 2020, ECLI:NL:HR:2020:447)).
73. Draft Explanatory note new CCP (version July 2020), p. 400.
74. This corresponds with the approach taken in the current case law; see *e.g.*, Gerechtshof Den Haag 25 May 2018, ECLI:NL:GHDHA:2018:1248 and HR 1 juli 2014, ECLI:NL:HR:2014:1563, *NJ* 2015.
75. The authority to hack someone's computer (draft Art. 2.8.17) is not discussed in this article. This draft provision is identical to the current Art. 126nba CCP and, because it is considered a method that seriously interferes with private life, it is regulated in a particularly precise manner and requires prior authorisation by a judge. As such, systematicness is not particularly relevant for the regulation of this investigative power.

through dial-history and searching a seized smartphone or social media accounts with a (very) narrow scope (*e.g.*, in an investigation concerning graffiti using only the search term graffiti).[76] When the investigation of data is done in a systematic manner, authorisation from a public prosecutor is required (draft Arts.2.7.39(1), 2.8.8 and 2.8.18). An investigation obtains a systematic character when it is reasonably foreseeable that a more or less complete image of certain aspects of someone's private life may be established (draft Art 2.1.1). How exactly this is to be interpreted in practice remains unclear (discussed further in section 3.2.2). For instance, open-source investigations and acquiring location data are assumed to lead only to limited intrusions or, if systematic, to intermediate intrusions, since there is no legal basis for the most intrusive category in the draft law.[77] The last step is reserved for severe interferences into private life, when it is reasonably foreseeable that a far-reaching image of someone's private life may be established (draft Art. 2.1.1). Such a far-reaching interference requires prior authorisation of the investigatory judge.

In the following section, we zoom in on three aspects of the regulation of digital investigation powers in the draft CCP that – in view of examined ECtHR jurisprudence – might require additional attention in the ongoing legislative process: the scope and precision of regulation, the normative relation between the level of intrusiveness and the designated authority and the importance of *ex ante* safeguards in the law.

3.2 The proposed regulation of digital investigatory powers in the new CCP in view of ECtHR case law

3.2.1 Scope and precision of regulation in the draft CCP

The first issue that emerges is the question whether the scope of the draft CCP can be seen as comprehensive in relation to the investigatory powers that it covers. The regulation of the investigation of data, open-source investigations and location tracking is restricted to the acquisition of and obtaining knowledge of the content (*kennis nemen van)*.[78] This means that the provisions do not provide rules governing further use – that is, processing or sharing – of the acquired information. In fact, as explicitly stated in the explanatory note, the principle of purpose limitation – a general principle that needs to be taken into account when employing criminal investigation powers – only applies to the use of the investigative powers provided in the new CCP but not to the use of its results. Even though data protection laws in the field of law enforcement exist,[79] they are considered to insufficiently deal with this issue.[80] As such, a future law is planned to cover data protection in the context of criminal law enforcement.[81] However, at the moment when such a law does not yet exist and, more importantly, when the relation between the power to gather data and the possibilities for storage, further use and/or further automatic processing remain unclear, the level of required *ex ante* safeguards in regard to all of these powers may fall short.

In this regard, ECtHR jurisprudence concerning the processing of personal data and bulk interception may offer some guidance (see paras. 2.1-2.5). Such guidance is particularly important in increasingly common cases, in which the use of investigatory powers results in the acquisition of a large amount of data that are subsequently searched with broad search terms.[82] The importance of end-to-end-safeguards emphasised by the ECtHR in cases dealing with bulk interception by intelligence agencies should therefore also be kept in mind in the context of criminal investigation. The requirement of end-to-end safeguards nicely demonstrates that the regulation of potentially very intrusive powers should not end with the acquisition of the data, but needs to extend to the further phases of data processing, such as selection, examination and further use of data, where the risk of privacy interference is actually the highest.

Furthermore, the manner in which the normative relation between the level of intrusiveness of the power and the required precision of the law has been elaborated in the draft CCP may not be sufficient for all types of data concerned. In recent case law, the ECtHR has emphasised that a clear-cut distinction between less and more serious intrusions into private life based on a distinction between content and traffic (including location) data can no longer be made. Although the intrusion into private life by the acquisition of location or traffic data is in principle less severe than the acquisition of content data, the Court considers that the aggregation of such data or the acquisition of a large amount of such data easily results in a serious interference with the private life. This might have implications for the generally formulated provision of 2.1.8, serving as a legal basis for (at first sight) non-systematic gathering of location or traffic data.[83] Moreover, considering ECtHR case law, an additional and more specific legal basis for an intrusive sys-

76. Draft Explanatory note new CCP (version July 2020), p. 410-411 and p. 500.
77. The level of intrusiveness becomes, for example, more severe, when an investigation is not conducted in relation to public sources but, instead, by using a false identity to obtain access to social media posts that are only accessible for 'connections' of the person concerned. In such a situation the legal basis for the investigation is found in draft Art. 2.8.11 (systematic gathering of information), which provides for more detailed rules (but not the authorisation of an investigatory judge).
78. 'Obtaining knowledge of' (*kennisnemen*) with regard to the investigation of data regulated in Chapter 7 and 'acquisition' (*overnemen*) of personal data with regard to the investigation on open sources.
79. Act on Police Data (*Wet politiegegevens*) and Act on Judicial and Criminal Law Enforcement Data (*Wet justititiële en strafvorderlijke gegevens*).
80. For a discussion of the limitations of the regulation of predictive policing in criminal procedure and data protection law see L. Stevens, M.F.H. Hirsch Ballin, M. Galič *et al*.., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling. Een analyse aan de hand van de casus "Sensingproject Outlet Roermond"', *TBSH* (forthcoming 2021).
81. Draft Explanatory note new CCP (version July 2020), p. 248 and see *Kamerstukken II* 2020/21, 32 761, nr. 173.
82. An example of such an investigation is the *Encrochat* hacking case. See *e.g.*, C. Driessen and J. Meeus, 'Unieke hack van EncroChat leidt tot veel lastige juridische vraagstukken', *NRC*, 9 June 2021.
83. See *e.g.*, *Ben Faiza v. France*, para. 2.3.

doi: 10.5553/BSb/266669012021002004007

tematic search of a large amount of location or traffic data – one, which would offer additional safeguards – might be needed.

3.2.2 The normative relation between the level of intrusiveness and the authority

Secondly, we posit that the manner in which the criterion of systematicness is used in order to determine the level of *ex ante* safeguards and the manner in which the criterion will be applied in practice, require further specification. Following the analysis in paragraph 2.2, for instance, the ECtHR does not distinguish between more or less intrusive digital searches (all searches and seizures are considered a serious interference with private life), where the requirement of a warrant issued by a judge acts as an important safeguard. It is thus uncertain whether sticking to the central position of the relation between the level of intrusiveness and the level or nature of authority in the new chosen system of regulation, will stand the test employed by the ECtHR.[84] In the context of digital investigations where sophisticated techniques are available, the requirement of a warrant thus seems to be a standard safeguard, which can only be remedied by a rigorous *ex post* judicial review. However, such *ex post* review will be difficult to realise in all circumstances. This namely depends on the fact, whether the investigation actually leads to a criminal trial and, if so, on the scope of the review within the context of the criminal trial which is dependent on the evidence included in the file and the manner in which 'irregularities' (*onrechtmatigheden*) in the criminal investigation are addressed.[85]

Something similar can be said regarding the acquisition of location data. The inclusion of a specific legal basis for location tracking (GPS surveillance) in the new CCP is certainly an important step forward compared to the current situation where no statutory regulation exists.[86] As already mentioned above, we may nevertheless need an additional provision for the most intrusive forms of acquisition of location data amounting to a far-reaching systematic (*ingrijpend stelselmatig*) intrusion, which would require the authorisation of the investigatory judge as additional safeguard.

Moreover, the manner in which the level of intrusiveness is determined on the basis of systematicness needs additional refinement.[87] According to the explanatory note, the scope of the investigation and the nature of the source primarily determine the intrusiveness of the interference. In this regard, four factors need to be taken into account: 1) the amount, nature and diversity of the data; 2) the nature of the source; 3) the manner in which data are searched (*e.g.*, with advanced techniques, considering the purpose and scope of the search and the specificity of search terms); 4) the storage and use of the data and the possible consequences for the person involved.[88] These factors indeed adequately reflect the relevant aspects for assessing the nature of the interference with private life.

However, the explanatory note does not make very clear which characteristics of the investigation lead to which level of (foreseeable) interference with private life. The first person that needs to make the required assessment in practice – usually the investigative officer or public prosecutor – seems to have a lot of discretion. Considering the relevant factors, it seems likely that the acquisition of bulk data indeed qualifies as a far-reaching systematic investigation, therefore, requiring prior authorisation by an investigatory judge. In this case, all of the factors – that is, the amount of the data gathered, the broad scope of the acquisition and the search, including the possible use of advanced techniques to search the data or aggregation with other data – point into that direction. But what about cases, in which the relevant factors point into opposing directions? Which should prevail and in which cases? Unfortunately, the explanatory note gives no guidance for such situations, which are likely to be predominate in practice. As such, case law will again need to do most the work filling in these abstract terms.

Considering the limited foreseeability of such regulation and the importance placed by the Court on *ex ante* safeguards (further discussed in 3.2.3), the room for interpretation in practice may still be too broad to offer sufficient safeguards against abuse. This is particularly relevant in relation to the acquisition and processing of data, including traffic data, in the context of bulk interceptions.

3.2.3 Ex ante safeguards

When it comes to *ex ante* safeguards, the draft digital powers in the CCP discussed in this article can be seen as an important improvement and mostly in line with ECtHR jurisprudence. According to the examined ECtHR case law, the definition of circumstances in which precise *ex ante* safeguards are required applies in particular when it comes to data covered by LPP and bulk interception. In this regard, the draft CCP is in line with the approach of the Court, as it provides for additional safeguards both in the case of interception of communications and LPP-data. Furthermore, specific

84. The same conclusion seems to follow from the judgment of the Court of Justice of the European Union of 2 March 2021 (*Prokuratuur)*, C-746/18. The Court nuances the difference between content data and traffic data and seems to require in general prior judicial (or other independent) authorization for investigative powers to order data.
85. M. Samadi, *Normering en toezicht in de opsporing. Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen* (diss. Leiden), Den Haag: Boom juridisch 2020, p. 242 and 291; see also M.F.H. Hirsch Ballin, *Over grenzen bij bewijsvergaring. Grondslagen voor geïntegreerde normering van strafrechtelijke bewijsvergaring* (oratie VU Amsterdam), Den Haag: Boomjuridisch 2018, p. 74-75.
86. Its regulation is now largely to be found in case law, *e.g.*, HR 1 juli 2014, ECLI:NL:HR:2014:1563, *NJ* 2015, 114 and ECLI:NL:HR:2014:1562, *NJ* 2015, 115.
87. See S.L.T.J. Ligthart, 'Het criterium van stelselmatigheid in het gemoderniseerde Wetboek van Strafvordering: redelijke voorzienbaarheid als voorwaarde voor meer dan geringe en ingrijpende privacyinbreuken', *RMThemis* 2019, 5.
88. Draft Explanatory note new CCP (version July 2020), p. 499-502.

doi: 10.5553/BSb/266669012021002004007

requirements are included with regard to the use of software for acquiring data on a large and systematic scale, for example in relation to open-source investigations and in the context of the procedure to be followed for sifting LPP data out of large data sets. The draft CCP also provides for a logging obligation, intended to make sure that the automated search of a computer or smartphone can be subjected to meaningful *ex post* review and that the integrity of the search is guaranteed.[89] In addition to these safeguards, the explanatory note also states that specific requirements in such automated searches should be included that would prescribe, which information needs to be included in the official police report (*proces-verbaal*) or reported otherwise. The reporting of information such as (logging) information, enabling control on the integrity of the data, and search terms applied is important considering the requirement of a (sufficiently) rigorous *ex post* review.[90]

Finally, we examine the design of the draft provisions of the proposed CCP for the investigation of data when LPP-data might be involved, especially when acquired in large datasets from third parties or through covert investigatory powers.[91] The draft CCP is based upon the assumption that when it is reasonably foreseeable that the investigation involves LPP data, the investigation qualifies as 'far-reaching systematic', requiring authorisation from an investigatory judge.[92] According to draft Article 2.7.67, the investigatory judge needs to determine the conditions for the investigation of data, when there is a reasonable expectation that LPP data are involved. The contours of such a procedure with regard to large datasets are currently the matter of complex discussions between defence lawyers, law enforcement and the judiciary.[93] As stems from our discussion of ECtHR jurisprudence in section 2.2 (particularly *Saber v. Norway*), the ECtHR seems to require explicit and specific procedural guarantees in the law in order to safeguard the LPP from being compromised by digital searches. This conclusion makes it doubtful whether leaving the responsibility for determining, such a procedure on case-by-case basis to the discretion of the investigatory judge, can be seen as an adequate *ex ante* procedural guarantee.

Draft Article 2.8.3(1) deals with LPP data in datasets acquired through covert techniques. When LPP data are encountered in such datasets, they either need to be destroyed or a warrant must be obtained before being able to use them as evidence (draft Art. 2.8.3(2)). Furthermore, a procedure prescribing the manner in which LPP data should be filtered from datasets acquired by means of covert techniques must be set out in an administrative ordinance (*Amvb)* (draft Art. 2.8.3(3)). The question whether sufficient *ex ante* safeguards are in place to avoid revealing LPP data to law enforcement authorities largely depends on the contents of this procedure. However, the delineation of such a procedure is at this moment still under discussion.[94] Moreover, based on ECtHR case law, such a procedure should be established not only for datasets acquired by covert techniques but also in relation to other types of investigation of data (covered by Chapter 7 of the draft CCP).

4. Conclusion

The ECtHR has demonstrated that it takes great care to strike the right balance between the public interest in the prevention and prosecution of crime and the protection of private life, in an era in which technological developments enable member states to investigate crime with advanced digital methods applied to increasingly large amounts of data. At the same time, the Court emphasises member states' own responsibility in this regard: any state who wants to stand at the forefront of technology development also needs to stand at the forefront of its regulation. The Netherlands has taken that responsibility seriously by investing in a brand-new set up of the regulation of criminal investigation, one that is geared towards technological developments and includes new legal bases for specific digital investigation powers. Considering the fast pace of technological developments, the possibilities they offer for law enforcement authorities and the state's responsibility for striking the right balance, it is indeed urgent that these new provisions are put into place.

Notwithstanding these efforts, the analysis of ECtHR case law shows that in order to fulfil this complex responsibility of the state, certain aspects of the proposed regulation of digital investigation in the new CPP require additional attention. In particular, the manner in which the role of the criterion of systematicness is currently understood and meant to regulate digital investigation powers, does not yet fully reflect the high level of safeguards stipulated by the ECtHR in its more recent judgments on digital investigatory powers. Furthermore, the emphasis on end-to-end safeguards, which the Court developed in the context of bulk interception by intelligence agencies, should also be considered in cases where law enforcement authorities employ digital investigation techniques for searching large amounts of data on a general legal basis and beyond the context of concrete suspicion. As such, we propose that the legislator take note of the suggestions in section 3 for further improvement of both the draft CCP as well as the explanatory note. The legislator should use the time before the actual entry into force of the new CCP so as to further develop the current drafts of the statutory provisions and explanatory note, in order to indeed

89. See *e.g.*, Arts. 2.8.3 and 2.8.8(3), Draft Explanatory note new CCP (version July 2020), p. 489 and 502.
90. Draft Explanatory note new CCP (version July 2020), p. 502.
91. Draft Arts. 2.7.67, 2.7.68 and 2.8.3.
92. Draft Explanatory note new CCP (version July 2020), p. 414.
93. Draft Explanatory note new CCP (version July 2020), p. 470-472. See also *e.g.*, M. van der Horst and R. Klein, 'Het verschoningsrecht, de toekomst met vertrouwen tegemoet?', *TVSO* 2019, 4 en D.R. Doorenbos and M.E. Rosing, 'Recht doen aan het verschoningsrecht', *TVSO* 2020, 5/6.
94. Draft Explanatory note new CCP (version July 2020), p. 489-490.

doi: 10.5553/BSb/266669012021002004007

stand at the forefront of both technological developments and its regulation in criminal procedure in 2026.[95] Finally, we should point out that we fully endorse the steps already taken in order to develop new adequate legal bases for investigative powers with a fundamentally different impact on privacy than what we have been used to.

95. 2026 is the targeted date for the new CCP to enter into force.

doi: 10.5553/BSb/266669012021002004007