# Case law on the data retention of electronic communications and its impact on national legislation and criminal proceedings

Georges Ravarani, Honorary Vice President of the European Court of Human Rights, Strasbourg

## *Case-law of the European Court of Human Rights*

1. The respect of private life is a fundamental value protected by **Art. 8 of the European Convention** on Human Rights (the Convention). The European Court of Human Rights (the ECtHR or the Court) has, from its early days, developed a comprehensive case law aimed at protecting this fundamental value.

2. Technological progress constitutes a major challenge to safeguarding private life as, on the one hand, individuals benefit from an extended range of means to communicate privately but, on the other hand, there are unprecedented means enabling the interception of communications and data retention, in turn leading to major challenges for personal data protection. Since its early days, the ECtHR has aimed at protecting individuals against the abusive **retention and processing of personal data**.[1]

3. Over the years the Court has examined many situations in which questions related to this issue have been raised. A broad spectrum of operations involving personal data, such as the collection, storage, use and dissemination of such data, is now covered by a body of case-law of the ECtHR. This case-law is in constant evolution, in line with the rapid development in information and communication technologies.

4. Unlike as provided for by the Charter of fundamental rights of the EU, the right to the protection of personal data is **not a self-standing or autonomous right** among the various Convention rights and freedoms. The ECtHR has nevertheless acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the Convention.[2] This Article is the main vector through which personal data is protected in the Convention system, even though considerations related to this protection may also come into play under other provisions of the Convention and its Protocols.[3]

---

[1] *Leander v. Sweden* judgment of 1987, in which the "old" Court analysed, for the first time, the question of the storage by a public authority of an individual's personal data.

[2] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], 2017, § 137; Z v. Finland, 1997, § 95; *L.B. v. Hungary* [GC], 2023, § 103

[3] There can be, e.g., in criminal proceedings, an issue with Article 6 of the Convention. The interception of a conversation as part of a covert police operation and the use of the evidence thus obtained as the basis for a conviction can lead to a finding of a violation of the said provision if the personal data used have been collected in a manner contrary to the requirements of domestic law or those of Article 8. However, the Court has held that the admission and use in judicial proceedings of evidence of this nature will not automatically lead to a finding that the proceedings were unfair if those proceedings as a whole were conducted fairly (*Bykov v. Russia* [GC], 2009, §§ 89-91; *Vukota-Bojic v. Switzerland*, 2016, §§ 91-100).

5. "**Personal data**" has a broad definition. The ECtHR has often referred to Convention no. 108 of the Council of Europe, entered into force in 1985 and updated in 2018, whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1). The Court has clearly indicated that, under Article 2 of Convention no. 108, the concept of personal data is defined as "any information relating to an identified or identifiable individual".[4] Such data cover not only information directly identifying an individual (the "data subject"), such as surname and forename, but also any element indirectly identifying a person such as a dynamic IP address.[5] Even though the question of personal data protection seems mainly to concern individuals, as regards their Article 8 right to respect for their private life, legal entities are also entitled to rely on this right before the Court if they are directly affected by a measure which breaches their right to respect for their "correspondence" or "home".[6]

Personal data can take many forms but for the purpose of the present intervention is sufficient to underline that electronic communications such as internet data, messaging, telephone communications are covered by the concept of personal data.

6. Under Article 2 of Convention no. 108, "**data processing**" includes: "any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data". The development of technologies has led to an increase in the types of operations involving personal data that can constitute processing.

7. The storing by a public authority of information relating to an individual's private life, however that information is obtained, amounts to an **interference** with the right to respect for the data subject's private life within the meaning of Article 8, whether or not the data is subsequently used.[7] In most cases where the processing of personal data was intended to allow the authorities to conduct an investigation into the data subject or to collect evidence in judicial proceedings before the domestic courts, the Court has found that such processing fell within the scope of Article 8 and had entailed interference with the respect for the private life of the person concerned.[8]

---

[4] *Amann v. Switzerland* [GC], 2000, § 65; *Haralambie v. Romania*, 2009, § 77

[5] *Benedik v. Slovenia*, 2018, §§ 107-108

[6] This was the case, for example, where a company had been ordered to provide a copy of all data on a server shared with other companies (*Bernh Larsen Holding AS and Others v. Norway*, 2013, § 106) or where the Ministry of Defence, under a warrant, had intercepted the communications of civil liberties NGOs (*Liberty and Others v. the United Kingdom*, 2008, §§ 56-57). However, in a case concerning measures involving the protection of personal data of members of a religious organisation and respect for their "private life", the organisation was not directly affected, and was thus not a "victim" within the meaning of Article 34 of the Convention (*Avilkina and Others v. Russia*, 2013, § 59)

[7] *Amman v. Switzerland* [GC], 2000, § 69; *Rotaru v. Romania* [GC], 2000, § 46; *S. and Marper v. the United Kingdom* [GC], 2008, § 67; *M.K. v. France*, 2013, § 29; *Aycaguer v. France*, 2017 § 33

[8] *Perry v. the United Kingdom*, 2003, §§ 39-43; *Uzun v. Germany*, 2010, §§ 51-52; *Vukota-Bojić v. Switzerland*, 2016, §§ 57-59; *López Ribalda and Others v. Spain* [GC], 2019, § 94 ; *Sârbu v. Romania*, 2023, §§ 38 and 41

8. Article 8 is a **qualified right** in the sense that para 2 of the said provision actually allows interferences with the right, provided that they are in accordance with the law and necessary in a democratic society, i.a. for the prevention of crime.

9. The interests of data subjects and the community as a whole in protecting personal data may be outweighed by the legitimate interest in the prevention of crime.[9] 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, such as sex offences.[10] While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders.[11]

The ECtHR has always taken the position that it **cannot call into question the preventive purpose** of such registers.[12] In fact, the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification.[13]

10. At the same time, since the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention, domestic law must afford **appropriate safeguards** to prevent any such use of personal data as may be inconsistent with the guarantees of this Article.[14]

Under Article 6 of Convention no. 108, personal data revealing racial origin, political opinions, religious or other beliefs, and information on an individual's health or sex life, or on any criminal convictions, cannot be automatically processed unless domestic law provides for appropriate safeguards. Information falling within these categories, described by the Court as "sensitive", warrant a heightened degree of protection in its view.

The intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned.[15]

It should be noted that at any rate, for Article 8 to come into play, the results of the personal data processing must attain a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to respect for private life.[16] However, it is difficult to imagine that the data retention of electronic communications is not serious.

---

[9] *S. and Marper v. the United Kingdom* [GC], 2008, § 104
[10] *B.B. v. France*, 2009, § 62; *Gardel v. France*, 2009, § 63; *M.B. v. France*, 2009, § 54; *N.F. and Others v. Russia*, 2023, § 44
[11] *S. and Marper v. the United Kingdom* [GC], 2008, § 100
[12] *Gardel v. France*, 2009, § 63; *B.B. v. France*, 2009, § 62; *M.B. v. France*, 2009, § 54
[13] *S. and Marper v. the United Kingdom* [GC], 2008, § 105
[14] *Glukhin v. Russia*, 2023, § 75
[15] *S. and Marper v. the United Kingdom* [GC], 2008, § 104
[16] *M.L. and W.W. v. Germany*, 2018, § 88

11. In its examination of the justification of the interference by public authorities, the ECtHR resorts to its traditional **three-step procedure** of assessing whether an interference with a qualified right is Convention compliant, i.e. whether it is provided for by law, pursues a legitimate aim and is necessary in a democratic society.

12. The constant development of technological progress has made it possible to go beyond individual targeted interceptions and to resort to **bulk interceptions** which present an even greater challenge to private life. The ECtHR has thus been obliged to adapt its case-law to the new technical developments. Some additional considerations dealing with the specificities of bulk interception will be added at the end.

**13. Lawfulness:** The Court has examined in a number of cases the question whether the requirement, as stated in Article 5 of Convention no. 108, that personal data undergoing automatic processing must have been obtained and processed fairly and lawfully, has or has not been met. In some cases the Court has found a violation of Article 8 solely on the grounds of a lack of legal basis at national level to authorise measures capable of interfering with the relevant rights.[17] In other cases the Court found a violation of Article 8 on the ground that domestic law, which was supposed to protect personal data, was inaccessible or confidential[18] or was not sufficiently clear and foreseeable.[19]

14. In the specific context of covert surveillance measures, such as the interception of communications, the Court has found that "**foreseeability**" cannot be understood in the same way as in many other fields. In its view, it cannot mean that an individual should be able to foresee when the authorities are likely to have recourse to such measures so that he or she can adapt his or her conduct.[20] However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on covert surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which, and the conditions upon which, public authorities are empowered to resort to any such measures.[21] In addition, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[22]

---

[17] *Taylor-Sabori v. the United Kingdom*, 2002, §§ 17-19; *Radu v. Moldova*, 2014, § 31; *Mockutė v. Lithuania*, 2018, §§ 103-104; *M.D. and Others v. Spain*, 2022, §§ 61-64; *Kaczmarek v. Poland*, 2024, §§ 74-80

[18] *Vasil Vasilev v. Bulgaria*, 2021, §§ 169-170; *Nuh Uzun and Others v. Turkey*, 2022, §§ 80-99

[19] *Vukota-Bojić v. Switzerland*, 2016; *Ben Faiza v. France*, 2018, §§ 58-61; *Benedik v. Slovenia*, 2018; *Rotaru v. Romania* [GC], 2000; *Zoltán Varga v. Slovakia*, 2021, § 162; *Haščák v. Slovakia*, 2022, §§ 94-95; *Kaczmarek v. Poland*, 2024, §§ 93-96. In the case of *Dimitrov-Kazakov v. Bulgaria*, 2011 (§ 33), the registration of an individual as an "offender" in the police registers was based on a non-public instruction at the material time which was confidential in character and was reserved, until its subsequent declassification, for the internal use of the Ministry of the Interior.

[20] *Adomaitis v. Lithuania*, 2022, § 83

[21] *Malone v. the United Kingdom*, 1984, § 67; *Leander v. Sweden*, 1987, § 51; *Valenzuela Contreras v. Spain*, 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 93; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 75; *Roman Zakharov v. Russia* [GC], 2015, § 229

[22] *Roman Zakharov v. Russia* [GC], 2015, § 230

15. In its case-law on the interception of communications in the **context of criminal investigations**, the Court has determined that, in order to prevent abuse of power, the law must at least set out the following six elements (*"Weber* safeguards"): the nature of the offences that may give rise to an interception order[23]; the definition of the categories of persons whose communications may be intercepted[24]; the time-limit on the implementation of the measure; the procedure to be followed for the examination, use and storage of the data collected; the precautions to be taken for the transmission of the data to other parties; and the circumstances in which intercept data may or must be deleted or destroyed.[25]

16. **Review and supervision** of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be carried out without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[26]

As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively[27] or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken.[28]

17. **Legitimacy:** In a number of cases the Court has examined whether the requirement, as stated in Article 5 of Convention no. 108, that personal data undergoing automatic processing must have been collected for explicit, specified and legitimate purposes, has or has not been met. In these cases, the examination of the legitimate aims which may justify interference with

---

[23] However, in *Roman Zakharov v. Russia* [GC], 2015, § 244, the Court underlined that the foreseeability criterion does not require States to exhaustively list the offences which can lead to an interception.

[24] Unlike the CJEU, the Strasbourg Court does not impose a temporal or geographical limit or a group of persons likely to be involved in a serious crime. In its judgments, it refers to a "reasonable suspicion" against a person or, more broadly, to the necessity in a democratic society (see *Roman Zakharov v. Russia* [GC], 2015, § 260).

[25] *Huvig v. France,* 1990, § 34; *Valenzuela Contreras v. Spain*, 1998, § 46; *Weber and Saravia v. Germany* (dec.), 2006, § 95; *Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria*, 2007, § 76

[26] see *Roman Zakharov v. Russia* [GC], 2015, § 233; see also *Klass and Others v. Germany*, 1978, §§ 55 and 56, Series A no. 28

[27] see *Roman Zakharov v. Russia* [GC], 2015, § 234; see also *Klass and Others v. Germany*, 1978, cited above, § 57, and *Weber and Saravia v. Germany* (dec.), 2006, § 135

[28] see *Roman Zakharov v. Russia* [GC], 2015

the exercise of the Article 8 rights, as listed in paragraph 2, is rather succinct. These aims are the protection of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. The Court generally finds the existence of one or more of these legitimate aims invoked by the Government.[29]

18. **Necessity:** In order to be necessary in a democratic society, any measure interfering with the protection of personal data under Article 8 must meet a "pressing social need" and must not be disproportionate to the legitimate aims pursued.[30] Although the States enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim, in its European supervision, the ECtHR examines the reasons invoked by the Government which must be pertinent and sufficient.[31] While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention.[32]

19. The following **factors** were considered **relevant for the assessment of necessity**[33]:

---

[29] The interception of telephone conversations of the applicant – a prison director, who had been suspected of corruption – the storage of that information and its disclosure in the disciplinary proceedings, which ultimately had led to his dismissal, were found to aim at preventing acts of a corrupt nature and guaranteeing the transparency and openness of public service, and thus had pursued the legitimate aims of the prevention of disorder or crime, and the protection of the rights and freedoms of others in *Adomaitis v. Lithuania*, 2022 (§ 84).

[30] *Z v. Finland,* 1997, § 94; *Khelili v. Switzerland*, 2011, § 62; *Vicent Del Campo v. Spain*, 2018, § 46

[31] *Z v. Finland*, 1997, § 94. See also, very recently, *Podchasov v. Russia,* 13 February 2024, where the statutory requirement for internet providers to store and retain internet communications, to decrypt end-to-end encrypted communications and to give authorities access to such data was found disproportionate and unnecessary in a democratic society. The Stats has thus been found to have overstepped its margin of appreciation.

[32] *S. and Marper v. the United Kingdom* [GC], 2008, § 101

[33] In the context of the interception of telephone conversations, the ECtHR has found **violations** of Article 8 in the following spheres: phone tapping and supply of records of metering to the police (list of telephone numbers called) (*Malone v. the United Kingdom*, 1984, §§ 63-89); monitoring and transcription of all the applicants' commercial and private phone calls (*Huvig v. France*, 1990, §§ 24-35); monitoring and recording of several of the applicant's phone conversations by tapping a third party's telephone line (*Kruslin v. France*, 1990, §§ 25-36); phone tapping of a person via a third party's telephone line (*Lambert v. France*, 1998, §§ 21-41); monitoring and recording by the public prosecutor of a telephone call received by an individual in his office from another individual in the then Soviet Embassy in Bern (*Amann v. Switzerland* [GC], 2000, §§ 45-62); phone tapping in the framework of a preliminary investigation (*Prado Bugallo v. Spain*, 2003, §§ 28-33); telephone conversations monitored in the context of a criminal prosecution and subsequently published in the press (*Craxi v. Italy* (no. 2), 2003, §§ 57-84); inclusion in the applicant's case file of a transcription from phone tapping carried out in proceedings in which he had not been involved (*Matheron v. France*, 2005, §§ 27-44); monitoring of phone calls by the authorities in the absence of authorisation by the public prosecutor issued in the name of the suspect and without legislation providing sufficient safeguards against arbitrariness (*Dumitru Popescu v. Romania* (no. 2), 2007, §§ 61-86); tapping of phone calls made by a lawyer for criminal investigations (*Kvasnica v. Slovakia*, 2009, §§ 80-89); insufficient safeguards against arbitrariness in domestic provisions on phone tapping (*Dragojević v. Croatia*, 2015, §§ 85102; *Liblik and Others v. Estonia*, 2019, §§ 132-143); lack of adequate judicial guarantees (*Moskalev v. Russia*, 2017, §§ 35-45); lack of effective supervision of the recoding of phone calls in the framework of criminal proceedings (*Pruteanu v. Romania*, 2015, §§ 41-58); monitoring of mobile phone calls (*Šantare and Labazņikovs v. Latvia*, 2016, §§ 56-63); unjustified failure to provide ex post notification of a temporary mobile phone tapping measure (*Cevat Özel v. Turkey*, 2016, §§ 29-37); and preventive monitoring of phone calls (*Mustafa Sezgin Tanrıkulu v. Turkey*, 2017, §§ 45-66); the interception, recording and transcription of a telephone conversation between a lawyer and one of his clients, a former defence minister, who was under covert surveillance in connection with a criminal investigation (*Vasil Vasilev v. Bulgaria*, 2021, §§ 167-181). – The Court found **no violation** of Article 8 concerning phone tapping which had been authorised by judicial decision, in the knowledge that the necessity of that measure had been assessed by the courts (*İrfan Güzel v. Turkey*, 2017, §§ 78-89). The Court also found no violation of Article 8 in the following cases: the registration by the police of telephone numbers called by an individual by metering his private telephone (*P.G. and J.H. v. the United Kingdom*, 2001, §§ 42-51); the tapping of a judge's telephone lines in the framework of criminal investigations into an illegal organisation of which he had been suspected of being a member, contributor or supporter (*Karabeyoğlu v. Turkey*, 2016, §§ 74-111); and the interception of telephone communications of a prison director in the

20. **Scope: nature of the data stored**. In several cases the Court has called into question the broad scope of the data storage system installed by the authorities, which failed to draw a distinction according to the nature or degree of seriousness of the offence leading to conviction[34], or depending on whether the data subject had been convicted, acquitted, discharged or merely cautioned, having been suspected of committing an offence.[35] The Court considers that the facilities put in place by the authorities to assist in punishing and preventing certain offences cannot be implemented as part of an abusive drive to maximise the information stored in them. 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 breaches which they would cause to the rights and freedoms which States must guarantee under the Convention to persons under their jurisdiction.[36]

21. There is a risk of stigmatisation where persons who have **not been convicted** of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons.[37] Even though the retention of private data concerning individuals suspected of an offence but acquitted or discharged cannot be equated with the voicing of suspicions, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed. Therefore,

---

context of a criminal investigation into his suspected corruption-related activity in the prison for personal gain, even though eventually that investigation was discontinued on the basis of a lack of incriminating evidence (*Adomaitis v. Lithuania*, 2022, §§ 81-90). 134. Several applications have been declared inadmissible as manifestly ill-founded, as regards: phone tapping in the framework of preventive intelligence activities by the police (*Deveci v. Türkiye* (dec.), 2022); phone tapping in the framework of a preliminary investigation (*Greuter v. the Netherlands* (dec.), 2002); phone tapping in the framework of a criminal investigation as one of the main investigative methods helping to prove the involvement of certain individuals in a major drug-trafficking network (*Coban v. Spain* (dec.), 2006); and monitoring of telephone communications effected by a Member of the European Parliament charged with misappropriation of corporate assets, and the inapplicability in that case of the special treatment given to national MPs (*Marchiani v. France* (dec.), 2008). 135. In the prison context, the illegal recording and storage of a prisoner's telephone calls by the prison authorities, and their subsequent use in evidence to convict the prisoner of a further offence, had breached Article 8, in the case of *Doerga v. the Netherlands*, 2004 (§§ 43-54). 136. In a range of other fields the Court has found violations of Article 8 concerning: an automatic system of monitoring all correspondence and telephone calls by minors housed in a correctional boarding school, ruling out any kind of confidentiality as regards the types of exchanges monitored (*D.L. v. Bulgaria*, 2006, §§ 100-116); the warranted interception by the Ministry of Defence of outgoing communications by organisations working in the civil liberties field (*Liberty and Others v. the United Kingdom*, 2008, §§ 56-70); the mere existence of legislation allowing the monitoring of telecommunications by a Moldavan non-governmental organisation specialising in representing applicants before the Court (*Iordachi and Others v. Moldova*, 2009, §§ 29-54); leaks to the media and broadcasting of a private conversation recorded with the authorities' approval on the telephone line of a politician who was under investigation by the prosecuting authorities (*Drakšas v. Lithuania*, 2012, § 62); shortcomings in the legal framework governing secret monitoring of mobile phone calls put in place by mobile phone network operators, enabling the Federal Security Service to intercept any kind of telephone communication without prior judicial authorisation (*Roman Zakharov v. Russia* [GC], 2015, §§ 163-305); the use in a disciplinary inquiry of phone tapping data from a criminal investigation (*Karabeyoğlu v. Turkey*, 2016, §§ 112-121); and the use in disciplinary proceedings against a lawyer of a transcription of a conversation with one of her client's whose phone had been tapped (*Versini-Campinchi and Crasnianski v. France*, 2016, §§ 49-84).

[34] *M.K. v. France*, 2013, § 41; *Aycaguer v. France*, 2017, § 43; *Gaughran v. the United Kingdom*, 2020, § 94; *N.F. and Others v. Russia*, 2023, § 49

[35] *S. and Marper v. the United Kingdom* [GC], 2008, § 119; *M.M. v. the United Kingdom*, 2012, § 198; *M.K. v. France*, 2013, § 42; *Brunet v. France*, 2014, § 41; *N.F. and Others v. Russia*, 2023, § 49

[36] *M.K. v. France*, 2013, § 35 ; *Aycaguer v. France*, 2017, § 34

[37] *S. and Marper v. the United Kingdom* [GC], 2008, § 122

the fact that a person has benefited from a discharge after being suspected of an offence justifies treating him or her differently from a convicted person.[38]

22. Even in case of a conviction, the data retention is not automatically justified. The Court has considered a series of cases relating to the recording in databases designed for the punishment and prevention of crime the personal data of individuals convicted of **minor offences**[39] or even for a series of offences that were neither minor nor particularly serious.[40]

23. **Data retention period and deletion**. The length of the period for which the authorities decide to store an individual's personal data is an important, albeit not a decisive, aspect to be taken into account in assessing whether or not the storage of personal data in a file or a database for police purposes is proportionate to the legitimate aim pursued.

24. Whereas the lack of a maximum period for the retention of personal data is not necessarily incompatible with Article 8[41], **procedural safeguards** are necessary where the storing of the data depends entirely on the diligence with which the authorities ensure the proportionality of the data retention period.[42] If no effective time-limit is provided for, there must be an available judicial procedure enabling the interested person to request the deletion of the data the conservation of which is no longer necessary. In such cases, where there is no automatic time-limit for the storage of the data, the existence or lack of independent review of the justification for retention of the information according to defined criteria such as the seriousness of the offence, the strength of the suspicion against the person, previous convictions and any other special circumstances, is a major safeguard for ensuring the proportionality of data retention periods.[43] The Court was satisfied with a system which did not provide for a maximum time of storage of data if there was an independent periodic review of the necessity of their continued storage.[44] The availability at the national level of a judicial

---

[38] *M.K. v. France*, 2013, § 42; *Brunet v. France*, 2014, § 40. In this latter case, where the applicant had benefited from a discontinuance decision following mediation, the Court called into question the indiscriminate nature of the personal data recorded in the authorities' files, drawing no distinction between convicted persons and individuals whose cases had been discontinued. In the case of *Aycaguer v. France*, 2017 (§§ 42-43), where personal data had been collected and retained following a conviction for offences which were not the most serious, the Court called into question the broad scope of the personal data collection by the authorities, which had drawn no distinction according to the level of seriousness of the offence leading to conviction, notwithstanding the wide range of situations liable to arise in the framework of the application of the law. The case of *N.F. and Others v. Russia*, 2023, (§§ 49-55), concerned a data storage system where information concerning criminal proceedings was automatically collected and stored once an individual was subjected to criminal prosecution. That system covered information on all criminal convictions, irrespective of the nature and gravity of the offence committed and irrespective of the fact whether those convictions had already been spent, as well as information on criminal proceedings that had been discontinued on "non-rehabilitative grounds". The Court found the scope and application of that system to be excessive. Moreover, it emphasised that the continued processing of data had been particularly intrusive for those individuals who had not been convicted of any criminal offences. As regards convicted individuals, the level of interference with their private life would also be intrusive after their convictions had become spent or were lifted by a court. In the absence of sufficient guarantees against abuse and the possibility of a review, such processing was found to be disproportionate.

[39] *M.K. v. France*, 2013, §§ 6, 8, 41; *Aycaguer v. France*, 2017, §§ 8, 43

[40] *P.N. v. Germany*, 2020, §§ 6, 81

[41] *Gaughran v. the United Kingdom*, 2020, § 88

[42] *Peruzzo and Martens v. Germany* (dec.), 2013, § 46; *Ayçaguer v. France*, 2017, § 38

[43] *S. and Marper v. the United Kingdom* [GC], 2008, § 119; *B.B. v. France*, 2009, § 68; *Gardel v. France*, 2009, § 69; *M.B. v. France*, 2009, § 60

[44] Conversely, the Court found no violation of Article 8 in several cases concerning the storage of the personal data of individuals convicted of sexual assault for a maximum thirty years, after which period the data was automatically deleted,

procedure for the removal of data that provides for independent review of the justification for retention of the information according to defined criteria and affords adequate and effective safeguards of the right to respect for the data subject's private life is an important factor in balancing the various competing interests.[45] The Court has found no violation of Article 8 in cases where, even though the data had been retained for "long" periods of up to thirty years[46], or indeed indefinitely[47], the data subject had benefited from a judicial procedure guaranteeing independent review of the justification for storing their data according to defined criteria, enabling them to secure the deletion of the data before expiry of the maximum period prescribed by law, or, in the case of indefinite data retention, as soon as such retention was no longer relevant.

25. It goes without saying that the maximum period of time for the storage must be effective. A maximum storage period for personal data laid down in domestic law may be more akin, in practice, to a norm than to a real maximum if the chances of acceptance of a request for deletion of the data before expiry of the period laid down by law are merely hypothetical.[48]

26. **Limit of the use of data to the purpose for which they were recorded**. The Court has taken the view that it is important to limit the use of data to the purpose for which they were recorded. Thus, e.g., the use in a disciplinary investigation of data that came from telephone tapping during a criminal investigation, and consequently for a different purpose from that which had justified their collection, was found to breach Article 8.[49]

27. Some final words on **bulk interception**. As underlined in *Weber and Saravia* and *Liberty and Others* and repeated in *Big Brother Watch*, the principles applicable to targeted interceptions are basically the same: Art. 8 is applicable and the decision to operate a bulk interception regime in order to identify threats to national security or against essential

---

because procedures had been introduced to enable the data to be deleted as soon as it was no longer relevant (*B.B. v. France*, 2009, § 67; *Gardel v. France*, 2009, § 69; *M.B. v. France*, 2009, § 59). The Court also declared manifestly ill-founded a case concerning the indefinite retention of the personal data of persons convicted of serious offences, accompanied by reviews at regular intervals of no longer than ten years, to determine whether the data storage was still necessary (*Peruzzo and Martens v. Germany* (dec.), 2013, §§ 44-49). In the case of *P.N. v. Germany*, 2020 (§§ 87-90), the Court found no violation of Article 8 with regard to the retention for five years, subject to guarantees and individualised review, of a repeat offender's personal data for the purposes of identifying him following the commencement of fresh criminal proceedings against him.

[45] *S. and Marper v. the United Kingdom* [GC], 2008, § 119; *Gardel v. France,* 2009, § 69

[46] *B.B. v. France*, 2009, §§ 66, 68; *Gardel v. France*, 2009, §§ 67, 69; *M.B. v. France*, 2009, §§ 58, 60

[47] *Peruzzo and Martens v. Germany* (dec.), 2013, § 46

[48] *M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45; *Ayçaguer v. France*, 2017, §§ 44-46. The Court has found a violation of Article 8 in several cases where the national system provided for maximum periods of storage of twenty or twenty-five years for offences in which proceedings had been discontinued (*M. K. v. France*, 2013, §§ 44-47; *Brunet v. France*, 2014, §§ 41-45), and indeed a maximum forty-year storage period in the case of an offence that had not been particularly serious but which had led to a conviction (*Ayçaguer v. France*, 2017, § 42). 220. In Catt v. the United Kingdom, 2019 (§ 120), the retention of the applicant's personal data in a national police database on extremism for at least six years, after which period it would be subject to a scheduled review had led to a finding of a violation of Article 8. The applicant had been completely dependent on the authorities' diligence in implementing the highly flexible safeguards laid down in the applicable code of practice, in ensuring the proportionality of the data retention period. The lack of safeguards to facilitate the deletion of the data as soon as the period of retention became disproportionate is particularly disturbing where data revealing political opinions, which attracts a heightened level of protection, is being retained indefinitely (ibid., §§ 122-123). 221. The case of *M.M. v. the United Kingdom*, 2012, concerned the consequences of changes of policy on the retention period for personal data on a criminal record in terms of the data subject's employment prospects (§ 204).

[49] *Karabeyoğlu v. Turkey*, 2016, §§ 112-121.

national interests is one which continues to fall within the States' margin of appreciation.[50] However, due to the technical developments since the ECtHR first ruled on bulk interception, enabling 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 and the potential abuses have increased, the Court felt the need to further develop its approach to bulk interception. It found that in assessing whether the respondent State acted within its margin of appreciation, the Court would need to take account of a wider range of criteria than the six *Weber* safeguards (see above, no. 15).

In the context of the margin of appreciation, one should not lose sight of the fact that it would be difficult for an international court to be too prescriptive as to the assessment of the imminence of terrorist threats and as to the means to be deployed in order to prevent such attacks. Science plays both ways, terrorists also use more and more sophisticated tools. And one should not forget that States also have a positive Convention obligation, namely, to protect their citizens' life as provided for by Art. 2 of the Convention.[51]

28. More specifically, in addressing jointly "in accordance with the law" and "necessity" as is the established approach in this area, the Court will examine whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[52]

29. In order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "**end-to-end safeguards**", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime.

---

[50] *Big Brother Watch v. the United Kingdom* [GC], 2021, § 340.
[51] *Tagayeva v. Russia,* 2017, §§ 481-493
[52] § 361

30. Data retention seems to be an endless story. And as always with scientific progress, law hopelessly runs behind, trying to frame the use of technological developments and to prevent the most blatant abuse. But what is abuse? Combatting crime certainly is not. Therefore, the exercise is extremely delicate and as in so many fields, the ECtHR has attempted and goes on attempting, the future will tell us how successfully, to strike a fair balance between the legitimate use of data retention and abuse which risks undermining the rule of law and the citizen's basic freedoms.