

DSA implementation: legal and policy framework on illegal and harmful content online

Country: Portugal

Contractor: Centre for Social Studies

Authors: Diana Barros and João Paulo Dias

Disclaimer

This document was commissioned under contract as background material for a comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project 'Illegal and other harmful content online – safeguarding fundamental rights and freedoms with respect to the DSA.' The information and views contained in the document do not necessarily reflect the views or the official position of FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

Contents

1. National definitions of illegal content online.....	3
2. National policy initiatives and measures for protecting children and young adults online	16

1. National definitions of illegal content online

Table 1. Legislation (maximum 500 words in total)

Type of content	Applicable Law	Legal definition	Penalties/actions
Defamation	There is no specific law regarding defamatory content. However, there are provisions on general laws that define and punish defamation and defamatory content. - Criminal Code Portugal, Decreto-Lei 48/95, que aprova o Código Penal (Decree-Law 48/95, which approves the Criminal Code), 15 March 1995.	Article 180 of the Criminal Code states that anyone who, when addressing a third party, accuses another person (even as a suspicion) of a fact or makes a judgment about them that harms their honour or reputation, or repeats such an accusation or judgment, is committing a crime of defamation. Although this refers to verbal defamation, Article 182 of the Criminal Code establishes that defamation committed in writing, through gestures, images, or any other form of expression is also treated the same as verbal defamation. Article 183 (a) of the Criminal Code establishes that if the offence of defamation is committed through means or in circumstances that facilitate its dissemination (such as online/digital contexts), the penalty applicable can be aggravated. The Criminal Code also criminalises additional behaviours associated with defamatory content that can be applied to digital/online contexts.	Article 180 (1) of the Criminal Code establishes that the crime of defamation is punishable by up to six months of imprisonment or a fine up to 240 days. However, if the offense is committed through means or in circumstances that facilitate its dissemination, the penalty is increased by one third of their minimum and maximum limits. If the offense is committed through the media, the perpetrator is punished with imprisonment of up to 2 years or a fine of not less than 120 days (Article 183 of the Criminal Code). Article 180 (2) (3) also establishes that the conduct is not punishable if the accusation was made to pursue legitimate interests and the person either proves the truth of the accusation or had a serious reason to believe it was true, acting in good faith. Nevertheless, this exemption does not apply when the accusation concerns someone's private or family life.

		Article 193 of the Criminal Code defines the offense of indecent exposure through the media, the Internet, or other means of public dissemination as the act of, without consent, sharing or contributing to the sharing of images, photographs, or recordings that violate a person's private life, particularly aspects related to family or sexual intimacy, using platforms such as the media, the Internet, or any other means capable of reaching a broad audience. Associated with this crime can also be the crime of invasion of privacy (Article 192 of the Criminal Code), which is defined as any act carried out without consent and with the intent to intrude upon the private life of another person, particularly their family or sexual intimacy. This includes: intercepting, recording, using, transmitting, or disclosing private communications, such as conversations, phone calls, or emails; capturing or sharing images of individuals or intimate objects and spaces; observing or eavesdropping on people in private settings; and disclosing personal information related to someone's private life or serious medical condition. Another crime that can be linked to defamation and defamatory content is foreseen in Article 199, which establishes the crime of illegal recordings and photographs. This provision	Article 193 of the Criminal Code establishes that the crime of indecent exposure through the media, the Internet, or other means of public dissemination can be punished with imprisonment up to five years. Article 192 of the Criminal Code foresees different penalties for different types of invasions of privacy. Conduct such as intercepting communications (conversations, phone calls, or emails) and observing or eavesdropping on people in private settings is punishable by up to one year of imprisonment or a fine of up to 240 days. More serious violations, such as capturing or sharing private images, or disclosing facts about someone's private life or serious medical condition, carry penalties of up to three years in prison or a fine. However, Article 192 (2) also establishes that conduct such as disclosing facts about someone's private life or serious medical condition is not punishable if done to serve a legitimate and significant public interest. Finally, Article 199 of the Criminal Code establishes that the conducts under the crime of illegal recordings and photographs are punishable by up to one year of imprisonment or a fine of up to 240 days.
--	--	--	--

		criminalises the unauthorised recording, photographing, or filming of individuals in situations that infringe upon their right to privacy. It covers conduct such as recording private conversations not intended for public disclosure (even when directed at the person making the recording) and using or allowing the use of such recordings without consent. It also criminalises photographing or filming someone against their will, even at events where the individual is legitimately present, as well as the use or distribution of those images, regardless of how they were obtained.	
Self-harm promotion (or giving instructions how to)	Although the acts of promoting, inciting, or aiding suicide are explicitly criminalised under Articles 135 and 139 of the Criminal Code, the promotion or incitement of non-fatal self-harm (such as cutting or other forms of self-injury not intended to cause death/suicide) is not directly covered by these provisions or any other specific provisions in the Criminal Code or in any other law. However, general provisions related to harassment may apply if the conduct is repetitive and causes fear, distress, or impairs	Article 154-A of the Criminal Code provides that whoever repeatedly follows or harasses another person, directly or indirectly, by any means, in a manner likely to cause fear, distress, or impair the victim's freedom of decision, is committing a crime of harassment. The conduct must be ongoing and capable of interfering with the victim's personal autonomy or/and well-being. Additionally, it should be noted that Article 154-A explicitly allows for the offence to be committed "by any means", which includes online or digital contexts or contents. Article 155(1) (b) foresees that if the crime of harassment is committed against a person who is particularly defenceless due to age, disability, illness or pregnancy, then the penalty can be	According to Article 154-A (1) of the Criminal Code, the crime of harassment is punishable by up to 3 years of imprisonment or a fine, unless a more severe penalty applies under another legal provision (for example, if the behaviour can also be classified as a crime of threat, coercion or even defamation). Additional penalties may also be imposed, including restraining orders (lasting from six months to three years) and mandatory participation in behavioural intervention programmes [Article 154-A (3)]. Article 155 (1) (b) and (2) of the Criminal Code further establishes that if the crime of harassment is committed against a person who is particularly defenceless due to age, disability,

	someone's freedom of decision-making. - Criminal Code Portugal, Decreto-Lei 48/95, que aprova o Código Penal (Decree-Law 48/95, which approves the Criminal Code), 15 March 1995.	aggravated. The penalty can also be aggravated if, as a result of the harassment, the victim or the person against whom the harm is directed commits or attempts to commit suicide [Article 155(2)].	illness or pregnancy, or if, as a result of the harassment, the victim or the person against whom the harm is directed commits or attempts to commit suicide, then the penalty can be aggravated. In these cases, the conduct is punishable with imprisonment of 1 to 5 years.
Body shaming and promotion of eating disorders	Body shaming and the promotion of eating disorders are not explicitly inscribed in any Portuguese law. However, as is the case with self-harm, general legal provisions in the Criminal Code, particularly those related to harassment, may apply if the behaviour is repetitive and causes fear, emotional distress, or interferes with the victim's freedom of decision-making. - Criminal Code Portugal, Decreto-Lei 48/95, que aprova o Código Penal (Decree-Law 48/95, which approves the Criminal Code), 15 March 1995.	Article 154-A of the Criminal Code provides that whoever repeatedly follows or harasses another person, directly or indirectly, by any means, in a manner likely to cause fear, distress, or impair the victim's freedom of decision, is committing a crime of harassment. The conduct must be ongoing and capable of interfering with the victim's personal autonomy or/and well-being. Additionally, it should be noted that Article 154-A explicitly allows for the offence to be committed "by any means", which includes online or digital contexts or contents. Article 155(1) (b) foresees that if the crime of harassment is committed against a person who is particularly defenceless due to age, disability, illness or pregnancy, then the penalty can be aggravated. The penalty can also be aggravated if, as a result of the harassment, the victim or the person against whom the harm is directed	According to Article 154-A (1) of the Criminal Code, the crime of harassment is punishable by up to 3 years of imprisonment or a fine, unless a more severe penalty applies under another legal provision (for example, if the behaviour can also be classified as a crime of threat, coercion or even defamation). Additional penalties may also be imposed, including restraining orders (lasting from six months to three years) and mandatory participation in behavioural intervention programmes [Article 154-A (3)]. Article 155 (1) (b) and (2) of the Criminal Code further establishes that if the crime of harassment is committed against a person who is particularly defenceless due to age, disability, illness or pregnancy, or if, as a result of the harassment, the victim or the person against whom the harm is directed commits or attempts

		commits or attempts to commit suicide [Article 155(2)].	to commit suicide, then the penalty can be aggravated. In these cases, the conduct is punishable with imprisonment of 1 to 5 years.
Suicide promotion	There is no specific law regarding the promotion of suicide. However, the Criminal Code includes provisions related to promoting suicide. - Criminal Code Portugal, Decreto-Lei 48/95, que aprova o Código Penal (Decree-Law 48/95, which approves the Criminal Code), 15 March 1995.	Under Article 135 of the Criminal Code, any person who incites another to commit suicide or assists in its execution commits the crime of incitement or assistance to suicide if the suicide is actually attempted or committed. If the person incited or assisted is under 16 years old or has a significantly diminished capacity for judgment for any reason, the penalty can be aggravated. Additionally, Article 139 criminalises the promotion of suicide, specifically through the advertising or promotion of a product, object, or method presented as a means of causing death, in a way that is likely to provoke suicide. Therefore, under the Criminal Code, the acts of promoting, inciting, or aiding suicide are all explicitly criminalised. In both provisions, the law does not expressly refer to an online element, but it can be applied to an online context and content.	Article 135 (1) of the Criminal Code states that whoever commits a crime of inciting or assisting suicide is punished with imprisonment of up to 3 years, if the suicide is actually attempted or consummated. Where the person incited or assisted is under 16 years old or has a significantly diminished capacity for judgment for any reason, the perpetrator shall be sentenced to imprisonment for between 1 and 5 years [Article 135(2)]. At the same time, Article 139 (1) of the Criminal Code establishes that whoever commits the crime of promoting suicide is punished with imprisonment of up to two years or a fine of up to 240 days. Although the acts of inciting, assisting, or promoting suicide are all criminalised, an exception to this general prohibition is established in the case of medically assisted death.
Other – please indicate here any other relevant legislation that addresses the protection of	There is some relevant legislation that addresses the protection of children and young adults in online spaces.	The Law for the Protection of Children and Young People in Danger defines how the State intervenes to protect the rights, safety, and well-being of children and young people facing situations of risk. While the law does not explicitly refer to online/digital contexts, its	Article 35 of the Law for the Protection of Children and Young People in Danger outlines the promotion and protection measures that can be applied in situations where a child or young person is considered to be in danger. These include support for parents or relatives

children and young adults online, in case this was not referenced under a) and b).	- Law for the Protection of Children and Young People in Danger Portugal, Lei 147/99, que estabelece a Lei de proteção de crianças e jovens em perigo (Law 147/99, which establishes the Law for the Protection of Children and Young People in Danger), 1 September 1999. - Personal Data Protection Act Portugal, Lei 58/2019, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Law 58/2019, which ensures the implementation, in national law, of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons	broad interpretation of "danger" enables its application to those contexts. Article 3(2) outlines the circumstances under which a child or young person is considered to be at risk. Among these are exposure to behaviours that seriously compromise their safety or emotional well-being, as well as the engagement in harmful behaviours without appropriate intervention by their parents or legal guardians [Article 3 (2) (f) (g)]. The Personal Data Protection Act, Article 16 establishes that children's personal data may only be processed on the basis of the consent provided for in Article 6(1)(a) of the General Data Protection Regulation and relating to the direct provision of information society services when they have reached the age of 13. If the child is under 13 years of age, processing is only lawful if consent is given by their legal representatives, preferably using secure authentication methods. Decree-Law 7/2004 establishes that intermediary network service providers are not required to monitor the information they transmit or store or to investigate possible offences committed within their scope (Article 12). However, according to Article 13, they are under the obligation: to immediately inform the competent authorities: when they become	through psychosocial, educational, and financial aid, as well as parental education programmes. Where necessary, children may be placed with a trusted non-relative or receive support for independent living, particularly if over 15. If staying at home is not safe, the law allows for placement in foster care or residential care facilities, with emergency placements available in urgent situations. All measures aim to protect the child's well-being and promote their development. Article 38 of the Personal Data Protection Act establishes that violations of the provisions of Article 8 of the GDPR, which concerns the processing of children's personal data, are considered serious administrative offences and are subject to significant fines depending on the type of offender. For large companies, fines range from €2,500 to €10,000,000 or up to 2% of the annual worldwide turnover, whichever is higher. Small and medium-sized enterprises (SMEs) may face fines ranging from €1,000 to €1,000,000 or up to 2% of their annual global turnover, whichever amount is greater. In the case of natural persons, the fines range from €500 to €250,000. Decree-Law 7/2004 establishes in its Article 18 a provisional dispute resolution mechanism according to which, following a complaint,
---	---	---	--

	with regard to the processing of personal data and on the free movement of such data), 8 August 2019. - Decree-Law 7/2004, of 7 January Portugal, <u>Decreto-Lei 7/2004, que no uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno</u> (Decree-Law 7/2004, which, using the legislative authorisation granted by Law 7/2003 of 9 May, transposes into national law Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular	aware of illegal activities carried out through the services they provide; to comply with requests to identify service recipients with whom they have storage agreements; to comply promptly with orders to prevent or end an infringement, in particular to remove or disable access to information; and to provide lists of owners of sites they host, when requested to do so. Article 19º-A further establishes that intermediary network service providers, shall also immediately inform the Public Prosecutor's Office of the detection of content made available through the services they provide whenever the availability of such content, or access to it, may constitute a crime, namely child pornography, discrimination and incitement to hatred and violence or, if there is a report from the victim or third parties that contributes to the indication of unlawful conduct, invasion of sexual or bodily privacy. Regarding media content, the Television Law establishes in its Article 27 that the programming of audio-visual media services must respect the dignity of the human person, the specific rights of children and young people, as well as fundamental rights, freedoms and guarantees. Therefore, audio-visual media services may not, through their programme elements, incite violence or hatred against groups of people or members of such groups on the grounds of sex, race, colour or ethnic or	intermediary service providers can appeal to the supervisory body, which must provide a provisional solution within 48 hours and then communicate it electronically to the involved parties. Anyone who has a legal interest in maintaining that content online may, under the same terms, appeal to the supervisory body against a decision by the provider to remove or disable access to that content, in order to obtain a provisional solution to the dispute. The supervisory body may at any time amend the provisional settlement of the dispute. The final settlement of the dispute is carried out under the terms and through the ordinary channels, which means that it will be up to the courts to decide on the final decision. However, simultaneously, the involved parties, including intermediary network service providers, can also resort to common judicial means, namely courts, without mobilising Article 18. In some instances, however, intermediary service providers have an immediate duty to block content on their platforms. Article 19-B establishes that intermediary network service providers are obligated to ensure, within 48 hours, the blocking of sites identified as containing child pornography or related material and, at the request of the victim or third parties contributing to the reporting of unlawful conduct, sexual or bodily intimacy or
--	--	---	--

	electronic commerce, in the Internal Market), 7 January 2004. - Television Law Portugal, Lei 27/2007, que aprova a Lei da Televisão, que regula o acesso à actividade de televisão e o seu exercício (Law 27/2007, approving the Television Law, which regulates access to and the exercise of television activity), 30 July 2007. - Law 74/2020, of 19 November Portugal, Lei 74/2020, que transpõe para a ordem jurídica interna a Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, alterando a Lei 27/2007, de 30 de julho, que aprova a Lei da Televisão e dos Serviços Audiovisuais a Pedido, e a Lei 55/2012, de 6 de setembro, relativa ao fomento, desenvolvimento e proteção da arte do cinema e das atividades cinematográficas e audiovisuais (Law 74/2020, which transposes into national law Directive (EU)	social origin, genetic characteristics, language, religion or beliefs, political or other opinions, membership of a national minority, wealth, disability, age, sexual orientation or nationality. At the same time, Article 69-A establishes that video-sharing platform providers shall take appropriate measures to protect: children and young people against programmes, user-generated videos and audio-visual commercial communications likely to harm their integral physical, mental or emotional development; the general public, against programmes, user-generated videos and audio-visual commercial communications containing incitement to violence or hatred against groups of persons or members of such groups on any of the grounds referred to in Article 27 (mentioned above). It should be noted that both provisions on Article 27 and Article 69-A stem from the changes made to the Television Law in the process of transposing the Audiovisual Media Services Directive into the national legal order (through Law 74/2020). However, it should also be noted that Article 27, even before the amendments introduced by the Audiovisual Media Services Directive, already provided safeguards for the protection of children and young people, which were reinforced during the transposition process.	related material, through a transparent procedure with adequate safeguards, in particular ensuring that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restrictions. This blockage can also be challenged in court. Still, according to Decree-Law 7/2004, the supervisory bodies, both the National Communications Authority (ANACOM - <i>Autoridade Nacional de Comunicações</i>) and the Media Regulatory Authority (ERC - <i>Entidade Reguladora para a Comunicação Social</i>), have the power (within their mandate): to initiate and carry out administrative offences and apply the fines foreseen; and to order the suspension of the activity of service providers in the event of serious irregularities and for reasons of urgency (article 36 (2) (d) (e)). Failure to remove or prevent access is an administrative offence punishable by fines between 5,000 and 100,000 euros (article 37 (2) (d) (e)). The Television Law foresees that the Media Regulation Authority must encourage video-sharing platform providers to adopt co-regulation and self-regulation mechanisms. Therefore, Article 69-C establishes that video-sharing platform providers are required to adopt a range of measures aimed at protecting users, particularly children and young people. These include: incorporating the relevant legal
--	--	--	---

	2018/1808 of the European Parliament and of the Council of 14 November 2018, amending Law 27/2007 of 30 July, which approves the Law on Television and On-Demand Audiovisual Services, and Law 55/2012 of 6 September on the promotion, development and protection of the art of cinema and cinematographic and audiovisual activities), 19 November 2020.	Therefore, currently, Article 27(3) prohibits the broadcasting, on free-to-air services, of programmes that could seriously and gravely harm the development of children and young people, violate their privacy, or contain pornography or gratuitous violence. Article 27(4) and (5) allow the broadcast of other programmes that may negatively influence the personality development of children and young people only during late-night hours (either between 22:30 and 06:00 or, in stricter cases, between 00:00 and 06:00) and require the permanent display of an appropriate visual identifier. Finally, Article 27(6) provides that on-demand audiovisual services must also display a permanent warning for such content and adopt technical measures enabling parents or guardians to block access by children and young people.	restrictions into their terms and conditions and ensuring their enforcement; providing tools for uploaders to declare whether their videos contain audiovisual commercial communications; establishing transparent and user-friendly mechanisms for the public to report, flag and classify harmful content, and informing users of the follow-up given to such reports; implementing age-verification systems and parental controls to protect children from content that could harm their physical, mental or moral development; creating effective and accessible complaint-handling procedures regarding these protective measures; and promoting media literacy by raising user awareness of these tools and safeguards. Additionally, Article 69-F establishes that video-sharing platform providers also have to create alternative dispute resolution mechanisms available to users who share videos generated by them on video-sharing platform services, as well as to the public, with respect for the fundamental rights of all the persons involved. The applicable regulations are published on the platform's Internet portal, and the exercise of rights does not require the appointment of a lawyer. The costs of using those mechanisms are borne entirely by the video-sharing platform providers, and these costs can only be claimed from the counterparty when litigation is
--	---	--	---

			pursued in bad faith. Alternatively, video-sharing platform providers can also join an arbitration centre to solve all disputes through arbitration. Moreover, all interested parties can additionally mobilise ordinary judicial courts to obtain a solution to the conflict. It should be noted that both provisions of Article 69-C and Article 69-F stem from the changes made to the Television Law in the process of transposing the Audiovisual Media Services Directive into the national legal order (through Law 74/2020). Furthermore, breaches of the obligations under Article 27 can be subject to fines between €20,000 and €375,000, depending on whether the breach is considered a minor, serious or very serious administrative offence (Articles 75,76 and 77).
--	--	--	---

Table 2. Case-law (maximum 400 words in total for all cases identified)

It is important to note that the indicated ruling marks the first judicial decision in Portugal to specifically address cyberstalking, although the decision does not refer to the obligations of service providers. It also represents the heaviest sentence ever handed down in Portugal for the crime of harassment. This landmark judgment establishes a crucial legal precedent for combating harmful online behaviour. However, other significant cases involving illegal and damaging online content are also under investigation. In 2017, following several incidents of self-harm among teenagers, the Prosecutor General's Office (PGR – *Procuradoria Geral da República*) assigned the Central Department of Criminal Investigation and Prosecution (DCIAP – *Departamento Central de Investigação e Ação Penal*) to lead investigations into the so-called “Blue Whale” Challenge. Authorities suspected a connection between the challenge and the self-harming behaviour reported. At the time, the PGR affirmed its readiness to pursue all appropriate legal measures, including the potential blocking of online content¹. While some of the cases reported to the Public Prosecution were eventually closed, no further official details have been made public. More recently, the Commission for Citizenship and Gender Equality (CIG – *Comissão para a Cidadania e Igualdade de Género*) filed a criminal complaint against a Portuguese YouTuber known for spreading misogynistic content. CIG's interpretation of his comments on social media about abortion can be seen as hate speech. In June 2025, the Prosecutor General's Office confirmed that a formal investigation into this case had been opened².

Decision	Description
Deciding body (in original language)	Tribunal Judicial da Comarca de Lisboa
Deciding body (in English)	Lisbon District Court
Case number	Judgement 319/19.7JGLSB

¹ Público (2017), “[PGR admite bloqueio de links do jogo Baleia Azul](#)” (PGR admits blocking links to Blue Whale game”, 2 May 2017. RTP Notícias Online (2017), “[PGR entrega investigação Baleia Azul ao DCIAP e reforça equipas](#)” (PGR hands over Blue Whale investigation to DCIAP and reinforces teams), 5 May 2017.

² SIC Notícias (2025) “[Youtuber alvo de queixa no Ministério Público por "discurso de ódio" contra mulheres](#)” (Youtuber targeted by complaint to the Public Prosecutor's Office for ‘hate speech’ against women), 7 June 2025.

Parties	Singular person vs. Public Prosecutors' Office and other singular persons
Decision date	15-02-2025
Web link to the decision (if available)	Not applicable. Provided by one of the legal professionals involved in the case.
Circumstances of the case, legal questions and key facts (max. 100 words)	Over two years, A. stalked a colleague, along with some of her other colleagues, friends, and family members. A. created fake social media accounts in the victim's name and placed false orders (including from beauty stores, sex shops, etc.) and scheduled numerous medical consultations, always using the victim's email address to cause ongoing distress. A. systematically sent disturbing messages and emails, disseminated images of the victim across various locations (including the victim's university and relatives' workplaces), and made repeated attempts to change passwords to the victim's email, social media accounts, and academic platforms, targeting not only the victim but also her friends, colleagues, and family members. A. also used spoofing techniques to impersonate the victim and registered the victim's phone number on multiple platforms to ensure she was constantly harassed with calls and messages. In addition, A. also created a false obituary for the victim and distributed it widely, and also organised a fake fundraising campaign to send the victim to Wuhan during the COVID-19 pandemic. The harassment escalated to involve the victim's social and family circles. These individuals were also targeted with similar tactics, including threats of data leaks unless they cooperated, such as unfollowing the victim on social media or providing new contact details and photos of the victim. Friends and colleagues were intimidated to distance themselves from the victim or even participate in the smear campaign against her. The perpetrator also sent false and damaging information about the victim to her aunt and brother, and created false narratives, intending to cause professional harm to the victim's aunt and brother. All these actions were aimed at harassing and destabilising the victim, pressuring her to leave her educational institution. To cover her tracks, A. pretended to support the victim and falsely accused others of being responsible for the harassment she herself was carrying out. A. was accused of 140 crimes: stalking, coercion, threat, disturbance of private life, invasion of privacy, illegal recordings and photographs, defamation (and aggravated defamation), insult, false accusation, simulation of crime, computer falsehood and unauthorised access. The Court had to ascertain whether the conduct described met the elements of one or more criminal offences, and whether there was sufficient evidence to attribute responsibility to A.

Final decision (if pending, please indicate)- here indicate what the responsible Court decided.	The Court concluded that, based on the “extensive documentary evidence”, the conduct of A. was intentional, creating a constant environment of discomfort and fear, to destabilise the lives of the victim, her friends, and her family. At the same time, by inputting information she knew to be false into various computer systems A. intended for that false data to be perceived as accurate, despite knowing that the individuals involved had not subscribed to services, placed orders, or made any communications. This conduct deliberately interfered with the relationship between users and the administrators of websites, stores, and telecommunications platforms, which A. sought to influence and successfully did so. Furthermore, while pretending to assist the victim, A. falsely accused other colleagues of carrying out the very conduct she herself had committed, thereby misleading authorities and causing these individuals to be wrongfully investigated. As a result, the colleagues were formally involved in the proceedings and subjected to house searches, during which computers and mobile phones, essential to their personal and academic lives, were seized. The Court held that all of these actions amounted to the crimes of harassment, computer-related falsehood, and false accusation. The Court found, however, that the legal requirements for the crime of coercion were not met, since, despite the creation of a climate of fear and anxiety, there was no use of violence or threat of serious harm to compel specific behaviour, which is an essential element of that offence. Similarly, the elements of the offence of invasions of privacy were also not satisfied, as the photographs used had been taken in public social contexts and were already publicly available on the victim's own social media profiles. Furthermore, the data disclosed was not intimate or private but belonged to the victims' public sphere. The Court also noted that these actions were already encompassed within the offence of harassment. It should also be noted that due to the application of Law 38-A/2023³, a law that established a pardon of sentences and amnesty for offences on the occasion of World Youth Day in Portugal, A. was acquitted of 122 crimes out of the 140 she was charged with. Therefore, A. was sentenced to seven years and nine months in prison for 18 crimes, including stalking, computer falsehood, and slanderous accusations. The defendant was also ordered to pay €50,000 in damages, €30,000 of which is to be paid to the primary victim. She was also sentenced to an additional penalty of prohibition of contact with the victim and all persons involved, as well as attending a specific programme for the prevention of typical stalking behaviour.
--	--

³ Portugal, Lei n.º 38-A/2023, que aprova [Perdão de penas e amnistia de infrações](#), (which approves Pardon for penalties and amnesty for offenses), 2 August 2023.

2. National policy initiatives and measures for protecting children and young adults online

Table 3. National policy frameworks (maximum 500 words in total)

Policy framework	Does the policy define any types of illegal/harmful online content?	Description
Carta Portuguesa de Direitos Humanos na Era Digital (Portuguese Charter of Human Rights in the Digital Era), https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244, 17 May 2021	Addresses hate speech broadly, including prejudiced language related to gender, sexual orientation, and other aspects, although it does not define it.	The Portuguese Charter of Human Rights in the Digital Era defines a core set of rights for individuals within digital environments. This legal framework guarantees a range of civil liberties adapted to the digital era. However, it focuses more on establishing digital rights and freedoms rather than defining types of illegal/harmful online content. The Charter also places a duty on the State to promote digital literacy not only to combat disinformation, but also to encourage responsible internet use and foster a safe, inclusive digital environment, free from discrimination and digital crimes (which includes crimes linked to illegal/harmful content). It includes references to gender and sexual orientation, affirming protections against discrimination, but only indirectly addresses age. Nevertheless, it establishes in its Article 20 that children have the right to special protection and care necessary for their well-being and safety in cyberspace, and that they may freely express their opinions and have the freedom to receive and impart information or ideas, in accordance with their age and maturity. Regarding the use of digital platforms, Article 14 establishes that everyone has the right to: receive clear and straightforward information about the conditions for the provision of services when using platforms that enable information and communication flows; exercise on these

		platforms the rights guaranteed by this Charter and other applicable legislation; have their profile protected, including its recovery if necessary, as well as obtain a copy of their personal data in accordance with the law; and lodge complaints and resort to alternative mechanisms of conflict resolution in accordance with the law.
Criação do Grupo de Trabalho para a execução do Regulamento dos Serviços Digitais (Creation of the Working Group for the implementation of the Digital Services Regulation), https://diariodarepublica.pt/dr/detalhe/despacho/1747-2024-852762925 , 15 February 2024.	Not directly.	Order 1747/2024 established a temporary working group to align Portugal's legal framework with the EU Digital Services Act. Coordinated by the National Communications Authority, the group included representatives from the Media Regulatory Authority, the Inspectorate-General for Cultural Activities (IGAC - <i>Inspeção-Geral das Atividades Culturais</i>), and other public entities with relevant responsibilities under Article 2 (4) of the Regulation, as well as any additional bodies deemed appropriate for its implementation. The group was tasked with presenting a final report within 90 days, containing: an assessment of the legal and regulatory changes needed to implement the Digital Services Regulation in Portugal and to enable the effective exercise of the powers of the Digital Services Coordinator; and the identification of other competent authorities for the Regulation's purposes and a clear definition of their roles, ensuring close and effective cooperation with the Digital Services Coordinator. The report produced by the working group led to Draft Law 32/XVI/1st⁴, which was submitted to Parliament in November 2024 and initially approved in the general voting; however, due to the dissolution of the Parliament, the Draft Law was considered to have expired in March 2025.

⁴ Portugal, [Proposta de Lei 32/XVI/1, que assegura a execução, na ordem jurídica interna, do Regulamento \(UE\) 2022/2065, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE](#) (Draft Law 32/XVI/1, which ensures the implementation, in the domestic legal order, of Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC), 4 November 2024.

Decreto-Lei 20-B/2024, que designa as autoridades competentes e o coordenador dos serviços digitais em Portugal (Decree-Law 20-B/2024, designating the competent authorities and the coordinator of digital services in Portugal), https://diariodarepublica.pt/dr/detalhe/decreto-lei/20-b-2024-852994087 , 16 February 2024.	Not directly.	With the approval of the Digital Services Regulation Decree-Law 20-B/2024, it was defined that the National Communications Authority is the competent authority and coordinator of the digital services in Portugal, while the Media Regulatory Authority is the competent authority for social communication and other media content.
Estratégia Única dos Direitos das Crianças e Jovens 2025-2035 (Single Strategy for Children and Young People's Rights 2025-2035), https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/34-2025-909307237 , 28 February 2025	Not directly.	Cybersecurity is one of the key strategic areas of the Single Strategy for Children and Young People's Rights 2025-2035, with a strong focus on safeguarding users, particularly children and young people. This area sets out goals, including promoting digital literacy, encouraging the safe and responsible use of technology, and ensuring the ethical application of artificial intelligence. These objectives aim to empower children and young people, bridge digital divides, and create a safer and more inclusive digital environment.

Table 4. Specialised authorities, bodies on protection of children and/or youth online which are not the DSA Coordinator (maximum 100 words)

Name of the authority/body	Website
Centro Internet Segura (Safe Internet Centre) Public initiative dedicated to promoting safe and responsible internet use. It is coordinated by the National Cybersecurity Centre (CNCS - <i>Centro Nacional de Cibersegurança</i>) in collaboration with various partners, including the Portuguese Institute of Sport and Youth (IPDJ - <i>Instituto Português do Desporto e Juventude</i>), the Foundation for Science and Technology (FCT - <i>Fundação para a Ciência e a Tecnologia</i>), the Directorate-General for Education (DGE - <i>Direção-Geral da Educação</i>), the Portuguese Association for Victim Support (APAV - <i>Associação Portuguesa de Apoio à Vítima</i>), and Microsoft Portugal. It offers educational resources, awareness campaigns, and support services for children, youth, and parents. The site also provides tools to report harmful online content and encourages youth participation in digital safety initiatives, helping create a safer online environment.	https://www.internetsegura.pt/
Entidade Reguladora para a Comunicação Social - ERC (Media Regulatory Authority) (regarding media content) Regulatory authority that is responsible for ensuring freedom of information and press, safeguarding media pluralism and independence from political and economic influence, protecting rights and freedoms, promoting diverse opinions, and overseeing political response and airtime rights. It also monitors market fairness in collaboration with the competition authority, contributes to spectrum planning, ensures state and local advertising complies with impartiality principles, and enforces media regulations.	https://www.erc.pt/pt/
Comissão Nacional de Promoção dos Direitos e Proteção das Crianças e Jovens – CNPDPCJ (National Commission for the Promotion of the	https://www.cnpdpj.gov.pt/inicio

Rights and Protection of Children and Young People) (if the child/young person is in a dangerous situation) Entity responsible for coordinating, monitoring, and evaluating actions to promote and protect the rights of children and young people. Its mandate includes advising on legislation, allocating resources, facilitating collaboration among local commissions, public services, and private organisations, commissioning studies, and overseeing the implementation of the UN Convention on the Rights of the Child. The Commission also supports, trains, audits, and provides guidance to Local Commissions for the Protection of Children and Young People and ensures effective cooperation among entities involved in child welfare.	
Comissão Nacional de Proteção de Dados – CNPD (National Data Protection Commission) (regarding data protection) Entity tasked with overseeing compliance with the GDPR and national data protection laws. It safeguards individuals’ rights and freedoms in personal data processing, provides non-binding opinions on legislation, supervises and enforces data protection compliance, maintains high-risk processing lists, develops accreditation criteria for monitoring and certification bodies, and coordinates with national and European institutions to ensure consistent application of data protection standards.	https://www.cnpd.pt/