EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Press Release
issued by the Registrar of the Court

ECHR 135 (2024)
28.05.2024

Right to respect for private life of applicants who complained about Polish legislation on secret surveillance: three violations

The case Pietrzak and Bychawska-Siniarska and Others v. Poland (applications nos. 72038/17 and 25237/18) concerned a complaint by five Polish nationals about Polish legislation authorising a secret-surveillance regime covering both operational control[1] and the retention of telecommunications, postal and digital communications data ("communications data") for possible future use by the relevant national authorities. In particular, they alleged that there was no remedy available under domestic law allowing persons who believed that they had been subjected to secret surveillance to complain about that fact and to have its lawfulness reviewed.

In today's **Chamber** judgment[2] in this case the European Court of Human Rights held, unanimously, that there had been **three violations of Article 8 (right to respect for private and family life and correspondence)** of the European Convention on Human Rights in respect of the complaints concerning the operational-control regime, the retention of communications data for potential use by the relevant national authorities, and the secret-surveillance regime under the Anti-Terrorism Act.

Given the secret nature and wide scope of the measures provided for by the Polish legislation and the lack of effective review by which persons who believed that they had been subjected to surveillance could challenge this alleged surveillance, the Court found it appropriate to examine the legislation at issue *in abstracto*. It considered that the applicants could claim to be the victims of a violation of the Convention, and that the mere existence of the relevant legislation constituted in itself an interference with their Article 8 rights.

The Court then held that all the shortcomings identified by it in the operational-control regime led to a conclusion that the national legislation did not provide sufficient safeguards against excessive recourse to surveillance and undue interference with individuals' private life; the absence of such guarantees was not sufficiently counterbalanced by the current mechanism for judicial review. In its view, the national operational-control regime, taken as a whole, did not comply with the requirements of Article 8.

It further considered that the national legislation, under which information and communication technologies ("ICT") providers were required to retain communications data in a general and indiscriminate manner for possible future use by the relevant national authorities, was insufficient to ensure that the interference with the applicants' right to respect for their private life was limited to what was "necessary in a democratic society".

Lastly, the Court concluded that the secret-surveillance provisions in the Anti-Terrorism Act also failed to satisfy the requirements of Article 8 of the Convention, noting, among other points, that neither the imposition of secret surveillance nor its application in the initial three-month period were subject to any review by a body that was independent and did not include employees of the service conducting that surveillance.

---

[1] "*kontrolę operacyjną*" –this term, which refers to secret surveillance, is translated in Article 19 of the official English translation of the Police Act as "operational control".

[2] Under Articles 43 and 44 of the Convention, this Chamber judgment is not final. During the three-month period following its delivery, any party may request that the case be referred to the Grand Chamber of the Court. If such a request is made, a panel of five judges considers whether the case deserves further examination. In that event, the Grand Chamber will hear the case and deliver a final judgment. If the referral request is refused, the Chamber judgment will become final on that day.
Once a judgment becomes final, it is transmitted to the Committee of Ministers of the Council of Europe for supervision of its execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A legal summary of this case will be available in the Court's database HUDOC (link)

Principal facts

In 2016 the Polish Parliament enacted laws amending the Police Act and certain other legislative provisions (the Law of 15 January 2016) and on the prevention of terrorism (the Anti-Terrorism Act). Those laws faced criticism, particularly from civil-society organisations which considered that the new laws, under the guise of implementing a Constitutional Court[3] judgment, strengthened the authorities' surveillance powers in several areas, and were incompatible with certain of Poland's international human-rights obligations.

The applicants in the present case are five Polish nationals who were born between 1973 and 1987. The first applicant is a lawyer and chair of the Warsaw Bar. The other four applicants are employees of, or experts for, non-governmental organisations based in Warsaw.

In 2017 the applicants submitted complaints to the Prime Minister and the respective heads of the various police and intelligence services about certain domestic-law provisions governing secret surveillance. In particular, they criticised the fact that, in their view, the impugned legislation permitted members of the services in question to monitor their telecommunications and to collect data concerning them without their knowledge. Given their professional and public activities, they considered it highly likely that they had been subjected to surveillance. In addition, the employees of the services in question were not required to inform them about any surveillance conducted, even after it had ended, and they argued that this failure to provide information was incompatible with Article 51 of the Constitution and prevented them from having the lawfulness of the surveillance reviewed by a court. They further submitted that the failure to inform individuals that they were being subjected to secret-surveillance measures, coupled with the lack of effective review and the shortcomings in the relevant national legislation, was incompatible with the rule of law in a democracy and infringed their legitimate interests.

The applicants received responses from the respective authorities, including from the relevant departments of the Prime Minister's Office, which informed them that the heads of the various police and intelligence services had provided extensive replies to their questions regarding possible surveillance. They specified that, in carrying out their respective tasks, the State special services had recourse to the secret-surveillance measures provided for by the relevant legislation, and that the methods and means used for that purpose were confidential and protected by the legislation governing the relevant services and the Confidential Data (Protection) Act.

Complaints

Relying on Article 8 (right to respect for private and family life and correspondence) of the Convention and Article 13 (right to an effective remedy), the applicants complained about the secret-surveillance regimes introduced by the Law of 15 January 2016 and the Anti-Terrorism Act, submitting that these interfered with their right to respect for their private life. The applicants alleged that they had no effective remedy enabling them to establish whether they themselves had been subjected to secret surveillance and, if necessary, to have the lawfulness of that surveillance reviewed by a court.

The Court decided to examine their complaints under Article 8 of the Convention.

[3] Judgment no. K 23/11 of 30 July 2014 of the Constitutional Court.

Procedure and composition of the Court

The applications were lodged with the European Court of Human Rights on 29 September 2017 and 12 February 2018.

A hearing took place on 27 September 2022. Several third parties were also given leave to intervene in the written proceedings.

Judgment was given by a Chamber of seven judges, composed as follows:

Marko **Bošnjak** (Slovenia), *President*,
Péter **Paczolay** (Hungary),
Krzysztof **Wojtyczek** (Poland),
Erik **Wennerström** (Sweden),
Raffaele **Sabato** (Italy),
Lorraine **Schembri Orland** (Malta),
Ioannis **Ktistakis** (Greece),

and also Ilse **Freiwirth**, *Section Registrar.*

Decision of the Court

Article 8: the applicants' victim status and the existence of an interference

The Court noted that the national legislation established two separate legal regimes for secret surveillance: the first concerned operational control, and the second concerned the retention and use of communications data.

In the Court's view, the impugned legislation had established a surveillance regime under which practically any telecommunications or internet user could have his or her data intercepted, without ever being informed about this surveillance. With regard to the Anti-Terrorism Act, the Court observed that, while it was applicable only to foreign nationals suspected of terrorist activities, the communications of any person who had been in contact with the latter could be monitored indirectly, irrespective of whether he or she had personally been placed under surveillance. Furthermore, no effective remedy was available under Polish law to persons who believed that they had been subjected to secret surveillance. Consequently, the Court considered that the applicants were not required to prove that they were at risk of secret surveillance on account of their respective personal circumstances.

Given the secret nature and wide scope of the measures provided for by the legislation challenged by the applicants, and the lack of effective review by which persons who believed that they had been subjected to surveillance could challenge this alleged surveillance, the Court found it appropriate to examine the legislation at issue *in abstracto*. Accordingly, it considered that the applicants could claim to be victims of a violation of the Convention, although they could not argue in support of their respective applications that they had been subjected to a specific secret-surveillance measure.

For the same reasons, the Court found that the mere existence of the impugned legislation constituted in itself an interference with their rights under Article 8 of the Convention.

Article 8: justification for the interference

The operational-control regime: The Court noted that in Poland, operational-control measures were governed by a series of laws which included the National Police (Regulation) Act and legislation governing various other State special services. These measures pursued the legitimate aims of, *inter*

alia, preventing crime, and protecting national security, public safety and the economic well-being of the country.

The Court considered, however, that the operational-control regime as it currently stood in Poland did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any secret-surveillance regime. Specifically, the scope both *ratione materiae* and *ratione personae* of the legislation on the surveillance in question was not delimited with sufficient precision, the overall duration of application of the surveillance was open to debate and the rules on factual justification for the surveillance were not sufficiently substantiated. While, at first sight, there was a judicial-review mechanism in place for the impugned surveillance regime, the Court was not convinced that the authorisation procedure, as applied in practice, was capable of ensuring that surveillance was used only where that measure was "necessary in a democratic society". In that connection, it observed, in particular, that the applicable legislation did not require the court deciding on a request for authorisation of surveillance to confirm whether there was a "reasonable suspicion" in respect of the person targeted and, in particular, to investigate whether there was any evidence that this person was planning, carrying out or had carried out criminal acts or any other offence permitting secret-surveillance measures, such as acts endangering national security. The Court considered that the existing authorisation procedure should be supplemented by other post factum procedural review mechanisms; for example, where the surveillance had not led to criminal proceedings, a remedy available to persons who were concerned that they had been subjected to surveillance, with the possibility of seeking judicial review and a separate review by an independent body. It noted that, as matters stood, the law did not appear to contain appropriate provisions in that regard; nor did it provide for an obligation to inform a person targeted by a surveillance measure, even after a certain period of time had elapsed and even where this would not compromise the aim of the measure. Lastly, the Court considered that the impugned legislation did not provide sufficient safeguards as concerned communications covered by legal professional privilege. All of these shortcomings led the Court to find that the national operational-control regime, taken as a whole, did not satisfy the requirements of Article 8 of the Convention.

The retention of communications data for possible future use by the relevant national authorities: the Court considered that the interference with the applicants' right to respect for their private life arising from the requirement on ICT providers to retain their communications data was very serious and could, with good reason, generate in the minds of the persons concerned a feeling of vulnerability and of being over-exposed to third-party scrutiny. The applicable legislation required ICT providers to retain, in a general and indiscriminate manner, the telecommunications, postal and digital communications data of all users of communications services without them ever being informed, and it had an impact even on persons who were not, even indirectly, in a situation that was liable to give rise to criminal proceedings. The data thus retained for a 12-month period were made available to the relevant police and intelligence services, which were able to access them at any time and without any intervention on the part of the telecommunications operators, and to use them for any purpose in the fulfilment of their respective statutory tasks. The Court, having regard to the seriousness of this interference with the applicants' Article 8 rights, found that the failure in the applicable legislation to provide minimum safeguards against possible abuse on the part of State services using this type of surveillance rendered the surveillance regime in question incompatible with this Convention provision.

The Court also considered that the relevant national bodies' access to the data made available to them by ICT providers as described above constituted a further interference with the applicants' Article 8 rights. Although some safeguards against possible abuse existed in respect of this access, including a mechanism for retrospective judicial review, these were not sufficient to bring the applicable regime into conformity with the requirements of Article 8. Where a regime for retaining communications data was incompatible with Article 8, access to the data in question, their retention and their potential use by the authorities could not, for the same reason, be compatible with that

Convention provision. In that connection, the Court referred to the judgment by the Court of Justice of the European Union in *Commissioner of An Garda Síochána e.a.*[4] and stated that it saw no reason to depart from the findings of the highest EU court.

The Court concluded that the national legislation, under which ICT providers were required to retain communications data in a general and indiscriminate manner for possible future use by the relevant national authorities, was not sufficient to ensure that the interference with the applicants' right to respect for their private life was limited to what was "necessary in a democratic society".

The secret-surveillance regime under the Anti-Terrorism Act: the Court observed that while in principle the Anti-Terrorism Act could be applied only to foreign nationals, in practice its scope was much wider, in that it permitted employees of the National Security Agency[5] ("ABW") to monitor indirectly the communications of any person who had been in contact with persons targeted by surveillance, irrespective of whether he or she had personally been placed under surveillance.

Furthermore, it observed that ABW employees conducted secret surveillance on the basis of a decision of the head of the ABW, who was subject to supervision by the Prosecutor General and the Minister for State Special Services. Therefore, neither the imposition of a secret-surveillance measure nor its application in the initial three-month period was subject to any authorisation or review by an independent body that did not include employees of the ABW conducting the surveillance, and which would be capable of restricting their discretion in interpreting the general wording used in the Anti-Terrorism Act and ensuring that there were sufficient grounds in each case to intercept a person's communications. Judicial intervention was provided for only in the event of a subsequent extension of secret-surveillance measures at the end of the initial three-month period.

Consequently, the Court considered that the fact that the secret-surveillance measures were authorised by the head of the ABW – to whom the employees of the service conducting them were subordinate– and that any subsequent review of the application of those measures was carried out by a member of the executive with political responsibilities and by a member of the public prosecutor's office who did not offer adequate guarantees of independence from the executive, did not provide the necessary safeguards against abuse, especially since persons subjected to surveillance were never informed of this fact and had no effective means of challenging its lawfulness. The Court also noted that the Prosecutor General had power to order the destruction of data which were not relevant. However, since the current Prosecutor General was also the Minister of Justice, the Court considered that the Prosecutor General's independence and impartiality were not sufficiently guaranteed. It followed that the secret-surveillance provisions in the Anti-Terrorism Act also failed to satisfy the requirements of Article 8 of the Convention.

Article 13

Having regard to its findings under Article 8 of the Convention, the Court considered that it was not necessary to examine the complaint under Article 13 separately.

Just satisfaction (Article 41)

The applicants did not submit a claim for damages, stating that the finding of a violation would constitute in itself sufficient redress. The Court therefore considered that no award in respect of pecuniary or non-pecuniary damage should be made. It held, however, that Poland was to pay three of the applicants the following amounts in respect of costs and expenses: 2,602.92 euros (EUR), EUR 252.58 and EUR 300.

---

[4] Judgment of the European Court of Justice of 5 April 2022 in *Commissioner of An Garda Síochána e.a*, C-140/20, EU:C:2022:258.

[5] *Agencja Bezpieczeństwa Wewnętrznego*.

The judgment is available only in French.

Press contacts
echrpress@echr.coe.int | tel.: +33 3 90 21 42 08

We are happy to receive journalists' enquiries via either email or telephone.

Inci Ertekin (tel.: + 33 3 90 21 55 30)
Tracey Turner-Tretz (tel.: + 33 3 88 41 35 30)
Denis Lambert (tel.: + 33 3 90 21 41 09)
Neil Connolly (tel.: + 33 3 90 21 48 05)
Jane Swift (tel.: + 33 3 88 41 29 04)