TRIS NOTIFICATION PROCEDURE

French Law to Secure and Regulate the Digital Space

January 2023

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the new notification of the French bill to secure and regulate the digital space under procedure TRIS 2023/0632e/FR (*Projet de loi visant à sécuriser et réguler l'espace numérique*, hereinafter referred to as the SREN bill)[1].

The SREN bill aims to cover numerous recently adopted European regulations, including the Digital Services Act (DSA), the Digital Markets Act (DMA) and the Data Act. Prior versions and certain provisions of the SREN bill were previously notified to the European Commission. This notification is the third one of the same bill, resulting from the adoption by the National Assembly on 17 October 2023.[2] CCIA Europe notes that this version of the SREN bill is not final since the final negotiations between the French Senate and National Assembly are still pending. Besides, the second notification of the SREN bill resulted in a detailed opinion and comments from the European Commission to the French Government, in a letter dated 25 October 2023. The third notification of the SREN bill does not address nor respond to the concerns raised by the European Commission, and fails to raise newly adopted amendments supported by the Government and which contravene EU law and international commitments.

CCIA Europe would like to point out that most of the provisions of the SREN bill contravene two major principles of European law vis-à-vis the DSA:

- **Direct applicability of European Regulations**: Numerous provisions of the SREN bill appear to introduce redundant and potentially adverse duplications of the DSA into national legislation. This is concerning as European regulations are intended to be directly applicable without the need for transposition into national law. The replication of EU regulations at the national level has the potential to create confusion and complexity for companies striving to comprehend and adhere to EU rules. Additionally, there is apprehension that such duplication may result in deviations from EU rules, leading to a fragmented implementation of recently adopted regulations across the Internal Market. This fragmentation poses a risk to the harmonising effect of the DSA and the fundamental rights and freedoms of business.

[1] Projet de loi visant à sécuriser et réguler l'espace numérique, Texte n° 593 (2022-2023) de M. Bruno LE MAIRE, ministre de l'économie, des finances et de la souveraineté industrielle et numérique, déposé au Sénat le 10 mai 2023, available here.

[2] The first notification was the TRIS procedure 2023/0352/FR, available here. The second notification was the TRIS procedure 2023/0461/F, available here.

- **Country-of-origin principle**: The DSA aims to provide a harmonised framework, as stated in its Recital 2. While Recital 9 of the DSA allows for additional national legislation applicable to providers of intermediary services, certain conditions such as the country-of-origin principle have to be respected as stated in Article 2 of the DSA and Article 3 of the e-Commerce Directive. The SREN bill does not seem to respect these conditions as it applies to all online platforms. The Court of Justice of the EU recently confirmed that a similar national approach was contrary to EU law "which ensures the free movement of information society services through the principle of control in the Member State of origin of the service concerned".[3] Member States should therefore refrain from adopting "measures of a general and abstract nature which apply without distinction to any provider of a category of information society services".

In addition, CCIA Europe is concerned that a blanket exclusion of non-EU cloud providers from public tenders would contradict GDPR data transfer rules, recent data flows commitments, and the principle of equal treatment under the Procurement and Utilities Directives and the EU's commitments to the Government Procurement Agreement.

Insofar as the SREN bill concerns matters which are covered by EU law and international commitments, CCIA Europe calls on the European Commission to block the final adoption of the contravening provisions of the SREN bill.

CCIA Europe would like to provide supplementary comments on specific provisions of the French SREN bill to the European Commission. These comments address Articles previously notified to the European Commission - given the various changes throughout the legislative process - the provisions which are part of this latest notification, as well as other provisions which have not been notified but should nonetheless be scrutinised to ensure consistency with EU law:

[3] CJEU, Press Release No 167/23, Luxembourg, 9 November 2023, Judgment of the Court in Case C-376/22 | Google Ireland and Others, Combating illegal content on the Internet: a Member State may not subject a communication platform provider established in another Member State to general and abstract obligations, available here.

I. Article 2 bis: Removing apps without age verification from app stores

The DSA establishes in its Article 28 the legal framework for the online protection of minors. This is then complemented in Articles 34 and 35 which allow for the identification and mitigation of systemic risks, mentioning in particular age verification as one of the targeted measures that could be taken to protect minors. However, as noted previously by the European Commission in its letter dated 25 October 2023, Article 2 bis of the SREN bill, as proposed, impinges on these DSA provisions.

Further, this Article builds on law no. 2023-566, establishing a digital majority.[4] In its current state of drafting of the SREN draft bill, if software application stores do not comply with law no. 2023-451, the Digital Service Coordinator can require them to prevent downloading these applications, extending this to all users, and not only minors. This provision would introduce disproportionate measures for a number of reasons.

Firstly, it would unduly limit access to online communication services, including social media applications, which risks infringing on the right to freedom of expression, as enshrined in the European Convention of Human Rights.[5] Secondly, requiring software application stores to prevent the download of software applications that have failed to set up an age verification and parental authorization system would significantly impact those protected by the law (minors under the age of 15) but also anyone wishing to access these services, regardless of their age. Thirdly, such a restrictive provision is of questionable necessity, particularly if assessed in relation to the seriousness of the infringement that motivates the decision to require software application stores to block the download of software applications.

The European Commission adopted in 2022 its new strategy for a better internet for kids (BIK+) as a way to ensure the protection and empowerment of children online. Within this strategy, work has started on an EU code on age-appropriate design and standardising age assurance and verification in Europe. Adopting such provisions while the EU is in parallel working on a comprehensive strategy increases the risk of inconsistencies throughout the European Union.

As a consequence of the above, retaining such an article which refers to a law that the European Commission has already called into question seems inappropriate and would encroach on the consistency of Union law.

[4] Loi no 2023-566, visant à instaurer une majorité numérique et à lutter contre la haine en ligne, available here.
[5] According to Article 10 of the European Convention of Human Rights (ECHR), everyone has the right to freedom of expression, regardless of the medium of communication they chose to use.

II. Article 3 bis: Removing non-consensual sexual content under 24 hours

The DSA sets a general liability framework based on which intermediary service providers can be held liable for illegal content they host if, once they become aware of the unlawfulness of the content, they fail to take prompt action to remove access to it.

According to Article 3 bis of the SREN bill, the French administrative authority would be enabled to issue an order requiring a hosting service provider to remove, within 24 hours, non-consensual sexual content. However, the DSA does not in any case provide a specific turnaround time for the removal of illegal content, as it presumably understands that every instance of illegal content being shared online should be assessed on a case-by-case basis.

Therefore, setting a specific deadline for removing content would go beyond what is foreseen in Union law. Further, Member States introducing specific deadlines for the removal of content would contravene the direct and uniform application of the DSA rules, which are expected to harmonise the legislative framework for intermediary service providers across the Union.

III. Article 5: Blocking any other account held by a convicted person

Article 5 of the SREN bill introduces a legal sanction prohibiting individuals convicted of multiple offences from accessing social media. This provision mandates platforms to identify and block existing accounts, as well as proactively preventing the creation of future accounts by the same individual.

However, there are significant issues with this article. Firstly, it disregards the technical challenges in preventing the creation of future accounts, contradicting Article 16 of the DSA, which emphasises the need for notification mechanisms for specific violations. Additionally, the article lacks clarity on the methodology for identifying existing accounts, which increases the risk of overblocking and potentially infringing freedom of expression. Methods such as IP address blocking are imperfect and may affect innocent users in the same household. Furthermore, using phone numbers or email addresses for identification is not foolproof, as individuals can easily circumvent these barriers. Lastly, implementing these sanctions would require platforms to handle sensitive criminal records routinely.

CCIA Europe would recommend blocking this Article. Alternatively, competent authorities should be in charge of identifying these accounts and communicating removal orders to online platforms.

IV. Article 5 quinquies: Warning minors' parents of cyberbullying

Article 5 quinquies of the SREN bill creates a new obligation for social media providers to issue a warning message to parents of minors, as soon as they receive notices of cyberharassment from trusted flaggers. The warning message should contain the criminal proceedings in the event of infringements, as well as the conditions under which they may incur civil liability.

This Article manifestly builds on law no. 2023-566, establishing a digital majority and Article 22 of the SREN bill, as it requires the identification of minors and minors' parents, which are already contravening the DSA's objectives and notably Article 28 of the DSA on the online protection of minors.

In addition, this provision requires social media providers to carry out massive processing of the personal data of minors and their parents. Such massive data collection could create significant frictions with data minimisation obligations, creating additional data risks and vulnerabilities and could therefore be considered as disproportionate with regards to the General Data Protection Regulation (GDPR).[6]

V. Article 22: Identifying minors' parents

Article 22 of the SREN bill requires social media providers to identify the parents of a minor user in order to share with them information of the legal risks their child faces online, upon registration of the minor.

As previously pointed out by the European Commission, the outstanding concern is the applicability of such an obligation. There is currently no established process for identifying parents on online platforms, a technical challenge extensively discussed during the debates surrounding law no. 2023-566.

VI. Article 10 bis A: Risk of blanket exclusion of non-EU cloud providers from procurement

Article 10 bis A risks being used to mandate state administrations and state operators to only use cloud offerings which are certified under version 3.2 of SecNumCloud.[7]

The current wording of Article 10 bis A provides that government agencies and operators must use solutions immune to extraterritorial laws without specifically mentioning SecNumCloud v3.2 (**'SNC 3.2'**). As such, the provision is aligned with the "Cloud au centre"

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available here, see Article 6 (3) and Rectial 41.

[7] Version adopted by the National Assembly, expanding on Article 10 bis adopted by the Senate;

doctrine[8] which requires public administrations to ensure that private cloud services implement security and data protection measures, especially protecting sensitive data from unauthorised access by non-EU public authorities. Under this government policy, SNC 3.2 is mandated only in very specific cases, a short percentage of use cases.

However, previous versions of this provision required state administrations and operators to use only cloud services certified under SecNumCloud version 3.2. Further, Article 10 bis A (IV) provides that a decree will define the terms of application of immunity requirements, including security and ownership criteria. This decree could reintroduce a broad scope of application for SNC 3.2, particularly regarding capital ownership. It is therefore crucial to monitor the upcoming decree and the final vote on the text of the "*Commission Mixte Paritaire*" to avoid a broad application of SNC 3.2 to most, if not all, procurements, for the reasons below.

First, SNC 3.2 is a national certification scheme which is only eligible for cloud service providers which localise personal and non-personal data within the EU, have their global headquarters in the European Union, and for which non-EU shareholders can individually hold not more than 24% of the capital or collectively hold 39% of the capital - among other eligibility criteria.[9] Those requirements would exclude non-EU cloud vendors from wherever SNC 3.2 is mandated. In practice, only two French companies would be able to bid for any future French public tenders.[10] And while additional French companies may soon seek this certification,[11] European cloud vendors outside France would be implicitly excluded from procurement bids in the country.[12]

Second, SNC 3.2 nullifies all adequacy decisions adopted by the European Commission to transfer personal data, including health data, outside the European Union. It also nullifies all other data transfer instruments, including EU delegated acts adopted pursuant to Article 46 of the General Data Protection Regulation. As far as non-personal data is concerned, this provision stands at odds with the EU's unilateral and multilateral commitments against data localisation requirements.[13]

Third, a broad application of SNC 3.2. would severely distort fair competition within the EU single market considering the current and foreseeable immaturity of the offering of SecNumCloud-certified products on the market. For the same reason, a broad scope of

[8] Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre»), 31 May 2023, available here;
[9] See sections 19.2 and 19.6 of version 3.2 of SecNumCloud;
[10] Sécurité du cloud : Outscale obtient la plus exigeante certification de l'ANSSI, 11 December, Le Figaro, available here; Après Outscale, OVH aussi certifié SecNumCloud 3.2, 9 January, Le Monde Informatique, available here;
[11] The list of cloud providers undergoing certification is available on ANSSI's website;
[12] While any European company can choose to undergo a SecNumCloud certification, testimonies from several companies show that obtaining a previous, less burdensome version of SecNumCloud was already a multi-year process (see for instance here and here);:,;
[13] See G7 Members' commitments (June 2021), G20 Digital Ministers' commitments (August 2021), G20 Rome Leaders' Declaration (October 2021), European Commission communication on an Open, Sustainable and Assertive Trade Policy (February 2021);

application of SNC 3.2 extending beyond matters which fall under national security and Article 346 TFEU would conflict with the principle of equal treatment and non-discrimination under Article 18 of the Procurement Directive (2014/24/EU). To the extent that "state operators" also include state-owned enterprises,[14] a broad application of SNC 3.2 is also likely to conflict with the principle of equal treatment under the Utilities Directive (2014/25/EU), and the Services Directive (2006/123/EC) which expressly prohibits restriction based on the holding of the share capital.

Fourth, a broad application of SNC 3.2 would also likely run counter to the EU's commitments to provide national treatment and market access for "Computer and Related Services" under CPC Section 84, which broadly encompasses cloud computing, under the Government Procurement Agreement (GPA).[15] While the protection of public order and public health constitute valid grounds to deviate from GPA commitments on a case-by-case basis, they do not constitute an exception for blanket discriminatory treatment against foreign vendors. Neither Article 10 bis A nor the accompanying explanatory note provide an obvious relation between those grounds and usage of a cloud computing service, and do not provide arguments to justify the underlying hypothesis that members of the GPA (mainly OECD countries) would seek to leverage the contract of a supplier from their jurisdiction that is supplying an EU entity cloud services, and use that data processing function to threaten public order or human health, or to misappropriate intellectual property[16] from that entity. The WTO has established a number of criteria that must be met in order for a measure to be considered compliant with GATS and GPA exemptions, i.e.:

- The measure must be *necessary* to protect a legitimate public policy objective, such as national security or public order.
- The measure must be applied in a *non-discriminatory* manner.
- The measure must be *least restrictive* in its impact on trade.
- The measure must also be *consistent with the overall objectives* of GPA, which is to open government procurement markets among its parties.

Finally, ensuring a narrow scope of application of SNC 3.2 is essential to avoid confusion and possible fragmentation of the cloud market in the EU, especially at a time of ongoing debates about the upcoming EU Certification Scheme for Cloud Services (EUCS) for which the specifications of the levels are still being developed.

Conclusion

CCIA Europe invites the European Commission to block the provisions of the SREN bill which contravene EU law, in particular conflicting with the implementation of the DSA. CCIA

[14] See definition of "operateurs" in Projet de Loi de Finances 2024;
[15] See European Union - Services* - Annex 5, available online;
[16] L-311-6 of the Code of relations between the public and the administration includes "administrative documents (...) [w]hose communication would infringe the business confidentiality, which includes the confidentiality of processes, economic and financial information and commercial or industrial strategies."

Europe also urges the European Commission to pay close attention to the final version of the bill and its implementation to ensure that all legislative and decree provisions governing cloud procurement are consistent with the GDPR, the principle of equal treatment under various directives, and the Government Procurement Agreement, and do not pre-empt the upcoming EU Certification Scheme for Cloud Services (EUCS).

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

For more information, visit: twitter.com/CCIAeurope or www.ccianet.org

CCIA is registered in the EU Transparency Register with number 281864052407-46.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org