Accepted version for Special Issue of New European Journal of Criminal Law. 18.10.2023.

To have or have not: Limiting the data available for subsequent use by the police.

Inger Marie Sunde

Professor

Abstract:

In search of evidence in criminal investigation police often collect data in bulk, and the question addressed concerns whether the bulk data as a whole or only in part may be deemed available for subsequent use. The article suggests that only data exposed to the police in the digital forensic analysis performed as part of the investigation, should be deemed available for subsequent use. Such data are termed *digital assessed information* and are contrasted to data whose content is not known to the police. The latter should be deleted or made inaccessible for further use once the original case is finalised. The position is anchored in the criminal procedural principles of purpose limitation and purpose orientation, recognised in case-law related to the ECHR Article 8, further validated in considerations of fairness, and coherence with the rules for use of excess information in intercepted communications.

Keywords: Digital evidence, purpose limitation; purpose orientation; bulk data

1. Introduction

Police collection of big data in search of digital evidence in criminal investigation, raises concern about the possible risks to the fundamental right of data protection. This right is laid down in the European Charter of Fundamental Rights ("Charter")[1] Article 8, as well as in the European Convention of Human Rights ("ECHR")[2] Article 8. In the Charter the right is laid down as a distinct right alongside the right to private life (Article 7), whereas in the ECHR as a dimension of the right to private life in so far as the processing is performed by or on behalf of a public authority, such as the police.[3]

[1] Charter of Fundamental Rights of the European Union [2000] C 364/01.
[2] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950 ETS 005).
[3] Karl Fridrik Kjølbro, *Den Euoropæiske Menneskerettighedskonvention – for praktikere* (6th edn, DJØF Forlag 2023) Ch. 16.5.

This article analyses legal limitations following from the principles of *purpose limitation* and *purpose orientation* in criminal procedural law concerning subsequent use of such data. The problem at hand is caused by the police collecting data in bulk, thus taking much more data into custody than needed for investigating the case that gave reason for collecting the data ("the original case"). The question is whether the bulk data as a whole may be deemed to be available for subsequent processing, or only the part that lawfully was exposed to the police in the investigation of the case. The importance of the question seems obvious: the more data available for search, the stronger the information position of the police, a position that comes at a cost to data protection rights and should be curtailed.

The principles of purpose limitation and purpose orientation are laid down in Norwegian criminal procedural law, as well as in case-law concerning police use of coercive measures under the ECHR Article 8. The principles are further underpinned by rules preventing use of unlawfully obtained evidence, developed in relation to the right to a fair trial laid down in the Norwegian Constitution[4] Article 95 and the ECHR Article 6. The present analysis draws on these rules in Norwegian law, where the primary legal source is the Criminal Procedural Code ("CPC").[5]

The European Law Enforcement Directive ("LED")[6] Article 4(1)(b) and (2) sets out the principle of purpose limitation for personal data processing (Art. 4(1)(b)) and conditions for subsequent use (Art. 4(2)).[7] The provisions read as follows:

> (1)(b) Member states shall provide for personal data to be *collected* for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (italics added).
>
> (2) Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are *collected* shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is

[4] The Norwegian Constitution 2014.
[5] The Norwegian Criminal Procedural Code 1981.
[6] Directive 2016/680/EC.
[7] In the context of law enforcement use of data for a purpose different from the original purpose is termed "subsequent use", see Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities', accessible via https://papers.ssrn.com/sol3/papers.cfm?abstract id=4016491.

necessary and proportionate to that other purpose in accordance with Union or Member State law (italics added).

The notion *collected data* stands at the centrepiece of both paragraphs, implying that the issue concerns subsequent use of the bulk data as such. This however must be a fallacy, as it overlooks that two questions must be asked, firstly whether or not all of the bulk data may be available for subsequent use, and secondly, for which purposes the available data may be used. As indicated, this article addresses the first question. In doing this, it explains the Norwegian situation where the "value chain" of the data processing begins with the collection of data in a criminal investigation in search of evidence. Such data collection is regulated by rules of criminal procedural law governing coercive measures. The next part in the chain is the purpose for which the data may be used, raising question about use for other purposes than as evidence in the original case, i.a., for intelligence and crime preventive purposes.

It is asserted herein that it is unreasonable to assume that *all data collected in bulk* should be deemed available for subsequent use. Firstly, it would allow the police to process data the content of which they got no advance knowledge about. The lack of knowledge makes it difficult to provide legitimate reasons for storing the data for further use. In the original case a digital forensic analysis must be performed to uncover digital evidence.[8] As explained further down this article, the analysis must be carried out in compliance with the principles of purpose limitation and purpose orientation in criminal procedural law. From these principles it follows that to make random searches, or intentionally to search for incriminating evidence concerning an offence not included in the criminal charge, is unlawful. Thus, the legal principles defining the aim and focus of the digital forensic analysis, protect the part of the bulk data irrelevant to the original case from being exposed to the police. This part of the data is simply windfall were it to be used by the police. This leads over to the next reason.

The coercive measures available in criminal investigation are predominantly suspicion based and targeted[9] as is the case with respect to interception and search, both used to collect digital evidence. The measures are *suspicion based* as they may be used only if there is "probable cause"[10] to suspect that somebody has committed a crime.[11] They are *targeted* in the sense

[8] Anders Flaglien "The Digital Forensic Process" in Andre Årnes (ed.) *Digital Forensics* (Wiley 2018).
[9] Some exceptions exist such as general and indiscriminate collection of traffic and content data from cell masts in specific geographic areas for limited periods to identify the communication devices located within that area, see e.g., CPPC § 216a third paragraph last sentence and § 216b second paragraph (c).
[10] In Norwgian: "skjellig grunn".
[11] CPC § 192 first paragraph (search) and § 216a first paragraph (interception).

that the location that may be intercepted/searched must be identified beforehand, in the court decision authorising the measure.[12] Predefined "locations" relevant to interception are for instance telephone numbers and IP-addresses, both identifying endpoints of communications that may be intercepted.[13] Corresponding locations relevant to search would be a physical place or a digital space, such as the suspect's home address, his electronic devices or user accounts.[14]

By establishing conditions ensuring that the coercive measures are suspicion based and targeted, criminal procedural law seeks to prevent arbitrariness and limit the search for evidence to be performed at relevant places. In addition, principles of necessity and proportionality apply, working to prevent more data than relevant to the case from being collected.[15] However, legal characteristics of the coercive measure itself, and weaknesses of the forensic tools used to secure data may still cause data to be collected in bulk. To illustrate: Interception is a real-time method where the police is supposed to listen in to the communication while it occurs. The law does not require the communications to be deleted once known to the police, and they thus accumulate as bulk data. However, as explained in section 4.3, use of such data is regulated in detail by law, primarily following the rationale that

> when the police lawfully have gained access to information relevant to the investigation of a crime, it would be unreasonable for the law to prevent the police from using it […] A prohibition against the use of excess information would be contrary to the general obligation of the police to investigate crime.[16]

The citation rests on the premise that the police have knowledge of the content, as this knowledge is what would make it unreasonable for the law to prevent the police from acting upon it. Hence, in the context of intercepted material the discussion about subsequent use is framed as concerning *excess information*, not bulk data per se. A further consequence is that the defence has a right of access pursuant to the principle of equality of arms laid down in the

[12] CPC § 197 third paragraph (search) and § 216a third paragraph (interception).
[13] CPC § 216a third paragraph, and E. Keiserud, K.E. Sæther. M. Holmboe, H.-P. Jahre, M Matningsdal and J.G. Smørdal *Straffeprosessloven. Lovkommentar* (5th edn.Universitetsforlaget 2020), point 3 to § 216a.
[14] Keiserud et al., (2020) points 3 and 4 to CPC § 192.
[15] CPC § 170a, which largely corresponds to the proportionality condition embedded in "necessary in a democratic society" of ECHR Article 8(2).
[16] Citation from preparatory works to the CPC § 216i about use of intercepted information including use of intercepted excess information, cf. Ot.prp. nr. 64 (1998-1999) Ch. 8, with further reference to Ot.prp. nr. 40 (1991-1992). Author's translation from Norwegian.

right to a fair trial.[17] The rationale is the same: As the police have knowledge of the content, equality may only be established by providing the defence with possibility to gain the same knowledge.

Concerning search and seizure the cause for securing data in bulk is different, rather stemming from limitations of the forensic tools available for securing such data as these are incapable of distinguishing between relevant and irrelevant data. Weaknesses of forensic tools however could hardly be a legitimate reason for subsequent processing of data the content of which is left in the dark.

Use of search and seizure do not necessarily imply that the police gain insight into the objects at the time when they are secured. They might have to be analysed further, as is the case with fingerprints, biological traces, potentially unlawful substances etc., as well as secured data. And regarding data, the outcome is regularly that (a) only a fraction is relevant,[18] (b) that a larger part (including the fraction) has come to the knowledge of the police, and (c) that the content of the better part of the bulk data has not been assessed and is thus not known to the police.

The thrust of the argument put forward in this article is *that only data the content of which is known to the police, should be deemed as being available for subsequent use.* This would shape the legal framework for subsequent use of data collected by search and seizure to correspond to the one applicable to intercepted material, as well as to the rules concerning defence rights of access. The consequence to the data not known to the police is that they should be deleted or made inaccessible for further processing in line with the principles of data minimalization and storage limitation. Given that the categorisation of different parts of the data in the bulk may be important to the legal implications, there is a need for a notion denoting 'data whose content is known to the police.' These may be referred to as *digital assessed information* as opposed to data with content not known to the police.

The significance of the procedural principles of purpose limitation and purpose orientation to the issue of subsequent use, is that they identify (and limit) the part of the bulk *that may be available for subsequent use*. Indirectly, by shaping the limitations for investigation, they have

[17] Keiserud et al., point 10 to CPC § 242.
[18] This is well illustrated in the case of *Einarsson*, where only 0,03 % of the data was produced as evidence (6300 out of 20 million email). *Sigurdur Einarsson and Others v Iceland.* Judgment 4 June 2019, § 71.

an impact on the expectations that are relevant to fairness considerations related to subsequent use.

2. Scope, method and outline of the article.

National law may authorise use of coercive measures also for preventive purposes, to deal with threats against national security, terrorism, or other equally serious threats. However, issues related to the processing of data collected for such purposes fall outside the scope of this analysis. In Norwegian law there are separate legal regimes for data collection and further processing for preventive and investigative purposes,[19] and the present article only addresses issues related to data collected in "ordinary" criminal investigation.

The question to be investigated concerns how the procedural principles of purpose limitation and orientation impact the scope of data that may be deemed as being available for subsequent use. It is assumed that the data are collected by search and seizure, as this creates a clear situation where a large part of the data may not be known to the police after the digital forensic analysis is finalised. The context is the digital forensic analysis which is a distinct step in the digital forensic process, in Norwegian procedural law deemed as search.[20] It must thus be carried out in compliance with rules of criminal procedural law. Pursuant to the case-law related to ECHR Article 8, search is a coercive measure that must comply with several conditions to be lawful (see section 3.3). This case-law is concerned with protecting affected persons against abuse and arbitrariness, and to this end the principles of purpose limitation and purpose orientation are applied. Breach of these principles may lead evidence to be deemed as unlawfully obtained.

The outcome of the analysis is then assessed in relation to fairness. The reason for bringing in fairness, is that it expresses the need for considering the situation of more data subjects than the suspect. This is due to the variations in the ways data may be collected and used. Other parties potentially affected are for instance third parties whose personal data are included among the data collected from the suspect ("third parties"), e.g., email correspondence located on the suspect's email account, or personal photographs on the suspect's smartphone. However, data could also be collected directly from the third parties themselves who then get

[19] Coercive measures used by the Norwegian Police Security Services for preventive purposes, are regulated in the Norwegian Police Act 1995. Coercive measures used in criminal investigation are regulated in the CPC Part IV.

[20] Case-law of the Supreme Court: HR-2018-1891-U; HR-2018-1517-U; HR-2018-699-A and Rt. 2011 s. 296; Flaglien (2018); Inger Marie Sunde, 'Regulating Digital Evidence', Expert Report for the Ministry of Justice, 18 June 2021 *("Effektiv, rettssikker og tillitvekkende behandling av databevis")*, Ch. 5, 7 and 8.

procedural status as witness ("witnesses"). This is the case when the police carry out search and seizure directly against devices and user accounts owned by such parties. Moving on to possible use of the data, the data could be useful for routine cross-check against intelligence databases containing information about persons already registered by the police ("registered person"). A search in the bulk data could thus provide the police with more information about registered persons, although the registered person might have nothing to do with the crime investigated in the original case. In this respect bulk data provides a possibility for the police randomly to gain more information about registered persons. The police could also create a pool of data consisting of datasets from different investigations. Cross-case analysis could produce new intelligence products uncovering unknown behavioural patterns, social networks and personal relations that could help build cases against individuals formerly out of sight of the police ("unknown persons"). This could enable police to initiate steps towards them, such as registration in intelligence databases, initiation of preventative intervention or opening a criminal investigation.

Finally, the rules regulating subsequent use of excess information applicable to intercepted communications are considered. The aim is to check for internal coherence between the rules concerning intercepted data and data stemming from search and seizure. A comparison with the rules concerning use of excess information in intercepted data is merited in the fact that these methods nowadays are largely comparable in terms of their privacy invasive nature. Technological development and social use of digital services cause massive amount of digital content and traces to be produced from everyday use of digital devices and services, entailing that search and seizure arguably have become at least as privacy intrusive as interception. For instance, large amounts of the data stored at searchable endpoints (thus available for seizure) is communication that otherwise could be intercepted. The distinction in criminal procedural law made between data under transmission (available for interception) versus stored data (available for search and seizure) seems largely irrelevant now that messaging services have largely replaced telephony as the dominant means of electronic communication. The digital development has thus made the respective methods' privacy invasive nature more similar than they historically were deemed to be. This calls for a critical approach to discrepancies in the legal regulation.

Accordingly, the article first explains the procedural principles of purpose limitation and purpose orientation applicable in Norwegian criminal procedural law, and how they are expressed in the case-law related to the ECHR Article 8, followed up by a discussion about

the data that may be deemed legitimate for subsequent use (section 3). Thereafter follows a discussion aiming to see if the interplay between the different principles and rules make sense in relation to the limitations set by the first analysis (section 4).

3. Analysing whether bulk data as a whole is available for subsequent use. The implications of purpose limitation and purpose orientation.

3.1 Introduction

The question is whether bulk data as a whole are available for subsequent use. As noted in the introduction, LED Article 4(2) can be interpreted to this end, however, there are also several reasons suggesting a narrow interpretation. The principle of purpose limitation in the LED (as opposed to in procedural law) seems inadequate to deal with the problem, leading *Catanzariti* to state that the "purpose limitation principle in the field of law enforcement is extraordinarily large in scope."[21] *Koning* further notes that the objectives of the LED Article 1(1) are "too vague to serve as processing purposes in the sense of Article 4(1)(b)."[22] *Koning* further suggests that Article 4(2) "would have been more on point with the purpose specification requirement if it, instead of [...] the purposes set out in Article 1(1) [...], would have stated: [...] a purpose *in pursuance of* any of the objectives set out in Article 1(1)" (italics added).[23] This looks like a call for supplementing the data protection principle of purpose limitation with a principle of purpose orientation.

Importantly, criminal procedural law relating to use of coercive measures includes such principles setting rather strict boundaries for processing of data collected by the police in a criminal investigation.

3.2 Purpose limitation and purpose orientation.

The procedural principles of purpose limitation and purpose orientation operate as guarantees against abuse and arbitrariness, i.a., underpinning the legal protection against unwarranted investigation. For a person to come into focus of a criminal investigation is burdensome and unpleasant. To avoid arbitrariness in this respect the law sets conditions for *opening* a criminal

[21] Mariavittoria Catanzariti, "Procedural rights through the Lenses of Data Protection. The Case of Data Subjects' Rights" in Guiseppe Contissa, Giulia Lasaghi, Michele Caianello and Giovanni Sartor (eds.) *Effective Protection of Rights of the Accused in the EU Directives* (Brill Nijhoff 2022).
[22] Merel Elize Koning, *The Purpose and Limitations of Purpose Limitation*, Doctoral Thesis, Radbroud University Nijmegen (2020) p. 182.
[23] Koning (2020) p. 182.

investigation, as well as for *widening the scope* of an ongoing investigation. This is laid down in e.g., the European Code of Police Ethics point 47: "Police investigations shall, as a minimum, be based upon reasonable suspicion of an actual or possible offence or crime."[24]A corresponding provision is laid down in the CPC § 224: "Investigation may be performed when there is reasonable ground to investigate whether a crime [is committed]." Criminal investigation may thus be opened only provided objective circumstances give reasonable ground to suspect that a crime is committed.[25] The scope of an investigation may be increased later, provided information collected within the scope and goal of the initial investigation give reasonable ground to suspect that also other crimes are committed. These may be deemed as *accidental findings* of evidence.[26]

The procedural principle of *purpose limitation* is an aspect of objectivity, entailing an obligation to stay focused on the offence at issue, not prying into aspects not relevant to this end. The criminal procedural code lays down the principle of objectivity both for prosecutors and investigators.[27] The principle of purpose limitation refers to the scope of the criminal investigation, defined by the offence that gave reason for opening the criminal investigation.

The "offence" is the criminal act the way in which it is defined in a criminal law provision. Pursuant to the principle of legality in criminal law, offences must be laid down in legal provisions that describe their legal characteristics with sufficient precision to make the law accessible and foreseeable.[28] The characteristics of the offences are supplemented with general conditions for criminal liability, typically concerning e.g., sanity, conspiracy, collusion, and attempt. Thus, the legal characteristics of the offence supplemented with the general conditions for criminal liability, determine the scope of the investigation.

The *criminal charge* issued by the public prosecutor is the procedural instrument for concretizing this scope.[29] It sets out the criminal provision accompanied with the relevant factual circumstances, thus framing the procedural identity of the crime. To investigate beyond the scope of the criminal charge would be arbitrary. The principle of purpose

[24] The European Code of Police Ethics. Recommendation Rec(2001)10 adopted by the Committee of Ministers of the Council of Europe (2001).
[25] Keiserud et al. (2020) points 3 and 4 to CPC § 224.
[26] See *The Legality Control with Criminal Investigations of the Public Prosecutors – On Relevant Purpose of the Investigation and Proportionality.* Letter from Norwegian General Attorney to the Chiefs of Police and Public Prosecutors 9 May 2021.
[27] CPC § 55 second para. (prosecutors) and § 226 third para. (investigators).
[28] The principle of legality in criminal law is laid down in ECHR Article 7 and the Charter Article 49. On the topic of legal clarity see. e.g., Kjølbro (2023) Ch. 14.3 p. 823 ff.
[29] CPC § 67.

limitation thus lies inherent in the procedural system from the very beginning to the end of a case.[30] In the procedural code it comes to fore as concrete instantiations in provisions e.g., concerning search, by requiring that the offence comprised by the criminal charge is of a certain seriousness (CPC §192 first para.), in other words, that the search may not concern an offence not included in the criminal charge, and that the court decision permitting search specifies "what the case is about" (CPC § 197 third para.). Also this is defined by the criminal charge.

The principle of *purpose orientation* refers to the goal of the investigation. In the procedural code this goal is set out as a mandate of the police to collect evidence that clarify whether the conditions for criminal liability (as set out in the criminal law provision) are fulfilled. The investigative steps must be orientated towards the goal of the investigation, that is, be relevant to achieve this goal. As clarified by the General Attorney, purpose orientation is important to establish clarity about several aspects related to use of coercive measures[31] (in the present case search): Purpose orientation is necessary to form an opinion about the concrete reason for and purpose of the search, and to perform a meaningful assessment concerning a) whether the level of suspicion is fulfilled (probable cause); b) the proportionality of the search and c) the concrete performance of the search; and finally, to perform an effective legality control.[32]

The ways in which the principles affect criminal investigation may thus be summarized as follows: The principle of purpose limitation sets limits concerning the kind of evidence the police may search for. In practice it requires the police right from the opening of a criminal investigation to have a clear description of the offence relevant to the suspected crime, and continually be checking whether sought after evidence is relevant to the offence. Intentionally to search for evidence not concerning the crime under investigation without objective circumstances giving reasonable cause for suspicion, would be unlawful.[33] The principle of purpose orientation sets the direction of the investigation. Only measures suitable to attain the goal of the investigation may be performed, others not. For instance, the principle prevents the police from performing searches into collected data if the burden of proof must be deemed to be fulfilled by the evidence already uncovered. Of course, the principles are closely related to each other as well as to principles of necessity and proportionality. However, to avoid

[30] At the end of the case, it typically protects the defendant from being randomly convicted for a different offence than set out in the criminal charge, cf. CPC § 38,
[31] The General Attorney (2021) p. 2.
[32] *Ibid.*
[33] *Id.*, p. 2 and 3.

arbitrariness and abuse the importance of having to concretize both scope and goal of the investigation, can hardly be overrated, and is accentuated in the application of coercive measures, as these intrude even more heavily on the suspect than does the mere opening of a criminal investigation.

3.3 Case-law related to the ECHR Article 8.

The principles of purpose limitation and purpose orientation play an important role in the case-law related to ECHR Article 8 in the context of search and seizure where they form aspects of the rule of law and proportionality.[34] The coercive measures at issue interfere both with the right to private life and data protection rights, and Article 8(1) encompasses both rights, see e.g., the case *S and Marper.*[35] To be lawful the methods must have legal basis, be performed for a legitimate aim and be necessary and proportionate (ECHR Article 8(2)). At the outset the ECtHR has emphasised that:

> search and seizure represent serious interferences with private life, home and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject.[36]

The paragraph concerns a case in which the coercive measures targeted a lawyer's premises. Obviously, this situation is very sensitive due to the risk of compromising the legal protection of client information. However, the strict view is upheld also in cases concerning non-lawyers. In the case of *Harju* the court indeed added that also "safeguards against possible abuse or arbitrariness" were required.[37] Summarized the conditions set out in the case-law concern

- Legal basis,[38]
- the accessibility and foreseeability of the law (the clarity of the law),[39]
- the rule of law, i.e., that "proper legal safeguards" against abuse and arbitrariness must be in place (the quality of the law),[40] and

[34] Sunde (2021) Ch. 7.
[35] *S and Marper v UK* Judgment 4 December 2008, §§ 66 and 67. See also Kjølbro (2023) Ch. 19.5.
[36] The leading case is *Petri Sallinen and Others v. Finland* Judgment 27 September 2005, § 90. See also e.g., *Wolland,* Judgment 17 May 2018, § 62, and *Saber,* Judgment 17 December 2020, § 50, both against Norway.
[37] *Harju v. Finland,* Judgment 15 February 2011, § 42.
[38] *Ibid.,* § 36 referencing *Societéteé Colas Est and Others v France,* Judgment 16 April 2002, § 43.
[39] *Id.,* § 35.
[40] *Id.,* §§ 35 and 39; *Saber* §§ 55-57.

- that the measures must be necessary and proportionate in relation to the objective of the criminal investigation (fulfil "a pressing social need").[41]

Regarding the conditions concerning the *rule of law* and *proportionality*, the court takes particular interest in the following points:[42]

1. Whether the search order issued by the court was sufficiently clearly delimited and provided sufficient information about the purpose intended to be achieved.
2. Whether the search (including the collection of data) was performed in a manner suitable to prevent any risk of exceeding the limitations set out in the court's permission.
3. Whether the search and the collection of data were sufficiently documented, thus affording possibility for effective control.

Points 1 and 2 show that the principles of purpose limitation and orientation are applied, to (1) the court decision authorizing the search where the "purpose intended to be achieved" indicates purpose orientation, and to (2) the police performance in carrying out the search is assessed in relation to both scope and purpose of the investigation (thus including both principles). For a search to be lawful both must be complied with. Jointly the principles act as a guarantee against intentional or aimless search and seizure beyond the information needs of the criminal investigation. One example could be performing a search under the pretext of being necessary in relation to the criminal charge, while really performed to seek answer to a request by the Police Security Service for a different purpose.

Point 3 about documentation is crucial for compliance control. A search involving data collection and analysis is performed in two main stages, initially as *a physical search,* thereafter as *a digital forensic analysis,* and both stages must be documented *ex ante* and *ex post*. The court decision provides the documentation ex ante regarding the search at the initial stage, while the documentation ex post typically consists of police reports describing the sources from which data were secured, how they were secured, the procedures for authenticating the data and preserving their integrity, the police officers involved etc.

It follows that with respect to the digital forensic analysis, the documentation ex ante must include a plan describing search criteria and tools suitable to achieve the goal of the analysis

[41] *Funke v France* Judgment 25 May 1993 § 55; Kjølbro (2023) Ch. 15.3.
[42] Sunde (2021) Ch. 7.

within the scope of the investigation. The documentation ex post must show how the analysis was performed, how results were achieved, when and by whom.

3.4 The categories of data at issue.

Having established that the digital forensic analysis must ensure that the search is relevant to the information needs of the investigation, it should be clear that to perform so-called "fishing expeditions" into collected data in search of incriminating information falling outside the scope of the investigation, is arbitrary and unlawful. As sophisticated detection technology is developed in certain crime fields – detection of child sexual abuse material ("CSAM") being the prominent example – certain types of incriminating material may easily and routinely be detected by the police in such analysis. However, to search for CSAM in an investigation for instance concerning economic crime, would be contrary to purpose limitation (as concerning an offence not included in the criminal charge) and to purpose orientation (as not be suitable for achieving the goals of the original investigation). It would thus be unlawful.

In practice the situation may not be as straightforward, as digital evidence may be a very complex entity, often more like a synthesis of different digital traces than an object in itself. This complicates matters because it opens for a wide discretion of the forensic examiner in deciding the strategy to be followed in the search for evidence. The chosen strategy must however be set out in writing as a plan ex ante, as per point 3 of the conditions set out in the case-law explained above. Faced with a large data set the forensic examiner may decide to structure the search in stages, starting out broadly, gradually narrowing down the amount until the data relevant to the investigation are identified. The aforementioned case of *Einarsson* provides an informative example of the challenges that may be encountered in this respect. The volume of data in that case (20 million emails) might seem extreme but is probably common nowadays given that the processing capacity and data quantities have doubled exponentially approximately 8 times since the investigation of that case.[43] Today also "small cases" have large data sets.

It follows that a proper forensic data analysis must be performed by use of automated tools. This entails that data not retrieved by the search, do not come to the examiner's knowledge. These data may be deemed as *not known to the police* in the sense that the police lack knowledge about their content. The next step of the data reduction process involves a

[43] Moore's law says that the processing capacity doubles every second year. Moore's law - Wikipedia (accessed 1 October 2023). The investigation in the case of *Einarsson* commenced in 2009 (§ 10 of the judgment).

relevance assessment of the retrieved data. As the initial search can hardly be precise, it is to be expected that parts of the retrieved data will turn out to be useless to the original case. This could happen even if the data retrieval is planned and performed in compliance with the principles of purpose limitation and orientation. It thus appears to be an inherent feature of the digital forensic analysis that the police get knowledge about more information in the collected data than relevant to the case.[44]

It follows that the assessment procedure may have different outcomes. Some data may be found to be relevant to the criminal charge, in which case they are categorized as *digital evidence* included in the case file. Conversely, some may be found to be of no interest whatsoever despite that they were retrieved in the initial search. These are categorized as *found irrelevant*. Furthermore, the forensic examiner may accidentally come across data causing reasonable suspicion about other offences than included in the criminal charge. The suspicion could relate to the suspect in the original case and/or indicate that other persons should be investigated, even concern offences quite unrelated to the present case against the original suspect. Other scenarios are possible as well, such as coming across data indicating that a serious crime is about to be performed, or that innocent persons are criminally charged. Such findings bring up questions about use of the data for other purposes than those set by the information needs of the original case.

Against this backdrop collected data may be divided into several categories: Data not known to the police, data found irrelevant, data relevant to the original case, and data relevant to other purposes than the criminal charge in the original case. Except for data not known to the police, the categories concern *digital assessed information* i.e., data whose content is assessed and known to the police.

As asserted in the introduction it is the position of this article that only digital assessed information may be deemed available for subsequent use, such as increasing the scope of the original investigation, opening a new investigation against other persons, making data available for other investigations, averting the commissioning of a crime, or taking measures to prevent innocent persons from being prosecuted. Other data should be deleted or made inaccessible for further processing. This outcome is deemed to be best in line with the limitations to the investigation described in this section. From the perspective of the police the

[44] All data assessed by the police should be made available to the defense as per the principle of equality of arms enshrined in the right to a fair trial, cf. *Einarsson* §§ 89-90.

position could seem dramatic, for instance giving cause to a claim that data pooled together from different cases over time *could* be a valuable resource. However, such claim rather resembles a "nice to have" argument that is plainly contradictory to the principle of data minimalization. The argument's legitimacy is further weakened by the fact that the digital forensic analysis is an iterative process that provides the police opportunity to search the data time and again. When relevant data are still not detected, it is hard to claim that further storage and processing is necessary.

4. Assessment.

4.1 Introduction.

In this section the proposition concerning the limitation of the scope of data available for further processing, is assessed in a broader view along the lines of fairness and the rules for subsequent use of intercepted data. As subsequent use in any case must have basis in law to be lawful (cf. ECHR Article 8(2) and LED Article 8) the aim of the assessment is to tease out guidelines for what such regulation could reasonably look like, rather than determining the content of existing law. In addition, question should be raised as to whether LED Article 4(1)(b) and (2) could be interpreted as suggested herein.

Starting out with the latter, the position taken in this article entails that "data" in the first paragraph of the LED Article 4 should be interpreted as data, because it makes sense that the digital objects (data) must be collected before they may be processed. In the second paragraph however, "data" could be interpreted as the data that lawfully have come to the knowledge of the police, i.e. digital assessed information. The conditions for lawfulness should be those following from the principles of purpose limitation and orientation explained in the foregoing. The data are still data, the difference is that they have acquired an additional quality by their exposure to the police, a quality that seems relevant for setting a suitable scope for lawful subsequent processing.

Scholarly analysis of the provisions of the LED seems mainly to deal with the understanding of the word "purpose", that is, whether it calls for an assessment of the concrete intended use of the data, or whether the intended use falls within the scope set by the LED Article 1(1). The scope of Article 1(1) is made relevant by the LED Article 4(2). The latter alternative makes Article 4(2) a *carte blanche* for subsequent use within the scope of Article 1(1). Realizing this, *Koning* has suggested that only *the intended concrete use* must be relevant, not whether

the intended subsequent falls within the scope of the LED.[45] *Fedorova* has further concluded that the objective of preventing crime in Article 1(1) is too vague to represent any meaningful limitation, thus is unsuitable as legitimate purpose for subsequent use.[46]

These considerations do not address the question dealt with here, as they seemingly take for granted that the bulk as a whole is at issue. As mentioned in the introduction, such interpretation is unreasonable, primarily because the data whose content is not known to the police is a windfall rather than the result of a systematic effort to cover defined information needs in a criminal investigation or for preventing crime (intelligence). Put differently, they have not come into the custody of the police due to a clearly defined goal, this in itself a contravention of the principle that data may only be collected for specified, explicit and legitimate purposes" (LED Article 4(1)(b)).

Take the case of possible subsequent use of the data as evidence in a future criminal investigation: As already explained, it is a principle in criminal procedural law that investigation and collection of evidence should commence only when there is reasonable suspicion to open a criminal investigation. To store data *in case* they might become useful in future investigations is plainly contradictory to this principle. *Koning* is therefore right in criticizing that "a purpose like the *investigation of crime* would justify all types of data to be stored for long periods because it might come in handy in a future investigation" (underlining added).[47] In terms of criminal procedural law this would be unlawful. Thus, to interpret the LED Article 4(2) to permit storage of bulk data for such use, is in conflict with criminal procedural law. This makes a case for a narrow interpretation as suggested above.

Furthermore, the case of possible use of the data for intelligence purposes in the prevention of crime also seems to lack merit. The reason is that – at least in Norwegian law – the intelligence process is

> a managed process consisting of *systematic* collection, analysis and assessment of information about persons, groups and phenomena in order to provide basis for decision-making (italics added).[48]

[45] Koning (2023) p. 181-182.
[46] M.I. Fedorova, R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade, T.F. Walree 'Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunkten bij de normering van het verwerken van persoongegevens voor strafvorderlijke doelinden', Radboud University Press, 2022, Ch. 3.2.1.2.
[47] Koning (2023) p. 183.
[48] The Police Directorate. *Intelligence Doctrine of the Police.* V.1.2. 2020 p.18. Author's translation from Norwegian.

To store data indiscriminately without knowing their content, may hardly be deemed a systematic step towards producing intelligence products, as required by the doctrine. Of course, the subsequent analysis might be performed in a systematic manner, and any relevant data thus identified might be deemed as systematically collected. But the fact remains that the data was collected in the first place without the production of intelligence products in mind, thus the content unknown to the police is excess data randomly fallen into the custody of the police. Opening for subsequent use for investigation or intelligence purposes thus seems to have weaknesses regarding scope, aim and proportionality resembling those of the former Data Retention Directive,[49] declared void in the case *Digital Rights Ireland.*[50]

Thus the point remains that the data are just nice to have, a reason that is never legitimate for storing personal data.

4.2 Fairness.

Turning to the principle of fairness, the point is that it may help evaluate the proposition set out in this article. Fairness is a key principle in data protection law laid down in the Charter Article 8(2) and the LED Article 4(1)(a), and regarding "the very sensitive context" where coercive measures are applied, the WG29 has emphasized the importance "that no doubt exists as to the fairness to the processing."[51] Fairness requires taking account of the expectations of the affected persons, individually or as a group.[52] This makes the list of data subjects set out in Section 2 above relevant to the analysis. In addition, given the overtones of unwanted surveillance implied in the issue, the expectations of ordinary law-abiding citizens should be considered as well. To determine expectations is primarily an empirical effort, which is out of scope of this article. An alternative method is trying to put oneself into the position of the different stakeholders, imagining their expectations. This could result in a list of possible expectations useful to the analysis, and is the method applied here.

Firstly, from the perspective of *the citizens*, there could be an expectation that the police once they decide to go to the highly privacy invasive step to collect large amounts of data, they also have the tools and expertise necessary to perform the forensic analysis safely within the

[49] Directive 2006/24/EC.
[50] European Court of Justice, judgment 8 April 2014; joined cases C-293/12 and C-594/12.
[51] Article 29 Data Protection Working Party Opinion 3/2015 *on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,* 3211/15/EN WP 233, p. 6.
[52] See e.g. the Information Commissioner's Office 'Lawfulness, fairness and transparency' (Principle (a): Lawfulness, fairness and transparency | ICO accessed 1 September 2023).

procedural limitations. By implication, the expectation is that data not retrieved in the forensic analysis (unknown data) should be a no go for the police. It is a no go because the police do not have any concrete circumstances providing the reasonable suspicion that is a condition for opening a criminal investigation. The principles of purpose limitation and orientation thus provides the backdrop of this expectation.

This is not to completely rule out the possibility of an expectation that the police routinely could search into "unknown data", when there is a need for a systematic effort to combat crimes that are deemed to be sufficiently serious as well as suitable for detection in such manner. Again, online sexual abuse of children is the principal example. A counter argument is that as technology develops and becomes increasingly sophisticated it can be specialized to detect many different forms of crime. Increased technical possibility to uncover crimes without prior indication of such crime, could cause an unwanted slippery slope effect where crime countering initiatives are steered by the possibilities of technology rather than the rules of a well-balanced procedural system. Thus, there is a risk of technologically driven function creep. It seems reasonable to assume that citizens have expectations about being able to have a say regarding the conditions and limitations for such development before it eventually might be a fact, thus that the issue should be brought up for public discussion rather than being developed under the radar of the citizens.[53] The expectation in this regard is therefore hard to determine.

Secondly, citizens could have expectations relating to police action when incriminating information is exposed in a lawfully performed forensic analysis. To disregard such information could be contrary to these expectations, even be detrimental to citizens' trust in the police. After all, the police are supposed to protect citizens from crime. At least for serious crime, such information should lead to initiation of a criminal investigations and if suitable, make the information available to other ongoing investigations. The same however could be said about use of the information to *prevent serious crime*. However, in this case, there could be a need for more clarification as to the applicable criteria. Prevention is a multifaceted notion that could encompass police initiatives on the levels of society, special groups at risk of committing or being victim of crime, and criminals.[54] Prevention involves i.a., registration in

[53] On the concepts of "slipperly slope" and "function creep", see Bert-Jaap Koops 'The Concept of Function Creep' [2021] LIT p. 29-56.
[54] This reflects prevention on primary, secondary, and tertiary level, see e.g., H.B. Ellefsen, B. Bjørkelo, I.M. Sunde & N. Fyfe 'Unpacking preventive policing: Towards a holistic framework', (2023) Int'l Journal of Police Science and Management, SAGE, p. 1-12.

police databases, which requires decision making regarding the role of the persons to be registered. The possibility of mistakes made due to incomplete information could affect innocent persons and have adverse consequences. There could thus be a need for distinguishing between preventing and averting crime. While citizens certainly expect the police to avert serious crime when the information is sufficiently precise to be actionable, it is less evident that the police are expected to store all information that might indicate some criminal activity that might be performed in the future. As already noted, in a recent study *Fedorova* thus rejects crime prevention as a legitimate purpose for subsequent use of data collected in criminal investigation.[55]

As seen from the perspective of *the suspect*, the limitations of the criminal charge and the resulting investigation, could reasonably cause an expectation that the police will stick to the matter at hand. Thus, that the police refrain from searching for each and every misstep made in the suspect's life. In consequence it would possibly be unexpected for the suspect to learn that the police searched his data also for purposes outside the scope of the criminal charge. Such data should be precluded from being used as evidence as they were obtained pursuant to unlawful fishing expeditions. On the other hand, a suspect who knows that his data contain incriminating information about other crimes than comprised by the criminal charge, might not be surprised if such information were to be uncovered by accident in the digital forensic analysis. For this to be acceptable, the police would have to provide documentation that the finding of the incriminating information was truly accidental.

Finally, there are the expectations of third parties of different kinds as mentioned in Section 2. In general, these may be aware of the data protection rights, entailing expectations similar to those set out above. Third parties without any connection to the crime under investigation are likely to be very sensitive of any interference with their personal data, implying that any use beyond what is necessary for the case at hand must be deemed as out of bonds.

To summarize, the expectations may be divided between digital assessed information and data not known to the police. While there is a general expectation that the police take appropriate measures based on digital information that has been assessed by them, there is hardly any expectation that the police searches through the part of the bulk data that were not retrieved in the digital forensic analysis. Exception might be possible in clearly circumscribed cases, but the risk of a slippery slope effect weighs in heavily against such an expectation.

[55] Fedorova et al. (2022) Ch. 3.2.1.2.

4.3 Subsequent use of excess information.

Finally, turning to *the regulation of excess information* in intercepted material, in this case illustrated by Norwegian law. The CPC§ 216i sets out an exhaustive list of permitted use of intercepted communication. Naturally, the material may be used as evidence for the offence that gave reason to perform the interception (use in the original case). In relation to the LED such use is "not incompatible" with the purpose for which interception was performed (Article 4(1)(b)). In addition, the material may be put to subsequent use for specific purposes. Subsequent use is thus a matter of use of *excess digital assessed information*.

The purposes are the following: use as lead in a criminal investigation, as evidence for a different offence provided this offence fulfils the conditions for interception, and for an offence where interception could not be used provided the investigation would otherwise be substantially impaired and use of the data is not deemed to be disproportionate.[56] Finally, intercepted data may be used to prevent an innocent from being convicted, and to avert a crime sufficiently serious to entail imprisonment.

The purposes for which excess information in such material may be used are limited to concern use in criminal investigation and prosecution, ruling out subsequent use for preventive purposes. Regarding crime prevention, the legislator would only go as far as to include use of the information to avert crime.[57] As the list is exhaustive, the possibility to register intercepted data for preventive purposes in an intelligence database or throw the material into a pool that could be analysed further, is excluded. This makes the Norwegian regulation in this respect much less broad than permitted by the LED Article 4(2), which as mentioned allows subsequent use for all the objectives set out in the LED Article 1(1).[58] However, the rules may be deemed to correspond with legitimate expectations of affected persons and stakeholders, in turn shaped in light of the principles of purpose limitation and orientation. Finally, data not used as per the possibilities set out in CPC § 216i must be made

[56] Use of intercepted data was rejected by the Court of Appeal in a decision 14 April 2023 (LB-2023-30228). Originally the criminal charge concerned corruption by a prison officer who allegedly smuggled smartphones to prisoners. This merited interception. The criminal charge was later reduced to concern negligence regarding a duty to prevent and report prisoners' use of drugs, an offence that could not merit interception. The Court of Appeal denied use of the evidence, a decision accepted by the public prosecutor.
[57] Ot.prp. nr. 64 (1998-1999) Ch. 8.9.3.3.
[58] One reservation should be made, as § 216 i also authorises the Police Security Service to make material intercepted in a criminal investigation available to the Foreign Intelligence Service, if necessary for preventive or security purposes." This provision relates to national security thus falling outside the substantive scope of the LED.

inaccessible to the police, whereas the data used as per the said provision shall be archived with the case in which they are used.[59]

The situation is different with respect to data collected by search and seizure. In this case the Norwegian Police Databases Act ("PDA")[60] § 4 states that data may be used "for the purpose for which they were collected, and for other police purposes unless it is provided by statute … that the right to process data is limited." The term "other police purposes" encompasses the objectives set out in the LED Article 1(1).[61]

As just noted for intercepted material, the CPC § 216i represents a statutory limitation to use for other police purposes, as the provision exhaustively sets out the lawful purposes for use. A corresponding limitation is not set out by statue specifically for data that are searched and seized. Thus, in theory the bulk data as a whole is available for subsequent use. Thus an attempt could be made to interpret the PDA § 4 in the same spirit as applied to the LED Article 4(1)(b) and (2). This would have the following implications: Firstly addressing the alternative that data that may be used "for the purpose for which they were collected": Reasonably interpreted this alternative must include use as evidence in the original case including evidence for other crimes provided that the incriminating information was uncovered accidentally. This alternative makes a distinction between digital assessed information and unknown data relevant, as it makes no sense that unknown data could be used as evidence.

The other alternative concerns use of the data for "other police purposes unless it is provided by statute … that the right to process data is limited." Given that "other police purposes" encompasses the objectives set out in the LED Article 1(1), the regulation of possible subsequent use corresponds to the LED Article 4(2). However, like the provision in the LED it is not clear whether "data" refers to the bulk as a whole or to the digital information disclosed in the digital forensic analysis. Authoritative legal sources do not seem to address the problem.

As seen from a procedural law perspective the alternative should be interpreted as concerning digital assessed information. This would be in line with the principles of purpose limitation and purpose orientation, and be coherent with the regulation of excess information of

[59] CPC §216g in conjunction with the Police Databases Act § 50 third paragraph.
[60] The Police Databases Act 2010.
[61] Cf. PDA § 2 no. 13.

intercepted data. The problem is that the scope of the PDA (reflecting the LED Article 1(1)) is much broader than that of the criminal procedural code. This creates a mismatch which as shown could be fixed by way of interpretation, but the better way is to enact more precise rules concerning subsequent use.

5. Conclusion.

The analysis has shown that the procedural principles of purpose limitation and purpose orientation may operate to limit the amount of data collected as bulk data in a criminal investigation to the digital information exposed to the police during the criminal investigation. As the principles are crucial to shaping the scope and direction of the investigation, they have an impact - albeit indirectly - on stakeholder's expectations concerning the amount of data that should be made available for subsequent use. There is a latent mismatch between the LED and criminal procedural law that could lead to uncertainty in national law about the limitations to subsequent processing, concretely, whether bulk data secured by search and seizure are available for such processing, or only the digital information. Considerations related to fairness and internal coherence in the legal framework suggest the latter, and could set a direction for more detailed regulation of the issue.