



## Children's rights and personal data protection in the jurisprudence of the European Court of Human Rights

Sergio Ruiz Díaz Arce\*

*ABSTRACT: This article analyses the jurisprudence of the European Court of Human Rights (ECtHR) in order to identify and characterise the argumentative conclusions produced by the Court in their decisions on personal data protection and that affect children's rights. The data collection technique consisted of a search and selection of the arguments in the Court's judgments on situations that refer to violations of personal data. For the argumentative analysis, through an argumentation scheme, a judgment of a case that refers to child protection against sexual online exploitation was selected. In this context, we have observed that the Court structured its arguments to verify the violation of privacy and protection of personal data using the following topics: (i) respect for private life; (ii) criminal-law provisions; and (iii) positive obligations. The use of these topics in the subsequent judgments of the ECtHR is also identified through the citations to justify their own decisions.*

*KEYWORDS: Children's rights – personal data protection – European Court of Human Rights – sexual online exploitation – jurisprudence.*

---

\* Researcher at the Research Centre for Justice and Governance (JusGov), University of Minho.

## 1. Introduction

Internet access is considered an inalienable human right by the United Nations,<sup>1</sup> which also enables the exercise of a series of rights, such as participation, freedom of expression, access to information and communication. However, the promotion, protection and enjoyment of human rights on the internet requires States to adopt a series of necessary measures to prevent, mitigate and remedy human rights violations. These human rights violations may include the collection, retention, processing, and use or disclosure of data on the Internet in a manner that may violate or abuse human rights, especially of those people who are in a special situation of vulnerability.

Given this scenario, children and adolescents, conceptualised as “*digital natives*”,<sup>2</sup> are the ones who are most affected by the use of so-called information and communication technologies (“ICTs”), due to their innate ability to incorporate them into their daily activities. For this reason, it is essential that specific protection mechanisms be established for this group of people, through public policies that guarantee both access and safe use of the Internet, as well as to prevent violations of rights.

The recognition of the rights of the child in the regional protection systems, and therefore the respect and guarantee of all their human rights without ethnic, racial, political, social, economic or any other kind of discrimination, is a characteristic of the specialised protection for this group of people in a “*situation of absolute vulnerability*”.<sup>3</sup> In addition to the written law rules, the jurisprudence of regional courts in this matter has been characterised by its dynamic development through the responses offered in particular cases.

This argumentative activity of the courts has made it possible to understand the scope of the protection norms and expand their content, as well as to identify problems or types of problems in new situations of violation of rights. Therefore, through the analysis of judicial decisions we are able to identify the types of problems, follow the argumentative development of a specific field of law and characterise the argumentative conclusions. In this manner, the analysis of the decisions of the European Court of Human Rights (“ECtHR”) on cases that address issues related to the protection of personal data in the field of children’s rights, constitutes the object of study of this investigation.

The data collection technique consisted of a search, selection and systematisation of the arguments in the ECtHR judgments to identify the conclusions produced in the judgments of cases involving children’s rights and protection of personal data. In this regard, the concept of protection of personal data was considered as a research variable, in order to determine its content and use in cases that violate the rights of the child. Therefore, the search aims to illustrate the argumentative

---

<sup>1</sup> See United Nations, Human Rights Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/38/L.10/Rev.1, 18 June–6 July 2018, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement>.

<sup>2</sup> See Marc Prensky, “Digital Natives, Digital Immigrants Part 1”, *On the Horizon* 9, no. 5 (October 2001): 1-6, <https://doi.org/10.1108/10748120110424816>.

<sup>3</sup> See Ernesto Garzón Valdés, “Desde la modesta propuesta de J. Swift hasta las casas de engorde: algunas consideraciones respecto de los derechos del niño”, *DOXA: Cuadernos de Filosofía del Derecho* 2, no. 15-16 (November 1994): 737-738, <https://doi.org/10.14198/DOXA1994.15-16.36>.

process by identifying the relevant elements or parts of a judicial decision. The analysis of the arguments, through an argument representation scheme, will allow for the determination of the reasons that support the decision of the Court.

## 2. The protection of personal data in the jurisprudence of the ECtHR

Under the Council of Europe, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) refers to the abuses that can be committed with respect to the processing of personal data, and in particular, its Article 15 states that “*specific attention shall be given to the data protection rights of children and other vulnerable individuals*”.<sup>4</sup> In that sense, the Consultative Committee of Convention 108+ adopted guidelines on children’s data protection in an education setting, which “*seek to help explain the data protection principles of Convention 108+ to tackle the challenges in the protection of personal data brought by new technologies and practices, whilst maintaining technologically neutral provisions*”.<sup>5</sup> Also, it is important to mention the Recommendation adopted by the Committee of Ministers of the Council of Europe on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, especially, about the responsibility of States to establish that protection: “*27. States must respect, protect and fulfil the right of the child to privacy and data protection. States should ensure that relevant stakeholders, in particular those processing personal data, but also the child’s peers, parents or carers, and educators, are made aware of and respect the child’s right to privacy and data protection.*”<sup>6</sup>

The importance of a legal framework in this matter consists in the possibility of establishing a series of protection obligations and determining certain limits when conflicts of rights may arise. Hence, “[*l*egislation is a foundational element in information sharing arrangements; and it is critical that the legislative framework finds the right balance between conflicting rights, in this case, the right to privacy and the rights of the child”.<sup>7</sup> However, this implies not only the regulation of behaviours that violate rights, but also offering legal inputs to deal with the different types of problems that judges and courts face. According to the case-law of the ECtHR, the protection of personal data is protected by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“European Convention on Human Rights” or

<sup>4</sup> Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 28 January 1981, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. See also Council of Europe, Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows, CETS No. 181, 8 November 2001, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181>; and Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223, 10 October 2018, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223>.

<sup>5</sup> Council of Europe, Consultative Committee of Convention 108, Children’s data protection in an education setting – Guidelines, T-PD(2019)06BISrev5, 20 November 2020, recital 6, <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b>.

<sup>6</sup> Council of Europe, Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Recommendation CM/Rec(2018)7, Section 3.4, 16, <https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html>.

<sup>7</sup> Carolyn Adams and Krista Lee-Jones. “Sharing personal information in the child protection context: Impediments in the Australian legal framework”, *Child & Family Social Work* 22 (2017): 1354-1355. <https://doi.org/10.1111/cfs.12352>.

“ECHR”): “Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.”<sup>8</sup>

The Court has analysed situations involving the interception of communications,<sup>9</sup> the use of surveillance<sup>10</sup> and the storage of personal data by public authorities.<sup>11</sup> Thus, for example, in the case of *Avilkina and Others v. Russia*, the Court addresses the disclosure of a two-year-old girl’s medical files to the prosecutor, following his request to be informed about all refusals by Jehovah’s Witnesses concerning blood transfusions: “[...] the protection of personal data, including medical information, is of fundamental importance to a person’s enjoyment of the right to respect for his or her private and family life guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention.”<sup>12</sup>

Likewise, in the case of *S. and Marper v. the United Kingdom*, an 11-year old’s fingerprints and DNA taken in relation to the suspicion of attempted robbery were retained without a time limit, even though he was ultimately acquitted. According to the ECtHR: “[...] The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.”<sup>13</sup>

In both cases, the Court considered that there has been a violation of Article 8 of the ECHR, due to a lack of adequate measures by the State against the violations of data protection rights. In the cited cases, the ECtHR concluded that the collection of confidential medical information must be accompanied by sufficient safeguards to prevent disclosure inconsistent with the respect for the private life, and that the retention of the fingerprints, cellular samples and DNA profiles without a time limit is a violation of Article 8. It means that “States should take measures to ensure that children’s personal data is processed fairly, lawfully, accurately and securely”, as well as the use of collected information “for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, carer or legal representative, or in accordance with another legitimate basis laid down by law”.<sup>14</sup>

<sup>8</sup> Judgment *Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 27 June 2017, Application no. 931/13, , recital 137, [https://hudoc.echr.coe.int/eng#{%22appno%22:\[%222931/13%22\],%22itemid%22:\[%22001-175121%22\]}](https://hudoc.echr.coe.int/eng#{%22appno%22:[%222931/13%22],%22itemid%22:[%22001-175121%22]}).

<sup>9</sup> See, for example, Judgment *Case of Malone v. the United Kingdom*, 2 August 1984, Application no. 8691/79, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57533%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]}); and Judgment *Case of Copland v. the United Kingdom*, 3 April 2007, Application no. 62617/00, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-79996%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}).

<sup>10</sup> See, for example, Judgment *Case of Klass and Others v. Germany*, 6 September 1978, Application no. 5029/71, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57510%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}); Judgment *Case of Uzun v. Germany*, 2 September 2010, Application no. 35623/05, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-100293%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-100293%22]}).

<sup>11</sup> See, for example, Judgment *Case of Leander v. Sweden*, 26 March 1987, Application no. 9248/81, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57519%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}); Judgment *Case of S. and Marper v. the United Kingdom*, 4 December 2008, Application nos. 30562/04 and 30566/04, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-90051%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}).

<sup>12</sup> Judgment *Case of Avilkina and Others v. Russia*, 6 June 2013, Application no. 1585/09, recital 45, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-120071%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-120071%22]}).

<sup>13</sup> Judgment *Case of S. and Marper v. the United Kingdom*, 4 December 2008, Application nos. 30562/04 and 30566/04, recital 103, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-90051%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}).

<sup>14</sup> Council of Europe, Consultative Committee of Convention 108, Children’s data protection in an education setting – Guidelines, T-PD(2019)06BISrev5, 20 November 2020, recital 29, <https://rm.coe>.

The storage of personal data also requires the adoption of special protection measures capable of responding to the dangers that threaten children in the digital environment. Although the use of ICTs has opened new ways of accessing and transmitting information, including contributing to freedom of expression, they have also had a direct impact on the lives of children, altering their social environment and the relationship dynamics between them. For this reason, and due to the characteristics of this problem, an issue that has become worrisome in today’s societies are the levels of violence against children in cyberspace.

In this sense, the analysis of the arguments produced by the courts of justice, *e.g.*, ECtHR, to offer a response to the problem raised and not just to adjust them to a normative response occupies a relevant place in the field of human rights. This becomes evident, especially, when the cases analysed by the courts refer to situations that place concepts or principles in tension that are characterised by their broad and abstract content, such as the protection of personal data.

### 3. Methodology: argumentation scheme

One way of illustrating the arguments, and then carrying out the analysis of the arguments, is by identifying the elements or parts that make it up. In this way it will be possible to observe the problem or type of problem raised in the case, the answers that were given and the reasons that led to obtaining a certain judicial decision. That is, the representation of the argumentation is an instrument to understand the justification of the decision from a series of elements that make up the structure of a judicial decision. The following elements can be considered the most important, as shown in table 1:

**Table 1.** Parts of an argument

Elements	Description
Facts	The facts of the case. <i>i.e.</i> , what has happened in the social and institutional world and that has led to the appearance of a legal problem.
Issue	Where does the argument start? That is, the translation of the above into the code (usually binary) characteristic of the judicial resolution of conflicts. For example: in view of the decision of the trial court, of the appeal documents, etc., should the sentence be ratified or not? Should Article A of Law L be declared unconstitutional or void? etc.
Question	For example: how to interpret such an Article of such a law? Should such a fact be considered proven?
Holding	Answer to the issues raised in the case. For example: Article A must be interpreted in the sense S; fact H is taken for granted.

---

[int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b](https://www.unio-eu.org/int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b).

Rationale	Rationale on which the previous answers are based. Here it is important to distinguish between the <i>rationes decidendi</i> and the <i>obiter dicta</i> , that is, between the reasons that the judge or the court considered essential to conform the premises (normative and/or factual) of the internal justification; and another series of reasons, of arguments, that appear in the motivation, but that did not play that role.
Judgment	The closing of the initial question. For example: the sentence must be ratified; Article A of law L must be declared constitutional (or must be declared constitutional but understood the expression E in the sense S).
Decision	For example: the sentence of court T is ratified; The constitutionality of the Article is declared according to Law L.

*Source:* elaborated by the author based on Atienza.<sup>15</sup>

The search for an answer to obtain the solution of a case is an activity reserved to judges, courts or other justice bodies, through the development of arguments aimed at solving problems concerning questions of fact or law. For an exhaustive analysis of this problem, a judgment of the ECtHR was selected with the aim of identifying the arguments used by the Court in its decisions on the protection of personal data in the field of children's rights.

#### 4. Analysis of the judgment in the case of *K.U. v. Finland*

The judgment of the ECtHR in *K.U. v Finland* refers to the protection of a child's personal data and the responsibility of the State to adopt adequate protection measures. According to the facts of the case, an unidentified person placed an advertisement on an Internet dating site in the name of the applicant, who was 12 years old at the time, without his knowledge. The advertisement mentioned his age, a detailed description of his physical characteristics, and a link to his web page, which showed his picture, as well as his telephone number. After becoming aware of the advertisement on the Internet, the police were requested to identify the person who had placed the advertisement in order to bring charges against that person. However, the service provider refused to divulge the identity of the owner of the IP used, due to the confidentiality of telecommunications established by law. In this same sense, the Court of First Instance held that there was no express legal provision that authorised a order to the service provider to reveal telecommunications identification data in breach of professional secrecy.

<sup>15</sup> Manuel Atienza, *Curso de argumentación jurídica* (Madrid: Editorial Trotta, 2013), 430-431.

**Table 2.** Parts of an argument – Judgment in the case of *K.U. v. Finland*

Elements	Description
Facts	An advertisement was placed on an internet dating website in the name of a 12-year-old boy without his knowledge. It mentioned his age, telephone number and physical description and contained a link to a web page containing his picture. The advertisement was of a sexual nature, suggesting that the boy was looking for an intimate relationship with a boy of his age or older. The internet provider could not divulge the identity of the person who placed the advertisement because of the legislation in place. The applicant claimed that the national legislation did not provide sufficient protection against the actions of the individual who published incriminating data on the internet about his person.
Issue	The case concerns to the children’s rights to privacy and data protection on internet
Question	In the present case, has there been a violation of Article 8 (Right to respect for private and family life) of the ECHR?
Holding	<p>1. The positive obligations, inherent in Article 8 of the Convention, may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. The choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State’s margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions.<sup>16</sup></p> <p>2. The States have a positive obligation to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution. Where the physical and moral welfare of a child is threatened, such injunction assumes even greater importance. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives.<sup>17</sup></p> <p>3. The Court considers that although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.<sup>18</sup></p>

<sup>16</sup> Cf. Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 42-43, <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-89964%22%5D%7D>.

<sup>17</sup> Cf. Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46.

<sup>18</sup> Cf. Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 49.

Rationale	To verify the violation of privacy and protection of personal data, in which the victim is a child, the Court justified its responses based on regulations from the Council of Europe, the United Nations and the European Union. Regarding the arguments produced by the Court, these refer, mainly, to positive obligations inherent in an effective respect for private life.
Judgment	The EctHR held that the positive obligation not only to criminalise offences but also to effectively investigate and prosecute them assumes even greater importance when the physical and moral welfare of a child is threatened. In this case, the EctHR found that by being exposed as a target for paedophilic approaches on the internet the child's physical and moral welfare was threatened. Therefore, the State did not put in place a system to protect child victims from being exposed as targets for paedophilic approaches via the Internet.
Decision	The Court finds that there has been a violation of Article 8 of the Convention in the present case.

*Source:* elaborated by the author based on the judgment in the case of *K.U. v. Finland*.

In the instant case, the EctHR focused its analysis on verifying the protection measures adopted by the State to prevent violations against the private life of individuals, specifically, the protection of personal data in the digital environment. To this end, the argument was structured around three topics: (i) respect for private life; (ii) criminal-law provisions; and (iii) positive obligations.

According to the Court, respect for private life includes the protection of the physical and moral integrity of the person, which can be aggravated when it comes to individuals in a situation of vulnerability. In the present case, this is configured in the potential threat against the physical and mental well-being of a child. Although the purpose of Article 8 of the ECHR is protection against arbitrary interference by public authorities – a negative obligation –, the ECtHR also highlights the importance of the positive obligations mentioned in the norm. The determination of the most appropriate measures will depend on the particular situation of the problem, as well as on the means that the State considers most appropriate to guarantee respect for the private life of individuals. However, when it comes to situations that put fundamental values and essential aspects of private life at risk, the ECtHR considers it necessary to establish legal provisions to combat these conducts, because “[t]he limits of the national authorities’ margin of appreciation are nonetheless circumscribed by the Convention provisions”.<sup>19</sup>

In the present case, although the State recognised the legal impossibility of requiring the operator of the Internet server to provide information about the author of the publication, it also argued that the victim had legal protection. “[...] by the mere existence of the criminal offence of malicious misrepresentation and by the possibility of bringing criminal charges or an action for damages against the server operator”.<sup>20</sup> Nevertheless, for the ECtHR “the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice”.<sup>21</sup> Consequently, the effectiveness of

<sup>19</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 44.

<sup>20</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46.

<sup>21</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46.



a protection measure must consist of an adequate regulation of conduct that can identify the perpetrator of the crime, especially when the victim is a child or other vulnerable individual(s).

Lastly, with regard to positive obligations, the Court considers that these “[...] *must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator*”,<sup>22</sup> in addition to, “*ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice*”.<sup>23</sup>

In the present case, the Court concluded that the State had failed in its positive obligation, because internal legislation has not provided an adequate regulatory framework to balance competing rights: protection of personal data and respect for private life. According to the ECtHR “*such framework was not in place at the material time, with the result that Finland’s positive obligation with respect to the applicant could not be discharged*”.<sup>24</sup>

In the case analysed, the Court concluded that the State did not adopt positive measures to protect child victims from being exposed as targets for paedophilic approaches via the Internet. The ECtHR recognises the difficulties presented by the adoption of these measures in the digital environment;<sup>25</sup> however, it also held that child sexual abuse is not a recent problem, and consequently, the State should have a system capable of identifying and prosecuting the person who had placed the advertisement on the internet.

Although the ECtHR’s decision does not specify the content of the protection measures in the digital environment aimed at children, they may consist of legislative, administrative and preventive measures.<sup>26</sup> Likewise, these could be grouped into the following types: (i) measures to address risks in the digital environment, protection and awareness-raising measures; and (ii) measures regarding child sexual abuse material.<sup>27</sup> About the last group, the Consultative Committee of Convention 108+ points out that: “*States should engage with business enterprises to provide assistance, including as appropriate technical support and equipment, to law-enforcement authorities to support the identification of perpetrators of crimes against children and collect evidence required for criminal proceedings*”.<sup>28</sup>

In the present case, the ECtHR held that “*users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected*”, but also that “*such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others*”.<sup>29</sup> In this regard, among the dangers that threaten children on the Internet, the following can be mentioned: “*grooming, bullying, harassment and stalking, or the recruitment of children for human trafficking, or the exploitation of minors for prostitution and*

<sup>22</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 48.

<sup>23</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 48.

<sup>24</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 49.

<sup>25</sup> See Lawrence Lessig, *Code: version 2.0* (New York: Basic book, 2006): 123.

<sup>26</sup> See also United Nations, General Comment No. 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021.

<sup>27</sup> Council of Europe, Committee of Ministers, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Recommendation CM/Rec(2018)7, recital 20 - 21.

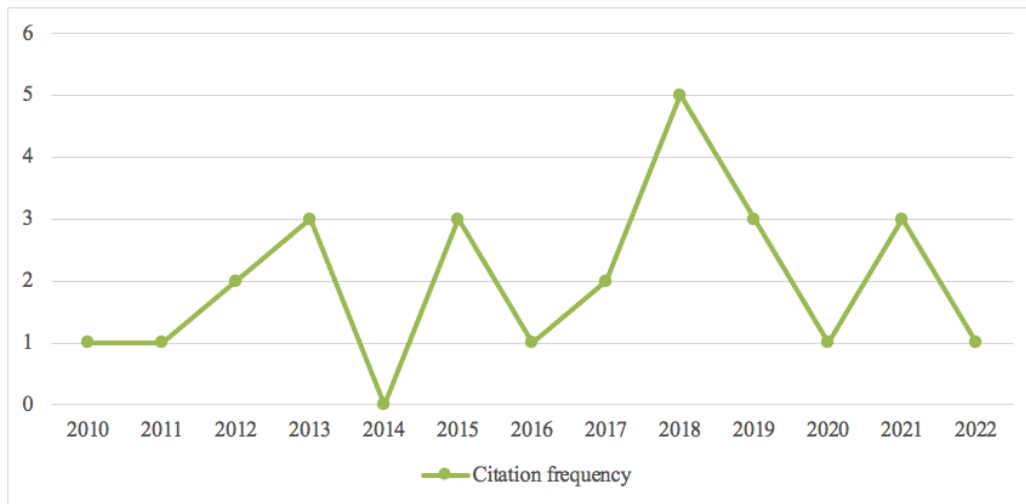
<sup>28</sup> *Idem* recital 63.

<sup>29</sup> Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 49.

*pornography*".<sup>30</sup> However, on multiple occasions, the situations described go beyond the geographical barriers of the States, thus requiring a broader spectrum of protection to combat this type of problem. Hence, the need to adopt different types of protection measures to protect children's rights.

### 5. Impact of the case on the ECtHR's case-law

To determine the use of the arguments identified in the analysed case, a search was carried out in the ECtHR database between the years 2010 and 2022. As a result, 25 (twenty-five) judgment of the Court were found that refer to the case of *K.U. v. Finland*. The frequent use of the decision in this period of time allows us to infer about its relevance for the ECtHR in the argumentative process on cases that address problems related to the protection of personal data.



**Figure 1.** Citations frequency of the ECtHR to the judgment in the case of *K.U. v. Finland* during the years 2010 - 2022.

*Source:* elaborated by the author

The analysis of the case, based on the argumentation scheme, allowed us to determine that the ECtHR's arguments were structured around the following topics: respect for private life, criminal-law provisions, and positive obligations. These topics were also identified in ECtHR's jurisprudence through the citations to the case of *K.U. v. Finland*.

<sup>30</sup> González Tascón, María Marta, "El nuevo delito de acceso a niños con fines sexuales a través de las TIC", *Estudios Penales y Criminológicos* 31, no. 1 (May 2012): 210.

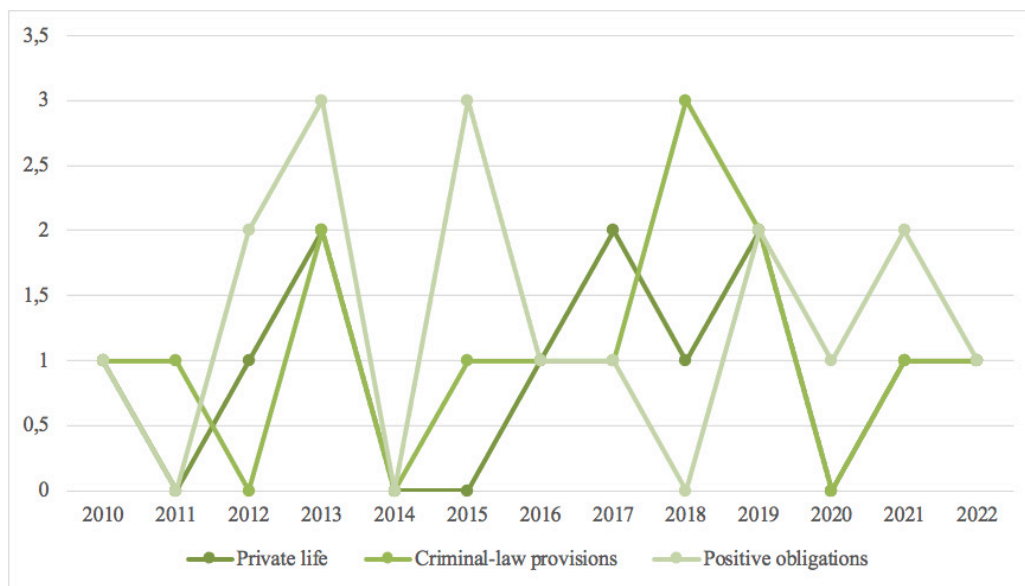


Figure 2. Use of the topics cited in the case-law of the ECtHR.

Source: elaborated by the author

The justification of decisions through the citations of their own cases is a frequent activity in international courts of justice. Yonatan Lupu and Erik Voeten understand that “ECtHR judges cite precedent at least in part to provide strategic legitimation for their decisions”.<sup>31</sup> Regarding the content of the citations, from these topics, in the decisions that refer to the case of *K.U. v. Finland*, these are distributed as follows:

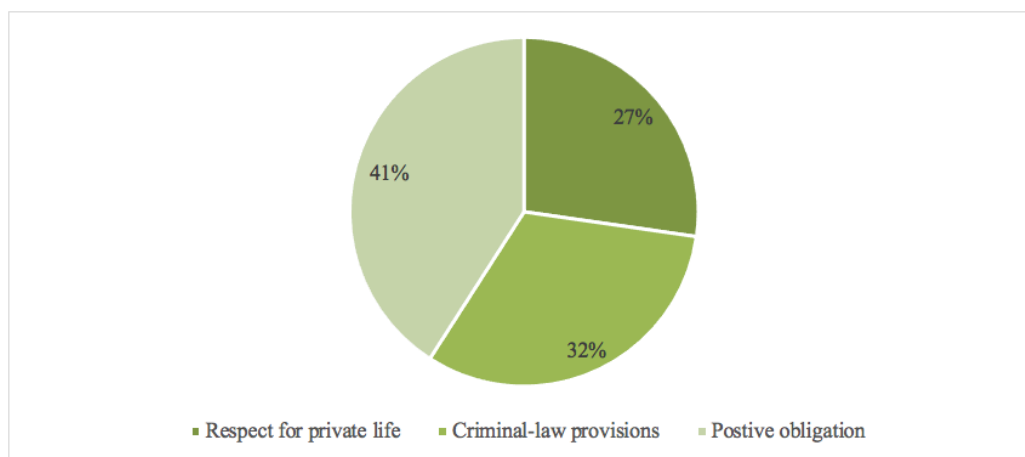


Figure 3. Topics mentioned in the jurisprudence of the ECtHR, from the judgment in the case of *K.U. v. Finland*.

Source: elaborated by the author

Regarding the development of these issues in the sentences identified, for the purposes of this investigation, it is appropriate to point out the use given to the arguments from the case of *K.U. v. Finland* on issues affecting children’s rights and their protection in the digital environment. For example, in the case of *Volodina v. Russia*, it has been pointed out that respect for private life includes protection

<sup>31</sup> Yonatan Lupu and Erik Voeten, “Precedent in International Courts: A Network Analysis of Case Citations by the European Court of Human Rights”, *British Journal of Political Science* 42, no. 2 (2012): 438, <https://doi.org/10.1017/S0007123411000433>.

against forms of online violence, and that, therefore, “[t]he 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”.<sup>32</sup> For this reason, it is common to observe in the jurisprudence of the Court on the importance of protection measures, “for children and other vulnerable members of society to benefit from State protection”,<sup>33</sup> especially when their physical and moral well-being is threatened.

However, to ensure the protection of children’s rights in the digital environment, a wide range of measures is required, capable of responding to the multiple situations in which they find themselves. In *K.U. v. Finland*, the ECtHR concluded that civil law damages from an Internet service provider was an inadequate measure of protection because there was no possibility of identifying the person who had posted the child personal data on a dating website, thus putting him at “risk of sexual abuse”.<sup>34</sup> Thus, in the case of *Benedik v. Slovenia*, the ECtHR noted that State obligations may include efficient criminal-law provisions, because “[c]hildren and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives, and that protection includes a need to identify the offenders and bring them to justice”.<sup>35</sup>

Likewise, in *K.U. v. Finland* the ECtHR’s observed the absence of adequate measures to protect the personal data of the victim, a twelve-year-old boy, because the State did not initiate an effective investigation due to the requirement of confidentiality of telecommunications. In this regard, in the case of *Delfi AS v. Estonia*, the ECtHR’s referred to the positive obligations of the State, through a regulatory framework, for the Internet service provider to disclose the information required for that purpose: “Although *K.U. v. Finland* concerned a breach classified as a criminal offence under the domestic law and involved a more sweeping intrusion into the victim’s private life than the present case, it is evident from the Court’s reasoning that anonymity on the Internet, while an important factor, must be balanced against other rights and interests.”<sup>36</sup>

In this way, in addition to illustrating the impact of the judgment on the ECtHR’s case-law, the identification of these topics makes it possible to observe more precisely how the ECtHR has made use of this precedent by citing its own

<sup>32</sup> Judgment *Case of Volodina v. Russia*, 14 December 2021, Application no. 40419/19, recital 48, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-211794%22%5D%7D>. See also Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 41.

<sup>33</sup> Judgment *Case of Wetjen and Others v. Germany*, 22 June 2018, Applications nos. 68125/14 and 72204/14, recital 74, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-181583%22%5D%7D>. See also Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46.

<sup>34</sup> Judgment *Case of Mosley v. the United Kingdom*, 15 September 2011, Application no. 48009/08, recital 120, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-104712%22%5D%7D>. See also Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46-47.

<sup>35</sup> Judgment *Case of Benedik v. Slovenia*, 24 July 2018, Application no. 62357/14, recital 99, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-182455%22%5D%7D>. See also Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 46.

<sup>36</sup> Judgment *Case of Delfi AS v. Estonia*, 16 June 2015, Application no. 64569/09, recital 149, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-155105%22%5D%7D>. See also Judgment *Case of Standard Verlagsgesellschaft mBH v. Austria*, 07 March 2022, Application no. 39378/15, recital 91, <https://hudoc.echr.coe.int/eng#%7B%22tabview%22:%5B%22document%22%2C%22itemid%22:%5B%22001-213914%22%5D%7D>; and Judgment *Case of K.U. v. Finland*, 02 June 2009, Application no. 2872/02, recital 49.

arguments in their subsequent decisions. Likewise, the frequent use of these topics in the case-law of the ECtHR allows us to infer the importance that they acquire for the analysis of problems related to data protection. In the same way, when the protection of personal data involves other issues such as online child sexual exploitation, the Court understands that the adoption of protection measures designed to secure respect for private life, even in the sphere of the relations of individuals between themselves, constitute the most adequate response that must be given by the State.

## 6. Conclusion

Crimes that refer to sexual violence are generally regulated within internal legal systems, such as sexual assault, sexual abuse, rape, and others. But as happened in *K.U. v. Finland*, due to the impact of technologies, new forms of these crimes have appeared that need to be regulated to ensure the protection of children's rights. As indicated in the arguments of the Court, this situation obliges States to update their internal regulations accompanied by an effective protection system and a series of regional and international guidelines to combat this problem.

However, this context also raises the dilemma about internet regulation, the need to balance rights and the protection of children in the digital environment. In the case analysed, the ECtHR understood that the violation of rights against children in the digital environment derives from the absence or failure to adopt protection measures by the State, since the victim was exposed as a target for paedophilic approaches on the internet. Also, it was highlighted that the positive obligation consists not only to criminalise offenses but also to effectively investigate and prosecute, especially when the physical and moral welfare of a child is threatened.

Finally, in the case of *K.U. v. Finland*, it is observed that the ECtHR's arguments were structured around the following topics: (i) respect for private life; (ii) criminal-law provisions; and (iii) positive obligations, which are frequently cited by the Court to justify their own decisions. The use of these topics in the case-law of the ECtHR demonstrates its relevance for the elaboration of arguments when the problems refer to personal data protection.