Section H: Conclusions

The findings elaborated in the present study give the picture of a snapshot. The situation is currently characterized by an as-yet very uncertain statistical data basis, the lack of systematic empirical studies and very different assessments among the practicing experts directly concerned, as expressed in the qualitative interviews.

1. Data Bases and Discourses

1. The effects of the BVerfG ("Federal Constitutional Court") ruling of March 2, 2010 are not yet quantifiable with reliable figures. The currently available statistical figures represent a period in which special conditions prevailed as a result of the temporary order issued by the BVerfG. As a result, regarding the ICT offenses in this period the access to the retained data in this segment was almost entirely blocked. Furthermore, the low proportion of unsuccessful proceedings is unlikely to be transferable to the current situation.

2. The investigation of gaps in protection due to the annulment of data retention of telecommunications traffic data can only be carried out to a limited extent, also with regard to the effects on crime clearance rates. This is due to the lack of specific empirical studies, the non-recording of procedure-related data for the query of traffic data as well as retained data or IP addresses, and the only fragmentary information available (and recorded) on the crime clearance rate in connection with special crime phenomena.

3. The debate on the benefits and consequences of data retention reveals that suitable data that could lead to a quantitative review of the effects of data retention on the crime clearance rate have not yet been gathered and, moreover, are not even intended to be gathered systematically.

4. The results of the responses to inquiries about the benefits of data retention in state parliaments to date also suggest that corresponding statistical surveys have not been carried out and will not be carried out because they are considered too costly.

5. For the European Commission, a particular problem emerges in this context. Data that could be used to evaluate Directive 2006/24/EC have not yet been supplied and cannot be supplied because a form of data collection suitable for this purpose was not even foreseen (see also the further conclusions under item 46 ff.).

6. The debate is therefore determined by referencing to individual cases and a special emphasis on the special need for protection of young and elderly people, which is expressed in the unmissable references to the suffering of sexually abused children and in emphasizing indications of the extraordinary perfidy of a deliberate exploitation of the weaknesses of elderly people.

7. The argumentation based on individual cases identifies the individual case as "typical", but without this being empirically proven or provable.

8. This is supplemented by the reference to the particular dangers posed by Islamist terrorists. It is precisely in this context, moreover, that there is no evidence whatsoever that traffic data retained in recent years has led to the prevention of a terrorist attack. Traffic data may have been suitable for aiding investigations after terrorist attacks, but at best it has led to the question of why digital traces of telecommunications that were already available and known could not have been used to prevent attacks.

2. Crime Clearance Rates: Trends in Selected Offense Areas

9. The evaluation of crime-specific clearance rates for the period 1987 to 2010 shows that the annulment of data retention is not a cause for changes in the crime clearance rate. This can be explained by the large number of cases registered by the police, compared to which the query of traffic data cannot be of any significance.

10. The crime-specific clearance rates in the areas of computer crime and so-called Internet crime also give no indication that the data retention phase would have brought about changes in the crime clearance rate tendency.

11. Taking a closer look at 2008 in particular, the year in which retained data were generally available, no query-related change in the crime clearance rate can be observed for any of the crime areas evaluated here in relation to the previous year or the subsequent years 2009/2010.

12. Comparing the crime clearance rates achieved in Germany and Switzerland in 2009, there is no evidence to suggest that data retention, which has been practiced in Switzerland for about 10 years, would have led to a systematically higher crime clearance rate.

13. Point-by-point comparisons between Germany, Austria and Switzerland, which are countries that have had different legal frameworks with regard to data retention since 2008 in particular (at least for a time), do not give rise to the conclusion that the systematic collection and storage of traffic data, or the lack thereof, would be associated with visible differences in the security situation.

14. After consulting other sources of information, no reliable indications arise that the possibilities for protection would have been reduced by the annulment of data retention.

14.1 Grandparent Scam

In connection with the evaluation of investigations into "grandparent scams", it became apparent that protection under criminal law (and gaps in protection) cannot be conditioned solely by recourse to retained data. This is underscored by successful investigations in Germany after the BVerfG ruling (which are further highlighted by police reports) as well as by comparing the developments of the "grandparent scam phenomenon" in Germany, Austria and Switzerland, where very different possibilities of recourse to traffic data exist. Furthermore, "grandparent scam" represents about 0.2% of all registered fraud cases and slightly less than 0.2% of the losses registered as fraud. This makes it a marginal phenomenon of fraud, which, incidentally, has only been countered in recent years by (apparently relatively successful) adjustments to investigative strategies (centralization) and whose particular relevance to criminal policy is seen precisely in the special need for protection of the elderly.

14.1. Homicides

For capital offenses, changes in crime clearance rates have not become visible due to the lack of data in the database. A separate evaluation of the homicides included in the BKA's case collection reveals no indication that the BVerfG's ruling would have impeded the clearing of the most serious crimes at all. Most of the cases reported as examples of cases that could not be investigated or could only be investigated with difficulty due to the absence of traffic data have been solved and, moreover, have already been adjudicated (without any indications of the need to access retained traffic data having become apparent). Furthermore, there are no indications suggesting that retained traffic data could have led to further investigations in the homicides that have not yet been solved.

14.2. Child Pornography

Investigations into the distribution and possession of child pornography are assigned particular importance, primarily because of the sexual abuse involved. However, the solving of cases of sexual abuse on the occasion of investigations into child pornography is at best a random occurrence. Furthermore, there are no indications suggesting that commercial websites are significantly involved in the production of child pornography. Finally, in view of the resources invested in the evaluation of data carriers and in view of the particular emphasis placed on the importance of prosecuting child pornography for the prevention of sexual abuse, the question may well arise as to whether the resources spent here would not have been better placed in other measures for the prevention and repression of child abuse.

14.3. Stalking

The criminal prosecution of stalking poses particular problems. However, these problems do not arise from the lack of recourse to telecommunications retention data. Furthermore, what such an assumption of a connection between protection against stalking and access to retained data could possibly be based on is not comprehensible against the background of the data on investigations and investigative findings, criminal proceedings and the outcome of criminal proceedings.

15. It can certainly not be ruled out that in complex proceedings and capital offenses, traffic data represent important circumstantial evidence or create additional investigative leads. However, such cases, if they can be identified beyond doubt, do not affect the overall trends.

3. Investigation Methods, Investigation Efficiency and Crime Clearance Rate

16. So far, there have been few systematic studies on the efficiency of investigative measures in the solving of crimes.

17. Accordingly, focusing on a single investigative measure, in this case the querying of retained traffic data, on the basis of empirical evaluations on investigations and criminal proceedings in the area of complex crime (especially organized crime) does not seem plausible.

18. Traffic data usually only matter in combination with other investigative measures.

19. From the perspective of crime clearance efficiency and possible security gaps, four constellations emerge from the previous debates and observations on the possible relevance of retained data:

19.1. The usage of traffic data in determining contacts or proximity to a crime scene/victim. This has been primarily addressed in the case of homicides. For homicides, the investigations have not revealed any evidence that the absence of traffic data would have prevented the case from being solved.

19.2. The usage of traffic data (in particular also geo-data) for retrospective identification of crime correlations in serial offenses (in particular by establishing historical movement profiles). Here, the historical-related query of traffic data represents one among several investigative methods (in the investigation of the correlations). So far, there is no conclusive data basis for an assessment of its (relative) importance in the identification of serial offenses.

19.3 The usage of retained traffic data to establish correlations between perpetrators (in individual cases (complicit commitment of robbery, etc.) or in the case of long-term commitment of crimes in groups or by means of transactions (narcotics, human smuggling, etc.). There is no empirical basis for a quantitative consideration of perpetrator correlations that cannot be solved because of the lack of traffic data. However, it can be ruled out that the absence of traffic data has had an impact on the overall development of, for example, narcotics trafficking[455].

---

455 See Reuter, P., Trautmann, F.: Report on Global Illicit Drugs Markets 1998-2007. European Community, Brussels 2009 for the links between law enforcement and narcotics markets.

19.4 The usage of retained traffic data in association with subscriber data for the most complete possible investigation in volume proceedings (child pornography, copyright infringements, computer fraud as well as attacks in networks related to viruses, Trojans, etc.). In some cases, these are sensitive crime areas. However, it is likely that they are either offenses that do not affect overall security at the same time, or offense areas that may indeed be relevant to security, but in which investigations in data networks related to the present or the future will be in the foreground. In particular, there is no evidence to date that sexual abuse can be prevented beyond chance by extensively tracking all traces that point to the downloading of child pornography.

4. Consequences from the Perspective of the Concerned Practicing Experts

20. The evaluations of the interviewed practicing experts, whose perceptions relate to the individual case perspective and are determined by their own field of work or the crime areas that are currently being processed, as well as the types of data required in each case, sometimes show a different focus. These factors contribute to widely varying experiences. Even within one agency and even more within one federal state, estimates of the current occurrence of measures, whether they have increased or decreased, also differ widely.

21. It is noticeable that the interviews revealed hardly any differences between the areas of operation of risk prevention and law enforcement. Although the occasions are different, the immediate objective of the measures is identical in both cases: in each case, it is a matter of identifying persons who are responsible for certain actions and therefore need to be identified. The only difference is that in one case it is about identifying suspects and in the other case it is about disruptors.

22. Failures in accessing traffic data are observed in several areas, according to the investigators interviewed:

22.1. The traffic data retention of incoming calls seems to have been almost completely eliminated at present. One-touch dialing as a possible substitute for situations in which the number being searched for is known is currently not possible at Deutsche Telekom, according to the unanimous report of all interviewees.

22.2. Particularly severe in the case of Internet-related searches or information requests is the fact that, on the basis of the current version of § 113 TKG ("Telecommunications Act"), telecommunications companies apparently regularly refuse to resolve IP addresses according to the subscriber data. As a result, numerous cases in the area of ICT crime currently remain obviously unsolved. This may also affect investigations into child pornography in particular.

22.3. The surveyed practicing experts also mentioned systematic failures with regard to specific device identifiers. In the case of IMSI and IMEI numbers, many queries were answered negatively due to a lack of billing relevance.

22.4. Further restrictions are observed in the case of radio cell queries, and in particular in the real-time variant. The latter does not appear to be technically possible with any of the providers, so that § 100g (3) StPO ("Code of Criminal Procedure") is dead law in this respect.

22.5. Real-time queries specifically in the mobile communications sector are currently only possible on the basis of a warrant pursuant to § 100a StPO, as there is no technical standard for separating content data.

23. To the extent that data are still retained notwithstanding the aforementioned restrictions, the situation is currently characterized by considerable differences in the retention practices of companies and, as a consequence, in the availability of traffic data. The variations are evident both in the overviews provided by the Bundesnetzagentur (Federal Network Agency) (see Tables C-5, C-6 above) and in the overviews provided by the authorities (see Table F-2 above). The threat of data loss creates a time pressure that has a noticeable effect on investigators and can lead to different reactions (see also items 29 to 31 right below). Investigative judges also feel this time pressure.

24. Especially short retention periods are observed with regard to IP addresses. In addition, a general reference is made to the frequent loss of data that dates back longer into the past. This is particularly evident in cases where there is often a delay in reporting. These are, for example, cases of phishing and Internet fraud, but also the so-called grandparent scam.

25. The accessibility of traffic data thus depends to a large extent on the retention behavior and the willingness to provide information of the respective telecommunications providers. Some practicing experts have suggested that perpetrators who have a certain understanding of telecommunications technology matters could take advantage of the different retention practices and systematically make themselves invulnerable. The probability of crime clearing may thus not only be dependent on chance - namely, on the question of which telecommunications provider and under which charging model a suspect handles his communications - but also susceptible to manipulation by the potential targets themselves.

26. According to the surveyed practicing experts, there is no adequate substitute for retrograde data that has been lost due to deletion. This applies in particular to investigations in the offense areas and risk situations listed in detail in section F under item 1.2.3.1.

27. Furthermore, missing traffic data cannot be replaced wherever they have an evidentiary function beyond their investigative function for the further course of proceedings and other evidence is not available.

28. Especially in Internet-related investigations, several aspects coincide: the particularly short retention periods for IP addresses, differing legal opinions between investigators and providers about the legal nature and the necessary requirements for merging IP addresses and subscriber data, and technical gaps regarding the configuration of ports at hotspots (keyword: IP sharing). These circumstances significantly complicate investigative work in the area of ICT crime. This is symbolized by the quote from one of the practicing experts from Baden-Württemberg, who compared the current situation on the Internet very vividly to road traffic without license plates. The interviews unanimously indicate that this is probably where the most serious protection gap is currently to be found.

29. The issues listed in item 22 are currently being addressed in practice in a variety of ways. In part - for example, in the area of cybercrime, where traffic data can sometimes be the only starting point (e.g., assignment of IP addresses or grandparent scams) - a query is often not performed from the outset if the presumed retention period has already expired. In other authorities, a decision is obtained as rapidly as possible or immediately in awareness of the imminent loss of data. This means that more queries may be carried out than in previous years, when such measures were not urgent and were only initiated after prior investigative work and thorough selection of suspects. The previously rather late application of the measure, depending on the case constellation, was also evident in the data of the 2008 MPI study.

30. According to many practicing experts, the filtering function of traffic data evaluations in the run-up to § 100a StPO measures is also frequently lost. In various investigative situations, this could lead to a wider spread and thus an increased number of surveillance of contents.

31. In addition, the more intrusive measures pursuant to § 100a StPO can also be used as a substitute for traffic data queries, albeit not on a broad basis. In this context, the special constellation of foreign head surveillance, which in certain cases can supplement or replace the one-touch-dial search that has become problematic, also seems to have a growing role to play. Some providers have reported such observations. This could also lead to an overall increase in the number of TKÜ warrants. In this respect, traffic data queries would be replaced by a more intrusive substitute. However, both cases are limited to the collection of future-oriented data. As already mentioned, retrograde data cannot be replaced.

32. The identification of potential gaps in protection cannot, after all, be made abstractly along the lines of individual offenses or offense areas. In fact, it depends largely on six factors:

- the type of offense,
- the type of data,
- the specific investigation situation,
- the operational objective,
- the responsible telecommunications company/provider,
- the course of time between the communication event relevant to the query on the one hand (related to the crime or to the hoped-for tactical knowledge of the investigation) and the point in time at which knowledge is first obtained (often the point in time at which the report is filed); as a rule, the authorities cannot control either point in time.

Each of the factors mentioned, as well as the coincidence of several, can lead to the inaccessibility of traffic data in individual cases and, as a result, to the case becoming unresolvable. This constellation is currently particularly frequent in the area of ICT crime. A reliable quantification is not yet possible. However, according to unanimous statements, the proportion is high.

33. In the preventative area, some additional problems arise in comparison to the repressive usage of traffic data queries. The surveyed police experts reported at least two cases in which the prevention of a concrete threat of death was said to have failed as a result of other traffic data queries being refused. With regard to Internet-related investigations, several examples were also described in which the perpetrators of amok and other violent threats originating on the Internet were not identifiable. The lack of radio cell information can also have a largely wider impact in the case of imminent threats than in the context of criminal investigations. It also appears that nationwide providers do not recognize and report queries based on state police laws if the agency responsible for the query is not located in the same state. Finally, it was reported that employees of the providers sometimes arrived at their own factual assessment that deviated from the ruling or the emergency warrant, for example, when assessing the existence of a specific risk situation.

34. Investigators find it particularly unsatisfactory that they are currently exposed to a feeling of arbitrariness on the part of the providers. They feel insufficiently informed and sometimes confronted with a non-transparent information practice and sometimes feel, to exaggerate, put in the role of a petitioner. Moreover, neither the usual understanding of the role of an investigator nor the external side effects are compatible, for example, the requirement to contact the responsible departments only via call centers, as is the case with private customers. In this respect, the corporate culture at German telecommunications providers also differs significantly from that in the USA, for example, where information about retention practices and query options is provided offensively and transparently.[456]

---

456 See Microsoft Criminal Compliance Handbook: Microsoft Online Services, Global Criminal Compliance Handbook, U.S. Domestic Version, March 2008, available under http://publicintelligence.net/microsoft-online-services-global-criminal-compliance-handbook/ [June 2011].

35. Many practicing experts have also expressed doubts about the accuracy of negative reports. The clearest statement was made by an investigator from Austria, who stated that the location data providers "lie to us [about the existence of stored data]". The German colleagues spoke more cautiously about corresponding assumptions.

36. Overall, the currently resumed usage of billing-related retention principles does not necessarily seem appropriate. The objective is completely different from that for data evaluation for law enforcement purposes. As a result, providers are currently unilaterally setting the conditions based on their own interests, but precisely not on those of the police in the context of their duties in averting threats and prosecuting offenders.

37. The practicing experts also identified the verification requirement for the purchase of SIM cards in general and prepaid cards in particular as another very practice-relevant regulatory gap. Investigators also repeatedly encounter limits when a so-called "Donald Duck account" is of relevance to investigations on the Internet.

5. Quick Freeze

38. Practicing experts across all professional groups do not see a quick freeze procedure as a suitable equivalent to data retention. This view was shared not only by the practicing experts from Germany, but also by those from Austria and Sweden. The survey respondents were unanimous in stating that this method would only selectively protect existing traffic data from deletion, but would not be able to generate the retrograde data that is particularly important from an investigative perspective ex post.

6. Situation Abroad

39. The foreign respondents also point out that traffic data queries are now an important element in the inventory of police investigative measures.

40. According to European and non-European police experience, telecommunications traffic data are unanimously of particular importance for criminal prosecution in the areas of gang and organized crime, telecommunications and computer crime. Due to the widespread use of modern means of communication, traffic data also offer additional investigative approaches in all areas of crime.

41. An international comparison reveals differences in the legal policy approach to data retention (with comparable assessments of the benefits of traffic data). In the USA, Canada, Australia and New Zealand in particular, there are no approaches to the introduction of comprehensive data retention beyond isolated and factually limited initiatives. In the USA, at least, this is also explained by the fact that telecommunications providers store a large volume of traffic data that can be accessed by law enforcement agencies due to the lack of restrictions under data protection law. These significantly different framework conditions must definitely be taken into account when evaluating the potential of the Quick Freeze procedure.

42. The current situation of the implementation of Directive 2006/24/EC in the member states of the European Union reveals considerable variation. In part of the member states, the directive has not yet been implemented or enforcement has been suspended. This is due to different reasons.

43. In Romania, the uncompromisingly negative decision of the Constitutional Court now blocks implementation of the directive. The constitutional issues are being pursued further with a pending decision by the Hungarian Constitutional Court and with a referral by the Irish Supreme Court to the European Court of Justice (Luxembourg) on the compatibility of the directive with the ECHR.

44. To the extent that the Directive has been implemented, the respective national legislations have led to differences, which are, however, already outlined in the Directive. This relates above all to the duration of retention, the scope (in terms of the crimes that can be prosecuted by means of retained traffic data and the way in which the prosecutable crimes are defined), and the other conditions under which traffic data can be queried.

45. Nevertheless, the Dutch and British governments in particular are very cautious about the potential of data retention along the lines of Directive 2006/24/EC. This is because, according to these statements, it is foreseeable that further developments in communications technology will overtake the current orientation of the Directive and trigger new needs for access to communications traffic data.

7. The Evaluation Report of the European Commission

46. The European Commission's evaluation report assumes that the retention of telecommunications data has contributed significantly to security in Europe.

47. However, the European Commission's evaluation could not refer to an assessment of data retention from the outset due to the lack of differentiation between retained and other traffic data. The report contains only data that describes solely the practice of generic traffic data queries.

48. The description of the usage of traffic data refers to data from about one third of the member states. Quite predominantly, the member states cannot even provide information on simple traffic data query structures.

49. The statistics on traffic data queries do not distinguish between subscriber data and traffic data in the narrower sense. Furthermore, no differentiation is made between different types of queries.

50. The description of the usage of traffic data and subscriber data does not differentiate according to the type or severity of the offense. The evaluation does not contain any statement on whether and to what extent retained data or generic telecommunications traffic data are relevant for investigations in the area of major crime.

51. The statistics provided by the member states do not in any case allow a statement on whether and to what extent (generic) traffic data in criminal investigations have (or have not) contributed to solving crimes.

52. The information and case reports that go beyond the few significant statistics are largely not comprehensible and therefore not suitable as a basis for evaluation.

53. For the reasons stated above, the evaluation of Directive 2006/24/EC presented by the European Commission does not give rise to any expectation that the potential for legal policy conflicts associated with the Directive will be eliminated in the foreseeable future.