PANORAMIC

ONLINE SAFETY REGULATION

France

LEXOLOGY

Online Safety Regulation

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Generated on: March 27, 2026

Contents

Online Safety Regulation

Contributors

France

White & Case LLP

WHITE & CASE

Bertrand Liard bliard@whitecase.com
Clara Hainsdorf chainsdorf@whitecase.com
Brian Robion brian.robion@whitecase.com

LEGAL FRAMEWORK

Legal regime

Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

France operates a multi-pillar regulatory framework for online safety, combining the following:

- directly applicable EU law, notably Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (the DSA) and Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (the TERREG);
- national implementation of the DSA and enforcement measures introduced by Law No. 2024-449 of 21 May 2024 on the Security and Regulation of the Digital Space (the SREN Act); and
- established French statutes and codes that remain fully applicable, including Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (the LCEN) (as amended by the SREN Act) together with the Law of 29 July 1881 on Freedom of the Press (the Press Law), the Consumer Code and the Criminal Code.

In light of the broad scope of application of the DSA, the interrelationship of some of the national laws set out in this chapter with the DSA still needs to be clarified.

The SREN Act designated the Regulatory Authority for Audiovisual and Digital Communication (ARCOM) as France's digital services coordinator:

- In that capacity, ARCOM is mandated to coordinate national enforcement of DSA obligations. As such, pursuant to article 8-1 of the LCEN, ARCOM mandates cover (1) for intermediary service providers, the obligations set out in paragraphs 1 and 5 of articles 9 and 10, and in articles 11 to 15 DSA; (2) for hosting service providers, the obligations in articles 16 and 17 DSA; and (3) for online platforms (excluding micro and small enterprises under article 19 DSA), the obligations in articles 20 to 24, article 25 (save for practices falling under article L. 133-1(1) of the French Consumer Code), points (a) to (c) of article 26(1), article 27 and article 28(1) DSA.
- ARCOM is also mandated to convene and cooperate with the data protection authority (CNIL) and the consumer protection authority (DGCCRF) via a national coordination network, and to exercise investigatory functions.

Area	Key Statute or Instrument	Scope
Illegal content and intermediary liability	Law No. 2004 - 575 of 21 June 2004 on Confidence in the Digital Economy (LCEN)	Establishes the liability regime for online intermediaries, distinguishing between hosting providers, publishers, and access providers. It introduces the statutory notice - and - takedown procedure,

		defines the conditions for exemption from liability when acting promptly upon notification, and imposes obligations to retain identification data. The LCEN is substantively aligned to the DSA.
Hate speech, harassment, defamation	French Criminal Code and Law of 29 July 1881 on the Freedom of the Press	Criminalises public insults, defamation, incitement to hatred or violence and online harassment.
Child protection and pornography	French Criminal Code, articles 227 - 23 et seq.	Governs the protection of minors from pornographic or violent material and mandates age - verification systems.
Disinformation and manipulation of information	Law No. 2018 - 1202 of 22 December 2018 on the Fight against the Manipulation of Information	Targets the dissemination of false information, particularly during electoral periods, and empowers ARCOM to act against coordinated disinformation.
Platform governance and systemic duties	Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act).	Imposes due - diligence, transparency, and risk - mitigation obligations on online platforms and search engines.
Terrorist content and online radicalisation	Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (TERREG Regulation) and the French Internal Security Code, article L. 228 - 1 et seq.	Empowers authorities to order the removal or blocking of terrorist content within one hour. Hosting providers must maintain procedures for rapid compliance, reporting, and prevention of re - uploads. France had a pre - existing domestic blocking regime, now aligned with the TERREG framework.

Law stated - 18 December 2025

Online harms covered

Which online harms are covered under the relevant legislation and how are these harms defined?

There is no statutory definition of 'online harms' in French law. French legislation focuses instead on whether a given online activity or content is unlawful. Below is an overview of the principal categories of unlawful online content under French law, with their legal basis and definition.

Category	Legal Basis	Definition / Scope
Hate speech and incitement to discrimination or violence	Law of 29 July 1881 on the Freedom of the Press (articles 23, 24, 32, 33); Criminal Code (article 222 - 33 - 2 - 2).	Prohibits public provocation to discrimination, hatred or violence; prohibits public insult or defamation on protected grounds (origin, religion, sex, sexual orientation, gender identity, disability); prohibits repeated or concerted online harassment.
Terrorism - related content	Criminal Code (articles 421 - 1 to 421 - 2 - 6); Internal Security Code (article L. 228 - 1 et seq).	Prohibits provocation to or apology for terrorism; empowers authorities to order removal or blocking of terrorist content within one hour; requires hosting providers to maintain rapid - response and re - upload - prevention mechanisms.
Child sexual abuse material (CSAM) and exposure of minors	Criminal Code (articles 227 - 22 to 227 - 24); SREN Act (2024).	Prohibits the production, distribution or possession of pornographic content involving minors; prohibits making pornographic content accessible to minors; requires adult - content services to implement age - verification systems.

Defamation, insult and protection of reputation	Law of 29 July 1881 (articles 29 to 33).	Prohibits public defamation and insult, including online publications and social - media content; distinguishes between public and private defamation.
Privacy, image rights and non - consensual intimate content	Civil Code (article 9); Criminal Code (articles 226 - 1, 226 - 2 - 1, 226 - 8).	Prohibits capturing, recording or transmitting a person's image or words without consent; prohibits dissemination of non - consensual intimate material ('revenge porn'); protects the right to private life and image.
Fraud, scams and deceptive commercial practices	Consumer Code (articles L. 121 - 2 to L. 121 - 4); Criminal Code (article 313 - 1).	Prohibits misleading or aggressive commercial practices; prohibits online fraud, including scams, phishing and deceptive sales schemes.
Intellectual - property infringement	Intellectual Property Code (articles L. 335 - 2, L. 521 - 4, L. 716 - 9 et seq).	Prohibits unauthorised reproduction, communication or making available of protected works, designs or trademarks online; enables blocking, delisting and injunction measures.
Disinformation and manipulation of information	Law No. 2018 - 1202 of 22 December 2018.	Prohibits deliberate and large - scale dissemination of false information likely to disturb public order or distort electoral integrity
Incitement to suicide or dangerous acts	Criminal Code (articles 223 - 13 to 223 - 15 - 2).	Prohibits provocation to suicide or dissemination of methods to commit suicide or self - harm; applies to online publications and platforms hosting such content.

Racist, xenophobic or Holocaust - denial content	Law of 29 July 1881 (article 24 bis).	Prohibits denial or trivialisation of crimes against humanity, including Holocaust denial; applies to all online publications and broadcasts.
Misleading or covert advertising by influencers	Law No. 2023 - 451 of 9 June 2023 regulating commercial influence; Consumer Code (articles L. 121 - 2 et seq).	Prohibits covert advertising and mandates clear disclosure (advertising or partnership labels); prohibits promotion of certain goods and services (eg, alcohol, tobacco, medical acts, gambling, or crypto - assets) without compliance with sector - specific restrictions; requires influencers and agencies to identify paid promotions and comply with consumer - protection and advertising standards.

Law stated - 18 December 2025

Online services covered

Which online services are covered under the law and how are these services defined?

France's online safety regime covers a broad spectrum of online services, all of which are defined primarily by the DSA.

The SREN Act adds to this framework by introducing specific national categories of regulated services, notably:

- adult-content websites, which are required to deploy certified age verification solutions and risk-mitigation measures;
- influencer and advertising platforms, now subject to transparency, labelling and fairness duties under both the SREN and the Consumer Code; and
- very large online platforms that have systemic reach in France are required to conduct cybersecurity and algorithmic-risk audits under article L.111-7-3 of the Consumer Code.

Law stated - 18 December 2025

Territorial scope

What is the territorial scope of the relevant law?

Considering the country-of-origin principle: only the digital services coordinator of the provider's establishment is competent to supervise and enforce DSA obligations (that fall within the competence of member states), save where the provider has no EU establishment or designated legal representative. Accordingly, ARCOM's direct DSA-enforcement powers should be limited to providers established in France for DSA purposes, or to non-EU providers without a valid EU representative.

Additionally, ARCOM may cooperate with the European Commission, other national regulators, or, where necessary, judicial authorities to investigate and sanction providers targeting the French market without complying with their obligations.

Law stated - 18 December 2025

Codes of practice

Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

France supplements its statutory online-safety regime (principally the DSA and SREN Act) with a growing set of soft-law instruments: codes of practice, recommendations, and guidance adopted by regulators or co-regulatory bodies. None of these instruments has binding legal force, but they shape compliance expectations and may be referenced by ARCOM or other authorities when assessing proportionality or diligence under the DSA. Below are the most relevant guidelines issued by French authorities.

Instrument / Issuing Body	Nature / Content
ARCOM Recommendations on Protection of Minors Online (2023 – ongoing)	Provide guidance to platforms on age - verification standards, parental - control design, default privacy settings and moderation practices.
ARCOM Guidelines on the Fight against Online Hate (formerly CSA Charte de bonnes pratiques, 2020)	Recommend reporting interfaces, response timelines and user - notification standards.
CNIL Recommendations on Age - Verification and Biometric Data (2023)	Outline privacy - preserving methods for age verification and criteria for certification of third - party providers.
DGCCRF Guidelines on Influencer and Commercial - Content Transparency (2023)	Explain disclosure obligations for paid partnerships, prohibited sectors (alcohol, gambling, crypto - assets), and good - practice examples for labelling and platform cooperation.

Cybersecurity Guidance by ANSSI for Digital Platforms	Non - binding technical recommendations on platform security, data - integrity controls and vulnerability management, complementing DSA risk - mitigation duties.

Law stated - 18 December 2025

Harmful versus illegal content

How does the law in your jurisdiction distinguish between harmful and illegal content?

Illegal content is content defined as unlawful under French law, such as that prohibited by the Criminal Code or the Law of 29 July 1881 on the Freedom of the Press. Its dissemination triggers statutory removal obligations and may expose both the author and, where applicable, the intermediary service provider to liability, namely where the content was not promptly removed after a valid notification.

Harmful content, by contrast, is not a legally defined category under French law. It refers to material that may cause harm to an individual, which could serve as the basis for a civil action for damages if actual prejudice can be demonstrated. In practice, such content often overlaps with, or may ultimately be characterised as, illegal content, depending on its nature and effects.

Law stated - 18 December 2025

Extremist and terrorism-related content

How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

France regulates the dissemination of terrorist and extremist content online through a combined framework of EU law, national criminal provisions, and administrative enforcement powers designed to ensure swift removal of such material while safeguarding fundamental rights.

At the European level, Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (the Terrorist Content Regulation (TERREG)) establishes the one-hour removal rule for hosting service providers.

At the national level, Law No. 2022-1157 of 16 August 2022 designates the competent authorities for implementing these obligations. It empowers the Central Office for Combating Crime Linked to Information and Communication Technologies (OCLCTIC) (part of the Central Directorate of the French Judicial Police) to issue national removal or blocking orders. ARCOM acts as the Digital Services Coordinator responsible for receiving and reviewing cross-border removal orders and for supervising hosting service providers established in France. ARCOM also monitors preventive and technical measures applied by platforms exposed to risks of terrorist content dissemination.

The SREN Act further strengthens this regime by granting ARCOM new powers to issue formal notices, request judicial blocking orders and require detailed reports on moderation systems, cooperation with law-enforcement authorities and prevention of re-uploads of terrorist material.

The Criminal Code complements these administrative measures by criminalising the direct provocation of terrorist acts or their apology (article 421-2-5), including when such acts occur on an online public-communication platform.

Law stated - 18 December 2025

Disinformation versus misinformation

How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

France has no statutory definition of misinformation, disinformation or malinformation. Instead, these notions are addressed through a set of targeted legal instruments aimed at protecting democratic integrity and transparency in online communication.

At the national level, Law No. 2018-1202 of 22 December 2018 on the Fight Against Information Manipulation (the Fake News Law), as amended by the SREN Act, imposes transparency obligations for VLOPs and VLOSEs (as defined under article 33 DSA). During the three months preceding the first day of any nationwide election, and until the relevant voting round is completed, VLOPs and VLOSEs must ensure enhanced transparency measures, given the public-interest need for informed electoral participation and the integrity of the vote.

They must make available, within the article 39 DSA advertising repository, the following information for any paid promotion of content linked to a matter of general interest:

- clear identification of the sponsor: accurate and transparent details about the natural person or the legal entity (including corporate name, registered office, and corporate purpose), and, where applicable, the entity on whose behalf it acts;
- transparent information on data use: clear disclosures on how users' personal data are used in the promotion of such content; and
- disclosure of consideration: the amount paid for the promotion of such content, where the remuneration exceeds €100.

The concept of malinformation is not expressly recognised under French law, although the malicious disclosure of true information may, depending on the circumstances, engage civil or criminal liability (for instance, under the Civil Code or the Criminal Code provisions on privacy, defamation or harassment).

Law stated - 18 December 2025

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

Aside from the obligations directly applicable under the DSA, providers of online services in France are subject to the following:

- SREN Act – introduces national due diligence and transparency duties in addition to those found in the DSA.
    - Article 1 and 2 establishes a set of online-safety obligations focused on the protection of minors. Most importantly, providers of pornographic or other adult-content services must deploy certified age-verification systems approved by ARCOM, in accordance with its ***Technical Framework for Age Verification*** published on 11 October 2024. It should be noted that comparable national regimes in other member states have already been the subject of legal challenges based on the DSA's harmonising effect — in particular, the scope of article 28 DSA and the Commission's related guidance. A similar challenge could therefore arise in France.
    - Article 4 amends article 6-2 I of the LCEN to create a criminal offence where a hosting-service provider or online platform fails to remove or block access to child-sexual-abuse material within the period set by ARCOM's withdrawal order. Non-compliance is punishable by up to one year of imprisonment and a fine of €250,000 for individuals, with higher penalties applicable to legal entities.
    - Article 11 empowers ARCOM to conduct inspections, audits and formal investigations, including requests for information, technical access and referrals to judicial authorities in cases of serious non-compliance.
    - Articles 40 to 42 extend online-safety duties to interactive entertainment and gambling platforms, prohibiting minors' access to pay-to-play or monetary-reward games.
- Consumer Code (articles L.111-7 to L.111-7-3) – requires online-platform operators to provide clear information on ranking criteria, the identity of professional sellers, and any financial or contractual links affecting content visibility. article L.111-7-3 further mandates cybersecurity and algorithmic-risk audits for very large platforms.
- CNIL and GDPR – ensure that safety measures implemented under this framework respect data-protection principles, including proportionality, data minimisation and users' rights.

Law stated - 18 December 2025

Risk assessments and mitigation

Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

Besides the obligations directly applicable under the DSA, France has introduced additional national duties through Law No. 2024-449 of 21 May 2024 on the Security and Regulation of

the Digital Space (the SREN Act) and the Consumer Code to ensure systematic assessment and mitigation of online-safety risks.

- Article 2 of the SREN Act further introduces specific national obligations targeting minors' protection, requiring adult-content platforms to deploy certified age-verification systems approved by ARCOM and to submit independent audits demonstrating their effectiveness.
- In parallel, article L.111-7-3 of the Consumer Code requires very large online platforms to carry out cybersecurity and algorithmic-risk audits. These reviews, supervised by the DGCCRF, complement the DSA's framework by addressing the integrity and reliability of platform systems.

Law stated - 18 December 2025

Protection of minors and age verification

Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

France imposes a multi-layered set of obligations to protect minors online.

- Age-verification for adult content. The SREN Act strengthened ARCOM's powers and created a national regime requiring certified age-verification for pornographic sites. ARCOM published its Technical Framework for Age Verification on 11 October 2024. Courts have since upheld ARCOM's ability to issue injunctions/formal notices against non-compliant services.
- Gaming/monetisable digital items. The SREN Act introduced rules for ***jeux à objets numériques monétisables*** (JONUM) and related protections for minors; article 41, in particular, restricts certain practices and access.
- Education/digital literacy. The Act amended the Education Code to reinforce digital-literacy programmes (article L.312-9), embedding online-safety awareness in schooling.
- Data-protection guardrails. CNIL guidance (non-binding but influential) requires data-minimisation and privacy-by-design for age-assurance and related safety tools. (CNIL guidance sits alongside SREN/DSA enforcement.)

Law stated - 18 December 2025

Civil and human rights

Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

Yes. French law requires that online safety measures be balanced with fundamental rights, in particular freedom of expression, privacy and due process.

Under the DSA and the SREN Act, ARCOM (France's digital services coordinator) must ensure that any removal or blocking measure is proportionate, transparent and grounded in law. Each restriction must pursue a legitimate public-interest aim and use the least restrictive means available.

The Law of 29 July 1881 on Freedom of the Press remains the benchmark for limiting speech online. Only precisely defined offences, such as defamation, hate speech, or incitement to violence, can justify restrictions.

The CNIL ensures that safety mechanisms (such as age-verification or identity-assurance tools) comply with the GDPR, notably the principles of proportionality, data minimisation and respect for user rights.

In judicial proceedings, any claim seeking the removal of online content is assessed against these same fundamental rights. Courts evaluate whether the requested measure is necessary and proportionate in light of the alleged harm, and whether it unjustifiably interferes with freedom of expression.

Overall, French regulators and courts apply a proportionality test to every online-safety intervention, balancing user rights with the protection of minors, public order and other legitimate objectives.

Law stated - 18 December 2025

Disinformation and misinformation

Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

France complements the DSA with Law No. 2018-1202 of 22 December 2018 on the Fight Against Information Manipulation (the Fake News Law). It applies mainly during electoral periods, allowing courts to order the removal or blocking of deliberately false or misleading information likely to affect the sincerity of the vote. Judges must rule within 48 hours.

The law also requires online platforms and advertising intermediaries to disclose the sponsorship and financing of political or issue-based content, under ARCOM's supervision.

The SREN Act complements this regime by amending article L.312-9 of the Education Code to make digital-literacy and disinformation-awareness training mandatory in schools, including verifying sources and identifying deepfakes.

Law stated - 18 December 2025

Notice and takedown

Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

France has a long-standing notice-and-takedown mechanism, first introduced by the Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (LCEN) and now aligned with the DSA through the SREN Act. The overall framework remains largely unchanged:

the LCEN continues to form the foundation of intermediary liability and content-removal obligations.

Under article 6-1 LCEN, ARCOM may order any person publishing an online public-communication service, as well as hosting-service providers, to remove content that breaches articles 421-2-5, 227-23, or 222-39 of the Criminal Code (terrorism, child-sexual-abuse material, and drug trafficking). Internet-access providers may also be notified to ensure prompt disabling of access.

Two specific removal deadlines apply:

- terrorist content must be removed or blocked within one hour of receipt of an ARCOM withdrawal order, under Regulation (EU) 2021/784 and article 6-1-3 LCEN; and
- child sexual abuse material must be removed or blocked within 24 hours of an ARCOM order, under article 6-2 I LCEN, as amended by the SREN Act.

Hosting-service providers have no general monitoring obligation, but must act promptly to remove or disable access to clearly unlawful content once they become aware of it. An intermediary services provider who fails to act expeditiously loses their safe-harbour protection and may incur civil or criminal liability.

Individuals whose lawful content is wrongfully removed may claim damages under article 1240 of the Civil Code.

Law stated - 18 December 2025

ENFORCEMENT AND PENALTIES

Enforcement
How is the online safety regime enforced in your jurisdiction?

At the national level, the Regulatory Authority for Audiovisual and Digital Communication (ARCOM) acts as France's digital services coordinator, enforcing the parts of Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (the DSA) that fall within the competence of member states and corresponding domestic provisions under Law No. 2024-449 of 21 May 2024 on the Security and Regulation of the Digital Space (the SREN Act). Enforcement is shared with other authorities:

- The data protection authority (CNIL) ensures that moderation and age-assurance systems comply with the GDPR, particularly regarding data minimisation and lawful processing.
- The consumer protection authority (DGCCRF) enforces transparency and consumer-protection obligations under the Consumer Code, including fairness of ranking systems and advertising disclosures.
- For criminal matters (eg, terrorist or child sexual abuse content), the Ministry of the Interior, through the OCLCTIC, retains enforcement powers, operating in coordination with ARCOM and public prosecutors.

The judiciary remains central. Civil and administrative courts can issue an order to remove or block illegal content. The Conseil d'État acts as the final appellate body for ARCOM decisions, ensuring full judicial oversight.

Law stated - 18 December 2025

Authorities

Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

ARCOM is the central enforcement authority for online-safety obligations in France. It enforces the DSA and the SREN Act, supervises intermediary service providers established or active in France, and ensures that enforcement measures respect freedom of expression and other fundamental rights. Its powers include:

- Investigatory powers: ARCOM may conduct compliance audits, request information or documents, and require detailed explanations on moderation systems.
- Corrective powers: it may issue formal notices and corrective orders, and impose administrative fines of up to 6 per cent of global annual turnover.
- Judicial referral powers: where a provider fails to comply, ARCOM may refer the matter to the public prosecutor or seek a court injunction ordering content removal or blocking.

ARCOM also enforces sector-specific duties introduced by the SREN Act, such as certified age-verification systems for adult-content services and the 24-hour withdrawal rule for child-sexual-abuse material.

The CNIL ensures that online safety and moderation systems comply with the GDPR, particularly regarding data minimisation and lawful processing. It supervises platforms' use of personal data for age assurance or profiling, and may issue warnings, corrective orders, or fines of up to €20 million or 4 per cent of global turnover.

The DGCCRF enforces consumer-protection and transparency rules under the Consumer Code, focusing on deceptive commercial practices and the fairness of ranking and recommendation systems. It may conduct inspections, request documents, issue administrative injunctions, and impose financial penalties (articles L.511-1 et seq Consumer Code).

The OCLCTIC, within the Central Directorate of the French Judicial Police, handles criminal enforcement for online offences such as terrorism and child-sexual-abuse content. It may issue removal or blocking orders, to be executed within one hour (terrorist content) or 24 hours (child-sexual-abuse material), and cooperates closely with ARCOM and the Ministry of the Interior for cross-border investigations and judicial referrals.

Finally, French judicial and administrative courts play a decisive role. Civil and criminal courts may issue injunctions requiring hosts or access providers to remove or block illegal content accessible in France.

Law stated - 18 December 2025

Penalties and liability

What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

Non-compliance with online-safety obligations in France may give rise to administrative, criminal, and civil sanctions, depending on the breach.

- Administrative sanctions: under the SREN Act (Law No. 2024-449 of 21 May 2024), ARCOM may issue formal notices and corrective orders. Persistent non-compliance can lead to administrative fines of up to 6 per cent of global annual turnover, in line with the DSA.
- Criminal sanctions: certain failures constitute offences under the Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (LCEN). In particular, article 6-2 I LCEN, as amended by the SREN Act, criminalises the failure of a hosting service provider to remove or block access to child-sexual-abuse material within 24 hours of an ARCOM order. Prosecution lies with the public prosecutor before the criminal courts.
- Consumer-law penalties: the Consumer Code (articles L.133-1 to L.133-3) empowers the DGCCRF to impose administrative fines of up to 6 per cent of worldwide turnover and daily penalties of up to 5 per cent of average daily turnover for non-compliance with transparency or fairness obligations, such as misleading rankings or deceptive commercial practices.
- Civil liability: providers remain exposed to claims under article 1240 of the Civil Code for negligent moderation or failure to remove clearly unlawful content after valid notice. Courts may award damages or injunctive relief.

Directors and officers

Under French law, there is limited personal exposure for managers or board members. Liability generally remains with the legal entity itself. Personal liability arises only where a director personally commits a criminal offence (for example, intentional obstruction of enforcement or complicity in an unlawful act) or acts outside the scope of corporate functions in a manner amounting to a personal fault. Routine compliance failures or corporate regulatory breaches do not in themselves create individual liability.

Law stated - 18 December 2025

DISPUTES

Claims

What claims relating to online safety are available and most common in your jurisdiction?

France does not recognise a standalone 'online-safety' cause of action. Disputes are brought under existing civil, administrative or criminal regimes depending on the alleged breach.

-

Civil liability: under article 1240 of the Civil Code, victims may seek damages for negligence, for example, where a host or platform fails to remove clearly unlawful content after valid notification. Article 9 of the same Code provides a basis for actions concerning privacy or image-rights infringements, while the Law of 29 July 1881 on Freedom of the Press governs defamation and hate-speech claims.

- Administrative complaints: individuals or associations may report breaches of online-safety duties (such as missing age-verification, deepfake labelling or moderation failures) to the Regulatory Authority for Audiovisual and Digital Communication (ARCOM), which can issue formal notices or corrective orders.
- Data-protection claims: where moderation or safety measures involve unlawful data processing, complaints may be lodged with the data protection authority (CNIL), which can investigate and impose corrective measures or fines under the GDPR.
- Consumer-law actions: users or consumer associations may invoke articles L.121-1 et seq of the Consumer Code for deceptive or unsafe commercial practices. The consumer protection authority (DGCCRF) may also initiate administrative proceedings for systemic breaches.
- Criminal complaints: the author of illegal content (for example, harassment, terrorism or child sexual abuse material) may be prosecuted under the Criminal Code following reports to the PHAROS platform or directly to the public prosecutor.

Law stated - 18 December 2025

Procedure

What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

France has no unified procedure for online-safety actions. Claimants must use the ordinary civil, administrative or criminal channels depending on the nature of the alleged breach.

- Administrative route: individuals, associations or public bodies may submit a complaint to ARCOM, France's digital services coordinator. ARCOM may investigate, issue a formal notice, and, where non-compliance persists, impose corrective orders or fines under the SREN Act.
- Civil route: victims of defamation, reputational harm or negligent moderation may bring proceedings before the Judicial Court. In urgent cases, they may seek summary proceedings (référé) under articles 834–835 of the Code of Civil Procedure, allowing the judge to order the withdrawal, blocking or delisting of unlawful content pending a full hearing.
- Criminal route: clearly unlawful material (terrorism, child-sexual-abuse, hate speech, fraud and harassment) can be reported through the PHAROS platform, managed by the OCLCTIC under the supervision of the French Judicial Police. Reports may lead to investigation or prosecution by the public prosecutor. Victims may also file a criminal complaint directly with the police or prosecutor.
-

Data-protection route: where moderation or verification systems raise privacy concerns, individuals may lodge a complaint with the CNIL, which can investigate and impose corrective measures or administrative fines under the GDPR.

Law stated - 18 December 2025

Remedies

What interim and substantive remedies may be imposed in relation to online safety claims?

French law provides both interim and final remedies to address breaches of online-safety obligations.

- Interim measures: civil courts may order the withdrawal, blocking, or geo-blocking of unlawful or harmful online content in urgent cases, particularly where there is a risk of ongoing harm. In criminal matters, courts may order the immediate suspension of online services used to disseminate serious illegal material such as terrorist or child-sexual-abuse content.
- Substantive remedies: individuals may seek damages before civil courts for harm caused by negligent moderation, dissemination of unlawful material or privacy infringements.
  Regulatory authorities, such as ARCOM and the DGCCRF, may impose corrective orders, periodic penalty payments or administrative fines — which can reach several percentage points of a provider's global turnover — for breaches of content-removal, transparency or minors'-protection obligations.
  Serious failures, including non-compliance with an official withdrawal order, may also lead to criminal sanctions.

Law stated - 18 December 2025

Defences and exemptions

Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

France maintains conditional liability exemptions for online intermediaries, now harmonised at EU level by articles 4–6 of the Digital Services Act (DSA). These rules mirror the earlier safe-harbour regime of article 6 of the Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (LCEN), which continues to apply where compatible.

Mere conduit, caching, and hosting service providers remain exempt from liability for third-party content when they act neutrally and remove or disable access to illegal material without delay once they have actual knowledge of it.

French courts are expected to interpret the DSA in line with established LCEN case law, distinguishing between passive hosts (benefiting from the exemption) and active providers that curate or promote content (potentially liable).

Law stated - 18 December 2025

UPDATE AND TRENDS

Key trends and future developments

What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

Throughout 2025, the most visible evolution in France has been the operational deployment of age-verification obligations for adult-content sites, coupled with intensified enforcement by the Regulatory Authority for Audiovisual and Digital Communication. Platforms faced concrete deadlines to deploy certified age-assurance solutions, and administrative courts confirmed the legality of injunctions and, where necessary, access-blocking measures for persistent non-compliance.

A second key development concerns marketplace enforcement against unlawful goods. French authorities have demonstrated a willingness to combine consumer-protection powers (notably under article L.521-3-1 of the Consumer Code) with Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy (LCEN) mechanisms and judicial referrals to compel online marketplaces to remove prohibited or dangerous products and, where required, suspend marketplace functionality pending compliance. Recent publicly announced actions show a coordinated approach across the consumer protection authority, customs authorities and criminal investigation services, including emergency injunctions, inspections of incoming parcels and parallel judicial proceedings. The government has publicly signalled that similar action will be taken against other platforms where illegal products are identified. This trend suggests heightened scrutiny of marketplace governance, product-listing controls and takedown responsiveness, alongside potential recourse to article 6-3 LCEN proceedings where alleged systemic failures may pose risks to public order.

Politically, 2025 also saw increasing attention on youth online-protection measures. Following high-profile incidents and parliamentary debates, the French executive indicated support for an EU-level initiative to restrict social-media access for users under 15, supported by enforceable age-verification duties. Proposals relating to digital curfews, youth-protection defaults, and enhanced parental-control standards continue to gain traction.

Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

Law stated - 18 December 2025