KEY THEME[1]
Terrorism
Surveillance measures[2]

(Last updated: 28/02/2025)

Introduction

Surveillance measures, and in particular covert surveillance measures, which are at the core of the fight against terrorism, may raise an issue under Article 8 of the Convention. The first paragraph of Article 8 defines the principle of respect for "private and family life", the "home" and "correspondence". The second paragraph provides for the possibility for States to restrict this right, particularly in the interests of national security and to protect public order. After determining whether an applicant can claim to be a victim (an issue when the surveillance remains covert), the Court applies a three-stage test: whether there has been an interference with the applicant's rights, whether the interference was in accordance with the law, and whether it was necessary in a democratic society in order to protect a legitimate interest.

Preliminary issue: victim status

- The first issue that the Court will have to address in the context of surveillance measures, which in most cases are conducted in secrecy, is whether an applicant has victim status, namely, whether he/she has been directly or indirectly affected by the alleged violation of Article 8.
- In determining victim status, the Court considers whether the person is covered by the scope of the legislation authorising secret surveillance measures and whether available remedies at the domestic level exist. Where the domestic system does not afford an effective remedy, the threat of surveillance constitutes for all users or potential users a direct interference with the rights guaranteed by Article 8. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the person may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures (*Roman Zakharov v. Russia* [GC], 2015, § 171; see also *Ekimdzhiev and Others v. Bulgaria*, 2022, §§ 263-277 and *Pietrzak and Bychawska-Siniarska and Others v. Poland*, 2024, §§ 140-146).
- Applying the above criteria in the context of bulk interception regimes, victim status may be established by the mere existence of the possibility of having communications and related data intercepted and analysed, without the need for an applicant to show that he is at such a risk due to his personal situation, where the domestic remedies available to

[1] Prepared by the Registry. It does not bind the Court.

[2] The judgments and decisions cited in this document do not all refer to cases of terrorism. However, they contain legal principles and reasoning which are particularly relevant in the context of terrorism.

persons who suspect that they are affected by bulk interception measures are subject to a number of limitations. Under these circumstances, an examination *in abstracto* of bulk interception legislation may therefore be justified (*Centrum för rättvisa v. Sweden* [GC], 2021, §§ 168-177).

- Regarding the remote retrieval of user data from a specific closed network, the fact that the applicants have been arrested and accused based on this data is sufficient to establish their victim status. Such applicants do not need to demonstrate that they had been using the closed network, as this would amount to compelled self-incrimination and a disproportionate obstacle to the effective exercise of their right of individual application (*A.L. and E.J. v. France* (dec.), 2024, §§ 113-114).

Interference

- Individual surveillance measures:
  - Interception and recording of telephone communications; the subsequent use of the stored information has no bearing on that finding (*Amann v. Switzerland* [GC], 2000, §§ 45 and 69).
  - Collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge (*Copland v. the United Kingdom*, 2007, §§ 43-44).
  - Although the monitoring of an employee's electronic messaging (Yahoo) by a private commercial company cannot be regarded as "interference" with his right by a State authority, the national authorities have a positive obligation to protect the applicant's rights under Article 8 (*Bărbulescu v. Romania* [GC], 2017, §§ 112 and 114). See also *López Ribalda and Others v. Spain* [GC], 2019, §§ 109-111, with regard to video surveillance at the workplace.
  - Placing audio and video-recording devices in the applicant's cell, and the prison visiting area (*Allan v. the United Kingdom*, 2002, §§ 35-36, and *Gorlov and Others v. Russia*, 2019, § 84).
  - Setting up a system for interception of conversations held in the prisons visiting area (*Wisse v. France*, 2005, §§ 29-30).
  - List of telephone calls made between two persons (*Heglas v. the Czech Republic*, 2007, §§ 60-61).
  - Tracking by GPS of the applicants' car (*Uzun v. Germany*, 2010, §§ 43-48).
  - Fingerprints and DNA samples (*S. and Marper v. the United Kingdom* [GC], 2008, §§ 77-86).
  - Search and seizure of electronic data and emails (*Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, 2015, § 92).
- Mere existence of legislation authorising secret surveillance of mobile telephone communications (*Roman Zakharov v. Russia* [GC], 2015, § 179; *Ekimdzhiev and Others v. Bulgaria*, 2022, §§ 263-277).
- Bulk interception regimes:
  - Unlike targeted interception, bulk interception is generally directed at international communications and predominantly used for foreign intelligence gathering and the identification of new threats from both known and unknown actors (among which global terrorism). Generally, bulk interception regimes may be described as starting with the interception and initial retention of data in bulk, followed by the application of specific selectors to the retained data, the examination of the selected data by analysts

and lastly the retention and use of the "final product", including sharing with third parties. Article 8 applies at each of these stages and the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. (*Centrum för rättvisa v. Sweden* [GC], 2021, §§ 239-245; *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 325-331).

- A bulk interception regime may also have repercussions on confidential journalistic material under Article 10, commensurate with that occasioned by the search of a journalist's home or workplace (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 448).

- In the case of receipt of intelligence from foreign intelligence services, the interference with Article 8 rights does not lie in the interception itself, where it was carried out under the full control of foreign intelligence services and thus did not fall within the receiving State's jurisdiction. Rather, the interference lies in the initial request and subsequent receipt of intercepted material, followed by its storage, examination and use by the intelligence services of the receiving State (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 495-496).

In accordance with the law and necessary in a democratic society in order to protect a legitimate interest

- In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question of whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (*Roman Zakharov v. Russia* [GC], 2015, § 236). The Court will assess in turn:
  - *Accessibility of the domestic law*
  - *Scope of application of secret surveillance measures*
  - *The duration of secret surveillance measures*
  - *Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data*
  - *Authorisation of interceptions*
  - *Supervision of the implementation of secret surveillance measures*
  - *Notification of interception of communications and available remedies*
- The legitimate interests capable of justifying interference with private life are exhaustively listed in the second paragraph of Article 8. The fight against terrorism is invariably viewed by the Court as a legitimate aim within the meaning of that provision, as it comes under the heading of defending national security and of protecting public order (see, for instance, *Klass and Others v. Germany*, 1978, § 48, and *Uzun v. Germany*, 2010, § 80).
- Domestic courts which authorise the covert surveillance must verify whether there was a "reasonable suspicion" against an applicant and apply the "necessity in a democratic society" and "proportionality" tests. Moreover, the refusal to disclose the surveillance authorisations to the applicant without any valid reason would deprive him or her of any possibility to have the lawfulness of the measure, and its "necessity in a democratic society", reviewed by an independent tribunal (*Zubkov and Others v. Russia*, 2017, § 132, *Denysyuk and Others v. Ukraine*, 2025, §§ 93-100, 158-159, *Romanchenko and Kharazishvili v. Georgia*, 2025, §§ 54-60).
- Due to the inherent risk of abuse and the legitimate need for secrecy of bulk interception regimes, the Court has stressed the need for fundamental "end-to-end safeguards" for

compliance with Article 8 requirements of any such regimes. This means 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. Bulk interception should be subject to an independent authorisation at the outset, when the object and scope of the operation are being defined, and there should be an independent *ex post facto* review of the operation. While *judicial* authorisation would be an important safeguard against arbitrariness, it is not a necessary requirement, for as long as the body authorising bulk interception is independent of the executive (*Centrum för rättvisa v. Sweden* [GC], 2021, §§ 263-265; *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 349-351).

- In particular, in assessing the "in accordance with the law" and "necessity" requirements in the context of bulk interception, the Court will examine whether the domestic legal framework clearly defined the following safeguards (*Centrum för rättvisa v. Sweden* [GC], 2021, § 275; *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 361):
  - *the grounds on which bulk interception may be authorised;*
  - *the circumstances in which an individual's communications may be intercepted;*
  - *the procedure to be followed for granting authorisation;*
  - *the procedures to be followed for selecting, examining and using intercept material;*
  - *the precautions to be taken when communicating the material to other parties;*
  - *the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;*
  - *the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;*
  - *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.*
- The general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (*Ekimdzhiev and Others v. Bulgaria*, 2022, § 395; *Škoberne v. Slovenia*, 2024, § 137).
- The nature and severity of the interference with privacy rights due to systemic surveillance (data retention) of all users of telecommunication services requires the Court to exercise a correspondingly stricter scrutiny in assessing the question of fair balance, including the requisite safeguards (*Škoberne v. Slovenia*, 2024, §§ 132-136).
- In the context of receipt of intelligence from foreign intelligence services, necessary safeguards have to be defined in domestic legislation for each of the two stages of the process, namely the initial request for intelligence and the actual receipt of the intercepted material:
  - As to the first stage (the initial request), States should not be able to circumvent their Convention obligations through requesting intercepted communications from non-Contracting States. Therefore, such a request must have a basis in domestic law which is accessible to the person concerned and foreseeable to its effects. In addition, there should be clear detailed rules as to the circumstances in which and the conditions on which such a request can be made and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 497).
  - As to the second stage (the receipt of the intercept material), the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. This applies to all material received

from foreign intelligence services that *could* be the product of intercept, even if the receiving State may not always actually be aware whether the material received is the product of interception (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 498).

- Finally, any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 499).

Use of evidence obtained through surveillance measures

- The administration of (unlawfully obtained) evidence[3] is particularly relevant where evidence has been obtained through secret means.
- Article 6 of the Convention does not lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law (*Schenk v. Switzerland*, 1988, §§ 45-46*; Moreira Ferreira v. Portugal (no. 2)* [GC], 2017, § 83).
- It is not the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible. The question is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair (*Bykov v. Russia* [GC], 2009, § 89; see also *Gäfgen v. Germany* [GC], 2010, §§ 166-167; *El Haski v. Belgium*, 2012, § 85; *Škoberne v. Slovenia*, 2024, § 146).
- Where evidence has been obtained in violation of Article 8, the Court looks at the overall fairness of the proceedings, in particular at whether the impugned evidence was the only evidence relied on by the domestic courts (*Vukota-Bojić v. Switzerland*, 2016, § 99; *Hambardzumyan v. Armenia*, 2019, § 79).
- In determining the overall fairness of the proceedings, an examination of the rights of defence is necessary, particularly whether the applicant was given the opportunity to challenge the authenticity of the evidence and opposing its use. The quality of the evidence must also be taken into consideration, especially when the circumstances in which it was taken cast doubt on its reliability or accuracy. Furthermore, regard may be had to the weight of the public interest in the investigation and punishment of the particular offence as compared to that of the individual interest that evidence be gathered lawfully (*Hambardzumyan v. Armenia*, 2019, §§ 75-76, *Macharik v. the Czech Republic*, 2025, §§ 51 -53).
- The right to an adversarial trial requires that, in a criminal case, both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party, for instance, a surveillance videotape (*Murtazaliyeva v. Russia* [GC], 2018, §§ 90-95).

The protection of confidential journalistic material in bulk interception regimes under Article 10 of the Convention

- The operation of a bulk interception regime requires fundamental safeguards for the protection, among others, of confidential journalistic material under Article 10. The Court distinguishes between *intentional* access to such material, for example, through the

[3] See the relevant Key Theme on Administration of (unlawfully obtained) evidence

deliberate use of a strong selector connected to a journalist or where there is a high probability that such material will be selected for examination as a result of such selectors, and *unintentional* access as a "bycatch" of such an operation (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 447-450).

- The Court considers that the deliberate use of selectors (intentional access) would lead to the acquisition of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source. It is for this reason that in this scenario the selectors or search terms used by the intelligence services must have been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 448).
- As to unintentional access, the Court considers that this type of surveillance, although not targeted, has the capacity to have a very wide reach indeed due to recent technological developments. Since the examination of a journalist's communications or related communications data by an analyst would be capable of leading to the identification of a source, it is imperative that domestic law contain robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, if and when it becomes apparent that the communication or related communications data contain confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is "justified by an overriding requirement in the public interest" (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 450).
- Finally, the safeguards identified by the Court for compliance with Article 8 of the bulk interception regime also have a role to play in the Court's analysis of an Article 10 complaint (*Big Brother Watch and Others v. the United Kingdom* [GC], 2021, § 458).

Right to an effective remedy under Article 13 of the Convention

- The secrecy of the measures renders it difficult, if not impossible, for the person concerned to seek any remedy of his own accord, particularly while the surveillance continues. An "effective remedy" under Article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance (*Klass and Others v. Germany*, 1978, §§ 68-69).
- An objective control mechanism may be sufficient as long as the measures remain secret. Once the measures have been divulged remedies must be available to the individual within a reasonable time (*Rotaru v. Romania* [GC], 2000, § 69).
- Surveillance legislation allowing the authorities to control correspondence and to record telephone conversations, even when the adoption and enforcement of the restrictive measures are not subject to appeal to the courts, may fulfil the requirements of Article 13, when certain other remedies are available to anyone who thought they were being watched. In *Klass and Others v. Germany*, 1978, §§ 65-72, the competent authority had to notify the person concerned as soon as the surveillance measures were lifted and various judicial remedies were then available to the individual.
- The storage of information and the refusal to advise the applicants of the full extent to which information on them was being kept may constitute an "arguable claim" under

Article 13 (*Segerstedt-Wiberg and Others v. Sweden*, 2006, §§ 116-122). In the absence of a remedy to challenge the archiving of data on the persons' private life, the Court found a violation of Article 13 in relation to Article 8 (*Rotaru v. Romania* [GC], 2000, §§ 68-73, and *Segerstedt-Wiberg and Others v. Sweden*, 2006, §§ 116-122).

Effectiveness of domestic remedies to be exhausted under Article 35 of the Convention

- Under Article 35 an applicant should normally have recourse to remedies which are available and sufficient to afford redress in respect of the breaches alleged. There is no obligation to have recourse to remedies which are inadequate or ineffective (*Akdivar and Others v. Turkey*, 1996, §§ 66-67).
- Raising the issue of covert surveillance in the criminal proceedings cannot, in principle, be regarded as an effective remedy in respect of a complaint under Article 8 where the domestic criminal courts, although they could consider questions of the fairness of admitting the evidence in the criminal proceedings, could not deal with the substance of the Convention complaint that the interference with the applicants' right to respect for their private life and correspondence was not "in accordance with the law" or not "necessary in a democratic society"; still less was it open to them to grant appropriate relief in connection with the complaint (*Zubkov and Others v. Russia*, 2017, § 88, and *Akhlyustin v. Russia*, 2017, § 24; *Hambardzumyan v. Armenia*, 2019, § 44).
- In a case concerning the transfer of data of British nationals from France to the United Kingdom under a European Investigation Order, the fact that the applicants lived outside France and had not freely chosen to come under its jurisdiction did not exempt them from their duty to exhaust the domestic remedy available in France. A remedy, transposing Article 14 of the Directive 2014/41/EU regarding the European Investigation Order, which could lead to a finding of a breach of Article 8 of the Convention and the exclusion of evidence obtained through the enforcement of the European Investigation Order, was found to be effective (*A.L. and E.J. v. France* (dec.), 2024,§§ 131-145).

Recap of general principles

- *Roman Zakharov v. Russia* [GC], 2015, §§ 227-234;
- *Centrum för rättvisa v. Sweden* [GC], 2021, §§ 166-167, 239-278;
- *Big Brother Watch and Others v. the United Kingdom* [GC], 2021, §§ 325-364, 448-450, 497-499.

KEY CASE-LAW REFERENCES

Leading cases:

- *Klass and Others v. Germany*, 6 September 1978, Series A no. 28 (no violation of Articles 6, 8 and 13);
- *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI (inadmissible under Articles 8, 10 and 13: manifestly ill-founded);
- *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010 (no violation of Articles 8, 6 and 13);
- *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015 (violation of Article 8);
- *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016 (violation of Article 8);
- *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021 (violation of Article 8);
- *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, 25 May 2021 (violation of Articles 8 and 10; no violation of Articles 8 and 10).

Cases under Article 8:

- *Amann v. Switzerland* [GC], no. 27798/95, ECHR 2000-II (violation of Article 8);
- *Allan v. the United Kingdom*, no. 48539/99, ECHR 2002-IX (violation of Article 8);
- *Wisse v. France*, no. 71611/01, 20 December 2005 (violation of Article 8);
- *Heglas v. Czech Republic*, no. 5935/02, 1 March 2007 (violation of Article 8);
- *Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I (violation of Article 8);
- *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008 (violation of Article 8);
- *Uzun v. Germany*, no. 35623/05, ECHR 2010 (extracts) (no violation of Article 8);
- *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, 3 September 2015 (no violation of Article 8);
- *Bărbulescu v. Romania* [GC], no. 61496/08, 5 September 2017 (extracts) (violation of Article 8);
- *Gorlov and Others v. Russia*, nos. 27057/06 and 2 others, 2 July 2019 (violation of Article 8);
- *López Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, 17 October 2019 (no violation of Article 8);
- *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022 (violation of Article 8);
- *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024 (violation of Article 8);
- *Pietrzak and Bychawska-Siniarska and Others v. Poland*, nos. 72038/17 and 25237/18, 28 May 2024 (violation of Article 8);
- *Denysyuk and Others v. Ukraine*, nos. 22790/19 and 3 others, 13 February 2025 (violation of Article 8);
- *Macharik v. the Czech Republic*, no. 51409/19, 13 February 2025 (violation of Article 8);
- *Romanchenko and Kharazishvili v. Georgia*, nos. 33067/22 and 37832/22, 18 February 2025 (violation of Article 8).

Cases under Article 6:

- *Schenk v. Switzerland*, 12 July 1988, Series A no. 140 (no violation of Article 6);

- *Bykov v. Russia* [GC], no. 4378/02, 10 March 2009 (no violation of Article 6);
- *Gäfgen v. Germany* [GC], no. 22978/05, ECHR 2010 (no violation of Article 6);
- *El Haski v. Belgium*, no. 649/08, 25 September 2012 (violation of Article 6);
- *Vukota-Bojić v. Switzerland*, no. 61838/10, 18 October 2016 (no violation of Article 6);
- *Moreira Ferreira v. Portugal (no. 2)* [GC], no. 19867/12, 11 July 2017 (no violation of Article 6);
- *Murtazaliyeva v. Russia* [GC], no. 36658/05, 18 December 2018 (no violation of Article 6);
- *Hambardzumyan v. Armenia*, no. 43478/11, 5 December 2019 (no violation of Article 6);
- *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024 (violation of Article 6);
- *Macharik v. the Czech Republic*, no. 51409/19, 13 February 2025 (no violation of Article 6).

Cases under Articles 13/35 § 1:

- *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V (violation of Article 13);
- *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, ECHR 2006-VII (violation of Article 13);
- *Akhlyustin v. Russia*, no. 21200/05, 7 November 2017 (preliminary objection as to the non-exhaustion of domestic remedies dismissed);
- *A.L. and E.J. v. France* (dec.), nos. 44715/20 and 47930/21, 24 September 2024 (inadmissible – non-exhaustion of domestic remedies).

Cases under Article 35:

- *Akdivar and Others v. Turkey*, 16 September 1996, Reports of Judgments and Decisions 1996-IV (admissible);
- *Zubkov and Others v. Russia*, nos. 29431/05 and 2 others, 7 November 2017 (admissible);
- *Akhlyustin v. Russia*, no. 21200/05, 7 November 2017 (admissible);
- *Hambardzumyan v. Armenia*, no. 43478/11, 5 December 2019 (admissible).