Université Paris Nanterre

EUCLID
Enseignement universitaire
clinique du droit
Université Paris Nanterre

OVERVIEW: LEGAL FRAMEWORKS ON CYBER VIOLENCE AGAINST WOMEN AND GIRLS IN FRANCE AND THE EU

Paris Nanterre University Law Clinic (EUCLID)

Paris Nanterre University in collaboration with Osez le Féminisme (OLF) & the French Coordination for the European Women's Lobby (CLEF)



Authors
Apolline Anastase,
Christine Cymovonyuk,
Louise Moreau Louapre,
Luna Zedjaoui

Under the supervision of
Professor Audrey Darsonville

With the support of
Alyssa Ahrabare, president of the French Coordination for the European Women's Lobby (CLEF) and advocacy officer at Osez le Féminisme (OLF)

OSEZ LE FÉMINISME

La Coordination Française pour le Lobby Européen des Femmes

Summary

Page 1
Acknowledgements

Page 2
Methodology

Page 6
Introduction

Page 12
Analysis

Page 56
Recommandations for the transposition of directive 2024/1385

Page 64
Table of contents

Page 65
Bibliography

Acknowledgements

We would like to warmly thank Alyssa Ahrabare for her commitment and support in this project carried out in collaboration with Osez le Féminisme (EN: Dare to be Feminist) and the French Coordination for the European Women's Lobby. We are grateful for the many opportunities offered within the framework of this partnership. We were particularly delighted to attend the conference in Strasbourg, which enabled us to interview several experts in the field. We would also like to thank Ms. Ahrabare for the valuable resources she shared with us, in addition to her proofreading, analysis, advice and support throughout our research.

We would also like to express our deep gratitude to Professor Audrey Darsonville for her guidance, availability, careful proofreading and advice. Her trust, encouragement and support were essential to the completion of this thesis.

Finally, we would also like to thank Cécile Mantel, Julie Caillet, Katty Jorge Maia, Céline Piques, Mariana Branco, Ruth Breslin, Mié Kohiyama and Alejandra Mariscal López for their availability, commitment, and the quality of the interview they gave us.

Methodology

This work, carried out as part of the Legal Clinic at Paris Nanterre University, was commissioned by the associations Osez le Féminisme and the French Coordination for the European Women's Lobby. Created in 2009, Osez le Féminisme is a feminist, universalist, secular, progressive and abolitionist organisation. Its main objective is to denounce and eradicate inequalities between women and men.

Today, the association has 15 branches across France. Since 9 January 2013, it has been a member of the High Council for Equality and is a board member of the French Coordination for the European Women's Lobby (CLEF).

The CLEF is a non-governmental organisation that brings together 40 French associations working for women's rights. It is a member of the European Women's Lobby, a network of 2,000 feminist organisations and the leading force for the defence of women's rights at the European level. The CLEF engages in advocacy with French, European and international institutions through its consultative status with the United Nations (ECOSOC).

Osez le Féminisme and the French Coordination for the European Women's Lobby collaborate to advocate for the fight against cyber violence against women and girls, in addition to online sexual exploitation. These issues, which inherently have a cross-border dimension, require not only a national response but also a European one.

It is in this context that the associations asked our team to carry out a legal study based on Directive (EU) 2024/1385 on combating violence against women and domestic violence. The analysis focused on the four offences targeting cyber violence against women and girls defined by the Directive as the non-consensual sharing of intimate material, cyber stalking, cyber harassment and cyber incitement to violence or hatred. The initial objective was twofold: on the one hand, to cross-reference the provisions of the Directive on cyber violence against women and girls with other European instruments aimed at regulating digital content to clarify the obligations of EU Member States in this area.

On the other hand, to take stock of French positive law on the subject and assess its compliance with European obligations. *Ultimately,* the main objective of this work is to develop a guide of recommendations for France to effectively combat cyber violence against women and girls. This guide has been translated and will be made available to all EU Member States to assist them in the process of transposing Directive 2024/1385 into national law (mandatory by 2027).

While the initial deliverables included an advocacy document for Member States, in addition to an educational version and communication materials, the various meetings held with partner associations and our supervising professor, Audrey Darsonville, were instrumental in refocusing the initial assignment and adapting it to our project's time constraints.

The first meeting took place on 25 November, attended by Alyssa Ahrabare, Advocacy Officer at Osez le Féminisme and President of CLEF, as well as our professor. This meeting proved particularly useful, as it clarified the associations' expectations and defined the precise scope of our mission.

Following this exchange, it was agreed that three deliverables would be produced. The first would focus on European obligations relating to the aforementioned offences, based on several EU legal instruments. The second would be devoted to obligations under French law. Finally, the third would present a comparative analysis of the legislation of three EU Member States, serving as a basis for formulating recommendations for transposition. An initial deadline was set for the completion of the first deliverable by the end of December.

On 17 January, a second meeting was held with Ahrabare and Justine Cassar (a trainee lawyer interning at the CLEF) to obtain feedback on this first draft. It was suggested that we expand on our analysis by adding contextual information, examples and comparisons with other offences. A meeting was scheduled for March, giving us sufficient time to focus on the second deliverable.

The meeting on 13 March, this time attended only by our professor, was decisive for the final structure of our report. We decided to organise it into four parts, corresponding to the offences studied. Each part was to be subdivided into four sub-sections. The first would cover the context, the second European obligations, the third French obligations, and the last would be an analytical section that would guide us in drafting our recommendations.

The meeting with Ahrabare on 23 April served to validate the proposed structure and to confirm that there would not be sufficient time to conduct the comparative analysis of legislation across three Member States, as initially planned. The meeting also focused on organising the various interviews we intended to carry out. To this end, Ahrabare provided a list of expert contacts in different countries to help arrange interviews aimed at clarifying key aspects of our research. She also offered guidance on how to structure the interviews to ensure they would meaningfully contribute to our work.

While our work was largely based on an analysis of legal and policy documents, it was guided and enriched by the contributions of our partners, who not only provided us with relevant resources but also suggested research avenues and recommended key readings. However, our approach was not purely theoretical; it also incorporated a field-based dimension.

On 14 February 2025, we had the immense privilege of attending a conference organised in Strasbourg by Osez le Féminisme and the CLEF, entitled "Online sexual exploitation: challenges and responses in Europe." Bringing together parliamentarians, MEPs, government officials and lawyers, this event enabled us to deepen our knowledge and take a more critical look at sexual cyberviolence. We took extensive notes on the presentations and discussions during the day, which have greatly contributed to the development of this work.

We also conducted several interviews to complement our analysis with a range of expert perspectives.

The first interview took place on 28 May with three representatives from MIPROF: Cécile Mantel, Julie Caillet and Katty Jorge Maia. On 30 May, we spoke with Céline Piques, a board member of Osez le Féminisme and rapporteur for the High Council for Equality's commission on violence against women. The third interview was held on 2 June with Mariana Branco, who is currently conducting an in-depth study on the OnlyFans platform. On 3 June, we had the honour

[1] Osez le Féminisme (Dare to be Feminist). (CP) International symposium: Online sexual exploitation: challenges and responses European – Osez le feminisme ! (accessed on 16 May 2025).

[2] Interministerial Mission for the Protection of Women against Violence and the Fight against Human Trafficking.

of meeting two prominent figures: Ruth Breslin, Director of the Sexual Exploitation Research and Policy Institute in Ireland, followed by Mié Kohiyama, co-founder of the association Be Brave France, which fights against child sexual abuse. Finally, on 6 June, we spoke with Alejandra Mariscal López, director of the association Point de contact, which specialises in combating cyberviolence and protecting fundamental rights in the digital space.

Introduction

The adoption of Directive (EU) 2024/1385 by the European Parliament and the Council on 14 May 2024 marks a major step forward in combating violence against women and domestic violence. The Directive addresses a major regulatory gap, particularly in relation to cyber violence. The European Council[3] has stressed that EU efforts to tackle this issue are unfolding against the backdrop of a troubling rise in online violence.

In France, for example, 348,000 digital offences were recorded in 2024, including 103,300 offences against individuals, representing a 7% increase on the previous year. Women and girls are disproportionately represented among victims, comprising 66% of adult victims and 70% of child victims of these offences[4]. Specifically regarding cyberviolence, a November 2022 study found that more than 4 in 10 French women reported having experienced such violence. Among all victims surveyed, 84% were women and 51% were under the age of 30.[5] This data indicates that cyberviolence primarily impacts young women.

In 2020, one in two young women in Europe experienced sexist cyberviolence, most often of a sexual nature.[6] According to a study by *The Economist Intelligence Unit,* in 2021, 85% of women worldwide were exposed to violence on the internet. Cyberviolence also disproportionately targets women active in the public sphere, such as journalists and politicians. In 2018, the United Nations Special Rapporteur on violence against women published a report[8]

[3] European Council and Council of the EU. (2024). "EU measures to end violence against women". EU measures to end violence against women - Consilium (accessed on 4 February 2015).

[4] Ministère de l'Intérieur. (2025). « Communiqué de presse : Les infractions liées au numérique enregistrées par les services de sécurité en 2024 ». (accessed on 17 February 2025).

[5] Féministes contre le cyberharcèlement. (2022). « Cyberviolence et cyberharcèlement : le vécu des victimes ». Enquête conduite par IPSOS auprès de 216 victimes de cyberviolences âgées de 16 ans à 60 ans ou plus. https://www.vscyberh.org/.

[6] European Parliament and European Council. (2022). "Proposal for a directive on combating violence against women and domestic violence." European Parliament and European Council. (2022). "Proposal for a Directive on combating violence against women and domestic violence." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0105, p.2.

[7] The Economist Intelligence Unit. (2020). "Measuring the prevalence of online violence against women." Measuring the prevalence of online violence against women.

[8] Simonovic Dubravka, United Nations Special Rapporteur on violence against women and girls. (2018). "Report on violence against women, its causes and consequences concerning

addressing online violence and violence facilitated by information and communication technologies (ICT), specifically concerning women and girls from a human rights perspective. The report highlighted that "*the online abuse against women journalists and women in the media are a direct attack on women's visibility and full participation in public life.*" Such attacks against women journalists impede the exercise of their profession, with harmful consequences on their participation in democratic life. For this reason, the preamble to Directive (EU) 2024/1385 highlights this issue, stating that "*Cyber violence particularly targets and impacts women politicians, journalists and human rights defenders.. (...) Cyber violence can have the effect of silencing women and hindering their societal participation on an equal footing with men*."

In light of these findings, the need for a harmonised European legal response became evident. Prior to the adoption of Directive 2024/1385, no specific framework existed for addressing cyber violence against women and girls in a coherent and consistent manner across the EU.

Cyberviolence refers to the use of digital technologies and communications – such as online platforms, social media and messaging services – to perpetrate, facilitate or threaten acts of violence against individuals.[9] This form of violence "*is rooted in gender inequality being a manifestation of structural discrimination against women.*"[10] As such, it is recognized as a form of violence against women, which encompasses "*all acts of gender-based violence that result in or are likely to result in physical, sexual, psychological or economic harm or suffering, including threats of such acts.*"[11] cyber violence against women and girls must therefore be understood as part of a continuum of sexist and sexual violence. A study published in November 2022 reported that for 72% of victims, violence that began online continued offline.[12] Digital violence is thus not only a new form of violence but also one that compounds and intensifies existing forms.

Online violence against women and girls from a human rights perspective. https://digitallibrary.un.org/record/1641160?ln=fr&v=pdf.

[9] European Women's Lobby. (2024). "Report on cyber violence against women. Executive summary and recommendations", p. 6.

[10] European Parliament and European Council. (2022). *Op.cit.*, p.1.

[11] *Ibid.*

[12] Féministes contre le cyberharcèlement. (2022). *Op. cit.*

Women "*are disproportionately represented as victims of both forms of violence due to the underlying patterns of coercion, power and/or control.*"[13] That is why, even though "*anyone can be a potential victim of such violence, regardless of their sex or gender,*"[14] we will focus solely on female victims in this report.

Research has shown that *"digital spaces reinforce and intensify systemic structural gender inequalities as well as patterns of harmful masculinities.*"[15] Masculinists believe that women and feminists are attempting to overturn (or have already overturned) the patriarchal order in favour of a matriarchal society — a development to which they are strongly opposed, convinced of the natural superiority of men over women.[16]

Among them is the "incel" (involuntary celibate) movement, which promotes online violence against women and glorifies such acts by portraying perpetrators as heroic figures.[17]

Another example is the Men Going Their Own Way (MGTOW) movement, which is based on the theory of social gynocentrism – the belief that society revolves around women. MGTOW advocates for the complete rejection of emotional relationships with women as a means of preserving masculinity.[18]

These groups are not isolated phenomena: they form part of a broader ecosystem known as the "manosphere" – a network of online communities where men advocate for what they perceive as their own interests, often by promoting misogynistic, anti-feminist and sexist ideologies.

The danger of cyberviolence stems as much from its scale and speed of growth as from its anonymity, in addition to the difficulty for victims to remove harmful content, and the public, repetitive and invasive nature of the attacks. These characteristics can have serious consequences on women.

On a psychological level, cyberviolence has an impact in 80% of cases. It can lead to

---

[13] European Parliament and European Council. (2022). *Loc.cit.*
[14] *Ibid.*
[15] European Women's Lobby. (2024). *Loc. cit.* p.15
[16] Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). *Fiche informative, « La Manosphère »*, p.5. FICHE MANOSPHÈRE _FR.pdf.
[17] European Parliament and European Council. (2022). *Op. cit.*, p.2.
[18] Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). *Ibid.*, p. 7.

post-traumatic stress disorder, which includes hypervigilance, anxiety and depressive disorders, eating disorders, and suicidal thoughts.[19] Secondly, at the economic and social level, 50% of victims report a moderate to severe impact on their education or professional life.[20] Some also encounter difficulties in securing employment, while others suffer the consequences of gossip or social exclusion.[21]

In face of these challenges, establishing minimum standards to guarantee the rights, support and protection of victims of all forms of sexist cybercrime[22] has proved essential. At the EU level, Parliament has repeatedly called on the Commission to propose legislation addressing violence against women, including sexist cyberviolence. The European Parliament has also adopted two own-initiative reports on the subject, grounded in Article 225 of the Treaty on the Functioning of the EU (TFEU). Subsequently, a proposal for a Directive aimed at ensuring a minimum level of protection against such violence in Member States was presented on 8 March 2022 and adopted on 14 May 2024. This occurred in a European context where specific legal instruments addressing cyber violence were lacking. The Directive is intended to complement the Istanbul Convention – a Council of Europe treaty central to the fight to end violence against women – which came into force in 2014 and was acceded to by the EU in 2023. Although this text remains a major reference framework in the fight to end violence against women, it does not explicitly address emerging issues such as cyber violence.

The preamble to Directive 2024/1385 of 14 May 2024 on combating violence against

---

[19] Féministes contre le cyberharcèlement. (2022). *Op. cit.*
[20] *Ibid.*
[21] Parliamentary Assembly of the Francophonie, Network of Women Parliamentarians. (2021). "Final report: cyber violence against women and children in the French-speaking world", p.5, 9. Microsoft Word - Final report on cyber violence against women and children.
[22] European Council and Council of the EU. (2024). *Op.cit.*
[23] Treaty on the Functioning of the EU (consolidated version). (2012). See Article 225.
[24] European Parliament and European Council. (2024). "Directive (EU) 2024/1385 of 14 May 2024 on preventing and combating violence against women and domestic violence." Directive - EU - 2024/1385 - EN - EUR-Lex.
[25] Council of Europe. (2011). "Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)".

women and domestic violence states that "*It is necessary to provide for harmonised definitions of offences and penalties regarding certain forms of cyber violence where violence is intrinsically linked to the use of information and communication technologies ('ICT').*"

The text specifies that the nature of the offence is specific because technologies "are *used to significantly amplify the severity of the harmful impact of the offence*." Cyber violence thus possesses an inherently harmful dimension.

Advances in communication tools have enabled new forms of offences, broadening the spectrum of violence with serious consequences for victims. These multifaceted manifestations of cyber violence have a profound impact, allowing perpetrators to create an environment of insecurity and exert constant control over the victim's life. This affects all aspects of the victim's life — public and private, online and offline.

It should be noted that a European Directive is not directly applicable. It only takes effect once transposed into national law, leaving Member States the discretion to determine how it will be implemented. Furthermore, it sets "minimum standards", allowing Member States to opt for a transposition of the text that is more protective for victims. Until transposition occurs, which must take place within three years of its adoption by the EU, Directive 2024/1385 is not binding and cannot directly be invoked by individuals.

This deliverable is structured around four key areas, corresponding to the four articles of Directive 2024/1385, each addressing specific offences related to online violence: non-consensual sharing of intimate or manipulated material (Article 5), cyber stalking (Article 6), cyber harassment (Article 7), and cyber incitement to violence or hatred (Article 8). For clarity and practical purposes, each offence will be examined using the same four-part structure. The first section situates the behaviours criminalised by the Directive within a broader context. The second section focuses on European legislation, including the Directive's provisions, cross-referenced with other relevant European instruments — such as the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and the Charter of Fundamental Rights of the EU – to clarify Member States' specific obligations in each area. The third section analyses how these offences are criminalised under French law. Finally, the fourth section provides a case law and doctrinal analysis of the relevant laws, identifying any gaps at both the European and French levels.

Ultimately, this work aims to formulate recommendations for the transposition of Directive 2024/1385 that align with the existing regulatory framework, ensuring effective implementation and enhanced protection for victims.

Analysis

1. Non-consensual sharing of intimate or manipulated material

1.1. Context

The non-consensual sharing of intimate images or videos, whether authentic or manipulated, constitutes a particularly harmful form of digital violence. Once posted online, this content is extremely difficult to remove as it can go viral, is often hosted on servers overseas, and some platforms are not cooperative.

The "French Bukkake" case perfectly illustrates this deadlock. Initiated in 2023 and still ongoing, it involves rapes committed during pornographic film shoots organised by Pascal Ollitraut and his company. There are 17 defendants and 42 civil parties, including Osez le Féminisme. Despite the gravity of the charges, many videos involving the civil parties in the trial remain online, causing ongoing retraumatisation and revictimisation of the victims, who endure assault, discrimination and blackmail. This situation is far from isolated: once intimate, sexual, or sexually violent content is published online, it is almost impossible to remove it permanently. This raises serious questions about the inaction of platforms and the responsibility of European institutions and Member States.

The issue is equally as concerning for manipulated material, most of which is pornographic. The publication on websites of sexual scenes featuring the faces of celebrities demonstrates the scale of the phenomenon, which is estimated to have begun in 2017. It should be noted that the fact that these images are not real does not lessen the suffering of the victims[26]. This kind of violence[27] has real consequences on victims' privacy and their right to dignity and integrity. Nothing is truly private on the Internet, and many websites make money from monetising violent erotic content.

[26] Osez le Féminisme and CLEF. (2025). Symposium: "Online sexual exploitation: challenges and responses in Europe". Strasbourg.
[27] *Ibid.*

Furthermore, the sharing of such images has current and potential future adverse effects on the prevalence of sexist violence, the protection of public health and minors, as well as serious consequences for the physical and mental well-being of individuals.

This raises major legal issues, particularly regarding the right to erasure – which is nevertheless guaranteed by the GDPR – and the right to privacy.

1.2. The European legal framework

The non-consensual sharing of intimate or manipulated material is one of the criminal offences covered by Directive 2024/1385. Article 5 defines it as "*producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent.*"[28] Threatening to commit these acts also constitutes a criminal offence.

Existing EU law already addresses the issue of the sharing and erasure of private images.

1.2.1. The Digital Services Act (DSA)

The Regulation of 19 October 2022 on a Single Market for Digital Services,[29] also known as the Digital Services Act, contains provisions relevant to the fight against the non-consensual sharing of intimate or manipulated content. Recital 12 of the text specifies that illegal content includes "the unlawful non-consensual sharing of private images."[30]

---

[28] European Parliament and European Council. (2024). *Op.cit.*, Article 5.

[29] European Parliament and Council. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (hereinafter: Digital Services Act). Regulation - 2022/2065 - EN - EUR-Lex.

[30] European Parliament and Council. (2022). *Op. cit.*, recital 12.

Although recitals have no binding force, they are drafted to make the content of European legislative acts clearer and serve as guidance for their interpretation.[31] The DSA imposes obligations on digital platforms concerning user-accessible content, particularly in relation to illegal content. **Recital 12 specifies that these obligations also apply in cases of unlawful and non-consensual dissemination of private images.**

> *"In order to achieve the objective of* ***ensuring a safe, predictable and trustworthy online environment,*** *for the purpose of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular,* ***the concept of 'illegal content'*** *should* ***be defined broadly*** *to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules* ***render illegal in view of the fact that it relates to illegal activities****. Illustrative examples include the sharing of images depicting child sexual abuse,* ***the unlawful non-consensual sharing of private images****, online stalking, harassment (...)."*

Under Article 18 of the DSA, **hosting service providers,** defined as entities that "*store information provided by the recipients of the service at their request,"*[32] are required to "***promptly***" **notify the competent authorities of any suspected criminal offence** "involving a threat to the life or safety of a person or persons." In such cases, they must transmit all relevant information available to them.

In other words, when hosting service providers have information indicating that a criminal offence threatening the life or safety of one or more persons has been committed, is being committed or is likely to be committed, they are obliged to inform the competent law enforcement or judicial authorities of the relevant Member State and share the pertinent data.

[31] Den Heijer, M; Abeelen, T; Maslyka, A. (2019). "On the Use and Misuse of Recitals in European ~~Union Law." *Amsterdam Law Sch~~ool Research Paper.* No. 2019-31. p. 3.

[32] European Parliament and Council. (2022). *Op.cit.*, Article 3§g iii).

If the hosting service provider is unable to determine with certainty the Member State concerned, it must notify the authorities of the Member State in which it is established, where its legal representative is located, or inform Europol. The Member State concerned is defined as the Member State where the offence has taken place, is taking place or is likely to occur, or where the alleged perpetrator or victim is located.

The non-consensual dissemination of intimate images, particularly on social media, constitutes a criminal offence that may threaten the life or safety of a person. Victims of such offences often face multiple forms of "revictimisation" (online harassment, blackmail, physical assault, sexual violence, etc.)[33] Hosting service providers are obliged to notify the competent authorities if they suspect such an offence. Measures should be put in place to ensure this reporting obligation is effective and that victims are systematically notified. This would facilitate the early removal of content, thereby better protecting victims and enabling the perpetrators to be brought to justice more quickly.

Articles 34 and 35 concern online platform providers, i.e. hosting services, defined as consisting of *"the storage of information provided by, and at the request of, a recipient of the service."*[34] Under these provisions, online platform providers are **required to analyse and assess any systemic risks arising from the design or operation of their services "diligently."**[35] In accordance with Article 35, they must take measures to **mitigate these "*actual or foreseeable*" risks,** which must be " ***reasonable, proportionate and effective***".

The Delegated Regulation on independent audits under the Digital Services Act, adopted by the European Commission following the DSA in 2023, sets out criteria for evaluating whether providers have conducted a "diligent" analysis of the systemic risks arising from the design or operation of their services. To determine diligence, the audit must consider, at a minimum, the

---

[33] *Ibid.*
[34] European Parliament and Council. (2022). *Op.cit.*, Article 3§i.
[35] European Parliament and Council. (2022). *Ibid.,* Article 34.

following elements: the provider's consideration of regional and linguistic aspects of the use of its service (including where specific to a Member State), the inclusion of technical and scientific expertise in the assessment process, the provider's compliance with the time limits set out in Articles 34 and 35 above, and the performance of risk assessments prior to the implementation of features that may have an impact on the risks identified in Articles 34 and 35.[36]

Concerning the measures to be taken by providers pursuant to Article 35 of the DSA, Article 14 of the Delegated Act on independent audits specifies only that, to assess whether such measures are reasonable, proportionate, effective and appropriate, the entity carrying out the audit must verify that the measures collectively address all identified risks, with particular attention to those affecting the exercise of fundamental rights.[37]

The list of systemic risks set out in Article 34 extends the mitigation obligation to include the non-consensual sharing of intimate images, as such practices constitute a violation of the right to human dignity and the right to respect for private and family life.
Platform providers must also **mitigate the negative effects of sexist violence, protect public health and minors**, and address **serious consequences for individuals' physical and mental well-being.**[38] To do so, they must review the design of their systems, their terms and conditions of use, and their data management practices, assessing how these elements contribute to or mitigate the identified risks.[39]

Article 34 also establishes a **duty of transparency.** It states that providers must retain data relating to risk assessments and be able to make such data available to the Commission and to the Digital Services Coordinator of the Member State in which the provider is established.

The risk assessment obligations outlined in the above-mentioned articles can therefore contribute to the protection of individuals.

---

[36] European Commission. (2023). "Delegated Act on independent audits under Digital Services Act, C/2023/6807". Article 13.
[37] European Commission. (2023). *Op. cit.,* Article 14.
[38] European Parliament and Council. (2022). *Op. cit.*, Article 34.
[39] Citron, D.K; Franks, M.A. (2014). "Criminalising Revenge Porn". *Wake Forest Law Review*, 49 (2), p. 346.

The explicit absence of any mention of violence against women online in the text does not in any way prevent it from being applied to such situations, such as the non-consensual sharing of intimate content referred to in Directive 2024/1385.

1.2.2. The General Data Protection Regulation

EU Regulation 2016/679 of 27 April 2016,[40] commonly known as the "General Data Protection Regulation" (GDPR), establishes protective standards focused on the protection of personal data. Article 4 defines personal data as "*any information relating to an identified or identifiable natural person […] an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

In its Breyer judgment of 19 October 2016[41], the Court of Justice of the European Union clarified the scope of the concept of "personal data" under the GDPR. The Court held that the mere possibility of identifying a person based on certain data does not automatically render that data "personal" within the Regulation.[42] While the judgment affirms the notion *of indirect identification* and thus appears to extend the definition of personal data, the assertion that the identification of a person is not sufficient to qualify data as personal data restricts the exercise of the rights granted under the GDPR in certain situations.

The Court states in paragraph 41 of the judgement: *"in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified".* It then

[40] European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[41] Court of Justice of the European Union. (2016). Breyer judgment. C-582/14, EU:C:2016:779. Points 39 and 41.
[42] *Ibid.,* paragraph 46.

specifies in the following paragraph that, *"to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.*"
This is where the Court indirectly sets a limit: if the identification of the data subject is "*practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power,*"[44] the data will not be considered personal. However, the "*impossible*" nature of identification is likely to be subject to subjective interpretation, both by those subject to the GDPR and by the courts.

It is important to note that the GDPR provides exceptions to the general prohibition on the processing of special categories of personal data. Recital 52 specifies that the processing of such data, including data related to a person's sex life, is only permitted "*when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights.*" This represents a restrictive approach to authorising the processing of special categories of data.

Regarding the processing of intimate images or videos without consent, Article 9 of the GDPR categorises **data concerning the sex life of natural persons** in the list of special categories of personal data. This article generally prohibits the processing of such data, except where the data subject has given their consent, or where one of the other legal grounds set out in the article justifies such processing.

Moreover, **the right to erasure** ("**right to be forgotten**") set out in Article 17 of the GDPR is particularly relevant in the context of the transposition of Directive 2024/1385. Under this article, any data subject may obtain, without undue delay, the erasure of their personal data if the personal data are no longer necessary for the purposes for which they were collected or processed

[43] *Ibid.,* point 42.
[44] Court of Justice of the European Union. (2016). *Op.cit.,* point 46.

(a); **the data subject withdraws consent on which the processing is based** [45] , and there is no other legal ground for the processing (b); **the data subject objects to the processing** pursuant to Article 21 [46] , and there are no overriding legitimate grounds for the processing (c); **the personal data have been unlawfully processed** (d); the personal data have to be erased for **compliance** with **a legal obligation** in Union or Member State law to which the controller is subject (e).

The "right to be forgotten" is a legal term encompassing several rights, including the right to erasure[47] and the right to be delisted.[48] It is exercised in the first instance with the entity that made the data public, which is required to take reasonable steps to inform data controllers that the data subject has requested the erasure of any links to their personal data, or any copies or reproductions thereof. "*The reasonableness of the measures shall be assessed in the light of the available technology and the costs of implementation."*[49]

If the request for erasure or de-referencing is denied, the individual can seek recourse from the relevant authority responsible for ensuring compliance with the GDPR. In France, this is the Commission nationale de l'informatique et des libertés (CNIL).

In a ruling dated 6 December 2019, the Conseil d'Etat provided guidance on how to assess requests to be forgotten. The CNIL must rely on a set of indicators that includes "*the nature of the*

---

[45] European Parliament and Council. (2016). Ibid. In accordance with Article 6(1)(a) or Article 9(2)(a)

[46] European Parliament and Council. (2016). Ibid. Article 21(1): *"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."*

[47] Andréani, A. (2020). « Le droit à l'oubli : étude comparée entre la France et les Etats-Unis ». Thèse de doctorat. Université Paris II Panthéon-Assas.

[48] Terwangne, C. (2015). « Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique ». *Enjeux européens et mondiaux de la protection des données personnelles.* Création information communication, Larcier. (p. 245-275).

[49] Boizard, M. (2016). « Le temps, le droit à l'oubli et le droit à l'effacement ». *Les Cahiers de la justice*, no 4, (p. 619-628).

data in question, their content, their objective character, their accuracy, their source, the conditions and date of their publication online and the repercussions that their referencing is likely to have for the person concerned and, on the other hand, the notoriety of that person, their role in public life and their function in society."[50]

Thus, although the right to be forgotten is based on the principle of consent, the mere withdrawal of consent is not sufficient. In the context of the right to be delisted, the exercise of this right is limited, insofar as courts and data controllers may make a subjective assessment of the appropriateness of such delisting[51].

The GDPR also requires the data controller to take **reasonable steps, including technical measures, to delete such data, as well as any copies or reproductions thereof**. However, these obligations are **limited by exceptions**, such as freedom of expression and information (Article 17(3)), public interests, or the exercise and defence of legal rights.

The need to protect freedom of expression is a reason often given for limiting online content regulation. This is especially true for violent pornographic videos. Directive 2024/1385 itself introduces restrictions on freedom of expression, as well as on the arts and sciences, in Article 5(2). The perceived blurring of the line between expression protected by freedom of expression and expression that constitutes a threat[54] encourages legislators to exercise caution, which does not always allow for effective protection of vulnerable groups online. **However, freedom of expression is a fundamental freedom that may be restricted by legitimate interests, including "*the prevention of crime, the protection of health or morals, the protection of the reputation or rights of others.*"[56]**

---

[50] Conseil d'Etat. (2019). 10e et 9e chambre réunies, n° 429154, 6 décembre.
[51] Andréani, A. (2020). *Ibidem.*
[52] UN. "Hate speech versus freedom of speech." https://www.un.org/en/hate- speech/understanding-hate-speech/hate-speech-versus-freedom-of-speech. (accessed 22 May 2025).
[53] Interview with Ruth Breslin. (3 June 2025).
[54] Udoh-Oshin, G. (2017). "Hate Speech on the Internet: Crime or Free Speech?" Undergraduate thesis. Long Island University. (pp. 5-6).
[55] European Convention on Human Rights
[56] Cyberharcèlement. « Cyberharcèlement et liberté d'expression : les enjeux juridiques ». https://cyber-harcelement.info/la-frontiere-entre-cyberharcelement-et-liberte-dexpression-les enjeux-juridiques/ (accessed 22 May 2025).

It is essential that these limitations, conditioned by a principle of necessity, are fully applied in the digital space. The right to erasure under the GDPR echoes the provisions of Article 23 of **Directive 2024/1385**, which requires that **rapid measures be taken to remove or block access to intimate material or content that incites violence.**

> *"Member States shall take the necessary measures to ensure that online publicly accessible material as referred to in Article 5(1), points (a) and (b), and Articles 7 and 8 of this Directive is* ***promptly removed or that access thereto is disabled****.*
> *Measures as referred to in the first subparagraph of this paragraph shall include the possibility for the competent authorities to issue binding legal orders to remove or to disable access to such material. Member States shall ensure that such orders meet, at least, the conditions set out in Article 9(2) of Regulation (EU) 2022/2065."*
>
> [Directive 2024/1385]

In practice, the primary challenge in cases of non-consensual sharing of personal images or videos is the rapid removal of such content from online platforms. For this reason, it may be relevant to invoke the right to be forgotten enshrined in the GDPR to facilitate the removal of content sanctioned by Directive 2024/1385.

The right to erasure is an important mechanism that allows individuals to regain control over their personal data, particularly in cases involving the non-consensual dissemination of sensitive material. However, it has significant limitations: it is not proactive, and its effectiveness depends largely on the cooperation of States, as well as on the responsiveness of platforms, which can vary considerably from case to case. **This reliance on cooperation sometimes makes the implementation slow or ineffective, particularly in urgent situations.**

Other legal frameworks present promising mechanisms that could be adapted for addressing the non-consensual sharing of intimate content, such as the European regulation on addressing the dissemination of terrorist content online.

1.2.3. European Regulation on addressing the dissemination of terrorist content online

This regulation is included in the analysis as it illustrates **how a coordinated and binding European response can effectively curb the rapid spread of highly harmful content.** It also sets an important precedent for adopting similar measures in the context of online sexist and sexual violence, particularly concerning the sharing of non-consensual intimate content, videos of sexual assaults and pornographic deepfakes. **As with terrorist content, a European framework should impose strict removal deadlines, reinforce platform obligations, and establish stronger cooperation between national authorities, hosting services, and EU institutions. Such measures would address existing gaps and provide stronger protection for the fundamental rights of victims of online sexist and sexual violence.**

The Pornhub case and the revelations from the *Traffickinghub* investigation have exposed the widespread dissemination of non-consensual sexual content, including material involving minors. This underscores the scale of the issue and the urgent need for structural solutions.[57] In the absence of binding mechanisms like those in place for terrorist content, victims are often left without effective recourse, forced to navigate lengthy and largely ineffective processes on their own.

European Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online, established a strict regulatory framework to prevent the misuse of hosting services for terrorist purposes.

To achieve this effectively, the regulation provides for the possibility of issuing a removal or blocking order for illegal content.[58] **These measures require hosting service providers to remove or block access to terrorist content in all Member States within one hour of receiving the order.** In cases where a provider cannot comply with the order for reasons of force

[57] Kristof, N. (2020). "The Children of Pornhub," *The New York Times*.
[58] European Parliament and Council. (2021). Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. Article 3.

majeure or factual impossibility not attributable to its responsibility (such as justifiable technical or operational reasons), it must inform the competent authority without undue delay, explaining the reasons for its inability to act.

The Regulation also imposes **preventive measures to limit or prevent exposure to terrorist content.**[59] These obligations apply to hosting providers identified as "*exposed to terrorist content.*" This designation is assigned by the competent authority of the Member State where the provider has its main establishment or legal representative. The decision is based on **objective criteria,** such as receiving several removal orders in the previous 12 months. Once the decision is made, it must be communicated to the provider, who will then be required to take **specific measures.** These measures include requiring providers to include a clause in their terms and conditions dedicated to preventing the misuse of their services for the dissemination of terrorist content, implementing appropriate technical measures to identify and quickly remove such content or block access to it, and providing accessible mechanisms for users to report or flag terrorist content.

According to the European Commission's report, the application of Regulation (EU) 2021/784[60] has had a positive impact on limiting the dissemination of such content online. At least 349 orders to remove terrorist content have been issued since it came into force. In addition, in most cases, hosting service providers took swift action to remove the content or block access to it. In only 10 out of 349 cases did the targeted provider exceed the maximum one-hour deadline for removal after receiving the order.

This report is part of the implementation of Article 22 of the Regulation. The Commission is required to report regularly to the European Parliament and the Council on the application of the text.

To ensure cross-border cooperation, **the PERCI tool (European Platform for the Removal of Illegal Content on the Internet) has been set up.** It allows both removal orders and reports to be forwarded to hosting providers in a centralised and coordinated manner.

---

[59] European Parliament and Council. (2021). *Op. cit.*, Article 5.

[60] European Commission. (2024). Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online.

PERCI provides a technical solution for processing referrals and removal orders and facilitates cooperation between competent authorities, hosting service providers and Europol.

Removal orders must comply with the principles of proportionality and necessity and guarantee respect for fundamental rights as set out in the EU Charter of Fundamental Rights, without discrimination. When such measures are implemented, providers are required to submit a report to the competent authority within three months. If the actions taken are considered insufficient, the authority may mandate additional measures.

1.2.4. EU Charter of Fundamental Rights

The Charter of Fundamental Rights of the European Union was adopted on 7 December 2000 and has been legally binding since the entry into force of the Treaty of Lisbon in 2009. This means that the rights it enshrines must be respected by both EU institutions and bodies, as well as by Member States **when implementing EU law.**

Several provisions of the Charter are particularly relevant to the non-consensual sharing of intimate material. **Article 8 guarantees the protection of personal data, while Article 7 protects the right to respect for private and family life, home, and communications**. Under Article 52(3), this right carries the same implications as **the right to privacy set out in the European Convention on Human Rights.** The European Court of Human Rights further established in *Dudgeon v. the United Kingdom* (22 October 1981) that a person's sexual activity constitutes an intimate aspect of private life.[61]

[61] European Court of Human Rights. (1981). "Dudgeon v. United Kingdom". Series A, No. 45, para. 41.

1.3. The French legal framework

Under French criminal law, the unauthorised sharing of intimate or manipulated material is punishable under multiple provisions of the Criminal Code. Articles 226-1 and 226-2, which address violations of privacy, make a criminal offence of "taking, recording or transmitting the picture of a person who is within a private place, without the consent of the person concerned." This offence is punishable by one year's imprisonment and a fine of €45,000.
An aggravating circumstance applies when the acts are committed by a spouse, live-in partner or partner linked to the victim through a civil partnership. In such cases, the penalty increases to two years of imprisonment and a fine of €60,000.

Article 226-2-1 specifically criminalises the capture, storage, and/or dissemination of images of a sexual nature without the consent of the person concerned. This provision highlights the "sexual nature" of the content and requires a clear distinction between the victim's consent to the creation of the images and their consent to their storage, recording, or transmission. The dissemination of such material thus constitutes an aggravated invasion of privacy, punishable by two years of imprisonment and a fine of €60,000.

> "*Where the offences referred to in Articles 226-1 and 226-2 relate to words or images of a sexual nature taken in a public or private place, the penalties shall be increased to two years' imprisonment and a fine of 60,000€.*
>
> *The same penalties shall apply to the act of making available to the public or to a third party, without the consent of the person concerned, any recording or document containing words or images of a sexual nature obtained with the express or presumed consent of the person concerned or by the person concerned themselves, using one of the methods provided for in Article 226-1.*

Law No. 2024-449 of 21 May 2024 on securing and regulating the digital space, known as the "SREN Law,"[62] aims to align French law with EU law, with a focus on the Digital Services Act. Article 17 of the latter amended Article 312-10 of the Criminal Code by adding three paragraphs to criminalise blackmail involving sexual content. In such cases, the penalty is seven years of imprisonment and a fine of 100,000 euros.

> "*Blackmail is the act of obtaining, by threatening to reveal or impute facts likely to damage someone's honour or reputation, either a signature, a commitment or a waiver, or the disclosure of a secret, or the handing over of funds, securities or any property whatsoever.*
>
> *Blackmail is punishable by five years' imprisonment and a fine of 75,000 euros.*
>
> *The term of imprisonment is increased to seven years' imprisonment and a fine of €100,000 where the blackmail is carried out by an online public communication service:*
>
> *1° By means of images or videos of a sexual nature;*
>
> *2° With the aim of obtaining images or videos of a sexual nature*.

Finally, Article 226-8-1, added by the "SREN Law" of 2024, specifically targets "*montages of a sexual nature*" made using the image or words of a person without their consent.

> "*Any person who, by any means whatsoever, brings to the attention of the public or a third party a montage of a sexual nature made using the words or image of a person without their consent shall be punished by two years' imprisonment and a fine of €60,000. The offence referred to in this paragraph shall be treated as equivalent to the offence referred to in this paragraph and shall be punishable by the same penalties if visual or audio content is brought to the attention of the public or a*

[62] Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

third party, by any means, generated by algorithmic processing and reproducing the image or words of a person without their consent.

An aggravating circumstance increases the penalties to three years' imprisonment and a fine of 75,000€ when the publication of the content in question was carried out "*using an online public communication service.*"

1.4. Analysis

At the European level, one provision of the DSA raises questions: recital 12, which refers to "*the unlawful non-consensual sharing of private images*." The use of the term "unlawful" implies that the non-consensual sharing of private images – such as intimate images, for example – could, in certain cases, be considered legal. This raises a crucial question: where should the line be drawn between the legality and illegality of non-consensual sharing of intimate images? The need to clarify the term "unlawful" is significant. In practice, the sharing of intimate images without the consent of the persons involved is strictly regulated, or outright prohibited, except in very exceptional cases. For example, certain images may be legally disseminated without authorisation when they relate to a recent event that is in the public interest.[63]

By contrast, no such exception exists for other offences, such as the sharing of images depicting child sexual abuse. The asymmetry between offences suggests a problematic hierarchy in the treatment of digital violence. **The choice of terminology in recital 12 can therefore be perceived as interpreted as reflecting a restrictive approach by the European legislator, or even as an implicit trivialisation of violence against women online.**

Furthermore, Regulation (EU) 2021/784 has demonstrated that it is possible to establish mechanisms for the rapid and justified issuance of removal orders, accompanied by specific preventive measures against the dissemination of illegal content. It would therefore be appropriate for this approach to be transposed into Directive 2024/1385. **This would allow providers hosting pornographic platforms or social networks (such as Twitter or Instagram) – often used for the dissemination of non-consensual intimate content –**

[63] Cour de cassation, Chambre civile. Arrêt du 21 mars 2018, n°16-28.741.

to be designated as "exposed to sexual content". The latter would then be required to implement specific measures to prevent the dissemination of intimate content, including manipulated content, without the consent of the persons concerned.

At the national level, the wording of Article 226-2-1 of the Criminal Code also raises questions. On 30 June 2021, the Conseil constitutionnel was asked to rule on a priority question of constitutionality (QPC)[64] concerning the conformity of the second paragraph of this provision with the rights and freedoms guaranteed by the Constitution.

The challenge arose from the lack of clarification regarding what constitutes words or images of a "sexual nature," with critics arguing that the principle of legality and necessity of offences and penalties had been disregarded. While the subjective and vague nature of this concept can indeed be highlighted, the Conseil constitutionnel ultimately concluded that the provision was sufficiently clear and precise to prevent arbitrariness, leaving it to the competent courts to determine whether words or images are of a sexual nature. **This approach, however, may lead to disparities in case law.**

Moreover, the amendments introduced by the 2024 "SREN Law," particularly those affecting Article 226-8 of the Criminal Code, are noteworthy. The legislator clearly sought to "*update the only offence presented as protecting the representation of the person, the offence known as 'montage.*'" [65] Like EU initiatives, this intervention can also be explained by the broader context, notably the emergence of artificial intelligence and pornographic "deepfakes".

Firstly, as mentioned above, Article 15 of the provision amended the verb "*publish*" on the grounds that the concept was too ambiguous and that the notion of publication applicable to the press could not be applied in this context. According to legal doctrine, this amendment is unlikely to change the state of the law, as the Criminal Division of the Cour de cassation has long affirmed the autonomy of the concept of publicity in Article 226-8 of the Criminal Code from that in Article 23 of the Law of 29 July 1981.

---

[64] Conseil constitutionnel. (2021). Décision n°2021-933 QPC du 30 septembre 2021.Decision No. 2021-933 QPC of 30 September 2021| Constitutional Council.

[65] Bossan, J. (2024). « La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0 ». *Légipresse*, n°426, (p. 380-385).

The Court considers that **even "restricted" advertising carried out knowingly is punishable**[66].

These developments represent positive steps forward, offering hope that France may follow the example of the United Kingdom, which has successfully shut down websites distributing deepfakes. Recognising the limitations of its existing legal framework, the UK adopted specific provisions in January 2025 explicitly criminalising the creation and dissemination of sexually explicit deepfakes without consent. Alongside South Korea, it is among the most advanced countries in this area.[67]

Article 5 of the Directive therefore appears to have relatively strong equivalents in French law, particularly due to the contributions of the "SREN Law". What remains to be assessed, however, is the situation regarding online stalking, also known as "cyber stalking".

[66] *Ibid.*
[67] Osez le Féminisme and the CLEF . (2025). Symposium: "Online sexual exploitation: challenges and responses in Europe". Strasbourg.

2. Cyber stalking

2.1. Context

In 2021, Apple released the first *AirTag* a device designed to be attached to items for geolocation purposes. While intended to track lost belongings, it can be misused, for example, to monitor the movements of a partner in cases of domestic violence[68] – behaviour that falls under the offence of "cyber stalking".

"Online stalking" or "cyber stalking" refers to the practice of using communication technologies to monitor, threaten, intimidate, or convey to victims an intention to cause harm.[69] Although there is no definitive list of behaviours that constitute "cyber stalking,"[70] the most commonly recognised acts include collecting and acquiring messages, emails, or images of the victim, often through spyware.[71]

It is the repeated nature of these behaviours that makes it possible to identify the offence.[72] In practice, however, proving this can be challenging, as it requires demonstrating that multiple acts, considered collectively, amount to stalking – a task made even more difficult when multiple perpetrators are involved.[73]

---

[68] Centre Hubertine Auclert. (2023). « Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyber violences conjugales ». Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales | Centre Hubertine Auclert (accessed on 23 May 2025).

[69] Adamson, D.M. et al. (2023). "Cyberstalking: A Growing Challenge for the U.S. Legal System." RAND Corporation.

[70] Kobets, P.; Krasnova, K. (2018). "Cyberstalking: Public danger, key factors and prevention." *Przeglad Wschodnioeuropejski*, vol. 9, no. 2, (pp. 43–53).

[71] Adamson, D.M. et al. (2023). "Cyberstalking: A Growing Challenge for the U.S. Legal System"; Dulaurans, M. (2024). "Violences en ligne: décrypter les mécanismes du cyberharcèlement". Presses universitaires de Bordeaux.

[72] Kamara, I. (2023). "Cyberstalking and online platforms' due diligence in the EU Digital Services Act . Tilburg University. https://research.tilburguniversity.edu/en/publications/cyberstalking-and-online-platforms-due-diligenc e-in- the-eu-digita

[73] *Ibid.*

Recital 21 of Directive 2024/1385 highlights that, in most cases, perpetrators of online stalking are individuals close to the victim, such as family members, former partners or acquaintances. It also specifies that this is a form of violence that serves to reinforce existing coercive, controlling and manipulative behaviour. Women are disproportionately affected, being nearly twice as likely as men to experience online stalking,[74] while men constitute the majority of perpetrators.[75] The consequences for victims are significant and varied, ranging from the financial burden of moving house to the psychological effects, such as anxiety or post-traumatic stress disorder.[76]

2.2. The European legal framework

Article 6 of Directive 2024/1385 establishes that repeatedly or continuously placing a person under surveillance (without their consent or legal authorisation) using information and communication technologies (ICT) to monitor and observe their movements or activities constitutes a criminal offence when it is likely to cause significant harm to the person concerned.

Recital 21 of this text specifies that this includes surveillance enabled by the processing of the victim's personal data, such as password theft. It also, however, sets a limit on criminalisation, stating that surveillance may sometimes be justified, such as in the case of parents monitoring their children's location.

Directive 2024/1385 further distinguishes between "*tracking*" and "*monitoring*."
The first verb refers specifically to tracing the location of a person and following their

[74] Morgan, Rachel E; Jennifer L. Truman. (2022). "Stalking Victimisation, 2019". U.S. Department of Justice, Bureau of Justice Statistics.
[75] Dulaurans, M. (2024). *Op.cit.*
[76] Dreßing H.; Bailer J.; Anders A.; Wagner H.; Gallas C. (2014). "Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims." *Cyberpsychology, Behavior, and Social Networking*, 17(2), (p. 61–67).

movements, while the latter encompasses broader surveillance, particularly the observation of someone's activities. In both cases, the underlying purpose is to exert control over the victim.

Cyber stalking is addressed under current European law as a **form of sexist violence, given its serious impact on the physical and mental well-being of victims.** Although the French translation of the DSA refers only to "cyber harassment" and not to online stalking, the English version of recital 12 includes "*cyber stalking*" among the types of content considered illegal. Consequently, the obligations set out by the DSA regarding illegal content are likely to apply to cases of online stalking.

As such, online stalking falls within the scope of **Articles 34 and 35 of the DSA,** which require online platform providers to mitigate the risks arising from the design of their services.

The obligations of providers with respect to cyber stalking are analogous to those concerning the non-consensual sharing of intimate material. Under the DSA, hosting providers are required to report any suspected criminal offences to the competent authorities if they become aware of information indicating that a criminal offence threatening the life or safety of one or more persons has been committed, is being committed or is likely to be committed. **Given that cyber stalking poses a threat to individuals' lives or safety, it should be included among the offences that providers must report.** Furthermore, the inclusion of online stalking in the list of illegal content in recital 12 obliges hosting providers to ensure the prompt removal or inaccessibility of content constituting online stalking once notified.[77] Providers are also required to implement accessible and user-friendly mechanisms for notification and follow-up actions.[78]

[77] See recital 22, *Digital Services Act,* 2022.
[78] See recital 50, *Digital Services Act,* 2022.

2.3. The French legal framework

Under French law, online stalking is initially addressed by Article 226-1, paragraph 3, of the Criminal Code, which criminalises geolocation without the consent of the person concerned. This may involve installing tracking devices on objects (cars, bags etc.) or spyware on a phone. Aggravating circumstances apply when the acts are committed by the victim's partner, in which case the offence is punishable by two years' imprisonment and a fine of 60,000 euros.

Installing spyware on a phone, tablet or computer to monitor a victim's online activity may also constitute an offence against automated data processing systems (Articles 323-1 to 323-3 of the Criminal Code). Article 323-3-1 further establishes that the same penalties apply to the possession of a device enabling the offence under Article 323-1 to be committed.

Article 226-15 of the Criminal Code, which addresses breaches of confidentiality of correspondence, may also cover the interception of private communications (text messages, emails, online conversations) as well as the installation of spyware to monitor another person's communications and online activity. The second paragraph explicitly refers to "*the setting up of a device designed to produce such interceptions*." This behaviour is punishable by one year's imprisonment and a fine of €45,000. As with other provisions, an aggravating circumstance applies when the perpetrator is the victim's partner, increasing the penalty to two years' imprisonment and a fine of €60,000.

2.4. Analysis

The definition of online stalking in Directive 2024/1385 refers to the absence of the victim's consent to the act committed. To qualify as an offence, it appears necessary to combine the specific act with the violation of consent and the resulting harm. While this combination helps define the offence, it may also restrict the scope of criminal liability. Moreover, the "non-consensual" criterion could be used against victims in abusive relationships. Directive 2024/1385 only provides for cases where online stalking follows an initial offence, such as theft or hacking. Recital 21 of the Directive specifies that "*such surveillance might be enabled by processing the victim's personal data, such as by means of identity theft, by stealing passwords, by hacking the victim's devices, by secretly*

activating keylogging software to access the victim's private spaces, by installing geo-localisation apps, including stalkerware, or by stealing the victim's devices."

The current wording suggests that consent given by the victim may negate the classification of the offence. This does not account for situations in which consent is vitiated by emotional pressure, blackmail, or manipulation. For example, a woman may have temporarily authorised access to her data or accounts without consenting to their ongoing misuse. In such cases, having "authorised" access does not mean that consent is legally free and informed, particularly in contexts of psychological control or domination. When transposing the Directive into national law, this concept should therefore be clarified. Specifically, it should be stated that consent is only valid if given freely, without any pressure, coercion, or dependence.

Furthermore, Article 6 of Directive 2024/1385 includes harm to the victim as an element of the offence, requiring that the acts are "*likely to cause serious harm to that person*". However, the text does not provide a harmonised method for assessing this harm. The concept of "serious harm" is undefined, which may restrict criminal proceedings or result in inconsistent case law. Consequently, serious impacts (such as social isolation, loss of autonomy or persistent anxiety) might not be recognised as constituting "serious harm". Since the offence is defined in relation to the harm caused to the victim rather than independently of it, this terminology should be reworded or, at the very least, clarified when transposing the Directive into national law.

A directive must have a precise legal basis. Article 83 TFEU provides that directives may establish "*minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension.*" Accordingly, the preamble to Directive 2024/1385 states that the objective is to "*set minimum rules for the most serious forms of cyber violence, the relevant offences defined in this Directive are limited to conduct which is likely to cause serious harm or serious psychological harm to the victim or to conduct which is likely to cause the victim to seriously fear for his or her own safety or that of dependants*." The concept of significant harm is thus used to justify the seriousness of the acts and legitimise the need for Directive 2024/1385. However, it is the responsibility of Member States to ensure effective enforcement when transposing the Directive, and France should consider using more flexible terminology to replace "serious harm."

Under French law, there is no separate offence specifically defining and punishing online stalking. Nonetheless, the scope of Article 6 of Directive 2024/1385 is reflected in several provisions of the Criminal Code, most of which, since the enactment of Law No. 2020-936[79] provide for an aggravating circumstance when the behaviour is committed by the victim's partner. While French law targets very specific types of behaviour, such as geolocation, interference with automated data processing systems and violation of the secrecy of correspondence, Article 6 of Directive 2024/1385 encompasses a broader range of intentional acts aimed *at* "*repeatedly or continuously placing a person under surveillance* " without their consent or to "*track or monitor*" their movements and activities. **This demonstrates that the Directive has a significantly wider scope than the current French provisions, which are more narrowly defined.**

However, following the recent enactment of the 2020 Law, several court decisions have recognised the use of geolocation or breaches of the confidentiality of correspondence as constituent elements of coercive control. This concept was formally established as a pattern of domestic violence in five judgments handed down by the Poitiers Court of Appeal on 31 January

[79] Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

2024, one of which condemned the victim's partner for exercising coercive control by monitoring all her movements using electronic devices. While coercive control is already recognised as an offence in several Anglo-Saxon jurisdictions (England, Wales, and Ireland), it remains a subject of heated debate in France. In these decisions, coercive control is defined as "*a violation of human rights in that it prevents the victim from enjoying their fundamental rights,*" including the freedom of movement and the ability to maintain social ties.[80] The Court further identifies "*the tools of coercive control*" as "*a set of acts with the same objective of controlling and subjugating the victim and which, without this common concept, would be treated in isolation or even ignored."*
Since coercive control is not yet a standalone criminal offence in France, the judgments characterise each offence in its entirety and then situate it within the broader context of coercive control.[81] This approach, as understood by French case law, could be applied to online stalking, thereby filling the existing legislative gap.

Furthermore, since 2023, the French Minister for Equality, Isabelle Rome, has expressed her intention to incorporate the concept of coercive control in the Criminal Code, drawing on the definition developed by American sociologist Evan Stark.[82] According to Stark, coercive control refers to "*the use of force or threats*" and entails "*structural forms of deprivation, exploitation, and command that compel obedience indirectly by monopolizing vital resources, dictating preferred choices, microregulating a partner's behavior, limiting her options, and depriving her of supports needed to exercise independent judgment.*"[83] This approach is clearly aligned with the judgment delivered by the European Court of Human Rights (ECHR) in Tunikova and Others v. Russia on 14 December 2021,[84] in which the Court highlighted the inadequacy of national law in

---

[80] Muller, Y. (2024). "« Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire". *Le club des juristes.* Consécration de la notion de contrôle coercitif…. Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire - Le Club des Juristes

[81] *Ibid.*

[82] Stark, E. (2023). "Coercive Control: How Men Entrap Women in Personal Life". p.228

[83] *Ibid.*

[84] European Court of Human Rights. (2021). *Judgment Tunikova and Others v. Russia*. TUNIKOVA AND OTHERS v. RUSSIA.

[85] Greffière de la CEDH. (2021). Communiqué de presse « Manquements, constitutifs de violations, à l'obligation de traiter les cas de violences domestiques ; modifications législatives requises de toute urgence ». In particular, it called on the Russian government to "*introduce into its domestic law a definition of domestic violence covering manifestations of controlling and coercive behaviour, as well as stalking and harassment, whether occurring in person or online*."

addressing violence against women through the prism of coercive control, framing it as a violation of fundamental rights.[86] On 3 April 2025, the Senate adopted at first reading Bill No. 669 of 3 December 2024 aimed at strengthening the fight against sexist and sexual violence. Although the draft law, as initially amended by MPs, provided for the creation of a new offence of coercive control (directly in line with the Poitiers judgments), this provision was ultimately removed by senators, "*fearing constitutional censorship in view of the fragility of the concepts of fear and apprehension*"[87] which were included in the definition. Nevertheless, the Senate's version preserved the constituent elements of coercive behaviour by redefining the offence of intimate partner violence as "*repeated words or behaviour intended to or having the effect of seriously restricting the victim's freedom of movement or private and family life, or of constraining their daily life through psychological, economic or financial threats or pressure."* While the explicit reference to "*coercive control*" has been abandoned, this wording could nonetheless encompass acts that fall within the scope of online stalking, such as the use of geolocation devices.

The creation of a standalone criminal offence of coercive control that includes all forms of violence in greater detail, as initially proposed by the Assemblée nationale on 28 January 2025 in Article 3 of the draft law, would have been more effective. By explicitly targeting *"the sole intention of the perpetrator to control and subjugate the victim,"* [89] such an offence would ensure a more adequate criminal response and provide broader alignment with the scope of Article 6 of Directive 2024/1385.

> "*Art. 222-14-3-1. – Without prejudice to the application of Articles 223- 15-3 and 222-33-2-1 of the Criminal Code, the act of imposing coercive control over one's spouse, civil partner or cohabiting partner through repeated or multiple statements or behaviour that infringe upon the victim's fundamental rights and*

---

[86] Hardouin-Le-Goff, C. (2023). "L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales? " " *Le club des juristes.* The criminalisation of coercive control: a future tool in the fight against domestic violence? - Le Club des Juristes.

[87] Public life. (2025). " Vie publique. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexistes et sexuelles ». Violences sexuelles et sexistes Contrôle coercitif Viol Proposition loi | vie-publique.fr..

[88] *Ibid.*

[89] Muller, Y. (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

freedoms or creating an atmosphere of fear and coercion in her home due to the fear of acts carried out directly or indirectly against herself or others, whether these acts are physical, psychological, economic, legal, social, administrative, digital or of any other nature, shall be punished by three years' imprisonment and a fine of €45,000 where such acts have caused total incapacity to work for a period of up to eight days or have not resulted in any incapacity to work."

[Article 3 of the draft law aimed at strengthening the fight against sexist and sexual violence[90]]

[90] Assemblée Nationale. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexuelles et sexistes ».

3. Cyber harassment

3.1. Context

In a report on the digital dimension of violence against women,[91] GREVIO refined the definition of harassment to include the online sphere. GREVIO stressed that Article 34 of the Istanbul Convention[92] must be interpreted as covering acts of harassment carried out with ICT to ensure effective protection under the Convention:

> *"The threatening behaviour may consist of repeatedly following another person, engaging in unwanted communication with another person or letting another person know that he or she is being observed. This includes physically going after the victim, appearing at her or his place of work, sports or education facilities, as well as* ***following the victim in the virtual world (chat rooms, social networking sites, etc.)."***

The President of the 77th United Nations General Assembly (September 2022 to September 2023) noted that *"[women] are 20 per cent less likely than men to use the Internet, but 27 times more likely to face online harassment or hate speech when they do."* [93]

According to a study on violence against women by the European Union Agency for Fundamental Rights,[94] **one in five young women report experiencing at least one instance of sexual cyber harassment since the age of 15**, and one in four teenage girls

---

[91] Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO).(2021). "General Recommendation No. 1 on the digital dimension of violence against women." https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

[92] Council of Europe. (2011). "Convention on preventing and combating violence against women and domestic violence". STCE 210 - Council of Europe Convention on preventing and combating violence against women and domestic violence.

[93] Csaba, K. (2023). "Message at the 67th session of the Commission on the Status of Women, UN."

[94] EU Agency for Fundamental Rights. (2014). Report: "Violence against women: an EU-wide survey.". https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-factsheet_fr.pdf.

report being victims of online humiliation and harassment related to their attitude, physical appearance, love life, or sexual behaviour.

3.2. The European legal framework

Cyber harassment is addressed in Article 7 of Directive 2024/1385, which sets out the acts constituting the offence and requires EU Member States to criminalise them at the national level. These acts include using ICT to threaten a person, acting alone or as part of a group, as well as practices such as "*cyberflashing*"[95] and "*doxing.*"[96]

Recital 12 of the DSA classifies online harassment as illegal content, meaning the obligations applicable to such content also apply here.[97] Recital 22 requires **service providers to ensure the prompt removal of this content,** which Recital 50 requires them to implement user-friendly **mechanisms for reporting or notifying illegal content.**

Articles 4, 5 and 6 of the DSA lay down the exceptions to the principle of provider liability. Article 6, in particular, grants hosting providers an exemption from liability for illegal content provided that they **were unaware** of its presence or **acted swiftly** to remove it once notified. Failing this, they may be held liable. However, Article 8 specifies "*No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers*." This provision significantly limits their duty of vigilance and risks **narrowing the practical effectiveness of this regulation.**

---

[95] European Parliament and Council. (2024). *Op.cit.*, recital 24. " *the unsolicited sending of an image, video or other similar material depicting genitals to a person.* "

[96] *Ibid.* "*the personal information of the victim is made available to the public by means of ICT, without the victim's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to the victim*."

[97] European Parliament and Council. (2022). *Op. cit.*, recital 12. "*Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking*."

In addition, under Article 18 of the DSA, providers may incur liability if they fail to inform competent authorities of illegal content they host. For example, **if a provider were to host doxing material or other content falling under Article 7 of Directive 2024/1385, without notifying the relevant authorities, it could be held accountable under Article 18.**

Finally, Articles 34 and 35 are equally relevant here. Content disseminated for the purpose of cyber harassment[98] is not only unlawful but also contributes to violence against women and has severe consequences for the physical and mental well-being of individuals. **Providers are therefore required to assess the risks of cyber harassment on their services and to implement effective mitigation measures.**

3.3. The French legal framework

To understand how Directive 2024/1385 may be transposed, it is essential to examine the framework in French criminal law concerning offences of cyber harassment.

As noted above, cyber harassment is a multifaceted form of violence that is part of a broader phenomenon of "*technology-facilitated violence.*" Its complexity and wide-ranging consequences cannot be fully captured by reference to Article 222-33-2 of the Criminal Code alone. Several different offences may be brought within this category.

"Classic" or "moral" cyber harassment is a criminal offence punishable under Article 222-33-2 of the Criminal Code. The use of digital tools acts as an aggravating circumstance: cyber harassment is therefore punishable by two years' imprisonment and a fine of €30,000.

[98] European Parliament and Council. (2024). *Op. cit,* recital 24. For example, as mentioned above, sharing the victim's personal information via ICT with the aim of inciting others to cause them harm.

Article 222-33-2-1 criminalises "*the act of harassing one's spouse, civil partner or live-in partner through repeated words or behaviour intended to or resulting in a deterioration of their living conditions, manifested by an alteration of their physical or mental health*". The provision also applies to acts committed by a former spouse, former live-in partner or former civil partner.

Cyber harassment of a sexual nature is criminalised under Article 222-33 of the Criminal Code: "*Sexual harassment is the act of repeatedly subjecting a person to words or behaviour of a sexual nature that either undermine their dignity because of their degrading or humiliating nature, or create an intimidating, hostile or offensive situation for them*." Paragraph 6 of section III specifies that the use of an online public communication service, or of digital or electronic media, constitutes an aggravating circumstance, increasing the maximum sentence from two to three years' imprisonment.

Both offences are deemed to be committed when the same victim is subjected to such conduct by several persons acting in concert, or at the instigation of one of them — even if each individual is not guilty of repeated action. The offence is also constituted when the same victim is targeted successively by several persons who, even in the absence of concerted action, are aware that their statements or behaviour form part of a repeated pattern (Article 222-33 and Article 222-33-2-2). By the Law of 3 August 2018,[99] the legislator specifically sought to address group cyber harassment, commonly referred to as "digital raiding". In a ruling of 29 May 2024[100], the Criminal Division of the Cour de cassation provided important clarification on how the offence of cyber harassment should be characterised. The Court held that the mere fact of the defendant's awareness that their act formed part of a pattern of behaviour was sufficient; consequently, trial judges were not required to identify, date and categorise each individual message sent by others against the victim. Nor was it necessary to establish that the plaintiff's message was actually read by the person targeted.

It follows that the publication of a single malicious message online, directed against a person already subjected to insults or threats on social media, may be sufficient to constitute the offence.

[99] Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexistes et sexuelles. (2018).
[100] Cour de cassation, Chambre criminelle. Arrêt du 29 mai 2024, n°23-80.806.

Paragraph d) of Article 7 of Directive 2024/1385 stipulates that cyber harassment includes: "d*) making accessible to the public, by means of ICT, material containing the personal data of a person, without that person's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to that person*."

This offence, commonly known as "*doxing*", consists of disclosing the identity of an internet user and thereby endangering their privacy. The information revealed may vary widely; it can include email addresses, telephone numbers, full names, or details about a person's professional life. Such acts represent a serious violation of privacy and illustrate the principle that online violence is not separate from, but rather a direct extension of, offline violence – forming a continuum of harm. In French law, Article 223-1-1 of the Criminal Code punishes with three years' imprisonment and a fine of €45,000 "*the act of revealing, disseminating or transmitting, by any means whatsoever, information relating to the private, family or professional life of a person that enables them to be identified or located for the purpose of exposing them or members of their family to a direct risk of harm to their person or property that the perpetrator could not have been unaware of.*"

Similarly, Article 226-1 – already discussed above in relation to the unauthorised sharing of intimate or manipulated material – deserves renewed attention, particularly paragraph 3, which criminalises "*capturing, recording or transmitting, by any means whatsoever, the real-time or delayed location of a person without their consent*."

Finally, Article 226-4-1 punishes "the *act of usurping the identity of a third party or using one or more pieces of data of any kind that could identify them with the intention of disturbing their peace or that of others, or of damaging their honour or reputation*," with aggravated penalties where the offence is committed via a communications network.

Repeatedly sending malicious messages or making malicious phone calls (Article 222-16 of the Criminal Code) may also fall within this context. Such acts contribute to the creation of a climate of continuous insecurity through the misuse of communication tools. When these acts are committed by a spouse, live-in partner or partner linked to the victim by a civil partnership, the penalty is three years' imprisonment and a fine of £45,000. Similarly, the offence of fraudulent

collection of personal data is criminalised under Article 226-18 of the Criminal Code. The commission of this offence is punishable by five years' imprisonment and a fine of €300,000.

3.4. Analysis

The formulation of the offence of moral harassment in French criminal law has been criticised by some authors for its use of vague terms, such as "*repeated acts*" or "*deterioration of living conditions and impairment of physical or mental health*". To constitute moral harassment, the acts must be capable of producing the consequences intended by law, namely "*a deterioration in the victim's living conditions resulting in an impairment of physical or mental health*." The law therefore imposes a dual requirement for establishing the offence: **not only must a deterioration in living conditions be demonstrated, but this deterioration must also have caused harm to the victim's physical or mental health.** This was confirmed by a ruling of the Criminal Division of the Cour de cassation on 9 May 2018[101] which found that the Court of Appeal had failed to show how the acts alleged against the defendant were intended or had the effect of degrading the victim's living conditions, resulting in harm to his physical or mental health. This decision reflects a material approach to the offence, requiring proof of actual impairment to the victim's health. This approach has been criticised for effectively denying the principle that "*punishment cannot depend on the victim's ability to resist psychological harassment."*[102]

Many experts also argue that the article fails to meet "*the constitutional objective of accessibility and intelligibility of the law enshrined in a decision of the Constitutional Council dated 16 December 1999.*"[103]

---

[101] Cour de cassation, Chambre criminelle. Arrêt du 9 mai 2018, n° 17-83.623.
[102] Segonds, M. (2014). « Un an de droit pénal du travail », *Dr. pénal. chron.*
[103] Chauvet, D. (2015). « Mérites ou démérites du délit général de harcèlement moral créé par la loi du 4 août 2014 ?". *Recueil Dalloz*, 2015, (page 174).).

It is therefore worth considering a review of the wording of this article when transposing Directive 2024/1385.

Under the Directive, Article 7 establishes thresholds for criminalisation. For 'cyberflashing', "doxing" and 'group threats', at least those behaviours likely to cause significant psychological harm to the victim must be criminalised. For threatening behaviour covered by paragraph (a), at least threats relating to the commission of criminal offences shall be punishable if they are likely to cause the victim to fear for their safety or that of their dependants.

While this provision obliges Member States to criminalise acts of cyber harassment, as noted in Recital 24, it primarily requires them **to implement minimum rules covering the most serious forms of such behaviour.** This includes forms of cyber harassment considered by the Directive to be likely to cause significant psychological harm, such as group attacks or harassment that occurs partly offline.[104] The article explicitly refers to the harm caused to the victim as part of the definition: the acts must be "*likely to cause serious harm*." However, **Directive 2024/1385 does not provide a harmonised method for assessing such harm. As the concept of serious psychological harm remains open to interpretation, this requirement may create obstacles for individuals seeking to assert their status as victims.**

[104] European Parliament and Council. (2024). *Loc cit.*

4. Inciting violence or hatred online

4.1. Context

Inciting to hatred refers to "*any act, attitude or behaviour that incites hatred towards others,*" [105] or, more specifically, to acts that encourage harmful action against an individual or group.[106] While the most familiar form today remains incitement to racial hatred,[107] many countries, including France, have recognised incitement to hatred based on religion, sexual orientation and disability.[108]

Members of minority groups are among the most affected by this phenomenon.[109] However, as frequent targets of sexist and sexual violence, women and girls are also recurrent victims.[110]

When such incitement occurs online, its impact is amplified by current events or conflicts reported in the media, often generating fear and anxiety for those targeted. Despite these serious consequences, the removal of hate speech and harmful content largely depends on the voluntary action of service providers, and initiating criminal proceedings against anonymous users remains practically challenging.[111]

Paragraph 25 of the preamble to Directive 2024/1385 notes that the widespread use of communication tools, the internet and social media has led to a sharp rise in incitement to violence, in particular sexist violence. The anonymity afforded by these tools facilitates the dissemination of hateful content. Women are therefore particularly vulnerable and often become targets of online hate speech, which can escalate into offline crimes and offences.

---

[105] Cammillieri-Subrenat A. (2002). « L'incitation à la haine et la Constitution ». *Revue internationale de droit comparé*. vol. 54. n°2. (p. 513-548).

[106] Gordon, G.S. (2013). "Hate Speech Persecution: A Contextual Approach". *Vanderbilt Journal of Transnational Law*. vol. 303. no. 2. pp. 303-373.

[107] Demaske, C. (2023). « L'opérationnalisation des discours de haine à l'échelle de la communauté Un plan de lutte contre les discours de haine ». *Réseaux,* vol. 241. n°5. (p. 197-235).

[108] *Ibid*.

[109] United Nations. "Hate speech: Impact and prevention: Targets of hate." Available at: https://www.un.org/fr/hate-speech/impact-and-prevention/targets-of-hate (accessed 23 May 2025).

[110] United Nations. *Ibid.*

[111] Humanrights.ch. (2016). "« Incitation à la haine sur Internet – Cas suisses et politique des portails d'informations en la matière ». https://www.humanrights.ch/fr/pfi/droits-humains/droits-politiques/incitation-haine-internet-cas-suisse s-politique-portails-informations (accessed on 23 May 2025).

4.2. The European legal framework

4.2.1. Digital Services Act

Recital 12 of the DSA classifies "*illegal hate speech*" as content that is considered unlawful. Recital 40 further specifies that, to ensure a safe and transparent online environment, measures must be implemented to protect the safety and trust of service users, particularly consumers, minors and individuals especially vulnerable to hate speech. Although these recitals are not legally binding, they provide guidance for interpreting the objectives and scope of the legislative text.

As noted above, Articles 34 and 35 of the DSA require online platform providers to **analyse and assess the systemic risks present on their platform and to implement measures to mitigate them.** These risks specifically include "*any actual or foreseeable negative effect [….] on gender-based violence.*"[112]
Gender-based violence, which according to a European Parliament report refers to **any form of violence directed against a woman because of her gender or which disproportionately affects women,**[113] may encompass incitement to hatred or targeted violence. Inciting gender- based hatred constitutes a form of gender-based violence in that it undermines women's freedom of expression, seeking to humiliate, objectify, diminish skills and opinions, destroy reputations, render women vulnerable and fearful, and punish women for failing to conform to prescribed behaviours.[114]

---

[112] European Parliament and Council. (2022). *Op.cit.*, Article 34(d).
[113] European Parliament. (2020). "Violence against women in the European Union: State of the Union".
[114] Council of Europe. *Factsheet on Combating sexist hate speech*. p. 5.

The severe consequences of this practice, whether psychological, emotional or physical[115], mean that it falls within the definition of violence against women as defined in Article 3 of the Council of Europe Convention on preventing and combating violence against women and domestic violence: the term "violence against women" *is "understood as a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."* In this context, noting that online sexist hate speech can also lead to offline hate crimes, Recital 25 of Directive 2024/1385 states: "*[This] conduct needs to be prevented or intercepted at an early stage. The language used in that type of incitement does not always directly refer to the gender of the targeted person, but the biased motivation can be inferred from the overall content or context of the incitement."*

More broadly, the Council of Europe defines sexism as: *"the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline."*[116] Although the European Convention on Human Rights is a non-binding instrument, its States Parties, including France, are expected to follow the Council of Europe's recommendations. Accordingly, they must combat sexist speech in the media, public spaces, education and the courts, and therefore address online sexist hate speech insofar as it constitutes violence against women.

Under the DSA, platform providers are thus subject to a series of obligations that indirectly address incitement to hatred and violence against women, recognising such acts as a form of sexist violence.

4.2.2. 2016 Code of Conduct

To address the proliferation of racist and xenophobic hate speech

[115] *Ibid.*

[116] Council of Europe. (2019). "Recommendation on preventing and combating sexism". CM/Rec(2019)1.

online, the European Commission, in collaboration with four major information technology companies (Facebook, Microsoft, Twitter and YouTube), presented a "Code of Conduct on Countering Illegal Hate Speech Online" on 31 May 2016.

Since then, other platforms such as Instagram, Snapchat, Dailymotion, TikTok, LinkedIn, and Twitch (in spring 2022)[117], have also applied this code. The code of conduct is a **voluntary commitment** by online platforms and is not a legally binding instrument for Member States.

The Code encourages technology companies to adopt clear and effective procedures to prevent and stop the spread of hate speech on their services. Illegal hate speech is defined as "*publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin.*"[118] **It does not cover hate speech of a sexist nature.**

These procedures aim, among other things, to review valid reports and subsequently **remove or block illegal content within 24 hours**. To ensure the reliability of reports, companies are expected to verify that **content flagged as inciting violence or hatred comes from experts, particularly through partnerships with civil society organisations that form a network of "trusted flaggers" communicated by the Commission.**

An assessment carried out by the European Commission in 2022[119] revealed that, on average, 69.6% of content inciting murder or violence against the referenced groups was removed, and 59.3% of content defaming these groups was removed.

The Code therefore establishes a framework with clear guidelines for platforms, helping to prevent and address hate speech. As part of transposing Directive 2024/1385, a similar initiative could be

---

117 European Commission. (2022). Press release: "EU Code of Conduct against online hate speech: latest evaluation shows slowdown in progress".
118 Council of the European Union. (2008). "Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law".
119 European Commission. (2022). "Countering illegal hate speech online 7th evaluation of the Code of Conduct".

considered to target incitement to violence and hatred specifically against women and girls. However, since the measures in this Code apply only to participating platforms and are not legally binding, the framework is insufficient to effectively combat this type of online violence.

4.2.3. 2008 Framework Decision

Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia through criminal law was adopted by the Council of the European Union in 2008. Its primary objective is to criminalise conduct that incites hatred and violence, and to ensure that Member States take effective measures, both criminal and preventive, to combat these phenomena. Although the Framework Decision does not create new offences per se, it imposes transposition obligations on Member States, requiring that acts such as incitement to hatred and racist or xenophobic violence be punishable under national law.

Article 1 specifies that public incitement to violence or hatred, through acts such as the public dissemination of written or visual material, must be punishable, particularly when directed against a group defined by race, colour, religion, descent or national or ethnic origin.[120] While the text initially focuses on groups defined by racial or ethnic criteria, **this approach can conceivably be extended to combat sexist violence and incitement to hatred or violence specifically targeting women.**

Like Article 8 of Directive 2024/1385, Article 1 of the Framework Decision adopts a restrictive approach, limiting the obligation to criminalise conduct likely to cause a breach of public order. It also provides that incitement or aiding and abetting such acts shall be punishable.[121] The Framework Decision further strengthens the concept of liability by including legal persons, defined

[120] Council of the European Union. (2008). *Op. cit.*, Article 1.
[121] *Ibid.* Articles 2 and 3,

as *"any entity having such status under the applicable national law, with the exception of States or other public bodies in the exercise of State authority and public international organisations."*[122] Each Member State must ensure that **legal persons** can be held **criminally liable** for offences committed on their behalf by individuals exercising managerial authority. Liability may also arise from **failure to supervise,** which enables such acts to be committed. This does not exclude the liability of the individuals involved.[123] **Holding legal persons responsible for incitement to hatred is crucial, as they often play a central role in disseminating messages** (such as platforms or companies), and without such liability, they could evade accountability for failing to remove hateful content. It also incentivises the implementation of preventive controls.

Framework Decisions sets out objectives to be achieved, leaving Member States free to choose the means of implementation. In France, a bill to transpose Framework Decision 2008/913/JHA was tabled on 6 February 2013[124] and could serve as a basis for inspiration for a similar adaptation. However, France's transposition has been partial: according to a 2024 EU Commission report, the bill reflected a restrictive approach, and certain provisions (particularly concerning the liability of legal persons) have not been fully incorporated into national legislation.

---

[122] *Ibid*. Article 5.4.
[123] Council of the European Union. (2008). *Op. cit.,* Article 5.
[124]Proposal for a law by Ms Valérie BOYER and several of her colleagues aimed at transposing into domestic law Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, No. 690, tabled on 6 February 2013.
[125] European Commission. (2014). "Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law."

4.3. The French legal framework

French criminal law currently includes several provisions aimed at combating incitement to violence, including incitement to racial hatred. Notably, Article 24 of the Law of 29 July 1881 on freedom of the press[126] penalises **provocation of sexism in the public space (**"*those who incite hatred or violence against a person or group of persons on grounds of their sex, sexual orientation or identity or disability*") as well as incitement to commit an offence ("*those who directly incite others to commit intentional attacks on life, intentional attacks on the integrity of the person and sexual assault*").

French law further provides for **aggravating circumstances** when such offences are committed against a person because of their **gender, sexual orientation, gender identity, or disability**, as set out in **Articles 32 and 33** of the same law.

4.4. Analysis

Incitement to violence or hatred online constitutes a criminal offence under Directive 2024/1385. Article 8 provides that: *"Member States shall ensure that intentionally inciting violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement is punishable as a criminal offence. (1)"*

Furthermore, "*for the purposes of paragraph 1, Member States may choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting. (2)*" However, paragraph 2 limits the scope of the article and allows certain States to punish only the most extreme or visible manifestations of hatred, possibly excluding more subtle, insidious, but equally discriminatory or hateful statements.

[126] Law of 29 July 1881 on freedom of the press. (Version in force since 25 May 2025).

Recital 25 clarifies that the language used in such incitement does not always explicitly reference the gender of the target. Nevertheless, such statements can still be considered as targeting a group or individual based on gender, as a discriminatory motive can be inferred from context or provocative comments.

Another limitation, set out in recital 26, concerns the definition given to *public dissemination*. The Directive specifies that this only includes situations where

"*users seeking to access the material are automatically registered or admitted without a human decision or without selecting to whom access is granted.*" This distinction, however, does not align with digital realities – very little is truly private online. **As a result, serious offences committed in private spaces, messaging apps such as WhatsApp, or online forums may fall outside the scope of the Directive, even though non-consensual content often circulates widely in these spaces.** Private social media loops can sometimes include **thousands of participants** and yet be considered non-public virtual spaces, thereby limiting the application of Article 8. This is evident in large WhatsApp and Telegram groups, where sexual assault, calls for rape, misogynistic and racist comments, and harassment frequently occur.[127]

These groups, which have sometimes included up to **70,000 men**,[128] are difficult to monitor due to their semi-private nature. Yet, beyond the online violence that occurs within them, they also **facilitate radicalisation** and contribute to **offline offences**.

---

[127] Garnier P. (2024). « Mascus, les hommes qui détestent les femmes – Le documentaire ». *Made In Perpignan*. https://madeinperpignan.com/mascus-hommes-detestent-femmes-documentaire-tv/ (accessed on 22 June 2025).

[128] Ouest France. (2024). « Sur Telegram des milliers d'hommes échangeaient des conseils pour droguer et violer des femmes »." . https://www.ouest-france.fr/faits-divers/violence-sexuelle/viol/sur-telegram-des-milliers-dhommes-echangeaient-des-conseils-pour-droguer-et-violer-des-femmes-44497442-c537-11ef-a562-4e48a3fc537f (accessed on 22 June 2025).

[129] Jaki S, De Smedt T, Gwozdz M, *et al.* (2019). "Online hatred of women in the Incels.me forum: Linguistic analysis and automatic detection." *Journal of Language Aggression and Conflict*, vol. 7, no. 2, pp. 240-268.

By restricting the recognition of the offence to public settings, the Directive risks underestimating the impact of violations of victims' privacy. It implies that content shared in a private space is less harmful, whereas, in reality, content shared online, even in a restricted setting, immediately escapes the victim's control and becomes irreversible.

This approach contradicts the principles protected by the European Convention on Human Rights (ECHR), which guarantees the right to privacy and dignity.

Directive 2024/1385 refers to content that is "publicly" accessible, which risks excluding subscription-based sites such as OnlyFans from its scope. However, such platforms are evidently often facilitators of numerous offences. According to the French association Mouvement du Nid, OnlyFans contributes not only to the normalisation of commodified sexuality, but also to the normalisation of online services used as "spaces where prostitution rings can scout for victims,"[130] with child prostitution rising sharply in recent years from 21 cases in 2015 to 192 cases in 2022.[131] OnlyFans is an online subscription service, primarily used for pornographic content, in which "content creators" directly monetise their posts for subscribers. Article 3 (I) of the Digital Services Act defines an online platform as "*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.*" OnlyFans fits this definition as a hosting service with interactive functionality and should therefore be considered an online platform under the DSA.

---

130 Ferrand, E. (2021). « Sur Onlyfans, les jeunes peuvent être facilement repérés par des proxénètes ». *Le figaro.*. https://etudiant.lefigaro.fr/article/sur-onlyfans-les-jeunes-peuvent-etre-facilement-reperes-par-des-reseaux- de-proxenetes_c88b05ea-607d-11eb-8fde-d92bf2ba0bfe/.

131 High Council for Equality. (2023). " « Pornocriminalité : mettons fin à l'impunité de l'industrie pornographique. ». https://haut-conseil-egalite.gouv.fr/IMG/pdf/hce-vio-rapport_pornocriminalite-v11-bdef.pdf

As such, it is subject to a range of European obligations under the Digital Services Act. Furthermore, Recital 18 of the preamble to Directive 2024/1385 clarifies that the terms "accessible to the public" and "publicly accessible" should be interpreted in terms of the potential reach of the content. In 2022, OnlyFans had over 3.2 million creators worldwide and nearly 239 million "*fans.*"[132] While based on a subscription model, its content is accessible to thousands of people and therefore qualifies as "publicly accessible." Including OnlyFans within the platforms covered by the DSA and Directive 2024/1385 would make the site liable for illegal content posted on its platform, requiring it to implement proactive means for de-listing, reporting and removal.

[132]Radio France. (2023). ""OnlyFans, plateforme favorite des créateurs de contenus sexuels, attire toujours plus d'utilisateurs." https://www.radiofrance.fr/mouv/podcasts/reporterter/onlyfans-plateforme-favorite-des-createurs-de-c ontenus-sexuels-attire-toujours-plus-d-utilisateurs-1200317

RECOMMENDATIONS FOR THE TRANSPOSITION OF DIRECTIVE 2024/1385

1. General recommendations

a. Recommendations at the French level

- Establish a National Council of Survivors and Victims in France, modelled on the German framework. The primary mission would be to provide public policy recommendations aimed at preventing and responding to cyber violence against women and girls.
    - The Council should be attached to an independent authority that also houses an investigative commission and a dedicated research centre.

b. Recommendations at the European level

- Strengthen the obligation of digital service providers to report any suspected criminal offences detected on their platforms to the competent authorities.
    - Impose shorter response times for legal requests directed at platforms and service providers.
    - Introduce dissuasive penalties for non-cooperation or delayed response to requests from authorities, such as financial sanctions or suspension of services.

- Require platforms to provide regular reports on their moderation activities to a competent authority, such as the European Commission, as part of the European Regulation on combating the dissemination of terrorist content online.

These reports could help identify and correct gender bias in algorithms and improve the regulation of illegal content.

- Establish regular audits of moderation mechanisms conducted by competent authorities, such as the Commission or certified independent auditors.

2. Sharing of intimate material (Article 5)

a. Recommendations at the French level

i. Legislative recommendations

- Clarify the concept of "sexual nature" used in Article 226-2-1 of the Criminal Code, which is currently too vague and subjective. A more precise reformulation, such as "images with sexual connotations or relating to bodily intimacy" would provide greater legal certainty while strengthening victim protection.

- Include subscription-based platforms offering sexually explicit content, such as Only Fans, within the scope of the transposition of Directive 2024/1385. At present, these platforms are not taken into account.[133]

- Amend the wording of Article 5 of Directive 2024/1385 during its transposition into French law. The current formulation – "*where such conduct is likely to cause serious harm to that person"* – is too restrictive. A broader formulation, such as "where such conduct is likely to impair the living conditions, mental health or safety of the person concerned" would lower the evidentiary threshold and ensure broader protection.

- Go beyond the minimum definition provided by the Directive when transposing it into national law, to prevent the offence from being ineffective in practice.

[133] Interview with Mariana Branco. (2 June 2025).

- The transposition text should specify that consent is only valid when given free from any relationship of dependence, pressure or manipulation, particularly in contexts of intimate relationships, minority or vulnerability.
- This clarification would exclude situations where the victim has "consented" to grant access to their accounts in an environment marked by control or coercion.

ii. Recommendations for adapting existing measures

- Require de-listing at the European level once content has been reported.
  - To ensure stronger protection for victims, the removal of illegal content should be required across all European versions of the relevant search engines and platforms once such content has been reported.
  - The Authority for Audiovisual and Digital Media Regulation could be tasked with monitoring the effectiveness of removals and penalising non-compliance. This would also necessitate enhanced cooperation between regulatory authorities across Member States.

- Promote the widespread use of digital signature and hashing technology so that platforms proactively detect and remove reuploaded content. This could involve integrating hashing into the reporting process (whereby reported content is hashed by the platform, which must then detect and remove all identical material) or strengthening collaboration with organisations already equipped with hashing tools, such as Point de contact or StopNCII. Platforms could, for example, be required to collect and apply hash data provided by these entities in their moderation processes.
  - Platforms should also be subject to a requirement to carry out periodic audits to identify traces of hashed content within their systems, with a corresponding obligation to ensure its removal.

- A European centre for hash centralisation could also be established, enabling the systematic removal of content that individuals wish to protect.

- Strengthen reporting tools for platform users by making them more visible, simple, accessible and effective.
  - Visibility: Platforms should launch information campaigns highlighting the reporting options available and explaining clearly how users can make use of them.
  - Accessibility: Platforms could draw inspiration from the "symptoms first" method[134] tested by Twitter in the United States. Instead of requiring users to categorise or describe the harmful content themselves, this method guides them through a structured questionnaire. The user indicates the type of harm experienced, with concrete examples such as harassment, non-consensual sharing of intimate material, or incitement to online hatred. It also allows the user to specify whether the content is racist, sexist, or homophobic. Twitter has emphasised that this approach uses simpler, more comprehensible language, making the reporting process more user-friendly. Other approaches, such as Facebook's model of removing reported content immediately – with reinstatement only after thorough verification – [135] could provide a safer system in which takedown is the default, thereby reducing the risk of ongoing harm to victims.

- Expand recognition of civil society actors as trusted flaggers to enhance user protection and ownership of the reporting process.

---

[134] Common Thread. (2021). "Twitter's new reporting process centres on a human-first design." https://blog.x.com/common-thread/en/topics/stories/2021/twitters-new-reporting-process-centers-on-a-human-first-design (accessed 22 June 2025).

[135] Public service. (2024). "How do I report illegal content posted on the Internet." https://www.service-public.fr/particuliers/vosdroits/F31979?lang=en (accessed 22 June 2025).

Currently, ARCOM recognises certain entities as trusted flaggers, such as associations and organisations with proven expertise in areas like child protection or the fight against anti-Semitism and racism. While Point de contact is a trusted flagger for cyber violence, there is no actor dedicated specifically to sexist cyber violence. It would therefore be appropriate for ARCOM to designate such an organisation. Involving civil society actors who are closely attuned to users' needs would not only improve integration of users into the reporting process but also ensure they receive more tailored support when reporting harmful content. However, ARCOM has specified[136] that any association wishing to obtain trusted flagger status must demonstrate recognised expertise and skills in detecting and identifying illegal content, maintain independence from online platform providers, and carry out its activities with diligence, accuracy, and objectivity.

.

b. Recommendations at the European level

- Introduce a binding injunction procedure requiring hosting providers to remove or block non-consensual intimate content within one hour of notification by a competent national authority. This procedure should operate under the supervision of the European Commission, following the model of the EU Regulation on combating the dissemination of terrorist content online.

- Ensure immediate protective measures upon notification by temporarily suspending access to the reported content while verification is carried out to minimise further harm to victims.[137]

- Simplify and centralise reporting procedures through the establishment of a national coordination system, modelled on the PERCI platform, to allow the unified transmission of reports and injunctions to hosting providers.

[136]ARCOM. « Signaleurs de confiance : conditions et candidatures ». https://www.arcom.fr/espace-professionnel/signaleurs-de-confiance-conditions-et-candidature s (accessed 22 June 2025).

[137] Interview with Céline Piques. (30 May 2025).

Such centralisation must be supported by enhanced human and technical resources for the competent authorities to guarantee swift and effective handling of cases.

- Strengthen the right to erasure under Article 17 GDPR by enabling the expedited removal of non-consensual intimate content based on a simple victim's declaration, particularly via "trusted flaggers," without requiring prior judicial authorisation. Removals should occur within a strict timeframe (e.g. one hour), with substantial financial penalties for providers who fail to comply.

- Implement a monitoring and automatic de-listing mechanism to prevent the re-uploading of content once removed. This could be coordinated by a dedicated body based on the PERCI model.

- Establish a European centre for regulation, coordination and research, linked to EUROPOL, with the mandate to proactively detect and remove illegal content.[138]
    - This centre should also provide a dedicated forum to support victims.

3. Online stalking (Article 6)

a. Recommendations at the French level

i. Legislative recommendations

- Adapt the wording of Article 6 of Directive 2024/1385 in the transposition process: "*where such conduct is likely to cause serious harm to that person.*" This could be reformulated more flexibly as: *"where such conduct is likely to adversely affect the living conditions, mental health, or safety of the person concerned."* Such a change would lower the threshold for qualifying harm and ensure broader protection for victims.

[138] Based on the model of the proposed regulation to combat child pornography on the internet. Interview with Mié Kohiyama. (3 June 2026).

- Introduce a distinct offence of coercive control that explicitly covers all forms of violence, including digital violence, as initially proposed by the National Assembly on 28 January 2025 in Article 3 of the draft law. This provision would recognise *"the sole intention of the perpetrator to control and subjugate the victim"*[139] thereby more effectively capturing the scope of behaviour targeted by Article 6 of Directive 2024/1385.

4. Online sexual harassment (Article 7)

a. Recommendations at the French level

i. Legislative recommendations

- Remove the requirement of "serious fear for one's own safety or that of persons under one's care" from Article 222-33-2 of the Criminal Code.

- Adapt the wording of Article 7 of Directive 2024/1385 ("*where such conduct is likely to cause serious psychological harm to that person*") in the transposition process to a more flexible formulation: *"where such conduct is likely to impair the living conditions, mental health, or safety of the person concerned."* Such a revision would make the harm threshold less restrictive and allow for more effective protection of victims.

ii. Recommendation for adapting existing mechanisms

- It would be appropriate here to apply the above recommendation on adding civil society actors to the list of trusted reporters.

[139] Muller, Y. (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

5. Sexist hate speech (Article 8)

a. Recommendations at the French level

i. Legislative recommendations

- Clarify the legal definition of incitement to hatred.
    - Remove the wording "conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting" which narrows the scope of the provision and restricts punishment to only the most extreme forms of hate speech.
    - Remove the phrase "by publicly disseminating", which excludes private groups on social media and communication platforms from its scope.
    - Define incitement to hatred more broadly as " *any act or behaviour which, through speech, writing, images, or any other means of communication, encourages, provokes, or directly incites discrimination, hostility, or violence against a person or group of persons on the basis of their origin, ethnic, national, or religious affiliation, gender, sexual orientation, disability, or any other characteristic protected by law.*"

Table of contents

Acknowledgements **1**
Methodology **2**
Introduction **6**
Analysis **12**
1. Non-consensual sharing of intimate or manipulated material 12
1.1. Context 12
1.2. The European legal framework 13
1.2.1. The Digital Services Act (DSA) 13
1.2.2. The General Data Protection Regulation 17
1.2.3. European Regulation against the dissemination of terrorist content online 22
1.2.4. Charter of Fundamental Rights of the EU 24
1.3. The French legal framework 25
1.4. Analysis 27
2. Online stalking 30
2.1. Context 30
2.2. The European legal framework 31
2.3. The French legal framework 33
2.4. Analysis 33
3. Cyberbullying 39
3.1. Context 39
3.2. The European legal framework 40
3.3. The French legal framework 41
3.4. Analysis 44
4. Inciting violence or hatred online 46
4.1. Context 46
4.2. The European legal framework 47
4.2.1. Digital Services Act 47
4.2.2. 2016 Code of Conduct 48
4.2.3. 2008 Framework Decision 50
4.3. The French legal framework 52
4.4. Analysis 52
RECOMMENDATIONS FOR THE TRANSPOSITION OF DIRECTIVE 2024/1385 ..... **56**
Table of contents **64**
Bibliography **65**

Bibliography

Specialist texts

Adamson, D.M. et al. (2023). "Cyberstalking: A Growing Challenge for the U.S. Legal System." RAND Corporation. 20 p.

Dulaurans, M. (2024). « Violences en ligne: décrypter les mécanismes du cyberharcèlement ». Presses universitaires de Bordeaux. 236 p.

Stark, E. (2023). "Coercive Control: How Men Entrap Women in Personal Life."

Theses

Andréani, A. (2020). « Le droit à l'oubli : étude comparée entre la France et les Etats-Unis ». Thèse de doctorat. Université Paris II Panthéon-Assas.

Udoh-Oshin, G. (2017). "Hate Speech on the Internet: Crime or Free Speech?" Undergraduate thesis. Long Island University.

Articles

Boizard, M. (2016). « Le temps, le droit à l'oubli et le droit à l'effacement ». *Les Cahiers de la justice*, no 4, (p. 619-628).

Bossan, J. (2024). « La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0 ». *Légipresse*, n°426, (p. 380-385).

Cammillieri-Subrenat A. (2002). « L'incitation à la haine et la Constitution ». *Revue internationale de droit comparé*. vol. 54. n°2. (p. 513-548).

Chauvet, D. (2015). « Mérites ou démérites du délit général de harcèlement moral créé par la loi du 4 août 2014 ?". *Recueil Dalloz*, 2015, (page 174).).

Chimchiuri, L. (2024). "Cyberbullying: A Threat to Freedom of Expression." *Proceedings of the 36th International RAIS Conference on Social Sciences and Humanities*. Scientia Moralitas Research Institute. (pp. 31-36).

Citron, D. K; Franks, M. A. (2014). "Criminalising Revenge Porn". *Wake Forest Law Review*, 49 (2), p. 346.

Demaske, C. (2023). « L'opérationnalisation des discours de haine à l'échelle de la communauté Un plan de lutte contre les discours de haine ». *Réseaux,* vol. 241. n°5. (p. 197-235).

Den Heijer, M; Abeelen, T; Maskyla, A. (2019). "On the Use and Misuse of Recitals in European Union Law." *Amsterdam Law School Research Paper*. No. 2019-31. 25.

Garnier P. (2024). « Mascus, les hommes qui détestent les femmes – Le documentaire ». *Made In Perpignan*.

Gordon G.S. (2013). "Hate Speech Persecution: A Contextual Approach." *Vanderbilt Journal of Transnational Law*. vol. 303. no. 2. (pp. 303-373).

Jaki S, De Smedt T, Gwozdz M, *et al.* (2019). "Online hatred of women in the Incels.me forum: Linguistic analysis and automatic detection." *Journal of Language Aggression and Conflict*, vol. 7, no. 2, pp. 240-268.

Kobets, P.; Krasnova, K. (2018). "Cyberstalking: Public danger, key factors and prevention." *Przeglad Wschodnioeuropejski*, vol. 9, no. 2, pp. 43–53.

Kristof, N. (2020). "The Children of Pornhub." *The New York Times.*

Ouest France. (2024). « Sur Telegram des milliers d'hommes échangeaient des conseils pour droguer et violer des femmes »."

Segonds, M. (2014). « Un an de droit pénal du travail », *Dr. pénal. chron.*

Terwangne, C. (2015). « Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique ». *Enjeux européens et mondiaux de la protection des données personnelles.* Création information communication, Larcier. (p. 245-275).

Official documents

1. European Commission

European Commission. (2014). "Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law."

European Commission. (2022). "Press release: EU Code of Conduct against online hate speech: latest evaluation shows slowdown in progress".

European Commission. (2022). Factsheet: Countering illegal hate speech online: 7th evaluation of Code of Conduct.

European Commission. (2023). Delegated Act on independent audits under digital services Act. C/2023/6807.

European Commission. (2024). "Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online."

2. Council of the European Union

Council of the European Union. (2008). *Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.*

Council of Europe. Factsheet on Combating sexist hate speech.

Council of Europe. (2019). "Recommendation on preventing and combating sexism ". CM/Rec(2019)1.

European Council and Council of the European Union. (2024). "Measures taken by the European Union to end violence against women". Measures taken by the EU to end violence against women - Consilium (accessed on 4 February 2025).

Council of the European Union. (2024). "Press release: Council adopts the first ever EU law on violence against women". Council adopts the first ever EU law on violence against women - Consilium. (accessed on 4 February 2025).

3. European Parliament

European Parliament. (2020). "Briefing: Violence against women in the European Union. State of play." https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659333/EPRS_BRI(2020)659333_EN.pdf

European Parliament and European Council. (2022). "Proposal for a Directive on combating violence against women and domestic violence." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0105

4. Other

La Assemblée Parlementaire de la Francophonie, Réseau des femmes parlementaires. (2021). *Rapport final : la cyber violence envers les femmes et les enfants dans l'espace francophone*, p. 5, 9. Microsoft Word - Final report on cyber violence against women and children.

Greffière de la CEDH. (2021). Communiqué de presse « Manquements, constitutifs de violations, à l'obligation de traiter les cas de violences domestiques ; modifications législatives requises de toute urgence ».

Ministère de l'Intérieur. (2025). « Communiqué de presse : Les infractions liées au numérique enregistrées par les services de sécurité en 2024 ». https://www.interieur.gouv.fr/actualites/communiques-de-presse/infractions-liees-au-numerique-enregistrees-par-services-de#:~:text=Les%20infractions%20li%C3%A9es%20au%20num%C3%A9rique%20enregistr%C3%A9es%20par%20les%20services%20de%20s%C3%A9curit%C3%A9%20en%202024,-Communiqu%C3%A9s%20de%20presse&text=En%20France%20en%202024%2C%20les,n%C3%A9cessaire%20de%20les%20analyser%20s%C3%A9par%C3%A9ment. (accessed on 17 February 2025).

Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). *Fiche informative, « La Manosphère »*, p.5. Home FR | IBZ - SPF Interior.

Reports and recommendations

European Union Agency for Fundamental Rights. (2014). Report: "Violence against women: an EU-wide survey." https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-factsheet_fr.pdf.

Centre Hubertine Auclert. (2017-2018). « Rapport Cyber violences conjugales ». Report "Cyberviolence in Intimate Relationships" | Centre Hubertine Auclert.

Féministes contre le cyberharcèlement. (2022). « Cyber violence et cyberharcèlement : le vécu des victimes ». Enquête conduite par IPSOS auprès de 216 victimes de cyber violences âgées de 16 ans à 60 ans ou plus. https://www.vscyberh.org/.

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). (2021). "General Recommendation No. 1 on the digital dimension of violence against women." https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

High Council for Equality. (2023). "Pornocriminalité: mettons fin à l'impunité de l'industrie pornographique ". https://haut-conseil-egalite.gouv.fr/IMG/pdf/hce-vio-rapport_pornocriminalite-v11-bdef.pdf

European Women's Lobby. (2024). "Report on cyber violence against women. Executive summary and recommendations."

Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains (MIPROF). (2024). « Guide cyber violences au sein du couple ». https://arretonslesviolences.gouv.fr/sites/default/files/2024-11/Guide-cyberviolences-au-sein-du-couple-Miprof-2024-version-accessible.pdf

EDVAW Platform. (2020). "The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform". 1680a933ae.

Simonovic Dubravka, United Nations Special Rapporteur on violence against women and girls. (2018). "Report on violence against women, its causes and consequences, with a focus on online violence against women and girls from a human rights perspective." https://digitallibrary.un.org/record/1641160?ln=fr&v=pdf.

UNESCO. (2021). "The Chilling: Global trends in online violence against women journalists." https://unesdoc.unesco.org/ark:/48223/pf0000377223 (accessed 9 March 2025).

Legislative provisions

Europe:

Council of Europe. (2011). *Convention on preventing and combating violence against women and domestic violence.* Open for signature in Istanbul on 11 May 2011. Council of Europe Treaty Series, No. 210.

Treaty on the Functioning of the EU (consolidated version). (2012).

European Parliament and Council. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)*. L119/1 https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC*. Official Journal of the European Union. L 277/1 Regulation - 2022/2065 - EN - EUR-Lex.

European Parliament and European Council. (2024). *Directive (EU) 2024/1385 of 14 May 2024 on combating violence against women and domestic violence.* Official Journal of the European Union, L 2024/1385. Directive - EU - 2024/1385 - EN - EUR-Lex.

France

Assemblée Nationale. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexuelles et sexistes ».

Law of 29 July 1881 on freedom of the press. (Version in force on 25 May 2025)

Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexistes et sexuelles. (2018).

Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

Case law

Europe:

Court of Justice of the European Union. (2016). *Breyer* . C-582/14, EU:C:2016:779. Points 39 and 41.

European Court of Human Rights. (1981), *Dudgeon v. United Kingdom*, Series A, No. 45, para. 41.

European Court of Human Rights. (2021). *Tunikova and Others v. Russia*. TUNIKOVA AND OTHERS v. RUSSIA

France:

Conseil constitutionnel. (2021). Décision n°2021-933 QPC du 30 septembre 2021. Decision No. 2021-933 QPC of 30 September 2021 | Constitutional Council.

Conseil d'Etat. (2019). 10e et 9e chambre réunies, n° 429154, 6 décembre.

Cour de cassation, Chambre civile. Arrêt du 21 mars 2018, n°16-28.741.

Cour de cassation, Chambre criminelle. Arrêt du 9 mai 2018, n° 17-83.623.

Cour de cassation, Chambre criminelle. Arrêt du 29 mai 2024, n°23-80.806.

Online references

ARCOM. « Signaleurs de confiance : conditions et candidatures ». https://www.arcom.fr/espace-professionnel/signaleurs-de-confiance-conditions-et-candidature s (accessed 22 June 2025).

Centre Hubertine Auclert. (2023). « Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyber violences conjugales ». Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales | Centre Hubertine Auclert (accessed on 23 May 2025).

Cyberharcèlement. « Cyberharcèlement et liberté d'expression : les enjeux juridiques ». https://cyber-harcelement.info/la-frontiere-entre-cyberharcelement-et-liberte-dexpression-les enjeux-juridiques/ (accessed 22 May 2025).

Common Thread. (2021). "Twitter's new reporting process centres on a human-first design." https://blog.x.com/common-thread/en/topics/stories/2021/twitters-new-reporting-process-cent ers- on-a-human-first-design (accessed 22 June 2025).

Ferrand, E. (2021). « Sur Onlyfans, les jeunes peuvent être facilement repérés par des proxénètes ». *Le figaro.* https://etudiant.lefigaro.fr/article/sur-onlyfans-les-jeunes-peuvent-etre-facilement-reperes-par

Hardouin-Le-Goff, C. (2023). "L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales? " *Le club des juristes.* The criminalisation of coercive control: a future tool in the fight against domestic violence? - Le Club des Juristes.

Humanrights.ch. (2016). « Incitation à la haine sur Internet – Cas suisses et politique des portails d'informations en la matière ». https://www.humanrights.ch/fr/pfi/droits-humains/droits-politiques/incitation-haine-internet-c as-suisses-politique-portails-informations (accessed 23 May 2025).

Muller, Y. (2024). "« Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire." *Le club des juristes.* Consécration de la notion de contrôle coercitif…. Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire - Le Club des Juristes

- (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

United Nations. "Hate speech: Impact and prevention: Targets of hate." https://www.un.org/fr/hate-speech/impact-and-prevention/targets-of-hate (accessed 23 May 2025).

United Nations. "Hate speech versus freedom of speech ». (https://www.un.org/en/hate-speech/understanding-hate-speech/hate-speech-versus-freedom-of- speech) (accessed 22 May 2025).

New York Times. (2024). "The troubling trend in teenage sex." https://www.nytimes.com/2024/04/12/opinion/choking-teen-sex-brain-damage.html. (accessed 9 June 2025).

New York Times. (2025). "These Internal Documents Show Why We Shouldn't Trust Porn Companies ." https://www.nytimes.com/2025/05/10/opinion/pornhub-children-documents.html. (accessed 9 June 2025).

Osez le Féminisme. Dare to be a feminist! – We are not born feminists, we become feminists... (accessed on 16 May 2025).

Radio France. (2023). "OnlyFans, plateforme favorite des créateurs de contenus sexuels, attire toujours plus d'utilisateurs." https://www.radiofrance.fr/mouv/podcasts/reporterter/onlyfans-plateforme-favorite-des-create urs-de-contenus-sexuels-attire-toujours-plus-d-utilisateurs-1200317.

Public Service. (2024). "How do I report illegal content posted on the Internet." https://www.service-public.fr/particuliers/vosdroits/F31979?lang=en (accessed 22 June 2025).

Tilburg University. Kamara, I. (2023). "Cyberstalking and online platforms' due diligence in the EU Digital Services Act." TTLF Newsletter on Transatlantic Antitrust and IPR Developments, Stanford-Vienna Transatlantic Technology Law Forum : https://research.tilburguniversity.edu/en/publications/cyberstalking-and-online-platforms-due-diligence-in-the-eu-digita (accessed on 12 February).

Vie publique. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexistes et sexuelles ». Violences sexuelles et sexistes Contrôle coercitif Viol Proposition loi | vie-publique.fr.

Symposium

Osez le Féminisme and CLEF. (2025). Symposium: "Online sexual exploitation: challenges and responses in Europe." Strasbourg.

contacts

Fanny Cocoa, EUCLID academic secretary:
equipe-master@parisnanterre.fr
(please specify “EUCLID” in the email’s subject line)

Céline Piques, spokesperson for Osez le Féminisme (OLF) : piques.celine@gmail.com

Alyssa Ahrabare, president of the French Coordination for the European Women's Lobby (CLEF):
alyssa.ahrabare.afev@gmail.com

Université Paris Nanterre

EUCLID
Enseignement universitaire
clinique du droit
Université Paris Nanterre

OSEZ LE FÉMINISME

La Coordination Française pour le Lobby Européen des Femmes

Université Paris Nanterre

EUCLID
Enseignement universitaire
clinique du droit
Université Paris Nanterre



OSEZ LE FÉMINISME

La Coordination Française
pour le Lobby Européen des Femmes