

# Overview 2024: Case Law of the European Court of Human Rights

*Bart van der Sloot\**

In 2024, the European Court of Human Rights (ECtHR) issued 196 judgments on Article 8 ECHR. 78 of those, meaning about two-fifth, were issues against Russia, which is no longer part of the Convention-mechanism, but on which the Court has a backlog of applications that were submitted before Russia ceased to be a member. Most of these cases are what could be called mini-judgments, that is, judgments in which often dozens of applicants with the same type of complaint are bundled per case, in which their names and complaints are included as an appendix to the judgment, and of which the operative part merely holds that, referring to established case law, Russia violated the Convention.<sup>1</sup>

Other substantial categories in 2024 were cases in which a country indiscriminately or without a legal basis monitored the correspondence of prisoners, for example with their lawyer; cases in which an immigrant was expelled, refused a residence permit or put under a re-entry ban, in which the ECtHR meticulously deals with the circumstances of the individual case, in particular how existing family relations would be affected by the decision by the Member State; cases in which applicants claim that the state had violated its positive obligation to ensure contact of a divorced parent with their child; cases in which people were evicted from their home or in which their homes and business premises were searched and their documents seized; and cases concerning the positive obligation of Member States to protect citizens against physical and psychological harm by third parties and to provide effective legal remedies in case of rape or physical assault. The Court has made clear that such a positive obligation may extend to the publication of revenge porn.<sup>2</sup>

The most consequential judgments issued by the Court on Article 8 ECHR do not revolve around informational privacy, but are still worth mentioning briefly. There is, according to the Court, a positive obligation on states to have in place an adequate legal regime to combat climate change.<sup>3</sup> CIA secret interrogation sites, in which suspects of terrorism, often with neither a European nor an American passport, are interrogated in a way violating many Con-

vention rights, will lead to a violation of the Convention by the European country on whose soil the stie is based, if they could or should have known about its existence.<sup>4</sup> There are inter-state complains by Ukraine and Georgia on the Russian occupation of disputed territory,<sup>5</sup> Russia's fight against what it calls 'foreign agents'<sup>6</sup> and the reliance on the state of emergency by Turkey to violate human rights, including the diplomatic immunity and special protection of diplomats' premises, cars and possessions.<sup>7</sup> Finally, there are several cases in which the Member State invokes the protection of 'health and morals', such as when imposing mandatory Covid-vaccinations<sup>8</sup> or a ban on paying for sexual acts,<sup>9</sup> when it concerns the recognition of children conceived abroad through medically assisted procreation<sup>10</sup> or the obligation to continue hormone therapy for an imprisoned transgender person,<sup>11</sup> and cases regarding the possibility for a terminally ill person to seek assisted dying or euthanasia<sup>12</sup> or the admission of blood to a patient against their will (for example expressed through an advanced directive).<sup>13</sup>

DOI: 10.21552/edpl/2025/3/16

\* Dr Bart van der Sloot, Associate Professor, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands.

1 See eg, <<https://hudoc.echr.coe.int/eng?i=001-229969>>. All internet links in this overview were last accessed 22 October 2025.

2 <<https://hudoc.echr.coe.int/eng?i=001-238271>>.

3 <<https://hudoc.echr.coe.int/eng?i=001-233206>>.

4 <<https://hudoc.echr.coe.int/eng?i=001-230250>>.

5 <<https://hudoc.echr.coe.int/eng?i=001-232000>>; <<https://hudoc.echr.coe.int/eng?i=001-235139>>; see also <<https://hudoc.echr.coe.int/eng?i=001-238515>>.

6 <<https://hudoc.echr.coe.int/eng?i=001-237425>>.

7 <<https://hudoc.echr.coe.int/eng?i=001-233214>>.

8 <<https://hudoc.echr.coe.int/eng?i=001-235475>>.

9 <<https://hudoc.echr.coe.int/eng?i=001-235143>>.

10 <<https://hudoc.echr.coe.int/eng?i=001-237948>>.

11 <<https://hudoc.echr.coe.int/eng?i=001-234807>>.

12 <<https://hudoc.echr.coe.int/eng?i=001-234151>>.

13 <<https://hudoc.echr.coe.int/eng?i=001-237795>>; <<https://hudoc.echr.coe.int/eng?i=001-236065>>.

The cases that are relevant in light of informational privacy and data protection can roughly be divided into four groups.

First, there are cases in which the reputation of the applicant has been affected by a publication in the media or on the internet, and the Court is faced with a conflict between the freedom of expression on the one hand and the right to privacy, which includes the protection of a person's reputation, honour and name, on the other hand.

- The case of *Oleg Balan v Moldova*<sup>14</sup> dealt with the distribution of fake news. The Court emphasized that the internet has become one of the principal means by which individuals exercise their right to freedom of expression, but that serving billions of users worldwide, internet publications are accompanied by a certain number of risks. Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated as never before, worldwide, in a matter of seconds, and sometimes remain available online for lengthy periods. It observed that in these cases, a Facebook user did not simply publish a Note with alleged information about the applicant, but captioned his Facebook post 'Received an interesting document in the post. Again our Timofte knew everything and kept silent about it'. Instead of warning the readers of his Facebook page about the unknown source and the doubts concerning the authenticity of the document, he presented it as being indisputably genuine. As the Court saw no evidence that the allegations were genuine, it finds a violation of Article 8 ECHR.
- In *Ungur v Romania*, the applicant, who was a well-known businessman and philanthropist in his town, filed a criminal complaint against the manager of an online publication, in which he accused her of blackmail. The Court notes that the freedom of expression carries with it 'duties and responsibilities' that also apply to the media, and that none of the arguments proved in any meaningful manner the allegation that the applicant attempted to bribe the authorities. Moreover, the applicant was not granted the opportunity to comment nor was

he afforded right to reply, which has the ECtHR conclude that there had been a violation of Article 8 ECHR.<sup>15</sup>

- *Kajganić v Serbia*<sup>16</sup> concerned the allegation by the applicant that the domestic authorities had failed to protect her right to reputation against defamatory statements made by a journalist, who alleged that the applicant, who is a lawyer, had arranged for her client to be granted the status of a cooperating witness in criminal proceedings relating to the assassination of the Prime Minister, in exchange for giving false testimony. The Court found no violation of Article 8 ECHR, because the domestic courts had adequately dealt with all circumstances of the case.
- In *Mursaliyev v Azerbaijan*,<sup>17</sup> the applicant complained before the domestic courts that another person had accused him of committing a serious crime against his own uncle in the statements made in his interview with the newspaper in question. The domestic courts, however, dismissed his complaints, holding mainly that the statements in question were not defamatory and that since the investigation concerning the disappearance of his uncle was ongoing, it was impossible to establish whether the statements were true or not. The ECtHR finds a violation because the domestic courts did not adequately balance the right to privacy and the right to freedom of expression.
- Finally, in *Daneş and Others v Romania*, a website published an article in which the author argued that the applicants' actions seemingly prioritised the interests of pharmaceutical companies over public health imperatives and raised concerns that overturning the directive could result in the unregulated circulation of antibiotics and antiparasitic agents, a scenario at odds with prevailing European standards. Additionally, the author ventured into potential corrupt practices, questioning whether the applicants had been motivated by pecuniary incentives. The domestic authorities dismissed the applicants' action. The ECtHR finds that the language employed by the journalist, albeit occasionally harsh, did not transgress the boundaries of acceptable journalistic exaggeration and provocation. In addition, the approach adopted by him in articulating suspicions concerning potential corrupt activities is such that it cannot be construed as a categorical accusation against the two applicants. The author merely ex-

14 <<https://hudoc.echr.coe.int/eng?i=001-233631>>.

15 <<https://hudoc.echr.coe.int/eng?i=001-231542>>.

16 <<https://hudoc.echr.coe.int/eng?i=001-236135>>.

17 <<https://hudoc.echr.coe.int/eng?i=001-231742>>.

pressed a viewpoint that their actions might reasonably prompt inquiries into the possibility of corruption being a factor. There is consequently no violation of Article 8 ECHR on this point. However, the Court also notes that the journalist articulated an explicit accusation of corrupt activities specifically targeting one of the applicants. Special grounds are required before the media can be dispensed from their ordinary obligation to verify factual statements that are defamatory of private individuals. As the regional court did not adequately assess the veracity of the statements and whether the journalist had respected its duties, the ECtHR finds a violation on this point.<sup>18</sup>

Then there are cases in which the employer or an organisation processes personal data about their employees or members, and one in which the applicant was an alleged customer:

- In *Papalea v Romania*,<sup>19</sup> the applicant exchanged electronic messages with female correspondents on a casual dating site, sent from an email account belonging to the employer. Because the domestic courts erred by finding that the interception of these messages by the employer did not fall under the scope of the right to privacy, they did not handle the case adequately. Hence, the Court finds a violation.
- In *Pinchuk v Ukraine*,<sup>20</sup> the applicant complained that his employer had collected his medical information, while he had duly notified his employer of his absence on health grounds and had promptly and duly provided official sick-leave certificates. In this context the Court did not accept the Government's argument that general legal provisions on the recruitment of police officers and the functioning of medical fitness commissions provided the legal basis for the applicant's superior to make direct and specific enquiries to the hospitals seeking detailed information on his treatment and diagnosis.
- In *Tena Arregui v Spain*, a political party hired a private investigator to intercept private communications and scrutinize private information, inter alia to uncover applicant's secret contacts with an opposing political party. That information was subsequently leaked to the press. No violation of Article 8 ECHR was found by the ECtHR, because political parties have considerable freedom in assessing the conduct of their members.<sup>21</sup>

- Finally, in *Vlaisavljevikj v North Macedonia*,<sup>22</sup> the applicant complained of the failure of the domestic authorities to protect the applicant from the unlawful collection and use of his personal data by a private heat supplier, which repeatedly sent him invoices for a standing heating charge despite the applicant's objections that he was not a user of the supplier's services. When deciding on the applicant's data protection complaint, the domestic courts never actually examined the core of the applicant's claim because of the lack of a comprehensive examination of the question whether, in the absence of a contractual or any other legal relationship between the applicant and the heat supplier, the continued retention and use of the applicant's data corresponded to that legitimate aim. That is why the Court found a violation of Article 8 ECHR.

Thirdly, there are cases in which the government collects and retains private information about citizens. In these types of cases, the Court increasingly relies on its 'quality of law' doctrine, meaning that the legal regime of Member States must be such that data collection is limited to what is necessary and that there are adequate safeguards, checks and balances and supervision by independent bodies in place.<sup>23</sup>

- In *Borislav Tonchev v Bulgaria*,<sup>24</sup> the Court found a violation of the right to privacy referring to its quality of law doctrine, because there was uncertainty over the question whether data on the applicant's administrative penalty had been retained or not.
- In *Neziric v Bosnia and Herzegovina*,<sup>25</sup> the Court found a violation of Article 8 ECHR because a legal professional's phone was seized and examined without appropriate safeguards being applicable.
- In *Škoberne v Slovenia*<sup>26</sup> the Court found that the domestic law required the retention for a period

18 <<https://hudoc.echr.coe.int/eng?i=001-230711>>.

19 <<https://hudoc.echr.coe.int/eng?i=001-233110>>.

20 <<https://hudoc.echr.coe.int/eng?i=001-235607>>.

21 <<https://hudoc.echr.coe.int/eng?i=001-229933>>.

22 <<https://hudoc.echr.coe.int/eng?i=001-234420>>.

23 <<https://hudoc.echr.coe.int/eng?i=001-233832>>; <<https://hudoc.echr.coe.int/eng?i=001-233733>>.

24 <<https://hudoc.echr.coe.int/eng?i=001-233106>>.

25 <<https://hudoc.echr.coe.int/eng?i=001-237816>>.

26 <<https://hudoc.echr.coe.int/eng?i=001-230885>>.

- of fourteen months of all communications data generated or processed during the provision of related public communications services, while national law should, as part of the minimum requirements of law, in a manner suitable to the particular form of surveillance, define the scope of application of the measure in question and provide appropriate procedures for ordering and/or reviewing it with a view to keeping it within the bounds of what is necessary. The absence of provisions or mechanisms aimed at ensuring that the measure was actually limited to what was ‘necessary in a democratic society’ rendered such a regime irreconcilable with the State’s obligations under Article 8. The mere limitation of the retention to fourteen months, which is a considerable period, cannot undermine this conclusion, the ECtHR found.
- The case of *Grande Oriente D’Italia v Italy*<sup>27</sup> is important because the Court allows a legal person, a Freemason lodge, to invoke Article 8 ECHR in relation to the processing of personal data of its members, something the Court rarely does as it prefers natural persons to submit an application on their own behalf. The Court found a violation of the right to privacy because there was no reasonable suspicion against the members.
  - In *Bersheda and Rybolovlev v Monaco*,<sup>28</sup> an applicant complained about the massive, indiscriminate, disproportionate collection, without respect for lawyers’ professional secrecy, of all the data accessible from the applicant’s mobile phone, including those that had previously been deleted, and their exploitation. The Court found that in addition to insufficiency in limiting the scope of the investigation, there was also the lack of control over the procedural guarantees due to the applicant by virtue of her status as a lawyer and respect for her professional confidentiality. Consequently, it found a violation of Article 8 ECHR.
  - In *Mukhtarli v Azerbaijan*,<sup>29</sup> the applicant complained that the search of the contents of his mobile telephone. The Court noted that the absence
- of a prior judicial warrant may be counterbalanced by the availability of an *ex post factum* judicial review of both the lawfulness and necessity of the measure in question. In particular, a review by domestic courts of a measure shall provide an appropriate remedy for the person concerned, provided that the judge effectively reviews the lawfulness of and justification for the contested measure and, where appropriate, excludes from the criminal proceedings the evidence collected. However, in the present case there was no review of the investigating authorities’ actions by the domestic courts, which refused to examine the applicant’s complaint concerning the lawfulness and necessity of the search of the contents of his mobile telephone.
- *Klaudia Csikós v Hungary*<sup>30</sup> concerned the tapping of the applicant’s telephone calls with a close acquaintance, apparently with the view of revealing her journalistic sources. Hungarian law contains no provision providing for any form of notification of secret surveillance measures, not even in cases in which notification could be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure. Also, the applicant did not have access to an independent and impartial body with jurisdiction to examine any complaint of unlawful interception, independently of a notification that such interception had taken place. Consequently, a violation of the Convention is found.
  - There are several cases on Russia’s undermining of end-to-end encryption by internet service providers,<sup>31</sup> of which the judgment in *Podchasov* stands out.<sup>32</sup> In that matter, the applicant complained about the statutory requirement for internet service providers to store the content of all Internet communications and related communications data, and to submit those data to law-enforcement authorities or security services at their request together with information necessary to decrypt electronic messages if they were encrypted. The Court concluded that the continuous storage of the applicant’s Internet communications and related communications data by Telegram, the authorities’ potential access to these data and Telegram’s obligation to decrypt them if they are encrypted, pursuant to the Information Act and its implementing regulations, amounted to an interference with the applicant’s Article 8 rights. The

27 <<https://hudoc.echr.coe.int/eng?i=001-238566>>.

28 <<https://hudoc.echr.coe.int/eng?i=001-234090>>.

29 <<https://hudoc.echr.coe.int/eng?i=001-235491>>.

30 <<https://hudoc.echr.coe.int/eng?i=001-238107>>.

31 See eg, <<https://hudoc.echr.coe.int/eng?i=001-235490>>.

32 <<https://hudoc.echr.coe.int/eng?i=001-230854>>.

Court was struck by the extremely broad duty of retention provided by the contested legislation and concluded that the interference was exceptionally wide-ranging and serious. Moreover, weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications.

- Finally, the case of *WA Baile v Switzerland*<sup>33</sup> does not have a direct data protection angle, but is important in light of ongoing discussions about racial profiling. In that matter, the applicant claims that the identity check to which he was subjected, the search he underwent and the fine imposed on him amount to discrimination based on the colour of his skin. The ECtHR does not deal in substance with the matter, but finds a violation of Articles 8 and 14 ECHR because the domestic authorities did not appropriately deal with the complaint.

A final category is cases in which the government published or disseminated private information about citizens.

- In *OG and Others v Greece*,<sup>34</sup> prostitutes were taken off the streets, subjected to HIV-tests and the results of these tests were made public. The Court found a violation because the testing had no appropriate legal basis and because the publication of sensitive information was disproportionate, and reasonable alternatives to protecting public health were available.
- In the case of *AP v Armenia*,<sup>35</sup> the applicant complained of the publication of information on Datalex (including her full name and address) concerning her civil claim for damages. The Court notes that the domestic courts did not take a decision on the request whereby the applicant – a particularly vulnerable minor due to her disability who had fallen victim of a serious sexual crime – had requested that her civil claim linked to the crime at issue be examined *in camera*. Given such circumstances, even though the impugned publication did not explicitly state that the applicant had been subjected to sexual abuse, it would be difficult to argue that, given all those details of the applicant's claim that it did contain, one could not

have been able to at least form the general idea that the applicant (a minor with a disability) had been subjected to some kind of ill-treatment. The Court thus finds a Convention violation.

- *Craco v Italy*<sup>36</sup> concerns the publication of the unredacted version of a judgment containing detailed references to the applicant's medical conditions on the Internet. The Court takes note that, under domestic law, the publication of health data in judgments and decisions made available to the public amounts to an unlawful interference in private life and thus finds a violation.
- In *Kaczmarek v Poland*,<sup>37</sup> the applicant complained that her personal data which had been gathered in the covert surveillance operation had been made public during a press conference. The Court finds that the lack of sufficient clarity in the legal framework at the time of the events and the absence of procedural guarantees relating specifically to the destruction of the applicant's communications mean that the interference with the applicant's rights was not 'in accordance with the law'.
- Finally, in *SVM v Ukraine*,<sup>38</sup> the Court deals with a right to be forgotten case of sorts. The applicant argued that the extract from the police register issued to him by the police had arbitrarily and unnecessarily disclosed sensitive information concerning his expunged criminal conviction. The Court finds that this interference had no proper legal basis and that moreover, and that the disclosure of information in the requested extracts, which could be required in a variety of situations where the applicant's expunged conviction was of no apparent relevance, did not pursue any of the legitimate aims listed in Article 8 § 2, nor answered any pressing social need or struck a fair balance between the applicant's rights under Article 8 of the Convention and the interests of any third party in knowing about his past conviction which had already been expunged.

33 <<https://hudoc.echr.coe.int/eng?i=001-231080>>.

34 <<https://hudoc.echr.coe.int/eng?i=001-230315>>.

35 <<https://hudoc.echr.coe.int/eng?i=001-234259>>.

36 <<https://hudoc.echr.coe.int/eng?i=001-234137>>.

37 <<https://hudoc.echr.coe.int/eng?i=001-231432>>.

38 <<https://hudoc.echr.coe.int/eng?i=001-235612>>.