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

THIRD SECTION

CASE OF VOLODINA v. RUSSIA (No. 2)

(Application no. 40419/19)

JUDGMENT

Art 8 • Private life • Positive obligations • Authorities' failure to protect victim of domestic violence from repeated acts of cyberviolence and to bring perpetrator to justice

STRASBOURG

14 September 2021

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Volodina v. Russia (no. 2),

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Paul Lemmens, *President,*
Dmitry Dedov,
Georges Ravarani,
María Elósegui,
Darian Pavli,
Anja Seibert-Fohr,
Andreas Zünd, *judges,*
and Milan Blaško, *Section Registrar,*

Having regard to:

the application (no. 40419/19) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") on 19 July 2019;

the decision to give notice of the complaints concerning the taking of measures against online harassment to the Russian Government ("the Government") and to declare the remainder of the application inadmissible;

the parties' observations;

Having deliberated in private on 24 August 2021,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The case concerns the State's obligation to protect the applicant from acts of cyberviolence, including the publication of her intimate photographs without consent, stalking and impersonation, and to carry out an effective investigation into these acts.

THE FACTS

2. The applicant is Ms Valeriya Igorevna Volodina; she is a Russian national who was born in 1985 and lives in an undisclosed location in Russia. In 2018, fearing for her safety, she obtained a legal change of name (see *Volodina v. Russia*, no. 41261/17, § 39, 9 July 2019). Her old name is used in the judgment to protect her safety. The applicant was represented before the Court by Ms Vanessa Kogan, director of the Stichting Justice Initiative, a human-rights organisation based in Utrecht, the Netherlands.

3. The Government were initially represented by Mr M. Galperin, former Representative of the Russian Federation to the European Court of Human Rights, and later by his successor in this office, Mr M. Vinogradov.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

CIRCUMSTANCES OF THE CASE

5. In November 2014 the applicant began a relationship with Mr S., an Azerbaijani national. After their separation in 2015, S. threatened her with death or bodily injuries; he abducted and assaulted her on several occasions. For details, see *Volodina*, cited above, §§ 10-36.

6. In June 2016 the applicant's brother told her that her account on the Russian social media platform VKontakte had been hacked. Her invented name had been replaced with the real name; her personal details, a photograph of her passport and her intimate photographs had been uploaded to the account. Classmates of her twelve-year-old son and his class teacher had been added as friends. The applicant attempted to log into her account only to discover that the password had been changed.

7. On 22 June 2016 the applicant complained to the Ulyanovsk police about a breach of her right to privacy. The police took a statement from the applicant's brother. He said that he had talked to S. on the phone and that S. had admitted that he had hacked into the applicant's email account and sent obscene messages to her contacts. He had done so out of desperation because he had "no good way of bringing [her] back". Claiming that they were unable to locate S. in their jurisdiction, on 21 July 2016 the Ulyanovsk police forwarded the matter to the police in the Krasnodar Region where S. had registered his residence. On 29 August 2016 the Krasnodar police sent the file on to the Samara Region where S. had moved. On 30 September 2016 the Samara police returned the case file to their colleagues in Ulyanovsk.

8. On 7 November 2016 the Ulyanovsk police declined to institute criminal proceedings on the grounds that the information had been made public on social media rather than in the media. The supervising prosecutor set that decision aside as unlawful because S. had not been interviewed. On 2 May 2017 the police again declined to open a criminal case, finding no indication that S. had collected or disseminated information about the applicant's private life. The decision stated that it had not been possible to locate S. who had no Russian nationality or proof of residence in Russia. On 1 February 2018 the supervising prosecutor annulled that decision. He directed the police to locate and interview S., to examine his electronic devices and records of his phone calls to the applicant.

9. On 6 March 2018 the Ulyanovsk police opened a criminal investigation under Article 137 of the Criminal Code. Over the following months, police investigators interviewed the applicant and S., first separately and later face-to-face, took statements from the applicant's family members, seized and examined their mobile phones, obtained logs of phone communications from mobile providers, received information from the company operating the VKontakte site, and talked to a social media expert.

10. In February, March and September 2018, new fake profiles in the applicant's name appeared on VKontakte and Instagram. The profiles used her intimate photographs and personal details.

11. On 13 August and 19 September 2018 the applicant complained to the Ulyanovsk police that S. had sent her death threats via social media and Internet messengers. She enclosed printouts of messages and asked the police to open a criminal case under Article 119 of the Criminal Code (threats of death or bodily injury) and to grant her protection. On 3 January 2019 the police refused to open a criminal case on the grounds that the threats had not been "real".

12. Following the creation of court orders prohibiting certain forms of conduct (see paragraph 32 below), on 28 September 2018 the applicant asked the investigator to seek an order which would prevent S. from using the Internet, contacting her by any means including via social media, e-mail or Internet messengers, or approaching her or members of her family. On 18 October 2018 the investigator replied that, on account of his independent standing in the proceedings, the parties could not dictate him what action needed to be taken. He refused her request on the grounds that "measures of restraint could be applied to suspects in exceptional circumstances only". By judgment of 27 November 2018, as upheld on appeal on 21 January 2019, the Ulyanovsk courts dismissed the applicant's complaint about the investigator's decision on the grounds that it had been issued by a competent official within his scope of discretion.

13. On 12 December 2018 the applicant complained to the Kuntsevskiy District Court in Moscow that the Kuntsevskiy district police had not responded in any way to her report of a tracking device she had found in her bag two years previously (see *Volodina*, cited above, §§ 28-29). On 26 December 2018 the District Court found no fault with the actions of the district police because the deputy chief had forwarded the applicant's report to the Special Technical Measures Bureau shortly upon its receipt. On 28 February 2019 the Moscow City Court dismissed, in a summary fashion, her appeal against the District Court's decision.

14. On 19 January 2019 the Ulyanovsk police suspended the investigation into the fake social media profiles. They established that two fake profiles had been created in February and March 2018 using IP addresses and phone numbers registered in Azerbaijan. According to the billing information of his phones and the police database, on critical dates S. had been in the Tambov Region in Russia. The investigators decided to ask their Azerbaijani counterparts to obtain records of phone communications from the Azerbaijani number.

15. Counsel for the applicant applied for judicial review of the investigators' decisions. She complained that the criminal case had been opened following a two-year period of inactivity after the first report, that the fake profiles created in 2016 had not been investigated, that S.'s friends

and connections had not been identified or interviewed, that communications between S. and the phone number in Azerbaijan had not been evaluated, and that the collected evidence had not been made available to the applicant.

16. On 25 June 2019 the Zavolzhskiy District Court in Ulyanovsk set aside the 19 January 2019 suspension decision as unlawful and premature in so far as it did not fix a time-limit for receiving a reply from Azerbaijan and as it prevented the applicant from requesting the investigator to follow the leads which she believed needed to be explored. On 19 August 2019 the Ulyanovsk Regional Court quashed the District Court's decision in respect of the applicant's complaints which had been granted. It held that the law did not require the investigator to make the case file available to the applicant until the investigation had been completed, and that the suspension decision had been lawful because "the investigator had ... given due consideration to all the circumstances" underlying that decision.

17. On 14 September 2019 the Kuntsevskiy district police in Moscow refused to open a criminal investigation into the tracking device. The decision listed the constituent elements of an offence under Article 137 of the Criminal Code and stated that the device had been identified as a Russian-made GPS tracker which was legally available for purchase. As the applicant had thrown away the device and the SIM card it contained, it was impossible to identify the owner. Her claim that "no one but [S.] could have planted the device" was speculation which could not be accepted as evidence. As there was no "objective evidence incriminating [S.]", the criminal case against him could not continue.

18. On 20 October 2019 the owner of the telephone number registered in Azerbaijan which had been used for the fake social media accounts was established and questioned. The applicant was not informed of this development. Nor was it mentioned in the investigator's subsequent decision of 25 December 2019 to suspend the criminal proceedings due to the failure to identify the perpetrator.

19. On 18 May 2020 the applicant was questioned about the fake profiles which had appeared in 2018 on Instagram and VKontakte. The investigator asked the applicant if she knew certain named individuals in Azerbaijan and whether she would accept a polygraph test. She said she did not know these people and refused the test.

20. On 14 October 2020 the Ulyanovsk police closed the criminal case under Article 137 of the Criminal Code. According to the decision, it was established that in February and March 2018 S. had created fake profiles on VKontakte in the applicant's name and had published nude photos of her without her consent. The published photos had been found on his phone during an inspection. On 13 October 2020 S. had filed a motion to discontinue the proceedings because the limitation period had expired. The

motion had been granted: as the offence under Article 137 was of lesser gravity, the two-year period of limitation had expired in March 2020.

21. The decision was not communicated to the applicant or her lawyer. On 14 April 2021 she became aware of its existence from the Government's Action Plan submitted to the Committee of Ministers in the framework of execution of the *Volodina* group of cases.

RELEVANT LEGAL FRAMEWORK

I. UNITED NATIONS

22. The 2015 report by the UNESCO-ITU Broadband Commission for Digital Development's Working group on Broadband and Gender, "Cyberviolence against Women and Girls: A World-wide Wake-up Call"[1], observes that "violence online and offline, or 'physical' violence against women and girls (VAWG) and 'cyber' VAWG, feed into each other" and that "abuse may be confined to networked technologies or may be supplemented with offline harassment including vandalism, phone calls and physical assault".

Forms of cyber VAWG fall into six broad categories which include "hacking", "impersonation" (the use of technology to assume the identity of the victim in order to embarrass or shame her, e.g., by sending offensive emails from the victim's email account), "surveillance/tracking" (stalking and monitoring a victim's activities either in real-time or historically; e.g., GPS tracking), "harassment/spamming" (the use of technology to continuously contact, annoy, threaten, and/or scare the victim), "recruitment" (luring potential victims into violent situations), and "malicious distribution" (manipulating and distributing defamatory and illegal materials related to the victim; e.g., threatening to or leaking intimate photos/video). In addition, some terminology is particular to cyber VAWG: thus, "revenge porn" consists of an individual posting intimate photographs of another individual online with the aim of publicly shaming and humiliating that person, and even inflicting real damage on the target's "real-world" life, such as getting them fired from their job.

Five characteristics that distinguish cyber VAWG are: "anonymity" (abusive person can remain unknown to victim), "action at a distance" (abuse can be done without physical contact and from anywhere), "automation" (abusive actions using technologies require less time and effort), "accessibility" (variety and affordability of many technologies make them readily accessible to perpetrators), and "propagation and perpetuity" (texts and images multiply and exist for a long time or indefinitely).

[1] https://en.unesco.org/sites/default/files/genderreport2015final.pdf. Last accessed on the date of the judgment.

23. A report by the UN Human Rights Council's Special Rapporteur on violence against women, its causes and consequences, on online violence against women and girls from a human rights perspective (A/HRC/38/47, 18 June 2018) has found that online and internet-facilitated forms of violence against women have become increasingly common, particularly with the use of social media platforms and other technical applications (point 12). Technology has transformed many forms of gender-based violence into something that can be perpetrated across distance, without physical contact and beyond borders. All forms of online gender-based violence are used to control and attack women and to maintain and reinforce patriarchal norms, roles and structures and an unequal power relationship (point 30).

Online violence against women may be manifested in different forms and through different means, such as non-consensual accessing, using, manipulating, disseminating or sharing of private data, photographs or videos, including sexualized images (point 34). New among other forms of violence, "revenge porn" consists in the non-consensual online dissemination of intimate images, obtained with or without consent, with the purpose of shaming, stigmatising or harming the victim (points 33 and 41).

The Special Rapporteur formulated a number of recommendations for States, including the recommendations that States should clearly prohibit and criminalise online violence against women, in particular the non-consensual distribution of intimate images and the threat to disseminate such images (point 101), and that States should allow victims to obtain protection orders to prevent their abusers from posting or sharing intimate images without their consent (point 104).

II. COUNCIL OF EUROPE

24. The Cybercrime Convention Committee's Working Group on cyberbullying and other forms of online violence, especially against women and children, carried out a mapping study on cyberviolence[2] and released its findings on 9 July 2018. The Working Group agreed to define "cyberviolence" as "the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities" (point 2.1.1). Acts of cyberviolence may take a variety of forms ranging from ICT-related violations of privacy, such as stalking, identity theft and impersonation, to cyber-harassment which comprises

[2] https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c. Last accessed on the date of the judgment.

"revenge porn", to cybercrime (point 2.1.2). With regard to "revenge porn", the study observed that "the phenomenon predominantly involves a partner in an intimate relationship disseminating the material in order to humiliate or intimidate the victim" and has been recognised as a crime in several jurisdictions (point 2.1.2.1.2).

Investigation and prosecution of cyberviolence was confronted with many challenges, including limited help by law enforcement: "Cyberviolence may involve methods that are particularly difficult for police forces to investigate, and victims may be told – correctly or incorrectly – that there is nothing that law enforcement can do. Like any other form of violence against women, online violence against women is often overlooked because of a lack of awareness and gendered understanding of violence. Victims' experience are often considered as 'incidents' rather than patterns of behaviour, and victims are blamed for the violence they face" (point 2.3).

III. RUSSIA

A. Protection of private life: civil law

25. The concept of "private life" embraces "the sphere of human life and activity which belongs to the particular person, exclusively concerns that person and is not subject to public or State control so long as it is not contrary to law" (Constitutional Court's decisions no. 248-O of 9 June 2005, no. 158-O-O of 26 January 2010, and no. 1253-O of 28 June 2012).

26. Article 150 of the Civil Code ("Intangible assets") stipulates that a person's dignity, honour, goodwill, business reputation, private life and family secrets constitute inalienable intangible assets. A court may recognise an infringement of the person's intangible assets and prevent actions that infringe or threaten to infringe them.

27. Article 151 ("Compensation for non-pecuniary damage") provides that a person who infringes another's intangible assets may be ordered by a court to pay financial compensation in respect of non-pecuniary damage.

28. Article 152.1 ("Protection of a person's image") establishes that a person's image may only be published or used with the consent of the person concerned. If an image is shared on the Internet without consent, the person may demand that it be removed and no longer used.

29. Article 152.2 ("Protection of a person's private life") prohibits the collection, storage, dissemination and use of information about a person's private life, including his or her origins, place of stay or residence, private or family life, without the consent of the person concerned.

B. Protection of private life: criminal law

30. Article 137 of the Criminal Code ("Breach of privacy") establishes that illegal collection or dissemination of information on the person's private life constituting his or her personal or family secrets, without the consent of the person concerned, or else dissemination of such information in public speech, in a work of art on public display or in the mass media, is an offence punishable by a fine or up to two years' imprisonment.

31. The Plenary Supreme Court of Russia's guidance on the judicial application of criminal-law provisions for the protection of constitutional rights and freedoms (Resolution no. 46 of 25 December 2018) indicates that, for the purposes of Article 137 of the Criminal Code, the collection of information on the person's private life must be understood as comprising the illegal obtaining of information by any means, such as surveillance, wiretapping, interviewing other persons, including with the use of audio, video and photorecording equipment, and copying, stealing or otherwise acquiring documents. Dissemination of information on the person's private life consists in communicating or disclosing it to one or more persons orally, in writing or otherwise, including by means of handing over the materials or publishing the information on ICT networks, such as the Internet.

C. Criminal procedure

32. In April 2018, a new measure of restraint in criminal proceedings in the form of a court order prohibiting certain conduct (*запрет определенных действий*) was introduced in Article 105.1 of the Code of Criminal Procedure. The court may, on an application from the investigator in charge of the case, issue an order requiring a suspect or defendant in criminal proceedings to appear when summoned, to abstain from certain conduct and to comply with the restrictions imposed (part 1). An exhaustive list of types of conduct which may be restricted includes a prohibition to leave the place of residence, a prohibition to visit or approach certain places or to attend certain events, a prohibition to communicate with certain persons, and a prohibition to receive or send letters, to use means of communication or the Internet (part 6).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

33. The applicant complained under Article 8 of the Convention that the Russian authorities had failed to protect her against repeated acts of online

violence and to investigate the matter diligently and efficiently. Article 8 reads as follows:

> "1. Everyone has the right to respect for his private ... life ...
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

1. Exhaustion of domestic remedies

34. The Government submitted that the applicant did not avail herself of civil-law remedies which clearly had a prospect of success. She could have introduced a civil claim under Articles 150-151.2 of the Civil Code to have her photos and fake profiles removed, to prevent their further use and to be granted compensation for non-pecuniary damage. The Government supported their position with the reference to a judicial decision (Krasnogorskiy District Court in Kamensk-Uralsk, 13 March 2017, as upheld on appeal by the Sverdlovskiy Regional Court) by which a plaintiff's former partner was ordered to pay her compensation for the unlawful use of her intimate photos. He had shown the photos, which he had taken during the time they cohabited, to her current partner and her mother-in-law. The courts had taken evidence from witnesses and established the facts according to the civil standard of proof. They had found that in civil proceedings, the courts were not bound by the police's decision declining to institute a criminal investigation on the plaintiff's report. In civil proceedings, the perpetrator did not benefit from the presumption of innocence, and the burden of proof was placed equally on both parties in relation to the circumstances they asserted.

35. The applicant disagreed that civil-law remedies offered a sufficient chance of success in the circumstances of her case. She did not need to seek a court order to have the photos removed, as the social media platforms had taken down the fake profiles as soon as she had reported them. Pursuing a civil claim to prevent a further use of her photos and obtain damages would have required her to adduce evidence showing that S. had been responsible for creating the fake profiles or used the services of someone who had done so. She could not have collected that evidence in a situation where the investigative authorities with all necessary powers, including access to phone registers, IP addresses, geolocation data, and cross-border cooperation, had not managed to establish the person responsible for creating the fake profiles and publishing her photos. The Kamensk-Uralsk case to which the Government referred did not involve cyberviolence. The defendant had personally visited the plaintiff's partner and mother-in-law to

show them the photos; he did not deny he had done so in order to defame her; her partner and mother-in-law had witnessed his actions. In contrast, the offence in the applicant's case had taken place in cyberspace which offers the perpetrator anonymity and the opportunity to cause harm across borders. Finally, unlike the Kamensk-Uralsk case where police had refused to open a criminal case, in the applicant's case, the criminal case had been opened, giving her reason to believe that a separate civil action would be redundant as she would be able to claim damages in criminal proceedings.

36. The Court notes that the applicant reported the fake social-media profiles and the discovery of a tracking device in her bag to the police (see paragraphs 7 and 10 above, and *Volodina v. Russia*, no. 41261/17, § 29, 9 July 2019). After an initial period of prevarication, the police accepted to open a criminal case under Article 137 of the Criminal Code, to which the decision on her report of the tracking device also referred (see paragraphs 9 and 17 above). It was not claimed that the acts which she complained about fell out of the scope of that provision. She could therefore legitimately expect that, once seized of the matter, the investigative authorities would pursue the investigation, identify the person responsible and bring the case to trial which would have enabled her to constitute a civil party and claim damages from the perpetrator. Accordingly, the Court finds that the applicant made use of a remedy available to her under domestic law which was apparently effective and offered reasonable prospects of success. Indeed, the Government did not claim that complaining to the police about these matters was not an effective remedy. As to their argument that she should have also instituted civil proceedings, the Court reiterates that, even assuming that a civil-law remedy could have been an effective one, an applicant who has pursued an apparently effective remedy cannot be required also to have tried others that were available but probably no more likely to be successful (see *Nicolae Virgiliu Tănase v. Romania* [GC], no. 41720/13, § 177, 25 June 2019, and, in a factually similar situation, *Buturugă v. Romania*, no. 56867/15, § 73, 11 February 2020). It follows that the Government's objection as to the alleged non-exhaustion of domestic remedies must be rejected.

2. "Substantially the same"

37. The Government submitted that the complaint about the applicant's alleged stalking with the use of a tracking device had already been examined by the Court in the applicant's first case (they referred to *Volodina*, cited above, §§ 28-29).

38. The applicant replied that, although the tracking device was indeed mentioned in the statement of facts of the first judgment, her complaints relating to ineffective investigation and judicial review had not yet been subject to the Court's examination.

39. The Court has identified the following criteria concerning Article 35 § 2 (b) of the Convention by which an application may be declared inadmissible if it "is substantially the same as a matter that has already been examined by the Court ... and contains no relevant new information": (i) an application is considered as being "substantially the same" where the parties, the complaints and the facts are identical; (ii) the concept of complaint is characterised by the facts alleged in it and not merely by the legal grounds or arguments relied on; and (iii) where the applicant submits new information, the application will not be essentially the same as a previous application (see *Kudeshkina v. Russia (no. 2)* (dec.), no. 28727/11, § 68, 17 February 2015).

40. The Court notes that the decisions by Russian courts and investigators in the matter of the tracking device (see paragraphs 13 and 17 above), which it did not have the opportunity to consider when adopting the *Volodina* judgment, constitute "relevant new information" within the meaning of the third criterion above. Accordingly, this part of the application cannot be rejected in accordance with Article 35 § 2 (b) of the Convention.

3. Conclusion

41. The Court finds that the application is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. Submissions by the parties

(a) The applicant

42. The applicant submitted that she had been the victim of repeated acts of online violence, including revenge porn, cyber harassment, and cyberstalking. The Russian authorities had failed to fulfil their positive obligations under Article 8 of the Convention to secure respect for her private life by providing effective protection against online violence, preventing further online violence and by carrying out an effective investigation. In her view, an adequate legal framework for protection from online violence should include: (1) criminalisation of online violence and acknowledging that online violence is a form of violence against women, (2) possibility for a victim to apply for protection order, (3) protection services for victims (e.g. helplines), (4) specialised trainings and protocols for the law enforcement officials. While many States had updated their existing legal frameworks or enacted specific laws to address online stalking, online harassment and the non-consensual sharing of intimate

images, Russia did not establish a holistic legal framework punishing all forms of domestic violence, including those perpetrated in cyberspace.

43. Unlike a majority of Council of Europe member States, the Russian legislation does not provide for protection orders for victims of domestic violence whether offline or online. The court may apply a new restraining measure under Article 105.1 of the Code of Criminal Procedure on the motion of the investigator; the decision to raise the motion before the court is at the investigator's full discretion. In the applicant's case, the investigator had refused to file the motion without even assessing her arguments. This provision of the Russian law is ineffective and insufficient to protect domestic violence victims. No member of the police or investigative team to whom she had appealed had any special preparation or qualification for dealing with cases of domestic violence. They had not conducted a gender-sensitive risk assessment of her situation, offered any form of protective measures, or explained her rights and opportunities to keep herself safe. The authorities had treated the cyberviolence and controlling behaviour as a trivial matter unworthy of their intervention.

44. An investigation into the dissemination of the applicant's intimate photos had been deliberately delayed; a criminal case was opened only in March 2018, that is two years after the first complaint of revenge porn in 2016. If the authorities had not known S.'s whereabouts they could have initiated a search for him but had not done so. He had been questioned by the police in August 2016 in connection with an attempt on the applicant's life (she referred to *Volodina*, cited above, § 23). That the authorities had not questioned him about the fake accounts indicated that they did not consider these actions to be part of the same pattern of domestic violence, refusing to make a connection between them and failing to acknowledge the various forms that domestic violence may take. It was not until 2018 that the authorities had first interviewed S. and made a request to VKontakte to establish the Internet addresses from which the fake profiles had been created. No request to provide information about the page owner had been sent to Instagram. The applicant had been first asked to give evidence about the fake Instagram accounts in May 2018, more than two years after her complaint. After the authorities established that the telephone number in Azerbaijan which had been used for creating two fake profiles in 2018 belonged to G., they did not declare him a suspect, establish his connection with S. or investigate how he had obtained the applicant's photos or her personal details and what his motive to create the fake profiles had been. The authorities had not informed the applicant of progress in investigation or given her access to the case file. Likewise, the investigation into the tracking device had been closed three years after her complaint. These elements indicated that the authorities in principle were not prepared to prosecute anyone for the cyberviolence of which she was the victim.

(b) The Government

45. The Government submitted that Russian law offers sufficient protection against interference with the person's private life, including non-consensual publication of the person's image. Alongside the criminal-law protection extended by Article 137 of the Criminal Code, there exist civil-law mechanisms offering redress for the violations that have already occurred, preventing the repetition of abusive behaviour and ensuing accountability of those responsible. The person affected may ask the court to recognise an infringement of his or her rights, demand that any unlawfully obtained content be removed and no longer used, claim compensation in respect of non-pecuniary damage (Articles 150, 151.1 and 152.2 of the Civil Code), and also make use of remedies available under the personal-data protection legislation. Accordingly, the Russian legislation, to the extent it was relevant to the circumstances of the applicant's complaint, was sufficient in its scope to satisfy the State's positive obligation under Article 8 to provide the applicant with the protection against online harassment.

46. On the effectiveness of the investigation, the Government emphasised that there was no absolute right to obtain the prosecution or conviction of any particular person provided that there were no culpable failures in seeking to hold perpetrators of criminal offences accountable. In 2016 the police in Ulyanovsk had registered the applicant's report and carried out an initial verification of the information. S.'s whereabouts had not been immediately ascertained and he had not been available for questioning. In 2018 a criminal case had been opened and S. had been required to sign an undertaking to appear. The investigation had taken evidence from the applicant, her family members, and S., and obtained data from phone service providers and social media platforms. Nevertheless, the evidence in support of the applicant's claim that S. was the perpetrator had been insufficient. She had carried on talking to him via social media and asking him for money which, in the Government's view, showed that their relationship was "not as straightforward and simple as the applicant described [it]". In those circumstances, a more restrictive measure, such as an order to prohibit certain conduct, could not be applied. The Russian courts had upheld the investigator's decision refusing application of that measure at two levels of jurisdiction. Further significant progress in the investigation had been achieved in 2019 when the Russian investigators had received information from their colleagues in Azerbaijan. Throughout the investigation, the authorities had kept the applicant informed of their actions.

2. The Court's assessment

(a) General principles

47. The Court reiterates that the concept of private life includes a person's physical and psychological integrity which the States have a duty to protect, even if the danger comes from private individuals (see *Söderman v. Sweden* [GC], no. 5786/08, §§ 78-80, ECHR 2013, and also *X and Y v. the Netherlands*, 26 March 1985, § 23, Series A no. 91; *M.C. v. Bulgaria*, no. 39272/98, § 150, ECHR 2003-XII; *A. v. Croatia*, no. 55164/08, §§ 59-60, 14 October 2010; and *Eremia v. the Republic of Moldova*, no. 3564/11, §§ 72-73, 28 May 2013). Children and other vulnerable individuals, in particular, are entitled to effective protection. The particular vulnerability of victims of domestic violence and the need for active State involvement in their protection has been emphasised both in international instruments and in the Court's well-established case-law (see *Bevacqua and S. v. Bulgaria*, no. 71127/01, § 65, 12 June 2008; *Hajduová v. Slovakia*, no. 2660/03, §§ 41, 30 November 2010; and *Volodina*, cited above, § 72).

48. The acts of cyberviolence, cyberharassment and malicious impersonation have been categorised as forms of violence against women and children capable of undermining their physical and psychological integrity in view of their vulnerability (see paragraphs 20, 23 and 24 above, and *K.U. v. Finland*, no. 2872/02, § 41, ECHR 2008). The Court has recently pointed out that "cyberharassment is currently recognised as an aspect of violence against women and girls and can take a variety of forms, such as cyber-violations of private life ... and the taking, sharing and handling of information and images, including intimate ones" (see *Buturugă*, cited above, § 74). In the context of domestic violence, intimate partners are frequently the likely perpetrators of the acts of cyber-stalking or surveillance (ibid., see also paragraph 20 above).

49. Online violence, or cyberviolence, is closely linked with offline, or "real-life", violence and falls to be considered as another facet of the complex phenomenon of domestic violence (see *Buturugă*, cited above, §§ 74 and 78, and paragraph 20 above). The States have a positive obligation to establish and apply effectively a system punishing all forms of domestic violence and to provide sufficient safeguards for the victims (see *Opuz v. Turkey*, no. 33401/02, § 145, ECHR 2009, and *Bălşan v. Romania*, no. 49645/09, § 57, 23 May 2017). The positive obligation applies to all forms of domestic violence, whether occurring offline or online. The Court has found that this positive obligation – in some cases under Articles 2 or 3 and in other instances under Article 8 taken alone or in combination with Article 3 of the Convention – includes in particular: (a) the obligation to establish and apply in practice an adequate legal framework affording protection against violence by private individuals; (b) the obligation to take the reasonable measures in order to avert a real and immediate risk of

recurrent violence of which the authorities knew or ought to have known, and (c) the obligation to conduct an effective investigation into the acts of violence (see, most recently, *Kurt v. Austria* [GC], no. 62903/15, § 164, 15 June 2021, and also *Bevacqua and S.*, § 65; *Eremia*, § 75; *Volodina*, §§ 76-77 and 86, and *Buturugă*, §§ 60-62, all cited above). The Court reiterates that the State's positive obligations under Article 8 to safeguard an individual's physical or psychological integrity may extend to questions relating to the effectiveness of a criminal investigation even where the criminal liability of agents of the State is not at issue (see *K.U. v. Finland*, § 46, and *Söderman*, § 84, both cited above).

(b) Application of the principles

50. There is no dispute as to the applicability of Article 8 in the instant case: the Court has found in the first judgment that the publication of the applicant's intimate photographs "undermined her dignity, conveying a message of humiliation and disrespect" (see *Volodina*, cited above, § 75). The non-consensual publication of her intimate photographs, the creation of fake social-media profiles which purported to impersonate her, and her tracking with the use of a GPS device interfered with her enjoyment of her private life, causing her to feel anxiety, distress and insecurity. Accordingly, it must be determined whether the authorities, once they became aware of the interference with the applicant's rights under Article 8 of the Convention, have discharged their obligations under that provision to take sufficient measures to put an end to that interference and prevent it from recurring (see *Eremia*, cited above, § 75).

51. The Court will first examine whether the respondent State has put in place an adequate legal framework providing the applicant with protection against the acts of cyberviolence (see *Söderman*, cited above, § 89-91). It reiterates that, as regards the acts which encroach on an individual's psychological integrity, the obligation of an adequate legal framework does not always require that a criminal-law provision covering the specific act be put in place. The legal framework could also be made up of civil-law remedies capable of affording sufficient protection, possibly combined with procedural remedies such as the granting of an injunction (ibid., §§ 85 and 108, with further references).

52. The Russian law contains both civil-law mechanisms and criminal-law provisions for the protection of an individual's private life. The definition of "private life" enshrined in the well-established case-law of the Constitutional Court (see paragraph 25 above) is sufficiently broad to cover multiple aspects of the person's physical and social identity and various elements of it, such as the person's name, image and personal data (compare *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 66, ECHR 2008).

53. The Civil Code prohibits, in a general manner, any information relating to an individual's private life from being gathered, kept, used or shared without the consent of the person concerned. It also specifically establishes the protection against the unauthorised use or publication of the person's image (see paragraphs 28 and 29 above). Infringements may give rise to injunctive relief and tort liability (see paragraphs 26 and 27 above).

54. More serious cases of interference with an individual's private life can lead to criminal liability. Article 137 of the Criminal Code makes it an offence to collect or disseminate the information relating to the person's private life without the consent of the person concerned (see paragraph 30 above). The Supreme Court's binding interpretation has upheld the application of this provision to all means by which information happens to be obtained, including various forms of surveillance with and without the use of technical equipment (see paragraph 31 above).

55. The applicant finds fault with the above-mentioned provisions in that they do not form part of a holistic framework punishing all forms of domestic violence and do not explicitly target its manifestations in cyberspace, such as online stalking or impersonation. For the Court, her criticism is part of the broader question of whether or not the Russian State has enacted legislation to criminalise acts of domestic violence, whether they happen to take place offline or online. The Court examined this question in detail in the first *Volodina* case and concluded that the existing Russian legal framework was deficient in several important respects and failed to meet the requirements inherent in the State's positive obligation to establish and apply effectively a system punishing all forms of domestic violence (see *Volodina*, cited above, §§ 80-85). It is not necessary to revisit this general finding in the instant case, in which the scope of the Court's inquiry is more limited. It needs not to review any alleged deficiencies of the private-life legislation *in abstracto*, but rather to determine whether or not the manner in which it was applied in the circumstances of the applicant's case gave rise to a violation of the Convention (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 164, ECHR 2015).

56. The applicant complained that her name, personal details and photographs had been used for creating fake social media profiles, that a GPS tracker had been planted to track her movements, and that she had been the target of death threats sent through social media (see paragraphs 6, 10, 11 and 13 above). The domestic authorities accepted that these acts presented the requisite elements of prosecutable offences under Russian law. The collection of information on the applicant's whereabouts and the dissemination of her images and personal details on information and communications technology (ICT) networks disclosed a serious interference with her privacy punishable under Article 137 of the Criminal Code, while death threats were prosecutable under Article 119 of the Criminal Code, regardless of the mode of their communication – offline or online. In the

light of the State's margin of appreciation in choosing legal means to ensure compliance with the Convention, the Court considers that the existing framework equipped the Russian authorities with legal tools for investigating the acts of cyberviolence of which the applicant was the victim.

57. The Court considers that the acts of cyberviolence in the instant case were sufficiently serious to require a criminal-law response on the part of the domestic authorities. The publication of the applicant's intimate photographs, calculated to attract the attention of her son, his classmates and their teacher (see paragraph 6 above), sought to humiliate and degrade her. As noted above, the tracking of her movements by means of a GPS device and the sending of death threats on social media caused her to feel anxiety, distress and insecurity. The Court also reiterates that both the public interest and the interests of the protection of vulnerable victims from offences infringing on their physical or psychological integrity require the availability of a remedy enabling the perpetrator to be identified and brought to justice (see *K.U. v. Finland*, cited above, § 47, and *Volodina*, cited above, § 100). Civil proceedings which might have been an appropriate remedy in situations of lesser gravity would not have been able to achieve these objectives in the present case.

58. The Court further reiterates that the State authorities have a responsibility to provide adequate protection measures to the victims of domestic violence in the form of effective deterrence against serious breaches of their physical and psychological integrity (see *Opuz*, cited above, § 176, and *Volodina*, cited above, § 86). Whereas in a large majority of Council of Europe member States victims of domestic violence may apply for immediate "restraining" or "protection" orders capable of forestalling the recurrence of domestic violence, Russia has remained among only a few member States whose national legislation does not provide victims of domestic violence with any comparable measures of protection (see *Volodina*, cited above, §§ 88-89). The respondent Government did not identify any effective remedies that the authorities could have used to ensure the applicant's protection against recurrent acts of cyberviolence. The civil law mechanism does not include the rigorous monitoring of the perpetrator's compliance with the terms of an injunction capable of ensuring the victim's safety from the risk of recurrent abuse (ibid., § 89).

59. As to the orders prohibiting certain conduct (see paragraph 32 above), the Court is unable to find that they offer sufficient protection to victims of domestic violence in the applicant's situation. The order is a measure of restraint limited to the sphere of criminal law, the availability of which depends on the existence of a criminal case. However, as noted above, the domestic authorities may delay or refuse to open a criminal case, including in respect of serious incidents such as threats of death, malicious

impersonation or stalking with the use of a tracking device. Moreover, it is also difficult to expect that such orders can be granted in practice with the urgency that is often essential in domestic violence situations. The application for an order is also conditional on the procedural status of the perpetrator: so long as the investigation has not gathered evidence to charge the perpetrator, a measure of restraint can be imposed on a suspect only in "exceptional circumstances" (see *Birulev and Shishkin v. Russia*, nos. 35919/05 and 3346/06, § 33, 14 June 2016). Since the case against S. had not progressed beyond the stage of suspicion, the shortcomings of the preceding investigation adversely affected the applicant's chances of having that measure of restraint applied to him.

60. It is even more significant that an order prohibiting certain conduct is not directly accessible to the victim who must petition the investigator to raise an application to that effect before a court. The investigator has full discretion to grant or deny the petition. The investigator's refusal is amenable to judicial review, for which the applicant unsuccessfully applied (see paragraph 12 above). The Ulyanovsk courts, however, did not undertake an independent scrutiny of the substantive grounds for refusal, confining themselves to a finding that the investigator had not overstepped the limits of his powers (compare *Lyapin v. Russia*, no. 46956/09, § 138, 24 July 2014).

61. The Court has found in the first *Volodina* case that the response of the Russian authorities to the known risk of recurrent violence on the part of the applicant's former partner was manifestly inadequate and that, through their inaction and failure to take measures of deterrence, they allowed S. to continue threatening, harassing and assaulting the applicant without hindrance and with impunity (see *Volodina*, cited above, § 91). This finding is applicable in the circumstances of the present case in which the authorities did not consider at any point in time what could and should be done to protect the applicant from recurrent online violence.

62. Turning to the manner in which the Russian authorities conducted an investigation into the applicant's reports, the Court reiterates that, to be effective, an investigation must be prompt and thorough. The authorities must take all reasonable steps to secure evidence concerning the incident, including forensic evidence. Special diligence is required in dealing with domestic-violence cases, and the specific nature of the domestic violence must be taken into account in the conduct of the domestic proceedings (see *Volodina*, cited above, § 92).

63. As regards the investigation into the fake social media profiles and the dissemination of the applicant's intimate photos, a criminal case was opened only on 6 March 2018, almost two years after the applicant had first reported the fake profiles to the police on 22 June 2016 (see paragraphs 7 and 9 above). Before that, it would appear that the police sought to dispose hastily of the matter on formal grounds, citing lack of territorial jurisdiction

or lack of an offence (see paragraphs 7 and 8 above), instead of making a serious and genuine attempt to establish the circumstances of the applicant's malicious impersonation on social media. Since States are responsible for delays, whether attributable to the conduct of their judicial or other authorities or to structural deficiencies in its judicial system which cause delays (see *Rutkowski and Others v. Poland*, nos. 72287/10 and 2 others, § 128, 7 July 2015), it is immaterial whether the initial two-year delay was caused by a lack of clear rules on jurisdiction for investigating online offences or by the reluctance of individual police officers to take up the case.

64. The Government sought to account for the delay by the fact that S. was unavailable for questioning. This explanation does not convince the Court. It is apparent from the circumstances of the first *Volodina* case that as early as August 2016 the police in Samara could have taken evidence from S. in connection with another offence committed against the applicant (see *Volodina*, cited above, § 23). If S. had indeed gone missing, the police could have made use of the extensive powers available to them under the Police Act and the Operational-Search Activities Act to search for and apprehend persons suspected of criminal offences (see *Shimovolos v. Russia*, no. 30194/09, §§ 33-38, 21 June 2011). In any event, whether or not S. was readily available for questioning, the police should have acted promptly and in good faith to secure forensic evidence of the alleged offences, including the identification of phone numbers and Internet addresses which had been used to create the fake profiles and upload the applicant's photos. However, this was not done until the criminal case was opened in 2018, resulting in a loss of time and undermining the authorities' ability to secure evidence relating to the acts of cyberviolence.

65. The investigation which was conducted from 2018 onwards cannot be said to have been expeditious or sufficiently thorough. It took the authorities nearly a year to obtain information about the Internet addresses of the fake accounts from the Russian company operating the social media platform VKontakte; the authorities did not send any requests to Instagram to identify the owner of the fake accounts. The questioning of the applicant and inspection of the fake pages on Instagram had taken place in May 2020, that is two years since her complaint in 2018. The authorities appear to have established both the person whose phone number and Internet address had been used to create the fake accounts in 2016, and the owner of the phone number in Azerbaijan which had been used to create two fake accounts in 2018. However, their communications and possible links with S. were not investigated; it was not established how the person in Azerbaijan could have come by the applicant's intimate photos and personal data.

66. A "pre-investigation inquiry" into the other offences which the applicant had reported to the police did not lead to any criminal case being opened. In the matter of the tracking device found in the applicant's bag, the

procedural decision on her complaint was issued almost three years later after her report to the police (see paragraphs 13 and 17 above). The investigative authorities did not contact her about the complaint, did not ask S. any questions about the device, and did not deploy technical means to determine the number of the SIM card installed in the device using the service provider's network infrastructure. The authorities also failed to investigate the death threats which the applicant had received online and reported to the police in August and September 2019 (see paragraph 11 above). Without undertaking any investigative steps, the police concluded that no offence had been committed. As the Court found in the first *Volodina* case, the police would arbitrarily raise the bar for evidence required to launch criminal proceedings, claiming that threats of death had to be "real and specific" in order to be prosecutable (see *Volodina*, cited above, § 98). Most importantly, the authorities failed to take a global view of the situation by considering whether those incidents could be said to be so connected in type and context with the physical assaults the applicant reported (see *Volodina*, cited above, §§ 31-36) as to justify the conclusion that they amounted to a single course of conduct (see *Buturugă*, cited above, § 78).

67. As a consequence of the slow-paced investigation into the fake social media profiles, the prosecution eventually became time-barred. The criminal case against S. was discontinued by application of the statute of limitations on his initiative, even though his involvement in the creation of the fake profiles appears to have been established (see paragraph 20 above). The Court has found violations of the obligation to conduct an effective investigation in cases where the proceedings had continued unduly or had ended by prescription allowing the perpetrators to escape accountability (see *Opuz*, cited above, § 151; *P.M. v. Bulgaria*, no. 49669/07, §§ 64-66, 24 January 2012, and, in a factually similar situation, *Barsova v. Russia* [Committee], no. 20289/10, §§ 35-40, 22 October 2019). The effectiveness principle means that the domestic authorities must on no account be prepared to let the physical or psychological suffering inflicted go unpunished. This is essential for maintaining the public's confidence in, and support for, the rule of law and for preventing any appearance of the authorities' tolerance of or collusion in acts of violence (see *Okkalı v. Turkey*, no. 52067/99, § 65, ECHR 2006-XII (extracts)). By failing to conduct the proceedings with the requisite diligence, the Russian authorities bear responsibility for their failure to ensure that the perpetrator of acts of cyberviolence be brought to justice. The impunity which ensued was enough to shed doubt on the ability of the State machinery to produce a sufficiently deterrent effect to protect women from cyberviolence.

68. In sum, the Court finds that, even though the existing framework equipped the authorities with legal tools to prosecute the acts of cyberviolence of which the applicant was a victim, the manner in which

they actually handled the matter – notably a reluctance to open a criminal case and a slow pace of the investigation resulting in the perpetrator's impunity – disclosed a failure to discharge their positive obligations under Article 8 of the Convention. There has accordingly been a violation of that provision.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

69. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

70. The applicant asked the Court to determine the appropriate amount of the award in respect of non-pecuniary damage. She claimed 5,386.46 euros (EUR) in respect of legal, administrative and postal expenses.

71. The Government submitted that the claim in respect of non-pecuniary damage was to be rejected for failure to specify the amount claimed. They further submitted that the legal costs relating to the threats of death and the tracking-device incident fell out of the scope of the case and should not be reimbursed.

72. Since non-pecuniary damage does not, by its nature, lend itself to precise calculation, the Court has accepted to examine claims in respect of non-pecuniary damage for which applicants did not quantify the amount, leaving it to the Court's discretion (see *Nagmetov v. Russia* [GC], no. 35589/08, § 72, 30 March 2017). Making its own assessment on an equitable basis, the Court awards the applicant EUR 7,500 in respect of non-pecuniary damage, plus any tax that may be chargeable. The payment is to be effected on the basis of the applicant's new identity documents which were communicated to the Government on giving notice of the application.

73. The Court further notes that the claim for costs and expenses has been properly substantiated, reasonable as to quantum and relevant to the matters considered in the present application. It awards the amount claimed in respect of costs and expenses, plus any tax that may be chargeable to the applicant, payable into the bank account of the applicant's representative.

74. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

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 from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts:

(i) EUR 7,500 (seven thousand five hundred euros), to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable, in respect of non-pecuniary damage;

(ii) EUR 5,386.46 (five thousand three hundred and eighty-six euros and 46 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.

Done in English, and notified in writing on 14 September 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

{signature_p_2}

Milan Blaško
Registrar

Paul Lemmens
President