dirittifondamentali.it

La Corte EDU su un caso di perquisizione domiciliare
(CEDU sez. V, sent. 24 ottobre 2024, ric. n. 67101/17)

Il caso sul quale si è pronunciata la Corte EDU ha riguardato le doglianze del ricorrente ai sensi dell'articolo 8 della Convenzione, in merito al sequestro e alla detenzione del suo computer nel corso di un procedimento penale. In breve, la Guardia di finanzia lettone aveva ricevuto informazioni su transazioni finanziarie sospette che coinvolgevano due società alle quali la società del ricorrente forniva servizi di contabilità. In ragione di ciò, era stato emesso un mandato di perquisizione presso l'abitazione della ricorrente, in cui la stessa esercitava anche la sua attività professionale. All'esito della perquisizione veniva sequestrato un computer per la decriptazione dei dati in esso contenuti. La Corte di Strasburgo, ritenuto ammissibile il ricorso, ha ricordato i principi riguardanti la liceità delle perquisizioni e dei sequestri effettuati presso l'abitazione o il luogo di attività professionale di un individuo, sottolineando come costituiscano un'ingerenza nel diritto di un individuo alla vita privata protetto appunto dall'articolo 8 della Convenzione. Tale ingerenza è ammissibile solo se è "conforme alla legge", persegue uno scopo legittimo e non va oltre quanto è necessario in una società democratica. Ora, nella specie, pur non potendo valutare la natura dei dati memorizzati nel computer, i Giudici hanno ritenuto che la privazione di accesso al pc ha avuto un impatto sugli aspetti personali e professionali del ricorrente. E, pur concordando sul fatto che potrebbe non essere sempre praticabile effettuare un'ispezione e un esame di un computer durante una perquisizione, la Corte EDU ha osservato che la denunciata impossibilità di decifrare i dati da parte degli esperti non giustifica la detenzione del dispositivo per una durata complessiva superiore a quindici mesi, ritenendo tale misura sproporzionata. Alla luce di tali considerazioni, la Corte ha concluso che vi è stata violazione dell'articolo 8 della Convenzione.

***

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

FIFTH SECTION

CASE OF Omissis v. LATVIA
(Application no. 67101/17)

JUDGMENT
STRASBOURG
24 October 2024

This judgment is final but it may be subject to editorial revision.

In the case of Omissis. v. Latvia,
The European Court of Human Rights (Fifth Section), sitting as a Committee composed of:
Stéphanie Mourou-Vikström, *President*,
María Elósegui,
Artūrs Kučs, *judges*,
and Martina Keller, *Deputy Section Registrar*,
Having regard to:
the application (no. 67101/17) against the Republic of Latvia lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") on 7 September 2017 by a Latvian national, N.B. ("the applicant"), who was born in 1975 and lives in Riga;
the decision to give notice of the application to the Latvian Government ("the Government"), represented by their former Agent, Ms XXX, and subsequently by their current Agent, Ms XXX,
the decision not to have the applicant's name disclosed;
the parties' observations;
the decision to dismiss the Government's objection to the examination of the application by a Committee;
Having deliberated in private on 3 October 2024,
Delivers the following judgment, which was adopted on that date:

SUBJECT MATTER OF THE CASE

1. The case concerns the applicant's complaints under Article 8 of the Convention about the seizure and retention of her computer in the course of criminal proceedings.

2. In September 2016 the Finance Police (*Valsts ieņēmumu dienesta Finanšu policijas pārvalde*) received information about suspicious financial transactions involving two companies to which the applicant's company provided accounting services ("the client companies"). The client companies were registered in Latvia but their registered owners and board members were foreign nationals. When interviewed by the Finance Police about one of the client companies, the applicant stated that, apart from the company's board member, she was its only authorised representative and that she had already submitted all the relevant documents that were in her possession to the Finance Police.

3. On 7 October 2016 the Finance Police instituted criminal proceedings in relation to a suspicion of large-scale tax evasion. On 12 December 2016 an investigating judge issued a search warrant for the applicant's home, from which she also conducted her professional activity. The warrant was issued with a view to

"find[ing] and seiz[ing] registration, transaction, accounting, banking and authorisation documents, payment cards, internet banking code cards and security tokens, rubber stamps, electronic storage devices and cash belonging to [the client companies] and other companies involved in the chain of suspicious financial transactions, and other documents and items that might have evidential value in criminal proceedings no. ...".

4. On 13 February 2017 an officer and an expert from the Finance Police conducted the search and seized several documents and the applicant's computer. When the expert from the Finance Police inspected the computer, he found that it was password protected and that the data stored on it were encrypted. On the same day the applicant was questioned as a witness.

5. The applicant challenged the lawfulness of the search warrant. By a decision of 10 March 2017, the Riga Regional Court found that the search warrant had been lawful. That decision was not subject to appeal.

6. At the same time, the applicant complained to the investigator, the head of the Finance Police, the supervising prosecutor, and then to higher-ranking prosecutors about the seizure of her computer and requested its return. Those domestic authorities rejected the applicant's requests, finding that the seizure of the computer had been lawful. The supervising prosecutor informed the applicant that her computer would be returned to her after it had been examined and that her refusal to provide the computer's password was hindering that process. On 17 March 2017, after dismissing one of the applicant's complaints, the supervising prosecutor instructed the Finance Police to take an immediate decision to carry out a forensic examination of the applicant's computer and a subsequent decision on returning it to the applicant.

7. The investigator contacted forensic experts by email, stating his intention to order an official forensic examination and enquiring whether it would be possible to access the encrypted data stored on the applicant's computer. On 28 March 2017 a State Police forensic expert replied by email that an examination of the computer without decrypting the data first would not yield useful results and that the State Police experts did not have the hardware necessary to create a mirror copy of the computer's hard drive. In an email of 5 April 2017, a forensic expert from the State Forensic Science Bureau informed the investigator that decryption of the data without the computer's password could take years and that the outcome of that process was unpredictable. On 12 May 2017 the Finance Police created a mirror copy of the computer's hard drive and added it to the criminal case file.

8. On 16 August 2017 the investigator ordered the State Forensic Science Bureau to carry out a digital forensic examination of the applicant's computer. On 24 January 2018 a forensic expert drafted a report in which he concluded that without the computer's password and without access to specialised hardware the data stored on the computer could not be accessed within a reasonable time.

9. The applicant again requested that the investigator return her computer. The investigator rejected her request. The applicant then complained to the supervising prosecutor, who also rejected her request and stated that the computer was subject to ongoing procedural activities which were being performed without undue delay and had been prolonged by her refusal to disclose the computer's password. The applicant subsequently complained to a higher-ranking prosecutor, who on 2 May 2018 took the decision to order the investigator to re-examine the applicant's request. The computer was returned to the applicant on 29 May 2018.

10. According to the latest available information, the criminal proceedings were suspended on 3 November 2020 because the person responsible for the alleged criminal offences could not be identified.

THE COURT'S ASSESSMENT

ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

11. The applicant complained under Article 8 of the Convention about the seizure and retention of her computer.

A. Admissibility

12. The Government put forward two arguments as to the admissibility of the applicant's complaint. They argued that the applicant had complained about State institutions having had access to her personal data and not about the seizure and retention of her computer as such. Since the data stored on the computer had not been accessed, the applicant could not claim to be a victim of a violation of Article 8. In their additional observations, the Government submitted that the arguments concerning the retention of the computer had been submitted by the applicant only after notice of the application had been given to the Government. Accordingly, she had lodged a new complaint which the Court was precluded from examining. Alternatively, the Government contended that the applicant had not suffered a significant disadvantage because the information stored on her computer had not been accessed and the search and seizure had been lawful. The applicant contested those arguments.

13. The Court finds that the applicant explicitly complained in her application form about the seizure and retention of her computer. Accordingly, when it gave notice of the case to the Government, the Court asked for observations regarding, among other things, the proportionality of the retention of the computer. Having regard to the circumstances of the present case (see paragraphs 4 and 9 above), the Court considers that the applicant can claim to be a victim of a potential violation of Article 8 on account of the seizure and retention of her computer. In view of the duration of that retention, the applicant cannot be said to have suffered no significant disadvantage within the meaning of Article 35 § 3 (b) of the Convention.

14. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention or inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

15. The general principles concerning the lawfulness of searches and seizures carried out at an individual's home or place of professional activity have been summarised in *Vinks and Ribicka v. Latvia* (no. 28926/10, §§ 101-04, 30 January 2020), *Buck v. Germany*, (no. 41604/98, §§ 44-45, ECHR 2005-IV) and *Smirnov v. Russia*, (no. 71362/01, §§ 43-44, 7 June 2007). It is well-established case-law that searches and seizures constitute an interference with an individual's right to private life protected by Article 8 of the Convention. Such interference is permissible only if it is "in accordance with the law", in pursuit of a legitimate aim and does not go beyond what is necessary in a democratic society.

16. The Court cannot speculate on the nature of the data stored on the applicant's computer. However, there is no doubt that she was deprived of access to her computer for more than fifteen months. Regardless of whether the data were personal or work-related, such deprivation of access had an impact on either the personal or the professional aspects of the applicant's private life, or on both. Therefore, the seizure and retention of the applicant's computer amounted to an

interference with her right to private life. The parties agreed that the interference had been "in accordance with the law" and in pursuit of a legitimate aim. However, they disagreed as to its necessity.

17. Given the nature of the particular criminal offence and the applicant's connection to the implicated client company (see paragraph 2 above), the Court considers that the search warrant was issued on the basis of a reasonable suspicion that items or documents with evidential value might be in the applicant's possession.

18. As to the scope of the search warrant, which the applicant considered to be overly broad, the Court notes that the warrant was indeed open-ended as to the kinds of items to be seized (see paragraph 3 above). However, the requirement that any items seized had to relate to the companies involved in the suspicious financial transactions and had to be of evidential value in the criminal proceedings sufficiently limited the scope of the search warrant. It is true that the wording referred to items "belonging" to the companies specified and did not explicitly refer to computers as items to be seized. Nevertheless, the Court considers that it is clear from the search warrant, when viewed as a whole, that its purpose was to find and seize items which could provide information about the suspicious financial transactions in question and the companies involved. A computer is an electronic device capable of storing electronic documents. Given the applicant's connection to the client companies, the data stored on her computer could have been relevant to the investigation. Having regard to the fact that the search warrant specifically referred to electronic storage devices, the Court finds that the applicant's computer was covered by the search warrant.

19. As to the retention of the applicant's computer, the Court agrees that it might not always be practicable to perform an inspection and an examination of a computer during a search and thus it may be necessary to seize it. However, the Government only put forward general statements regarding possible difficulties which might be encountered when inspecting or examining a computer and did not explain how those statements applied to the present case or why it was necessary to retain the applicant's computer for more than fifteen months. In addition, the Government did not provide an explanation as to why there were some periods when the investigating authorities were inactive during this time (see paragraphs 6-9 above). In this connection, the Court notes, in particular, that after forensic experts had informed the investigator that decrypting the data stored on the computer would be impracticable, the investigator still went on to hold the computer for more than four months before ordering an official forensic examination, only for an expert to reaffirm that the data could not be accessed within a reasonable time (see paragraphs 7 and 8 above). In these circumstances, the Court finds no justification for the retention of the applicant's computer for a total duration of more than fifteen months and considers that measure to have been disproportionate.

20. These findings in themselves are sufficient for the Court to conclude that there has been a violation of Article 8 of the Convention. It is therefore unnecessary for the Court to address the rest of the arguments put forward by the parties.

APPLICATION OF ARTICLE 41 OF THE CONVENTION

21. The applicant claimed 10,000 euros (EUR) in respect of non-pecuniary damage and EUR 28.04 in respect of costs and expenses incurred before the Court.

22. The Government contested the claim in respect of non-pecuniary damage but did not contest the claim in respect of costs and expenses.

23. The Court, ruling on an equitable basis, awards the applicant EUR 4,000 in respect of non-pecuniary damage, plus any tax that may be chargeable.

24. Having regard to the documents in its possession, the Court considers it reasonable to award the applicant EUR 28,04 covering costs for the proceedings before the Court, plus any tax that may be chargeable to the applicant.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;
2. *Holds* that there has been a violation of Article 8 of the Convention;
3. *Holds*

(a) that the respondent State is to pay the applicant, within three months, the following amounts:

(i) EUR 4,000 (four thousand euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;

(ii) EUR 28.04 (twenty-eight euros and four cents), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 24 October 2024, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Martina Keller	Stéphanie Mourou-Vikström
Deputy Registrar	President