N° 777

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 27 juin 2023

RAPPORT

FAIT

au nom de la commission spéciale (1) sur le projet de loi visant à **sécuriser** *et* **réguler** *l'***espace numérique** *(procédure accélérée),*

Par MM. Patrick CHAIZE et Loïc HERVÉ,

Sénateurs

(1) Cette commission est composée de : Mme Catherine Morin-Desailly*, présidente ;* Mmes Florence Blatrix Contat, Alexandra Borchio Fontimp, Toine Bourrat, MM. Thomas Dossus, Bernard Fialaire, Xavier Iacovelli, Mmes Micheline Jacques, Marie Mercier, M. Pierre Ouzoulias, Mme Sylvie Robert, M. Pierre-Jean Verzelen*, vice-présidents ;* Mme Nadine Bellurot, M. Jérôme Durain, Mme Anne-Catherine Loisier*, secrétaires ;* MM. Jean-Michel Arnaud, Julien Bargeton, Mme Annick Billon, MM. Jean-Marc Boyer, Rémi Cardon, Patrick Chaize, Mmes Nathalie Delattre, Patricia Demas, M. Rémi Féraud, Mme Pascale Gruny, MM. Ludovic Haye, Loïc Hervé, Pierre-Antoine Levi, Mmes Marie-Noëlle Lienemann, Laurence Muller-Bronn, Sylviane Noël, MM. Cyril Pellevat, Christian Redon-Sarrazy, André Reichardt, Mmes Laurence Rossignol, Elsa Schalck, M. Laurent Somon.

Voir les numéros :

Sénat : **593** et **778** (2022-2023)

SOMMAIRE

L'ESSENTIEL

Le Sénat a choisi de constituer une commission spéciale, rassemblant des membres de toutes ses commissions permanentes, afin d'examiner le projet de loi visant à sécuriser et réguler l'espace numérique. Présidée par Catherine Morin-Desailly, la commission a désigné Patrick Chaize et Loïc Hervé rapporteurs.

L'ampleur du texte et la variété des thèmes qui y sont abordés ont motivé le recours à cette procédure. Dans des délais rendus extrêmement contraints par un calendrier d'examen accéléré, la commission spéciale a organisé huit réunions plénières, complétées par 21 auditions des rapporteurs et reçu de très nombreuses contributions écrites.

Lors de sa réunion du 27 juin, la commission a adopté le projet de loi, modifié par 80 amendements permettant de prendre en compte les préoccupations déjà exprimées par les différentes instances du Sénat, qui mènent depuis des années un travail en profondeur sur les différents aspects d'un espace numérique qui, aussi risqué que source d'opportunités, nécessite une véritable régulation ambitieuse et adaptée.

I. UN ESPACE NUMÉRIQUE À RÉGULER

En vingt ans, l'Internet, le réseau des réseaux, s'est rapidement éloigné de la promesse initiale d'un espace ouvert, synonyme de progrès, de développement et de partage illimité de la connaissance.

A. UNE MEILLEURE RÉGULATION POUR FAIRE FACE À LA MULTIPLICATION DES CONTENUS ILLICITES ET PRÉJUDICIABLES

Alors que l'Internet reposait à ses origines sur des standards ouverts, les utilisateurs se sont progressivement retrouvés enfermés dans des **écosystèmes « propriétaires » et des « bulles informationnelles » reposant sur des algorithmes complexes**. L'Internet est devenu un espace non sécurisé pour nos concitoyens, un monde d'hyper-surveillance et de vulnérabilité, avec en particulier :

- un accès illimité et sans contrôle réel à des contenus préjudiciables pour les mineurs, notamment la **pornographie** ;

- le développement en ligne de **toutes les formes de criminalités**, allant du cyberharcèlement à la pédocriminalité en passant par toutes formes d'escroqueries et d'abus, avec des conséquences parfois dramatiques ;

- la diffusion d'informations fausses ou présentées hors de leur contexte, sans aucune hiérarchisation, des tentatives de manipulation des opinions, voire des scrutins électoraux, à travers des **campagnes d'ingérence et de déstabilisation,** parfois menées depuis l'étranger, comme l'a révélé en 2016 l'affaire « Cambridge Analytica ».

B. UNE MEILLEURE RÉGULATION CONCURRENTIELLE POUR FAIRE FACE À LA DOMINATION SANS PARTAGE DE QUELQUES GRANDS ACTEURS ÉTRANGERS

À la faveur des innovations technologiques, l'économie numérique s'est développée autour de nouveaux usages pour les utilisateurs, particuliers, administrations comme entreprises : accès à l'information, et à de nouveaux formats de divertissements, accroissement des échanges, réactivité, *etc*.

Cependant, si l'Europe s'est dotée dès 2000 d'un cadre réglementaire, ce dernier a essentiellement profité aux **usages**, sans considération pour sa position comme acteur du monde numérique et non plus simplement comme consommateur. En conséquence, **force est aujourd'hui de constater que quelques grandes entreprises extérieures à l'Union européenne**, principalement les « *BigTech* », dont la richesse et l'influence concurrencent désormais directement les États, **en ont été les principales bénéficiaires**. Elles ont profité des caractéristiques économiques du monde numérique, qui démultiplie les effets de réseaux, pour imposer leurs standards et leurs modèles économiques, déstabilisant les modèles d'affaires de secteurs entiers de notre économie et le fonctionnement de pans entiers de notre société. Aujourd'hui, on peut parler de quasi monopole. Les **phénomènes de verrouillage et de dépendance** sont si importants qu'il est impératif de faire évoluer la législation vers de vraies règles de concurrence, afin de redonner une **autonomie stratégique** aux européens.

La crise sanitaire et la crise ukrainienne ont révélé ces fragilités structurelles, ce qui a permis à la Commission européenne, avec l'impulsion décisive de la Présidence française de l'Union européenne (PFUE), de faire adopter un cadre réglementaire inédit et plus protecteur auquel les grands acteurs du numérique devront bientôt se conformer et les États membres s'adapter.

II. REHAUSSER NOTRE NIVEAU DE PROTECTION COLLECTIVE DANS L'ESPACE NUMÉRIQUE

A. ASSURER LA PROTECTION DES PUBLICS LES PLUS VULNÉRABLES

- **Protéger les mineurs de l'exposition précoce aux contenus pornographiques**

Conscient des ravages de l'exposition précoce des enfants aux images pornographiques, le Sénat a voté dans le cadre de la discussion de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales, à l'initiative de **Marie Mercier**, rapporteure, une procédure judiciaire de blocage des sites ne respectant pas les restrictions d'accès aux mineurs, sur le

modèle de la procédure existante en matière de sites illicites de jeux d'argent[1].

2,3 millions de mineurs visitent chaque mois un site « adulte », et ce dès 12 ans pour plus de la moitié des garçons[2].

Faisant le constat des lenteurs et difficultés de la procédure judiciaire de blocage et de déréférencement des sites pornographiques accessibles sans restriction aux mineurs, le Gouvernement a souhaité **changer de méthode**.

L'article 1er du projet de loi tend à confier à l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) la compétence d'élaborer **un référentiel général déterminant les exigences techniques auxquelles devraient répondre les systèmes de vérification d'âge** tout en respectant la vie privée des utilisateurs. Pour rendre ce référentiel contraignant, l'Arcom disposerait d'un pouvoir de mise en demeure et de **sanction pécuniaire à l'encontre des éditeurs de sites pornographiques** ne se conformant pas à celui-ci. **L'article 2** transformerait la procédure judiciaire de blocage et de déréférencement des sites ne respectant pas la restriction d'accès aux mineurs en **procédure administrative**, **confiée également à l'Arcom et sous le contrôle *a posteriori* du juge administratif**, après une phase contradictoire préalable auprès de l'éditeur.

Enfin, l'article 3 vise à **compléter le dispositif de lutte contre les contenus pédopornographiques** en **créant une sanction pénale applicable aux hébergeurs** qui ne satisferaient pas à la demande émise par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de procéder au retrait en vingt-quatre heures d'un contenu. Il serait ainsi aligné sur les dispositions déjà applicables en matière de contenus terroristes[3].

- **Protéger les citoyens face aux campagnes de désinformation et de déstabilisation**

Le projet de loi vise à mieux protéger les citoyens contre les contenus diffusés en ligne qui contribuent à la propagation de fausses informations en provenance d'États soumis à des sanctions internationales. Il prévoit ainsi à **l'article 4** l'extension des possibilités de **bloquer la diffusion sur l'Internet** des contenus produits par des médias visés par des sanctions européennes, à l'instar de *Russia Today* ou de *Sputnik*.

---

[1] *Article 23 de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.*

[2] La fréquentation des sites « adultes » par les mineurs, *Arcom, mai 2023.*

[3] *Règlement européen du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (« règlement TCO ») et des articles 6-1-3 et 6-1-5 de la LCEN.*

- **Protéger les internautes face aux infractions les plus graves**

Le projet de loi prévoit également, dans son **article 5**, la **création d'une peine complémentaire de « bannissement »** se traduisant, à l'occasion d'une condamnation pénale pour certains délits (pédopornographie, proxénétisme, négationnisme, apologie du terrorisme, harcèlement sexuel, sur conjoint ou scolaire…), par l'obligation faite aux fournisseurs de plateforme en ligne de **bloquer le compte ayant servi à commettre l'infraction**. Le texte vise également à leur imposer de prendre des mesures visant à bloquer **les autres comptes** détenus par une personne condamnée, qu'ils soient préexistants ou nouvellement créés pour échapper aux conséquences de la peine.

B. ASSURER LA PROTECTION DE TOUS LES INTERNAUTES FACE AUX ACTES QUOTIDIENS DE CYBERMALVEILLANCE

- **Constater la hausse des actes quotidiens de cybermalveillance**

Les tentatives d'arnaques et d'escroquerie en ligne ne cessent de se multiplier et font désormais partie de notre quotidien, prenant différentes formes (piratage de comptes en ligne, hameçonnage, arnaques aux faux supports techniques et à la livraison de colis, faux ordres de virement, attaques par rançongiciel, spams électroniques et téléphoniques, *etc.*).

- **Créer un nouveau dispositif national de filtrage dédié à la cybermalveillance**

Partant du constat que les actes de cybermalveillance sont en hausse et qu'il n'existe pas en France de dispositif national de filtrage des contenus sur l'Internet permettant de prévenir ces actes, **l'article 6 du projet de loi prévoit la création d'un « filtre national grand public de cybersécurité »**.

Les autorités administratives compétentes pour constater les infractions correspondant à ces actes (usurpation d'identité, usage frauduleux d'un moyen de paiement, collecte frauduleuse de données à caractère personnel, *etc.*) pourront d'abord **ordonner l'affichage d'un message d'avertissement à destination des internautes qui se connectent à des sites frauduleux, puis ordonner le blocage de ces sites**, dans un souci de meilleure protection de notre vie en ligne, sous la vigilance et le contrôle de la Commission nationale de l'informatique et des libertés (Cnil).

III. CRÉER LES CONDITIONS DE NOTRE SOUVERAINETÉ NUMÉRIQUE

A. RÉÉQUILIBRER LE MARCHÉ EUROPÉEN DE L'INFORMATIQUE EN NUAGE

• **Constater la hausse des pratiques anticoncurrentielles sur ce marché**

Pilier de l'économie de la donnée, l'informatique en nuage est aujourd'hui en forte croissance et représentait en 2021, selon l'étude d'impact du projet de loi, **un marché de 65 milliards d'euros en Europe et de 16 milliards d'euros en France qui pourrait atteindre, à l'échelle mondiale, jusqu'à plus de 1 200 milliards d'euros d'ici 2025**.

Or, ce secteur est également **fortement concentré** autour de trois acteurs (AWS, Azure-Microsoft et Google Cloud Platform), qui **captent environ 70 % des parts de ce marché en France comme dans le monde**. Un tel niveau de concentration pénalise les fournisseurs français et européens qui dénoncent, depuis plusieurs années déjà, des abus de position dominante, des pratiques **anticoncurrentielles « d'enfermement propriétaire », de « verrouillage » et qui rendent le marché de moins en moins contestable et interopérable**, telle que la « vente liée d'infrastructures et de logiciels ».

65 % des start-up françaises affirment être dépendantes des GAFAM tandis que 73 % d'entre elles utilisent au moins un de leurs services[1].

C'est la raison pour laquelle le *Data Act* prévoit de rendre possible la portabilité des données et les systèmes interopérables.

• **Encadrer la facturation abusive de frais de transfert de données et l'octroi de crédits**

La facturation de frais de transfert sortant de données *(« egress fees »)* est aujourd'hui particulièrement contestée. Considérés comme « artificiels », ces frais, surtout appliqués par les acteurs dominants *(hyperscalers)*, **peuvent parfois représenter jusqu'à 80 fois le coût réel du transfert de données et s'élever à plusieurs centaines de milliers d'euros[2]**.

Le *Data Act* prévoit la **suppression de ces frais**, ainsi que celle, progressive, des frais de changement de fournisseur, mais **ne prévoit pas d'encadrement spécifique des avoirs d'informatique en nuage, au contraire de l'article 7 de ce projet de loi**. Il s'agit d'une initiative française bienvenue car, comme le souligne l'Autorité de la concurrence[3], la facturation abusive

[1] *Baromètre de France Digitale sur la performance économique et sociale des start-up en 2021.*
[2] *Ofcom, Étude sur le marché de l'informatique en nuage, Rapport intermédiaire, 5 Avril 2023.*
[3] *Autorité de la concurrence, Avis sur certaines dispositions du projet de loi, 20 Avril 2023.*

des frais de transfert de données permet de compenser l'octroi, à titre gratuit, d'avoirs d'informatique en nuage. Autrement dit, **« l'entrée du marché » est gratuite, mais il y a un « péage à la sortie »**.

B. SOUTENIR L'INNOVATION AFIN DE POSITIONNER NOS ENTREPRISES COMME PREMIERS ACTEURS DES NOUVEAUX MARCHÉS ET D'EN ENCADRER LES RISQUES

- **Définir et autoriser de façon expérimentale les jeux à objets numériques monétisables**

Les jeux à objets numériques monétisables (**Jonum**) sont un nouveau type de jeux en ligne, à la croisée entre les jeux d'argent et de hasard et les jeux vidéo. Aujourd'hui en pleine croissance, **l'Autorité nationale des jeux estimant qu'entre 1 200 et 2 500 jeux sont en phase de développement dont une quinzaine en France, ils échappent aujourd'hui à tout cadre de régulation**, la législation existante sur les jeux n'étant pas adaptée à leurs spécificités.

Pourtant, ces jeux présentent également **des risques de jeu pathologique et addictif, en particulier auprès des mineurs et des personnes les plus vulnérables**, ainsi que des risques de blanchiment d'argent, de financement du terrorisme, de détournement de l'interdiction actuelle des casinos en ligne ou de concurrence avec le marché physique des jeux.

La commission spéciale estime indispensable de supprimer le recours à une habilitation à légiférer par ordonnance, prévue à l'article 15 de ce projet de loi, afin de pouvoir proposer une première définition en droit des Jonum et une expérimentation relative à leur autorisation, dans la perspective de l'adoption d'une nouvelle législation dédiée et adaptée à leurs spécificités, distincte de celle des jeux d'argent et de hasard et de celle des jeux vidéo. Cette expérimentation, comme la future législation, ne sauraient déstabiliser les acteurs déjà en place.

- **Anticiper le développement du marché de l'intermédiation des données**

Le règlement européen sur la gouvernance des données *(Data Governance Act)* crée en même temps qu'il encadre un nouvel acteur de l'économie numérique, les **prestataires de services d'intermédiation de données** (SID). Ces services doivent permettre de favoriser l'échange de données, notamment industrielles et commerciales, de façon plus transparente et plus concurrentielle entre acteurs économiques, administrations et particuliers, grâce à la **séparation** de l'échange, de la collecte et du traitement des données.

L'Union européenne anticipe une augmentation de 530 % du volume mondial des données en sept ans. Les applications de ce nouveau marché sont donc prometteuses, notamment dans le domaine de l'intelligence artificielle.

IV. ADAPTER NOTRE DROIT NATIONAL AUX RÈGLEMENTS EUROPÉENS

A. ADAPTER NOTRE DROIT AU RÈGLEMENT SUR LES SERVICES NUMÉRIQUES (RSN)

La Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) est désignée comme l'autorité chargée de contrôler le respect de l'ensemble des obligations des fournisseurs de places de marché en ligne, notamment en termes de **traçabilité des professionnels**, de **conformité des interfaces dès leur conception**, de **droit d'information** des consommateurs et **d'interdiction d'utiliser** des interfaces conçues de façon à tromper, manipuler ou entraver la capacité des consommateurs à prendre des décisions libres et éclairées.

La compétence de la Cnil serait affirmée pour la vérification du bon respect, par les plateformes en ligne, des obligations posées par le RSN en matière de limitation de l'utilisation des données personnelles pour le profilage publicitaire, **une telle pratique étant complètement proscrite pour les publicités qui touchent les mineurs**.

B. ADAPTER NOTRE DROIT AU RÈGLEMENT SUR LES MARCHÉS NUMÉRIQUES (RMN)

L'Autorité de la concurrence et le ministère de l'économie se voient reconnaître le pouvoir de conduire des **investigations**, de recevoir des **renseignements** et de coopérer avec la Commission européenne sur les pratiques des contrôleurs d'accès, dans le cadre du « **Réseau européen de concurrence** ». Conjointement avec trois États membres, le ministre de l'économie peut enfin demander l'ouverture d'une enquête de marché en cas de soupçon d'éventuel « contrôleur d'accès ».

C. ADAPTER NOTRE DROIT AU RÈGLEMENT SUR LA GOUVERNANCE DES DONNÉES **(DGA)**

La mise en œuvre du règlement européen sur la **gouvernance des données** repose sur deux piliers : la reconnaissance, d'une part, de la compétence de l'Arcep pour **réguler le nouveau marché d'intermédiation des données** et, d'autre part, des prérogatives de la Cnil sur l'altruisme en matière de données.

La désignation d'une autorité avant le 24 septembre 2023 pour réguler les services d'intermédiation de données (SID) répond à une

obligation européenne, que ce projet de loi traduit tardivement. L'Arcep disposera dans ses nouvelles missions de pouvoirs de sanction et d'enquête étendus. La Cnil sera compétente pour gérer le nouveau « *registre des organisations altruistes en matière de données* » et pour veiller au respect, par les organisations reconnues, des critères posés par le *DGA*.

D. ADAPTER NOTRE DROIT AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Si le règlement général sur la protection des données (RGPD) exclut de la compétence de la Cnil le contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions et leurs ministères publics dans l'exercice de leurs fonctions juridictionnelles, ces opérations doivent cependant faire l'objet d'un contrôle qui garantisse à la fois l'indépendance de l'autorité judiciaire et la protection des données personnelles des justiciables.

C'est pourquoi **il est créé, au sein du Conseil d'État, de la Cour de cassation et de la Cour des comptes, une autorité de contrôle de ces opérations de traitement des données à caractère personnel, respectivement compétente pour les juridictions administratives, judiciaires et financières**.

E. ADAPTER NOTRE DROIT AU FUTUR RÈGLEMENT SUR L'ACCÈS ET L'ÉQUITÉ DES DONNÉES

La proposition de règlement européen sur les données *(Data Act)*, toujours en cours de négociation à l'échelle européenne, a pour but de **garantir l'équité dans la répartition de la valeur produite par les données entre les acteurs de l'économie fondée sur les données ainsi que de favoriser leur accès et leur utilisation**. C'est une condition préalable essentielle à la concrétisation des possibilités offertes par l'ère numérique dans laquelle nous vivons.

Les articles 7 à 10 de ce projet de loi anticipent la mise en œuvre de cette proposition de règlement. L'Arcep est notamment désignée comme « gendarme du *cloud* », c'est-à-dire comme autorité compétente chargée de contrôler **l'encadrement des avoirs d'informatique en nuage**, la suppression progressive des frais de transfert de données et les litiges entre opérateurs ainsi que d'édicter les règles techniques d'interopérabilité, de portabilité et d'équivalence fonctionnelle qui s'appliqueront aux fournisseurs de service d'informatique en nuage.

V. LES APPORTS DE LA COMMISSION POUR MIEUX SÉCURISER ET RÉGULER L'ESPACE NUMÉRIQUE

A. ASSURER LA PROTECTION DES PLUS VULNÉRABLES

Favorable au principe d'une procédure administrative confiée à l'Arcom pour **essayer d'accélérer et de massifier la lutte contre les sites pornographiques** qui refusent d'instaurer un contrôle d'âge pour empêcher l'accès des mineurs à leurs contenus, la commission a souhaité **renforcer la solidité juridique du dispositif** en ne créant qu'une **unique procédure de mise en demeure et de sanction vis-à-vis de l'éditeur**. Elle a distingué les dispositions relatives au référentiel de celles relatives aux sanctions.

À l'article 5, la commission spéciale a estimé nécessaire d'aller plus loin que le dispositif proposé par le Gouvernement pour faire du bannissement une sanction réellement efficace.

Elle a ainsi étendu substantiellement la liste des délits pour lesquels cette peine complémentaire sera encourue, pour y intégrer notamment les délits « voisins » à la pédocriminalité mais aussi, dans une période marquée par la montée en puissance des violences contre les élus, dont témoigne dramatiquement l'actualité récente, les **menaces et intimidations à l'encontre des dépositaires d'une fonction publique**.

Elle a également fait de cette sanction une obligation susceptible d'être imposée dans le cadre des **alternatives aux poursuites**, pour qu'elle puisse être facilement imposée aux délinquants qui ont reconnu avoir commis un délit et **prévu son application comme modalité d'exécution des peines, ce qui rend le « bannissement » applicable dans de nombreuses hypothèses**.

Conjugués, ces dispositifs viendront apporter une réponse à la fois dissuasive et répressive à celles et ceux qui utilisent l'Internet pour répandre des discours haineux ou pour humilier, offenser et harceler.

B. PROTÉGER LES CITOYENS FACE AUX CAMPAGNES DE DÉSINFORMATION ET DE DÉSTABILISATION

La commission a adopté plusieurs amendements à l'article 4 visant à mieux lutter contre les ingérences en renforçant les moyens de l'Arcom. Un amendement vise à **combler un « trou dans la raquette » en donnant au régulateur une compétence sur les services de télévision et les services de médias audiovisuels à la demande (SMAD) extra-communautaires diffusés en France** ne relevant pas de la compétence d'un autre État membre de l'Union européenne.

C. ASSURER LA PROTECTION DE TOUS LES INTERNAUTES FACE AUX ACTES QUOTIDIENS DE CYBERMALVEILLANCE

Afin de rendre le dispositif plus opérationnel et plus protecteur, la commission spéciale a adopté plusieurs amendements visant à :

- **faciliter la constatation des infractions entraînant le déclenchement du dispositif** de filtrage afin de pouvoir mettre en demeure les éditeurs de services de communication au public en ligne frauduleux ;
- **s'assurer que le message d'avertissement à destination des internautes tentant d'accéder à des sites frauduleux soit clair, lisible, unique, compréhensible** et permette le renvoi vers la plateforme Cybermalveillance.gouv.fr ;
- **responsabiliser l'ensemble des intermédiaires techniques** chargés de mettre en œuvre les procédures de blocage à la demande des autorités administratives compétentes ;
- **renforcer l'information de la personnalité qualifiée au sein de la Cnil** chargée de contrôler le caractère justifié et proportionné des mesures de blocage.

D. RÉÉQUILIBRER LE MARCHÉ EUROPÉEN DE L'INFORMATIQUE EN NUAGE

Afin de **rééquilibrer les déséquilibres concurrentiels sur le marché de l'informatique en nuage** et de soutenir le développement de nos entreprises françaises et européennes, la commission spéciale a adopté des amendements visant à :

- **plafonner la durée d'octroi des avoirs d'informatique en nuage à un an** tout en laissant la possibilité au pouvoir réglementaire de détailler les différentes pratiques de marché visées ;
- **interdire toute condition d'exclusivité lors de l'octroi de tels avoirs** ;
- **préciser l'articulation de la suppression progressive des frais de transferts de données et des frais de changement de fournisseurs** avec les dispositions du *Data Act* ;
- **différencier les règles d'interopérabilité et de portabilité des services d'informatique en nuage édictées par l'Arcep en fonction de la nature de ces services** (infrastructure, plateforme, logiciel), tout en prenant en compte les règles techniques édictées par les autres autorités européennes et les standards industriels existants.

E. SOUTENIR L'INNOVATION AFIN DE POSITIONNER NOS ENTREPRISES COMME ACTEURS DES NOUVEAUX MARCHÉS ET D'EN LIMITER LES RISQUES

Afin d'accompagner le développement des jeux à objets numériques monétisables (Jonum), de soutenir l'innovation de l'économie numérique et d'en identifier en amont les risques associés, la commission spéciale a décidé de **supprimer l'habilitation à légiférer par ordonnance** sur cette question. Une **première définition, en droit, des Jonum est posée**, afin de reconnaître leurs spécificités, entre jeux d'argent et de hasard d'un côté et jeux vidéo de l'autre.

Par ailleurs, la commission a souhaité **autoriser, à titre expérimental pour une durée de trois ans, la création des Jonum**, tout en prenant les précautions nécessaires pour s'assurer de la protection des mineurs et pour se prémunir des risques de création détournée de casinos en ligne.

Enfin, pour **soutenir le développement des nouveaux marchés des services d'intermédiation** des données, la commission a souhaité conforter le rôle de l'Arcep en la matière.

F. ADAPTER NOTRE DROIT NATIONAL AUX RÈGLEMENTS EUROPÉENS

Afin de faciliter l'évaluation et la compréhension de l'évolution des marchés numériques et des risques systémiques, la commission spéciale a souhaité **renforcer la capacité de collecte de données du Pôle d'Expertise de la Régulation Numérique (PEReN), y compris au niveau des applications installées sur les systèmes d'exploitation**, afin de lui permettre de mieux analyser les risques systémiques liés aux grandes plateformes et aux grands moteurs de recherche en ligne.

La commission a également souhaité **faciliter la mise en œuvre de la procédure d'échange des données de location de meublés de tourisme entre les communes et les plateformes numériques** de location, afin de limiter la charge administrative des communes.

Dans l'optique de préserver les dispositifs « mieux-disants » que le RSN, la commission spéciale a notamment rétabli, à l'article 29, **le dispositif de signalement des fausses informations** instauré par la loi *Infox* du 22 décembre 2018.

Aux articles 31 et 32, la commission spéciale a adopté des amendements visant à **faciliter l'exercice par la Cnil de ses prérogatives et à sécuriser l'action de ses contrôleurs**. Cet objectif suppose l'existence d'un cadre stable et cohérent, s'appliquant sans distinction inutile aux pouvoirs d'enquête et de sanction de la Commission dans leur ensemble. Les nouveaux pouvoirs que la Cnil tire du RSN pourront ainsi s'appliquer aux manquements de toute nature, de même que les « *injonctions à caractère provisoire* » créées par le projet de loi.

G. POUR UNE MISE EN ADÉQUATION DES MOYENS BUDGÉTAIRES AUX MISSIONS

Même si cela ne relève pas du périmètre du projet de loi, la commission spéciale tient à souligner avec force que les nouveaux pouvoirs des administrations et des régulateurs doivent être accompagnés d'une mise à niveau de leurs moyens, sans quoi les dispositions ambitieuses du projet de loi resteront largement lettre morte.

*

* *

La commission spéciale a adopté le projet de loi ainsi modifié.

INTRODUCTION

La commission spéciale sur le projet de loi visant à sécuriser et réguler l'espace numérique a été constituée en séance publique au Sénat le 1er juin 2023. Elle a tenu sa réunion constitutive le 6 juin, et a désigné à cette occasion Catherine Morin-Desailly présidente, Patrick Chaize et Loïc Hervé rapporteurs. Les membres de la commission spéciale représentent **toutes les commissions permanentes et tous les groupes politiques du Sénat**.

Le calendrier d'examen du texte n'a laissé qu'un temps très réduit au Sénat pour mener ses travaux[1], d'autant plus que le projet de loi aborde un grand nombre de thématiques dans différents domaines des politiques publiques, ainsi que des sujets innovants qui n'ont encore jamais fait l'objet d'un examen parlementaire. Malgré tout, en ce temps très contraint, la commission spéciale a organisé huit auditions plénières[2] et 21 auditions des rapporteurs, de nombreuses contributions écrites ayant été également communiquées.

Les travaux de la commission spéciale avaient cependant été largement préparés en amont par les différentes instances du Sénat, qui ont analysé en profondeur ces dernières années **les différents aspects de la régulation de l'économie et des usages numériques**, aux niveaux national et européen.

Les travaux de la Haute Assemblée avaient notamment porté sur les trois axes majeurs du projet de loi :

– **la protection des mineurs** contre les contenus à caractère pornographique et le cyberharcèlement, notamment dans la lignée des travaux de la **délégation aux droits des femmes** ;

– la reconquête d'une **souveraineté économique européenne**, un objectif conforté par la crise pandémique et la guerre aux frontières de l'Europe et dont le numérique constitue une part essentielle. La commission des affaires européennes et la commission des affaires économiques avaient longuement travaillé sur cette question ;

[1] *Dans son avis du 27 avril, le Conseil d'État déplore également* « les délais particulièrement resserrés » *de présentation du texte, ce qui n'est* « pas de nature à permettre de garantir pleinement la sécurité juridique ».

[2] *L'ensemble des comptes rendus et des captations sont disponibles sur la page Internet de la commission spéciale.*

– la régulation d'ensemble de l'économie, des marchés et des services numériques, avec des résolutions européennes adoptées pendant la phase de négociation par la France des trois projets de règlements sur les services numériques, les marchés numériques et la gouvernance des données, et qui ont permis d'en améliorer le contenu. Le projet de loi procède aux adaptations nécessaires de notre droit interne pour rendre ces règlements d'application directe pleinement opérationnels.

Même si beaucoup reste à faire, l'examen du projet de loi permet ainsi au Sénat de faire valoir ses propositions afin de renforcer la régulation d'un espace numérique autant source d'opportunités que d'inquiétudes.

I. PREMIER AXE : LA PROTECTION DES CITOYENS ET DES MINEURS

La protection des mineurs constitue une préoccupation constante du Sénat. Ainsi, le rapport[1] de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes d'Annick Billon, Alexandra Borchio Fontimp, Laurence Cohen et Laurence Rossignol, consacré à l'industrie pornographique a largement décrit les effets toxiques de l'accès des plus jeunes aux sites à caractère pornographique, tandis que la commission des lois, à l'initiative de son rapporteur Marie Mercier, a doté l'Arcom d'un rôle en matière de contrôle de la restriction d'accès des mineurs aux sites à contenus pornographiques[2].

A. DES RÈGLES EUROPÉENNES (ENFIN) PLUS PROTECTRICES

Le règlement européen sur les services numériques comprend **trois dispositions** permettant précisément de renforcer la protection des mineurs en ligne :

- de manière générale, chaque fournisseur de services intermédiaires doit, à la suite d'une injonction émise par les autorités compétentes, agir contre les contenus **illicites** (dont les contenus pédopornographiques) ;

---

[1] *Rapport d'information n° 900 (2021-2022), fait par Annick Billon, Alexandra Borchio Fontimp, Laurence Cohen et Laurence Rossignol au nom de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes, sur l'industrie de la pornographie, déposé le 27 septembre 2022.*

[2] *Dans le cadre de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales (dossier législatif en ligne).*

- plus spécifiquement, les fournisseurs de plateformes en ligne accessibles aux mineurs doivent mettre en place des « *mesures **appropriées** et **proportionnées** pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service* » ;
- enfin, ces fournisseurs de plateformes ne doivent pas développer des publicités en ligne ciblées **visant les mineurs**.

Une proposition de règlement européen établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, en cours de négociation au niveau européen, et au sujet de laquelle le Sénat a adopté, le 15 février dernier, une résolution européenne[1] sur le rapport des sénateurs Catherine Morin-Desailly, Ludovic Haye et André Reichardt, tend à **renforcer les obligations** imposées aux fournisseurs de services d'hébergement et de communications interpersonnelles afin d'assurer la protection des mineurs en ligne. Ce texte leur impose en particulier, sur injonction des autorités nationales compétentes, de détecter les contenus pédopornographiques en ligne, de les retirer ou d'en bloquer l'accès, sous peine de sanctions.

B. LES DISPOSITIONS DU PROJET DE LOI RELATIVES À LA PROTECTION DES MINEURS EN LIGNE

Dans le cadre de ses fonctions de **coordinateur pour les services numériques**, l'Arcom, se voit attribuer des pouvoirs renforcés au titre de la protection des mineurs en ligne.

- ✓ **La vérification de l'âge des utilisateurs des sites pornographiques est mise en place par les articles 1er et 2** du projet de loi

L'Arcom serait désormais chargée de veiller « *à ce que les contenus pornographiques mis à disposition du public par un service de communication au public en ligne ne puissent pas être accessibles aux mineurs* ».

Cette disposition peut être considérée comme l'une des « *mesures appropriées et proportionnées* » que l'article 28 du règlement européen sur les services numériques (RSN) ordonne aux fournisseurs de plateformes en ligne de mettre en œuvre pour protéger les mineurs.

Elle répond surtout à une demande réitérée du Sénat, qui l'a exprimée dans ses résolutions européennes du 14 janvier 2022 et du 13 février 2023, ainsi que dans les recommandations de sa délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes sur l'industrie de la pornographie.

---

[1] *Résolution européenne n° 77 (2022-2023) du 15 février 2023 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants - COM(2022) 209 final, présentée par Ludovic Haye, Catherine Morin-Desailly et André Reichardt.*

L'article 2 du projet de loi mettrait en place une sanction administrative des éditeurs de services de communication au public en ligne qui permettent l'accès des mineurs à des contenus **pornographiques et permettrait à l'Arcom de délivrer directement des injonctions de blocage et de déréférencement aux fournisseurs d'accès à Internet et aux moteurs de recherche.**

Cette disposition constitue, là encore, une déclinaison française des articles 28, 51 et 52 du règlement sur les services numériques (RSN) : « *mesures appropriées et proportionnées* » exigées des fournisseurs de plateformes en ligne afin de permettre la protection de la vie privée, la sûreté et la sécurité des mineurs sur les services concernés ; pouvoirs d'enquête et de sanction du coordinateur des services numériques ; sanctions définies par les États membres avec un montant maximal égal à 6 % du chiffre d'affaires mondial du fournisseur concerné.

Elle constitue enfin et surtout une actualisation du dispositif sénatorial mis en place en France par la loi du 30 juillet 2020 à l'initiative du sénateur Marie Mercier, qui permet déjà au président de l'Arcom (alors CSA) de **mettre en demeure** tout éditeur de services de communication au public en ligne qui offre l'accès des mineurs à des contenus pornographiques. Et, si cette mise en demeure reste sans effet, de saisir le président du tribunal judiciaire de Paris, afin que ce dernier ordonne la fin de l'accès à ce service et, le cas échéant, son déréférencement.

L'application de ce dispositif essentiel pour la protection des mineurs a malheureusement été **sans effet** jusqu'à présent, suite à de nombreux recours contentieux menés par les sites concernés.

- ✓ L'article 3 du projet de loi met en place **la pénalisation du défaut d'exécution en vingt-quatre heures d'une demande de l'autorité administrative de retrait de contenu pédopornographique**.

Le droit français, depuis 2004, a confié à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), responsable de la plateforme Pharos, le soin d'ordonner aux fournisseurs de services d'hébergement le retrait de contenus terroristes et pédopornographiques sur Internet. À défaut, si dans un délai de vingt-quatre heures le retrait des contenus visés n'est pas effectif, l'autorité administrative précitée impose, par notification aux fournisseurs d'accès, le blocage de l'accès à ces contenus. En complément, le service concerné peut aussi faire l'objet d'une demande de déréférencement.

Cette procédure administrative se déroule sous le contrôle d'une personnalité qualifiée de l'Arcom, qui examine la régularité des demandes de retraits (article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).

Le projet de loi introduit dans cette loi de 2004 trois articles 6-2, 6-2-1 et 6-2-2 pour compléter ce cadre juridique et le rendre plus efficient.

La procédure de retrait des contenus pédopornographiques en ligne existe en France depuis 2004 – notre pays a été pionnier en la matière – et elle fonctionne de manière satisfaisante.

Les dispositions complémentaires du projet de loi seraient conformes à « *l'injonction d'agir contre les contenus illicites* » prévue à l'article 9 du RSN et seraient partie intégrante des « *mesures appropriées et proportionnées* » que son article 28 demande aux fournisseurs de prendre au nom de la protection des mineurs.

Elles seraient également compatibles avec les dispositions de la proposition de règlement visant à prévenir et à combattre les abus sexuels sur enfants (délai de vingt-quatre heures pour respecter l'injonction de retrait ; énonciation des motifs légitimes de ne pas la respecter : force majeure, impossibilité de fait ; droit au recours effectif des fournisseurs contre une injonction ; sanctions déterminées par les États membres dans un plafond de 4 % du chiffre d'affaires mondial de l'exercice précédent du fournisseur…).

Enfin, le projet de loi désigne la Cnil pour faire respecter l'interdiction de présentation aux mineurs de publicités fondées sur le profilage par les fournisseurs de plateformes en ligne. En application de cette compétence, la Cnil peut procéder à des contrôles dans les locaux ou installations permettant le traitement de données personnelles afin de vérifier si de telles publicités ciblées sont pratiquées et de demander au responsable de ce traitement de lui communiquer tous les documents utiles. Si elle estime que le responsable de traitement compétent méconnaît cette interdiction, la Cnil peut lui adresser un avertissement.

Cette disposition est la mise en œuvre de l'article 28, paragraphe 2, du RSN, qui prohibe toute publicité ciblée à l'égard des mineurs.

C. LA PRISE EN COMPTE DES TRAVAUX DE LA DÉLÉGATION AUX DROITS DES FEMMES

De manière générale, on retrouve dans le dispositif proposé une ample prise en compte des **recommandations contenues dans le rapport de la délégation aux droits des femmes** précité sur l'industrie pornographique, avec en particulier la faculté pour l'Arcom de prononcer des **sanctions administratives** contre les sites ne respectant pas leurs obligations *(recommandation n° 12)*, *via* des agents assermentés *(recommandation n° 11)*, de même que l'édiction par l'Arcom de règles exigeantes de vérification de l'âge au moment de la connexion sur un site à caractère pornographique *(recommandations nos 14 et 15)*. Le projet de loi ne rentre cependant pas dans les détails de ce dispositif technique, qui pourrait largement recourir à la solution du **double anonymat** promu par la délégation.

Par ailleurs, à la suite de l'adoption de la loi du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à Internet[1], dont les mesures d'application devraient prochainement entrer en vigueur, l'usage du contrôle parental devrait être facilité, car le dispositif voté prévoit une pré-installation par défaut d'un outil de contrôle parental sur les terminaux vendus en France et permettant d'accéder à Internet, notamment les téléphones portables

Dans l'ensemble, les travaux de la délégation ont été pris en compte, même si les auditions menées par la commission spéciale et les rapporteurs ont soulevé des interrogations sur la mise en œuvre pratique des dispositifs, face à des sites Internet peu coopératifs.

D. LA LUTTE CONTRE LA HAINE EN LIGNE

Le Sénat a mené en 2021 une mission d'information[2] sur le harcèlement scolaire et le cyberharcèlement, un sujet revenu de manière dramatique sous les feux de l'actualité avec le suicide de la jeune Lindsay.

L'article 5 du projet de loi propose de mettre en place une peine complémentaire de **suspension de compte sur les réseaux sociaux** pour les utilisateurs condamnés pour certains délits, au premier rang desquels la diffusion de la haine en ligne ou pour cyberharcèlement.

II. DEUXIÈME AXE : LA SOUVERAINETÉ ÉCONOMIQUE ET NUMÉRIQUE EUROPÉENNE

A. UN SUJET AU CŒUR DES PRÉOCCUPATIONS DU SÉNAT

La question de la souveraineté numérique de l'Europe est évoquée de longue date au Sénat.

Dès 2013, Catherine Morin-Desailly alertait sur le risque de voir l'Union européenne devenir « *une colonie du monde numérique*[3] ». Le rapport[4] de 2019 de la commission d'enquête présidée par Franck Montaugé avec comme rapporteur Gérard Longuet intitulé « *Le devoir de souveraineté numérique* »

---

[1] *Rapport n° 397 (2021-2022) de Sylviane Noël, fait au nom de la commission des affaires économiques, sur la proposition de loi visant à renforcer le contrôle parental sur les moyens d'accès à Internet, déposé le 26 janvier 2022.*

[2] *Rapport d'information n° 843 (2020-2021), de Colette Mélot, fait au nom de la mission d'information sur harcèlement scolaire et le cyberharcèlement, déposé le 22 septembre 2021.*

[3] *Rapport d'information n° 443 (2012-2013) de Catherine Morin-Desailly, fait au nom de la commission des affaires européennes, intitulé* L'Union européenne, colonie du monde numérique ?, *déposé le 20 mars 2013.*

[4] *Rapport n° 7 (2019-2020), de Gérard Longuet, fait au nom de la commission d'enquête sur le devoir de souveraineté numérique, déposé le 1er octobre 2019.*

a relancé le débat sur la nécessité de mettre en place une véritable stratégie « *globale et lisible* ».

Les événements récents, tels que la crise pandémique ou la guerre en Ukraine, ont plus que jamais mis en avant l'impératif pour l'Europe de se doter de réels outils de souveraineté, dans le domaine numérique comme dans tant d'autres. La voie à emprunter n'est pas cependant pas simple, tant les intérêts des États peuvent apparaître en premier abord divergents, même si des progrès notables ont été réalisés ces derniers mois. Pour autant, il est indéniable que, face à des entreprises géantes, soutenues par leur gouvernement, l'Europe est le bon échelon d'action. Ainsi, la commission des affaires économiques, sur le rapport de Patrick Chaize[1], a approuvé le 13 juillet 2022 la proposition de résolution européenne[2] adoptée le 14 juin 2022 à l'initiative de Florence Blatrix Contat et Catherine Morin-Desailly sur le programme d'action numérique de l'Union européenne à l'horizon 2030.

Sans constituer une réponse exhaustive, le présent projet de loi permet quelques avancées notables sur la question sensible des données « en nuage ».

B. LA RÉGULATION DE L'INFORMATIQUE EN NUAGE

Dans leur rapport[3] au nom de la commission des affaires économiques *Cinq plans pour reconstruire la souveraineté économique*, Sophie Primas, Amel Gacquerre et Franck Montaugé consacrent de larges développements à **la réduction de la dépendance de notre pays dans le secteur de la donnée.**

Ils **mettent en particulier en avant la pratique des « crédits *cloud* » par les grandes entreprises américaines, à destination des jeunes entreprises,** afin de leur permettre d'utiliser gratuitement et temporairement leurs logiciels et services d'hébergement de données.

Cette stratégie des « crédits *cloud* » peut être vue comme un moyen de soutenir la croissance et le développement des jeunes entreprises, en particulier celles qui sont actives dans le domaine de la technologie. Cependant, à terme, cette pratique commerciale « enferme » littéralement les entreprises dans leur phase de croissance dans une relation de **dépendance**

---

[1] *Rapport n° 774 (2021-2022) de Patrick Chaize, fait au nom de la commission des affaires économiques, sur le programme d'action numérique de l'Union européenne à l'horizon 2030, déposé le 13 juillet 2022.*

[2] *Proposition de résolution européenne n° 664 (2021-2022) présentée par Florence Blatrix Contat et Catherine Morin-Desailly sur le programme d'action numérique de l'Union européenne à l'horizon 2030, déposée le 14 juin 2022, devenue résolution du Sénat (n° 138, 2021-2022).*

[3] *Rapport d'information n° 755 (2021-2022) de Sophie Primas, Amel Gacquerre et Franck Montaugé, fait au nom de la commission des affaires économiques, intitulé* Cinq plans pour reconstruire la souveraineté économique*, déposé le 6 juillet 2022.*

avec leur fournisseur. En raison de la durée d'octroi de ces crédits, des montants distribués et des conditions restrictives imposées par les grandes entreprises américaines du numérique pour transférer les données qu'elles hébergent vers d'autres infrastructures et logiciels, **ces pratiques ont été considérées comme ayant des effets anticoncurrentiels importants dans le rapport précité de la commission des affaires économiques**.

De plus, si les entreprises françaises de l'informatique en nuage suivent désormais cette stratégie commerciale, **elles ne peuvent en réalité pas rivaliser avec les géants américains qui monopolisent le marché**…

La dépendance induite par ces pratiques a par ailleurs des effets de **long terme**. Ainsi, les jeunes entreprises qui auront recouru aux services des opérateurs américains lors de leur lancement seront invités à poursuivre avec le même fournisseur, ce qui a des impacts à plus long terme à la fois pour elles-mêmes, pour le marché du travail des jeunes diplômés et pour les entreprises européennes qui souhaiteraient se développer dans cette branche.

Dans leur rapport[1] au nom de la commission des affaires européennes sur la proposition de résolution européenne sur le projet de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données du 11 mai 2023 (dit *Data Act*), Florence Blatrix Contat, André Gattolin et Catherine Morin-Desailly ont également fixé comme ambition de « *supprimer les obstacles au changement de fournisseur* ». Ce rapport est assorti d'une proposition[2] de résolution européenne déposée le même jour, qui propose des objectifs ambitieux en matière de traitement des données et de souveraineté. En particulier, il appelle à « *renforcer l'effectivité du droit de changer de fournisseur de services de traitement des données* », avec plusieurs mesures comme la limitation des frais de transfert et de migration.

Le *Data Act*

Le projet de règlement européen sur les données, dit *Data Act*, est actuellement en cours de discussion. La finalisation des négociations en trilogue semble à ce stade en bonne voie, et le texte pourrait être adopté d'ici la fin de l'année 2023.

[1] *Rapport d'information n° 597 (2022-2023) fait par Florence Blatrix Contat, André Gattolin et Catherine Morin-Desailly au nom de la commission des affaires européennes sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) - COM(2022) 68 final, déposé le 11 mai 2023.*

[2] *Proposition de résolution européenne n° 596 (2022-2023) présentée par Florence Blatrix Contat, André Gattolin et Catherine Morin-Desailly sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) COM(2022) 68 final, déposée le 11 mai 2023, devenue résolution du Sénat (n° 140, 2022-2023).*

Plusieurs points d'accord **vont dans le sens de la résolution européenne du Sénat** :

– l'affirmation de la primauté des **règles de protection des données à caractère personnel** ;

– le renforcement des droits des utilisateurs sur les données produites ;

– le partage de données avec des tiers : encadrement des frais de mise à disposition pour prévenir les abus.

Le projet prévoit le droit de changer de fournisseur des services de traitement de données. Comme le souhaitait le Sénat, il est prévu de renforcer l'information préalable à l'acceptation de l'offre sur le droit de changer de fournisseur et les modalités de ce changement. En cas de demande de changement, le processus doit être lancé dans les deux mois suivant la notification (ce qui devrait écarter les délais résultant de crédits gratuits), et il est précisé que les frais doivent correspondre aux coûts de transferts vers le nouveau prestataire. En revanche, le délai de trois ans prévus pour la suppression progressive des frais ne serait pas réduit.

Les conditions de transfert vers des pays tiers avec lesquels l'Union Européenne n'a pas d'accord sont très strictement encadrées, mais l'opportunité de mettre en place un cloud souverain n'est pas évoquée.

Le projet de loi a tenu compte des remarques formulées par la commission des affaires européennes et la commission des affaires économiques visant à limiter la dépendance excessive à quelques fournisseurs d'infrastructures « en nuage » et à permettre le développement d'une véritable industrie européenne de la donnée.

Ainsi, le titre III (articles 7 à 14) vise à renforcer la confiance et la concurrence dans l'économie de la donnée et **transpose par anticipation plusieurs dispositions du *Data Act***, notamment sur les frais de transfert et de migration des données.

L'article 7, qui n'est pas prévu dans le projet de règlement, prévoit pour sa part **une limitation de la durée des « crédits *cloud* »**, dans une temporalité fixée par décret mais que le ministre, lors de son audition devant la commission spéciale le 8 juin, a souhaitée comprise entre **trois et six mois**. Ce sujet a fait l'objet d'une table ronde spécifique qui s'est tenue devant la commission spéciale le 15 juin.

III. TROISIÈME AXE : DES RÈGLEMENTS EUROPÉENS QUI PORTENT LA MARQUE DES TRAVAUX DU SÉNAT

Le projet de loi est pour une large partie consacré à l'adaptation de notre droit à **trois règlements européens** : le règlement sur **les marchés numériques** (RMN, ou *DMA*)[1] du 14 septembre 2022, le règlement relatif à un marché unique des **services numériques** (RSN, ou *DSA*)[2] du 19 octobre 2022 et le règlement du 30 mai 2022 sur la **gouvernance européenne des données (*Data Governance Act*, ou *DGA*)[3].**

A. LE RÈGLEMENT SUR LES MARCHÉS NUMÉRIQUES (RMN)

Présenté fin 2020 par la Commission européenne et adopté en juillet 2022, le règlement sur les marchés numériques vise à lutter contre les **pratiques anticoncurrentielles dans l'économie des plateformes en ligne**, qui enferment les utilisateurs dans leurs applications et empêchent le développement de nouveaux concurrents, et à corriger les déséquilibres résultant de leur domination sur le marché numérique européen.

Il définit à cet effet de **nouvelles obligations** que ces dernières devront respecter, au profit de l'innovation, de produits et services numériques de qualité, de la création de valeur et de son partage équitable pour le bénéfice des entreprises en relation d'affaires avec ces plateformes et du libre choix des consommateurs.

Entré en vigueur le 1er novembre 2022, le RMN est en grande partie applicable depuis le 2 mai 2023 et les contrôleurs d'accès, qui seront désignés à partir de juin 2023, devront s'y conformer à partir de **décembre 2023** et au plus tard le **6 mars 2024**.

1. Une régulation *ex ante* des contrôleurs d'accès

Le droit de la concurrence, qui sanctionne *a posteriori* des ententes ou des abus de position dominante, mais à l'issue de longues enquêtes et de contentieux nourris, n'incitait pas jusqu'à présent les grandes plateformes à modifier en profondeur leurs comportements, motif pour lequel le RMN les a soumis au respect *ex ante* d'obligations et interdictions concernant des comportements très généralisées et préjudiciables aux utilisateurs.

---

[1] *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).*

[2] *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).*

[3] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).*

Celles-ci s'appliquent uniquement aux « contrôleurs d'accès » *(gatekeepers)* qui contrôlent un ou plusieurs services de plateforme essentiels dans au moins trois États membres, réalisent un chiffre d'affaires **annuel d'au moins 7,5 milliards d'euros** au sein de l'Union européenne ou dont la capitalisation boursière excède **75 milliards d'euros**, et qui ont plus de **45 millions d'utilisateurs finaux mensuels au sein de l'Union européenne** et **10 000 entreprises utilisatrices**.

Les entités qui franchissent ces seuils doivent se déclarer auprès de la Commission européenne. À défaut, celle-ci peut les désigner unilatéralement. Elle peut également désigner comme tels des entreprises qui n'atteignent pas tous ces seuils en raison des barrières qu'elles imposent et de leur domination du marché.

Ces contrôleurs d'accès sont soumis à un ensemble d'obligations, en particulier :

- permettre aux utilisateurs de désinstaller les applications préinstallées sur leurs smartphones et de choisir leurs services par défaut pour certains services clefs de l'économie numérique ;
- rendre les services de messagerie instantanée interopérables avec d'autres services de messagerie ;
- permettre aux développeurs d'applications d'accéder dans des conditions équitables aux fonctionnalités auxiliaires et matériels informatiques des smartphones ;
- permettre aux entreprises qui utilisent les plateformes d'accéder à un certain nombre de données essentielles.

Il leur est en outre **interdit**, notamment, de :

- classer leurs propres produits ou services de façon plus favorable que ceux des concurrents (auto-préférence) ;
- utiliser, sans le consentement des utilisateurs, les données personnelles collectées entre différents services ;
- empêcher les entreprises utilisatrices de proposer leurs produits ou services sur d'autres plateformes ou d'autres canaux de distribution, à des conditions différentes.

De manière générale, il s'agit ainsi de remettre en cause les techniques qui ont permis aux grandes plateformes d'asseoir leur domination et d'offrir une plus grande liberté aux utilisateurs, afin qu'ils puissent se désabonner plus facilement, désinstaller de leurs appareils des logiciels préinstallés, utiliser d'autres services (portabilité et interopérabilité). **L'accent est mis sur les coûts des transferts et les biais comportementaux**. Certaines obligations concernent plutôt les utilisateurs professionnels, en particulier la possibilité de promouvoir leur offre et de conclure des contrats en dehors de la plateforme sur laquelle ils proposent

biens et services, comme par exemple la pré-installation exclusive des systèmes d'exploitation et des navigateurs en imposant des écrans multi-choix.

En cas de méconnaissance de ces obligations et interdictions, le contrôleur d'accès est passible d'une amende pouvant atteindre **10** % de son chiffre d'affaires mondial total (20 % en cas de récidive).

Lorsqu'un contrôleur d'accès adopte un comportement de non-respect **systématique** du RMN (enfreint les règles au moins trois fois en huit ans), la Commission européenne peut ouvrir une enquête de marché et, si nécessaire, imposer des mesures correctives comportementales ou structurelles (dont l'interdiction de réaliser des acquisitions dans le domaine du numérique).

La Commission européenne est seule habilitée à faire appliquer le règlement mais elle peut être appuyée par les autorités nationales de concurrence, qui peuvent ouvrir des enquêtes sur d'éventuelles infractions au *DMA* et lui transmettre leurs conclusions.

Une obligation d'information de la Commission sur les acquisitions envisagées est par ailleurs prévue, même en deçà des seuils nationaux ou européens de contrôle des concentrations. La Commission européenne peut procéder à un contrôle *proprio motu* ou à la demande d'un État membre.

Trois comités contribuent à la mise en œuvre du RMN : le Réseau européen de concurrence (REC), qui assurera la cohérence entre les actions menées au niveau national ou par la Commission, le groupe de haut niveau, qui réunit au niveau européen les représentants de l'ensemble des régulateurs sectoriels concernés, et le comité consultatif, qui joue un rôle très important dans la mise en place, pour les textes d'application.

2. Les apports du Sénat au règlement européen

La proposition de règlement a fait l'objet d'un examen par la commission des affaires européennes, dans la suite du rapport d'information[1] présenté par Catherine Morin-Desailly et Florence Blatrix Contat, qui a conduit à l'adoption d'une proposition de résolution européenne devenue résolution européenne du Sénat le 12 novembre 2021 et d'un avis politique qui en reprend les termes, destiné à la présidente de la Commission européenne et à la présidente du Parlement européen.

[1] *Rapport d'information n° 34 (2021-2022), fait par Catherine Morin-Desailly et Florence Blatrix Contat au nom de la commission des affaires européennes, sur la proposition de règlement sur les marchés numériques* (DMA), *déposé le 7 octobre 2021.*

La résolution du Sénat a été suivie sur plusieurs points, en particulier :

- ✓ l'ajout de **services essentiels** : navigateurs, assistants vocaux et services de messagerie en ligne ainsi que des services que la résolution qualifiait de secondaire : *cloud* et publicité en ligne ;
- ✓ des précisions sur les **interdictions**.

Elle a été partiellement prise en compte sur la coopération entre la Commission européenne et les autorités nationales, y compris en matière de contrôle des concentrations en deçà des seuils.

3. Un projet de loi qui adapte le droit français au RMN

S'agissant d'un règlement **directement applicable** en droit interne et qui n'ouvre pas d'options, **la mise en œuvre en France du RMN s'accompagne de mesures de coordination dans le code de commerce** (en particulier des renvois au RMN pour certaines définitions).

L'Autorité de la concurrence et la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), en coopération avec la Commission européenne dans le cadre du « Réseau européenne concurrence », sont désignées comme autorités compétentes pour l'application du RMN et des juridictions spécialisées sont chargées de traiter des litiges ressortissant de celle-ci.

En cas de méconnaissance par les contrôleurs d'accès des obligations et interdictions définies par le RMN et lorsque les manquements se produisent sur le territoire national et qu'elles sont mandatées à cet effet par la Commission, il est prévu que l'Autorité de la concurrence et la DGCCRF sont habilitées à mener des inspections (art. 23 § 3, 4 et 7 à 10 du RMN).

Elles pourront en outre prêter assistance à la Commission pour mener des auditions et recueillir des déclarations dans les locaux d'une entreprise (art. 22 § 2 du RMN). Elles pourront également recevoir des signalements de tiers et prendre des mesures appropriées (art. 27 du RMN).

Il est également prévu qu'elles peuvent mener, de leur propre initiative des enquêtes, sur la méconnaissance éventuelle de ces obligations et interdictions (art. 38 § 6 et 7 du RMN).

Enfin, le ministre chargé de l'économie ou son représentant est habilité à adresser à la Commission européenne, conjointement avec au moins trois autres États membres, une demande d'ouverture d'enquête de marché lorsqu'il existe des motifs raisonnables de soupçonner qu'une entreprise est « contrôleur d'accès » (art. 41 du RMN).

B. LE RÈGLEMENT SUR LES SERVICES NUMÉRIQUES (RSN)

Le règlement relatif à un marché unique des services numériques (RSN), définitivement adopté le 4 octobre 2022, doit entrer en vigueur le 25 août 2023 s'agissant des très grandes plateformes et le **17 février 2024 pour le reste des dispositions**. Il établit un cadre juridique européen sur la fourniture de services d'intermédiation en ligne dans le marché intérieur pour responsabiliser les grandes plateformes numériques, mieux définir les contenus pouvant être disponibles en ligne et, simultanément, lutter contre les contenus illicites (contenus terroristes ou pédopornographiques, vente de stupéfiants, de produits contrefaits, *etc*.).

1. Une régulation des fournisseurs de services d'intermédiation en ligne

Le RSN vise :

- les fournisseurs d'accès à Internet (FAI) ;
- les services d'informatique en nuage *(cloud)* ;
- les plateformes en ligne (boutiques d'application, réseaux sociaux, plateformes de partage de contenus…) ;
- les très grandes plateformes et les très grands moteurs de recherche (définis avec le critère du RMN de 45 millions d'utilisateurs mensuels dans l'Union européenne).

Chaque État membre doit nommer un « coordinateur des services numériques », autorité indépendante chargée de faire appliquer le cadre juridique européen et la Commission européenne va mettre en place une supervision sur les très grandes plateformes, au sein d'un réseau de contrôle européen (« Comité européen des services numériques ») qui réunit les autorités de régulation nationales.

Le règlement prévoit des mesures pour **lutter contre les contenus illicites** (injonctions des autorités compétentes, rapports de transparence sur les actions de modération des contenus, mécanismes de signalement de ces contenus par les utilisateurs, transmission des informations conduisant à soupçonner une infraction pénale aux autorités compétentes).

Ces mesures sont renforcées pour les plateformes en ligne (« signaleurs de confiance » et traitement de leurs demandes dans les meilleurs délais ; possibilité, pour ces fournisseurs, de suspendre, après un avertissement préalable, la fourniture de leurs services à ceux qui fournissent fréquemment des contenus manifestement illicites ; rapports de transparence renforcés ; information des consommateurs ayant acheté un produit ou un service en ligne illégal sur l'illégalité de ce produit ou service, l'identité du professionnel concerné et les voies de recours ; protection des mineurs en ligne par des « *mesures appropriées et proportionnées* »).

En outre, les places de marché *(market places)* devront **mieux identifier** les vendeurs de produits ou de services sur leurs plateformes et mieux en informer les consommateurs.

Une transparence accrue du fonctionnement des plateformes est également prévue (mise en place de systèmes internes de traitement des réclamations, mise à disposition d'informations sur les algorithmes choisis pour recommander des contenus publicitaires, obligation de proposer un système de recommandation de contenus transparent et non fondé sur le profilage).

Les très grandes plateformes et les très grands moteurs de recherche sont en outre soumis à des obligations renforcées (évaluation de tout risque systémique issu de la conception ou du fonctionnement de leurs services, atténuation de ces risques s'ils sont avérés, audits indépendants, accès à leurs données et contrôle de ces dernières par les coordinateurs des services numériques des États membres et la Commission européenne, mécanisme de réaction aux crises) à compter du 25 août 2023. La Commission européenne a ainsi récemment désigné les dix-sept grandes plateformes (AliExpress, Amazon Store, App Store, Booking, Facebook, Google Maps, Google Play, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipédia, YouTube, Zalando) et les deux très grands moteurs de recherche en ligne concernés (Bing et Google Search).

Certains types de publicités ciblées sont interdits lorsqu'elles visent **les mineurs** ou utilisent certaines données à caractère personnel telles que les opinions politiques.

En cas de **non-respect du RSN** par des entreprises, les coordinateurs nationaux et la Commission européenne pourront prononcer des astreintes ou infliger des sanctions (jusqu'à 6 % du chiffre d'affaires mondial). En cas de violations graves et répétées au règlement, les plateformes pourront se voir interdire d'activités sur le marché européen.

2. Le Sénat entendu sur le RSN, en dépit de quelques regrets

Sur proposition des rapporteures Florence Blatrix Contat et Catherine Morin-Desailly, et à la suite de leur rapport[1], la commission des affaires européennes a adopté une proposition de résolution européenne devenue **résolution européenne du Sénat le 14 janvier 2022**.

[1] *Rapport d'information n° 274 (2021-2022) fait par Florence Blatrix Contat et Catherine Morin-Desailly au nom de la commission des affaires européennes, sur la proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques intitulé* Amplifier la législation européenne sur les services numériques *(DSA)* pour sécuriser l'environnement en ligne, *déposé le 8 décembre 2021.*

Le Sénat a en particulier été entendu sur l'inclusion des **très grands moteurs de recherche** dans le périmètre des obligations définies par le règlement et la prise en compte du critère d'audience (45 millions d'utilisateurs actifs du service dans l'Union) pour définir les très grandes plateformes en ligne et les très grands moteurs de recherche. Il n'est toutefois pas prévu que les régulateurs puissent soumettre au cas par cas d'autres plateformes aux obligations renforcées des très grandes plateformes, notamment en raison de leur taux de pénétration chez les jeunes publics.

En revanche, contrairement à ce que souhaitait le Sénat, le texte adopté n'a pas remis en cause le régime de responsabilité limitée des hébergeurs[1], y compris des plateformes en ligne, par exemple lorsqu'ils ont permis la conclusion de contrats de vente de produits illicites ou dangereux ayant causé des dommages ou la diffusion de contenus illicites. On peut toutefois noter que, depuis lors, les obligations des fournisseurs de services d'hébergement ont été renforcées en matière de **lutte contre le terrorisme en ligne**[2].

Le Sénat avait également attiré l'attention sur le fait que de nombreux fournisseurs de services sur Internet, autres que les plateformes en ligne, permettent de conclure des contrats de vente en ligne, y compris à titre accessoire mais le règlement n'a pas inclus cette problématique.

Par ailleurs, même si elle va mettre en place une **supervision** sur les très grandes plateformes, au sein d'un réseau de contrôle européen (Comité européen des services numériques) qui réunit les autorités de régulation nationales, **la Commission européenne n'est pas dotée de pouvoir d'enquête et de sanction** sur les très grandes plateformes, **ce qui ne permettra pas de pallier l'inégale diligence des différentes autorités de régulation nationales à faire appliquer les régulations numériques**.

S'agissant des signaleurs de confiance, le règlement ne permet pas non plus que ce statut puisse être accordé à certaines entités représentant des intérêts particuliers, telles que des marques, des sociétés de gestion de droits d'auteur ou des journalistes, dans le cadre d'activités de vérification de faits.

Il apparaît également que **les spécificités du modèle économique des grandes plateformes en ligne ne sont pas pleinement prises en compte** (exploitation par des algorithmes, aussi puissants qu'opaques, de très grandes quantités de données – en particulier de données à caractère personnel –, utilisées pour le ciblage des contenus et des publicités, en vue de maximiser le temps passé par l'utilisateur sur leurs services et, partant,

---

[1] *Une résolution européenne avait été adoptée en ce sens par le Sénat le 27 septembre 2018. Il s'agit de la résolution n° 31 (2018-2019), présentée par Catherine Morin-Desailly et plusieurs de ses collègues, sur la responsabilisation partielle des hébergeurs.*

[2] *Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne qui permettent la détection et le retrait des contenus en ligne concernés.*

les revenus publicitaires des plateformes) et que la responsabilité des fournisseurs de services intermédiaires utilisant des algorithmes d'ordonnancement des contenus n'a pas été renforcée.

Enfin, de manière générale, les dispositifs de protection des consommateurs prévus par le texte ne prennent pas pleinement en compte les recommandations du Sénat (par exemple en matière **d'éthique** et de respect des droits fondamentaux, obligatoires pour tous les algorithmes, dès leur création (*lega by design*) ou de lutte contre la **viralité** des contenus illicites ou de protection des mineurs (interdiction de la publicité ciblée pour les mineurs et droit à l'oubli pour les mineurs).

3. Adaptation du droit national et désignation des autorités nationales compétentes

S'agissant là encore d'un règlement directement applicable en droit interne et qui n'ouvre pas d'options, la mise en œuvre en France du RSN s'accompagne de **mesures d'adaptation de la loi pour la confiance dans l'économie numérique** (articles 22 à 24) pour la mise en œuvre (procédures, sanctions) et la mise en cohérence avec le RSN (définitions par renvois), y compris en matière de lutte contre les contenus terroristes et pédopornographiques.

Les autorités compétentes françaises pour la mise en œuvre du RSN sont, selon le cas, l'Arcom, la Cnil ou la DGCCRF, l'Arcom étant désignée comme coordinateur national des services numériques (article 25).

Les pouvoirs d'enquête, d'exécution et de sanction de l'Arcom pour la mise en œuvre du RSN sont précisés, ainsi que ceux de la DGCCRF et de la Cnil, pour faire respecter certaines obligations du RSN (profilage, publicité ciblée notamment) par les fournisseurs en ligne (article 32).

Des mesures d'adaptation sont également introduites dans le code de la consommation (article 26), afin de les rendre cohérentes avec la mise en œuvre du RSN (contrôles par la DGCCRF et amendes civiles voire sanctions pénales en cas d'infraction, astreintes pouvant être prononcées par le juge aux fins de mise en conformité).

Il est également renvoyé **aux définitions du RSN** dans les lois relatives à la liberté de communication et la lutte contre la manipulation de l'information ainsi que dans le code électoral (articles 28 à 30).

Enfin, des coordinations sont prévues en matière de protection de la propriété intellectuelle (article 34).

C. LE RÈGLEMENT SUR LA GOUVERNANCE EUROPÉENNE DES DONNÉES (DGA)

1. Faciliter la réutilisation des données du secteur public

Le règlement prévoit qu'un plus grand nombre de données détenues par le secteur public seront éligibles au **droit de réutilisation** à compter du 24 septembre 2023, y compris des données protégées par la confidentialité commerciale, le secret statistique, les droits de propriété intellectuelle de tiers et certaines données à caractère personnel, pour que celles-ci servent, *in fine*, à améliorer la productivité et à stimuler l'innovation.

Pour faciliter la réutilisation de ces données, une obligation **d'assistance du demandeur** est prévue, chaque État membre devant créer un point d'information unique destiné à fournir aux réutilisateurs potentiels des informations sur les données détenues par les autorités publiques. Un point d'information unique sera également mis en place au niveau européen par la Commission. Pour permettre une disponibilité maximale de ces données détenues par les organismes publics, il est interdit aux organismes publics de conclure des accords d'exclusivité de réutilisation des données, sauf exceptions liées à l'intérêt public.

Le règlement crée par ailleurs un nouveau modèle commercial encadré : **le service d'intermédiation de données**, qui vise à « *établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel* ». Afin de garantir leur neutralité et renforcer ainsi la confiance dans le partage des données, ces intermédiaires ne devront pas exercer une autre activité et l'accès à leurs services, leurs conditions ainsi que les prix pratiqués devront respecter des principes d'équité, de transparence et de non-discrimination. Les personnes souhaitant exercer une telle activité devront le notifier à l'autorité nationale compétente, qui les autorisera à l'exercer et à utiliser le label de « Prestataire de services d'intermédiation de données reconnu dans l'Union ».

Enfin, **l'altruisme en matière de données est encouragé et encadré** : les entités qui mettent à disposition des données devront ainsi répondre à un ensemble de conditions telles qu'exercer leurs activités dans un but non lucratif et être juridiquement distinctes de toute entité exerçant des activités à but lucratif, afin, là encore, de renforcer la confiance dans le partage des données.

2. La Cnil désignée comme autorité compétente

Chargée de veiller à l'application du *DGA*, la Cnil est dotée en conséquence de nouvelles attributions en matière de contrôle et de sanction (article 31).

*

* *

Ambitieux dans ses objectifs, le projet de loi ne constitue cependant qu'une **étape** dans la régulation de l'espace numérique.

- D'une part, il sera nécessaire de mettre à disposition des autorités indépendantes (Arcom, Cnil, Arcep) les **moyens nécessaires** à leurs nouvelles missions, et ce dès le prochain projet de loi de finances. Le contrôle qu'elles vont devoir exercer sur des sociétés aux moyens très importants doit mobiliser une expertise de haut niveau, tant technologique que juridique, qui doit être recherchée rapidement.

- D'autre part, si le cadre européen a progressé, il reste encore à parfaire, notamment sur la réforme du statut des hébergeurs ou sur le développement d'une authentique industrie européenne du numérique, seule à même de garantir pleinement notre souveraineté.

EXAMEN DES ARTICLES

TITRE IER
PROTECTION EN LIGNE DES MINEURS

Section 1
Renforcement des pouvoirs de l'Autorité de régulation de la communication audiovisuelle et numérique en matière de protection en ligne des mineurs

Articles 1er et 2
Renforcement des pouvoirs de l'Arcom en matière de restriction d'accès des mineurs aux sites pornographiques

L'article 1er tend à confier à l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) la compétence d'élaborer un référentiel général déterminant les exigences techniques auxquelles devraient répondre les systèmes de vérification d'âge mis en place pour l'accès à des sites comportant des contenus pornographiques pour se conformer aux exigences de l'article 227-24 du code pénal. Pour rendre ce référentiel contraignant, l'Arcom disposerait d'un pouvoir de mise en demeure et de sanction pécuniaire à l'encontre des éditeurs de sites pornographiques ne se conformant pas à celui-ci.

L'article 2 transformerait la procédure judiciaire de blocage et de déréférencement des sites ne respectant pas la restriction d'accès aux mineurs en procédure administrative confiée également à l'Arcom, sous le contrôle *a priori* du juge administratif, après une phase contradictoire préalable auprès de l'éditeur.

Le rapporteur Loïc Hervé est favorable à ce transfert de la procédure du juge judiciaire vers une autorité administrative déjà expérimentée en la matière, dans un souci d'efficacité et de « massification » de la réponse face à la prolifération de contenus pornographiques en accès libre sur Internet. Il a noté que les procédures menées par l'Arcom seraient entourées de garanties suffisantes (phase contradictoire, collégialité, procédure de recours rapide…).

À son initiative, la commission spéciale a adopté les articles 1er et 2 en fusionnant les deux procédures de mise en demeure et de sanction de l'Arcom prévues à l'encontre de l'éditeur, pour éviter tout empiétement entre elles et une éventuelle procédure pénale. Elle a également souhaité intégrer l'ensemble de ces dispositions dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Elle a adopté ces deux articles ainsi modifiés.

Les articles 1er et 2 du projet de loi visent à mettre en œuvre **plusieurs recommandations formulées par la délégation aux droits des femmes** dans son rapport précité *Porno : l'enfer du décor* consacré à l'industrie pornographique, en particulier aux violences exercées en son sein et aux représentations sexistes, racistes, homophobes et inégalitaires qu'elle véhicule.

Ils s'inscrivent également dans la ligne de la directive « Services de médias audiovisuels »[1] qui a prévu que les États membres veillent à ce que les fournisseurs de plateformes de partage de vidéos relevant de leur compétence prennent les mesures appropriées pour protéger les mineurs, notamment par l'utilisation de « *systèmes permettant de vérifier l'âge des utilisateurs des plateformes de partage de vidéos en ce qui concerne les contenus susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs* ». Ces articles rejoignent également les objectifs de deux articles du RSN qui instaurent la mise en place de **mesures appropriées et proportionnées** par les fournisseurs de plateformes en ligne accessibles aux mineurs **pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs** (article 28) et l'adoption de **mesures ciblées** par les très grandes plateformes visant à protéger les droits de l'enfant, y compris notamment la **vérification de l'âge** (article 35).

1. Le constat : une interdiction de la diffusion d'images pornographiques susceptibles d'être vues par un mineur qui reste lettre morte sur Internet

a) Le visionnage d'images pornographiques par les mineurs sur Internet : un phénomène d'ampleur aux graves répercussions

Le fait de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère pornographique est puni de trois ans d'emprisonnement et de 75 000 euros d'amende **lorsque ce message est susceptible d'être vu ou perçu par un mineur,** en application de l'article 227-24 du code pénal. Lors de l'entrée en vigueur de la réforme du code pénal en 1994, cette infraction s'est substituée à celle existante d'**outrage aux bonnes mœurs**, tout en en restreignant le champ **aux seuls mineurs**[2].

---

[1] *Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels»), compte tenu de l'évolution des réalités du marché.*

[2] *Loi n 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes.*

La loi du 30 juillet 2020 *visant à protéger les victimes de violences conjugales* est venue préciser qu'une **simple déclaration de majorité n'était pas susceptible d'écarter cette incrimination**[1]. Les éditeurs de sites pornographiques[2] doivent donc procéder à des vérifications qui ne peuvent se limiter à une simple question : « Avez-vous plus de 18 ans ? ».

Force est pourtant de constater que **les mineurs peuvent consulter avec une facilité déconcertante les sites « adultes »** qui sont devenus le premier canal d'accès aux contenus pornographiques.

Le rapport précité de la délégation aux droits des femmes *Porno : l'enfer du décor* a parfaitement décrit cette massification de l'accès à la pornographie qui est intervenue à partir de 2006-2007, avec l'apparition de grandes plateformes comme Pornhub et Youporn qui diffusent **gratuitement et sans aucune restriction d'accès** une multitude de contenus pornographiques, par ailleurs souvent piratés.

L'état des lieux dressé par la délégation sur l'accès des mineurs à la pornographie par Internet est particulièrement édifiant. Selon les acteurs associatifs entendus par la délégation, **la première exposition involontaire des enfants intervient souvent dès l'école primaire**. Un sondage Opinionway[3] de 2018 cité par le rapport indiquait qu'à l'âge de 12 ans un enfant sur trois a déjà été exposé à des images pornographiques, **le plus souvent de façon involontaire**. Selon un sondage Ifop[4] également cité, réalisé en avril 2021 auprès d'**adolescents âgés de 15 à 17 ans**, **41 %** des adolescents interrogés **ont déjà consulté des sites pornographiques**.

En mai 2023[5], l'Arcom et Médiamétrie ont mis en évidence que **la part des mineurs fréquentant des sites « adultes » a progressé de neuf points en cinq ans, passant de 19 % fin 2017 à 28 % fin 2022.**

On compte 2,3 millions de mineurs visitant chaque mois un tel site pour y passer en moyenne 50 minutes, dont **75 % y accèdent exclusivement depuis leur téléphone**.

---

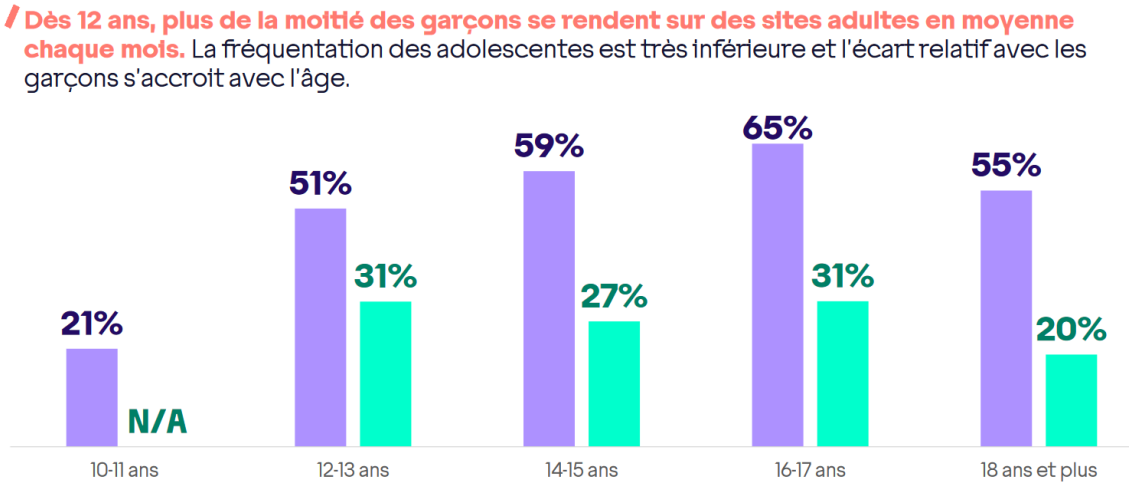
[1] *Article 22 de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.*

[2] *Dans sa délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique (Demande d'avis n° 21007330), la Cnil note que ce dispositif recouvre principalement des éditeurs de services de communication au public en ligne dont l'activité unique ou principale consiste en la diffusion de contenus pornographiques, mais peut s'étendre à de très nombreux sites qui éditent des contenus pornographiques.*

[3] *Sondage OpinionWay , #MoiJeune – Les 18-30 ans et la pornographie , avril 2018.*

[4] *https://www.ifop.com/publication/etude-sur-les-effets-et-consequences-de-la-loi-du-30-juillet-2020-sur-le-visionnage-de-contenus-pornographiques-par-les-adolescents-francais/*

[5] *La fréquentation des sites adultes par les mineurs, Arcom, mai 2023.*



Source : Extrait du rapport de l'Arcom sur la fréquentation des sites « adultes » par les mineurs, mai 2023

La délégation aux droits des femmes a documenté avec précision les **conséquences néfastes de cette exposition précoce des mineurs aux images pornographiques**, après avoir entendu de nombreux experts psychologues : traumatismes voire « viols psychiques » pour les plus jeunes, vision déformée et violente de la sexualité, sexualisation précoce et développement des conduites à risque ou violentes.

b) La procédure d'injonction judiciaire confiée à l'Arcom

Pour lutter contre ce phénomène préoccupant, le Sénat a voté dans le cadre de la discussion de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales, à l'initiative de Marie Mercier, rapporteure pour la commission des lois, une **procédure judiciaire de blocage des sites ne respectant pas les restrictions d'accès aux mineurs**, sur le modèle de la procédure existante en matière de sites illicites de jeux d'argent[1].

Cette procédure prévoit plusieurs étapes successives :

– l'organisation de **constats par des huissiers de justice** pour prouver que les contenus pornographiques sont susceptibles d'être vus par les mineurs ;

– l'envoi d'une **mise en demeure** par le président de l'Arcom enjoignant à l'éditeur de prendre toute mesure de nature à empêcher l'accès des mineurs au contenu incriminé ; l'éditeur dispose alors d'un délai de quinze jours pour présenter ses observations ;

– à l'issue de ce délai de quinze jours, en l'absence de réaction satisfaisante, la **saisine du président du tribunal judiciaire de Paris** selon une procédure accélérée au fond, afin que ce dernier ordonne **le blocage technique de l'accès au service en cause par les fournisseurs d'accès à**

[1] *Article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.*

Internet. Le président de l'Arcom peut également demander que soit ordonnée toute mesure destinée à faire **cesser le référencement du service par un moteur de recherche ou un annuaire**.

S'agissant des sites « miroirs »[1], il est prévu que le président de l'Arcom puisse saisir aux mêmes fins le président du tribunal judiciaire de Paris sur **simple requête**.

Cette procédure a été mise en œuvre à l'encontre de cinq sites pornographiques (Pornhub, Tukif, Xnxx, Xhamster et Xvideos) qui ont été mis en demeure le 13 décembre 2021. Faute de mise en conformité, le président de l'Arcom a saisi une première fois le président du tribunal judiciaire de Paris le 8 mars 2022.

Plus récemment, le 6 avril 2023, l'Arcom a mis en demeure les sociétés Technius Ltd. et Techpump Solutions S.L d'empêcher l'accès des mineurs à respectivement un et deux sites pornographiques qu'elles éditent. Elle a également saisi le président du tribunal judiciaire de Paris pour ordonner aux principaux fournisseurs d'accès à Internet d'empêcher l'accès à deux sites édités par société MG Freesites[2].

c) Des éditeurs de sites pornographiques qui veulent maintenir un statu quo *inacceptable*

Les sites pornographiques visés sont gérés par des entreprises très puissantes qui génèrent un chiffre d'affaires très significatif. Selon le rapport de la délégation aux droits des femmes, le site **Pornhub,** par exemple, **aurait généré** un total de **42 milliards de visites** en 2019 et afficherait un nombre de près de **220 000 vidéos vues chaque minute dans le monde**. Le marché mondial du X représenterait environ **huit milliards de dollars** de chiffre d'affaires.

Ainsi que l'a rappelé le président de l'Arcom lors de son audition devant la commission spéciale le 13 juin, les sites de l'industrie pornographique n'ont pris **aucune initiative pour se conformer à la loi du 30 juillet 2020 depuis son adoption**. Seul un éditeur mis en cause a mis en place un système de vérification d'âge. Ils ont en revanche mobilisé leur énergie pour mener une « **guérilla contentieuse** », selon son expression, pour faire obstacle à la mise en œuvre de la procédure de blocage. Le décret d'application a fait l'objet d'un recours pour excès de pouvoir. Trois mises en demeure ont été contestées devant les juridictions administratives. La procédure judiciaire a ensuite connu de multiples péripéties – dont une question préalable de constitutionnalité (QPC) posée par la société chypriote MG Freesites, éditrice du site Pornhub, et une médiation prononcée par le juge[3].

---

[1] *Même site rendu accessible à partir d'autres adresses.*
[2] *Décision consultable sur sur le site de l'Arcom.*
[3] *Tribunal judiciaire de Paris, 8 septembre 2022 (RG n°22/55687).*

Par décision du 5 janvier 2023[1], la Cour de cassation a estimé qu'il n'y avait pas lieu de renvoyer la QPC au Conseil constitutionnel, jugeant que les articles 227-24 du code pénal et 23 de la loi du 30 juillet 2020 étaient **suffisamment clairs et précis pour exclure tout risque d'arbitraire** et que **l'atteinte portée à la liberté d'expression**, en imposant de recourir à un dispositif de vérification de l'âge de la personne accédant à un contenu pornographique, autre qu'une simple déclaration de majorité, **était nécessaire, adaptée et proportionnée à l'objectif de protection des mineurs.**

D'autres délais sont en revanche incompressibles : ils sont liés aux délais d'assignation de personnes morales étrangères (plus deux mois[2]) et aux formalités de coopération européenne en application de la directive « e-commerce »[3]. Une décision est annoncée le 7 juillet 2023.

2. La proposition du Gouvernement : créer un référentiel de vérification d'âge obligatoire et renforcer les pouvoirs de sanction de l'Arcom

a) Confier le soin à l'Arcom d'élaborer un référentiel obligatoire pour les systèmes de vérification d'âge (article 1er)

Lors de la procédure judiciaire engagée par l'Arcom, de nombreux débats ont eu lieu sur la solution technique à déployer pour empêcher l'accès d'un site pornographique aux mineurs. Les éditeurs de ces sites ont invoqué le fait que, faute de solution éprouvée et faisant consensus, ils ne pouvaient leur être demandé plus qu'une vérification purement déclarative de l'âge.

Le Gouvernement souhaite donc l'élaboration d'un référentiel fixant le cadre des systèmes de vérification d'âge. Elle relèverait d'une nouvelle mission de l'Arcom qui serait inscrite dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique[4] (LCEN), celle de veiller à la non-accessibilité des contenus pornographiques en ligne aux mineurs.

Il reviendrait à l'Arcom, après avis de la Commission nationale de l'informatique et des libertés (Cnil), de fixer les **exigences techniques** propres à garantir tant la **fiabilité du contrôle de l'âge** des utilisateurs que le **respect de leur vie privée**. L'Arcom se verrait ainsi attribuer un **pouvoir normatif**, sanctionné par une amende administrative prononcée, après mise en demeure préalable, selon la procédure habituelle[5] prévue à l'article 42-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication. Cette sanction serait d'un maximum de 75 000 euros

---

[1] Cour de cassation, civile, Chambre civile 1, 5 janvier 2023, 22-40.017, Publié au bulletin.
[2] Article 643 du code de procédure civile.
[3] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
[4] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[5] Article 42-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

ou **1 % du chiffre d'affaires mondial hors taxes réalisé**, le plus élevé des deux montants étant retenu, ou de 150 000 euros ou 2 % du chiffre d'affaires mondial hors taxes en cas de réitération du manquement dans un délai de cinq ans après une première sanction.

Les termes « référentiel général » ont été suggérés par le Conseil d'État de préférence à « recommandation », pour faire ressortir son caractère obligatoire. Cette notion existe déjà dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

L'avancée des travaux sur le référentiel

La Cnil, l'Arcom et le Pôle d'expertise de la régulation numérique (PEReN) sont d'ores et déjà en train de travailler sur la rédaction d'un référentiel reposant sur le **double anonymat** conformément à la position de la Cnil publiée en juillet 2022 et dans laquelle elle a formulé un certain nombre de recommandations afin de permettre de concilier la nécessaire **protection des mineurs** avec, d'une part, la **protection de la vie privée des internautes** et, d'autres part, la **limitation des risques en matière de cybersécurité**.

La Cnil a exclu :

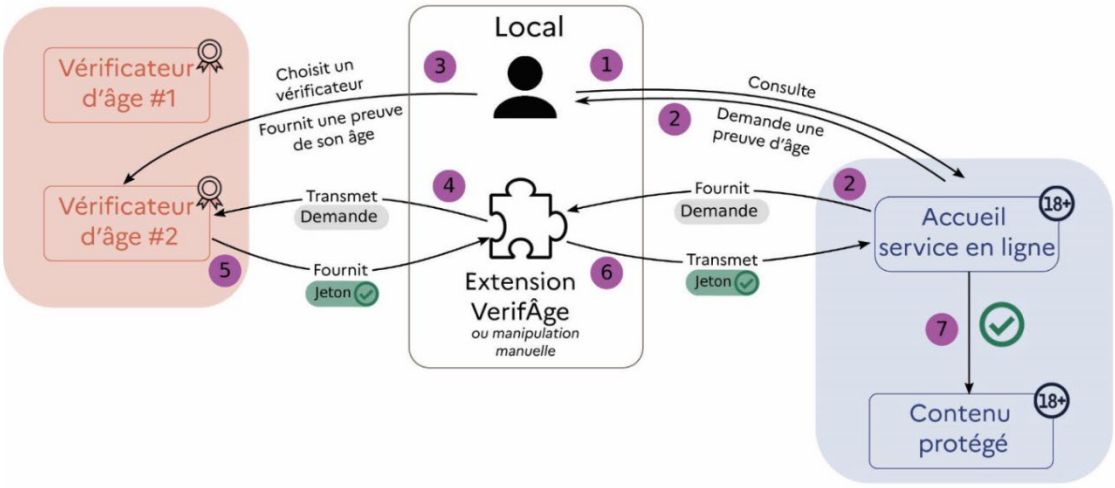
– la **collecte directe de pièces d'identité** par l'éditeur du site pornographique ;

– l'**estimation d'âge à partir de l'historique de navigation** de l'internaute sur le Web ;

– le **traitement de données biométriques** aux fins d'identifier une personne physique de manière unique.

Elle a préconisé le recours à un **tiers de confiance indépendant** destiné à faire obstacle à la transmission directe de données identifiantes relatives à l'utilisateur au site ou l'application proposant des contenus pornographiques.

Schéma de principe du mécanisme de double anonymat avec extension de navigateur



Source : « Éclairage sur la détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? », PeREN, Mai 2022, n° 4

Dans l'attente du déploiement de systèmes plus vertueux, notamment au regard des risques cyber, la Cnil a jugé **acceptables le recours à la vérification par carte bancaire** ou des **procédés d'estimation de l'âge reposant sur une analyse faciale**, sans toutefois avoir pour but l'identification de la personne. Dans ces deux cas, elle recommande toutefois que ces systèmes ne soient **pas mis en œuvre directement par le site Web consulté** mais par un tiers indépendant.

À travers son laboratoire d'innovation numérique, la Cnil a également proposé en mai 2022 un **démonstrateur** d'une solution reposant sur le double anonymat, c'est-à-dire un schéma de transmission de preuve d'âge qui garantirait la protection de la vie privée de la personne.

Source : réponses de la Cnil au questionnaire du rapporteur

b) Substituer un blocage administratif au blocage judiciaire existant (article 2)

Prenant acte des difficultés de mise en œuvre de la procédure judiciaire, le Gouvernement a souhaité **lui substituer une procédure administrative** qui serait menée de bout en bout par l'Arcom – et non plus son président –, sous le contrôle *a posteriori* du juge administratif. L'article 23 de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales serait reformulé en conséquence.

Il a écarté l'option consistant à enserrer la procédure judiciaire dans des délais plus contraints. Le Premier président de la Cour de cassation a suggéré à cet égard que le président du tribunal puisse **statuer sur requête dans le cadre des dispositions de l'article 845 du code de procédure civile** qui permet au président du tribunal de statuer **sur toutes mesures urgentes** lorsque les circonstances exigent qu'elles ne soient pas prises contradictoirement.

Le précédent : l'Autorité nationale des jeux

L'article 23 de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales a repris un dispositif mis en place pour l'Autorité de régulation des jeux en ligne (Arjel) – depuis devenue Autorité nationale des jeux (ANJ)[1] – pour obtenir le blocage et le déréférencement des sites de jeux ou de paris en ligne non autorisés[2].

[1] *Ordonnance n° 2019-1015 du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard.*

[2] *Article 61 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.*

À l'instar de ce que propose le projet de loi, la loi du 2 mars 2022 visant à démocratiser le sport en France[1] a **transformé cette procédure judiciaire en procédure administrative** à la suite d'un amendement du Gouvernement adopté au Sénat le 15 janvier 2022. Le président de l'ANJ peut désormais, à la suite d'une mise en demeure de l'opérateur illégal et de son hébergeur restée sans réaction pendant huit jours, ordonner aux fournisseurs d'accès à Internet d'empêcher l'accès au site en cause, sous peine d'une amende pénale de 250 000 euros. Cette demande de blocage du président de l'ANJ peut être contestée devant le juge administratif.

Le premier ordre administratif de blocage et de déréférencement pris par la présidente de l'ANJ a été rendu le 13 juin 2022. **Cette nouvelle procédure a conduit à l'édiction de 228 ordres administratifs, correspondant au blocage de 853 URL au total**. Le délai de traitement d'un dossier se situe désormais entre un et deux mois. Par comparaison, de 2010 à mars 2022, 369 ordonnances judiciaires ont été rendues, menant au blocage de 1 394 URL au total. Les délais étaient alors de quatre à six mois.

L'ouverture d'un compte joueur auprès d'un opérateur agréé de jeux ou de paris en ligne suppose **une vérification préalable de l'identité des joueurs**, et donc de leur majorité. L'article 4 du décret du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux[2] prévoit que la personne communique « *dans le délai maximum de trente jours à compter de la demande d'ouverture du compte, la copie de sa carte nationale d'identité, de son passeport, de son permis de conduire, de son titre de séjour ou de sa carte de résident en cours de validité justifiant de son identité et de sa date de naissance* », ainsi qu'un justificatif de domicile.

Une alternative consiste en l'usage de moyens d'identification électronique renforcés[3], peu utilisés par les opérateurs qui l'estiment trop lourde. Ces formalités sont nécessaires pour vérifier que les utilisateurs du site ne sont **pas inscrits au fichier des interdits de jeux**. Elles le sont également au titre des obligations des opérateurs de jeux ou de paris en matière de lutte contre le blanchiment et le financement du terrorisme[4].

L'ANJ mène des actions d'accompagnement à la conformité et des opérations de contrôle par les opérateurs. Elle développe des algorithmes pour détecter les cas où le joueur aurait renseigné une mauvaise date de naissance.

Source : site anj.fr et réponse au questionnaire du rapporteur

Des agents de l'Arcom, spécialement habilités à cet effet et assermentés, pourraient **constater directement les infractions** commises par les sites pornographiques et dresser des procès-verbaux, à l'instar de ce qu'ils font déjà pour constater certaines infractions relatives aux services de communication audiovisuelle[5].

L'Arcom serait ensuite dotée d'un pouvoir d'injonction direct contre l'éditeur d'un site litigieux et, en cas d'échec, à l'encontre des fournisseurs d'accès à Internet et des moteurs de recherche.

---

[1] *Loi n° 2022-296 du 2 mars 2022 visant à démocratiser le sport en France.*
[2] *Décret n° 2010-518 du décret du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.*
[3] *1° et 2° de l'article R. 561-5-1 du code monétaire et financier.*
[4] *Article L. 561-2 du code monétaire et financier.*
[5] *Article 78 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.*

L'injonction serait précédée par l'envoi **d'une simple lettre d'observations** à l'éditeur lui accordant un délai de quinze jours pour y répondre. Passée cette période, une mise en demeure serait adressée accordant un **nouveau délai de quinze jours minimum** pour empêcher l'accès des mineurs au contenu incriminé. Cette mise en demeure serait simultanément portée à la connaissance **des fournisseurs d'accès à Internet**.

Ce n'est qu'en cas d'inexécution de cette première injonction à l'éditeur, ou si ce dernier n'a pas mis à disposition sur son site ses coordonnées, que l'Arcom pourrait notifier à ces derniers les adresses électroniques des services de communication en ligne faisant l'objet de la procédure **afin qu'ils en bloquent l'accès sous quarante-huit heures**.

L'Arcom pourrait également notifier ces mêmes adresses aux **moteurs de recherches ou annuaires** afin de **déréférencer les sites contrevenants**, ainsi que leurs sites miroirs, **dans un délai de cinq jours**.

Ces mesures seraient **prononcées pour une durée maximum de vingt-quatre mois** et réévaluées tous les douze mois minimum, d'office ou sur demande. Elles seraient rendues publiques dans un rapport d'activité remis annuellement au Parlement et au Gouvernement.

Un **éditeur** de site ne se conformant pas à une injonction de l'Arcom d'empêcher l'accès aux mineurs aux contenus pornographiques encourrait une sanction pécuniaire de **4 % de son chiffre d'affaires mondial hors taxes ou de 250 000 euros**, le plus élevé des deux montants étant retenu, ces montants étant portés respectivement à **6 % maximum ou 500 000 euros** en cas de **réitération**. Ces pénalités seraient de 1 % du chiffre d'affaires mondial hors taxes ou 75 000 euros d'amende maximum s'agissant des fournisseurs d'accès à Internet, moteurs de recherche ou annuaires, ces montants étant portés à 2 % ou 150 000 euros en cas de réitération.

Cette nouvelle mission, indique l'étude d'impact, supposerait **des moyens supplémentaires ou une réorientation des priorités de l'Arcom.**

Ces dispositions nouvelles seraient applicables aux **procédures engagées à compter du 1er janvier 2024**[1]. Les procédures engagées antérieurement à cette date continueraient, elles, à relever de la compétence du président du tribunal judiciaire de Paris.

[1] *Voir article 36 du projet de loi.*

3. La position de la commission spéciale : accepter le principe d'une procédure administrative et réorganiser les articles 1er et 2 pour une meilleure cohérence

a) Accepter une nouvelle procédure pour lutter contre les sites pornographiques accessibles aux mineurs

Compte tenu du peu de résultat de la procédure judiciaire – aucun blocage obtenu en trois ans – le rapporteur estime souhaitable de prendre la voie d'une nouvelle procédure administrative pour accélérer et massifier la réponse aux sites pornographiques qui ne prennent aucune mesure pour protéger les mineurs.

La procédure administrative proposée pourrait présenter l'avantage d'un **caractère plus dissuasif** compte tenu des pouvoirs de blocage administratif et de sanctions pécuniaires octroyés à l'Arcom – même s'il semble en pratique difficile d'exécuter les sanctions pécuniaires à l'encontre d'éditeurs établis hors de France – et plus efficace avec la possibilité **d'agir directement auprès des fournisseurs d'accès à Internet et des moteurs de recherche ou annuaires**, même en l'absence de réponse du site contrevenant.

Cette nouvelle procédure présenterait une « originalité » au regard des autres procédures administratives de blocage existantes : contrairement aux contenus terroristes ou pédopornographiques, ou encore aux sites de jeux d'argent illégaux, **les contenus mis en ligne par les sites pornographiques ne sont pas en eux-mêmes illicites**, sauf à révéler des infractions autres que celles de l'article 227-24 du code pénal.

Cet élément doit être pris en compte pour l'analyse de la **proportionnalité de l'atteinte à l'exercice des libertés d'expression et de communication** protégées par l'article 11 de la Déclaration des droits de l'homme et du citoyen et par la Cour européenne des droits de l'homme (CEDH) au regard de **l'objectif d'intérêt général de protection des mineurs contre la pornographie et ses effets**.

Les garanties prévues ont été jugées suffisantes par le Conseil d'État, en particulier :

– l'existence d'une **procédure contradictoire de deux fois quinze jours** (lettre d'observations puis mise en demeure) permettant à l'éditeur du service de mettre fin à l'infraction pour ne pas s'exposer à des mesures coercitives de l'Arcom ; ainsi seuls les éditeurs qui **persisteraient délibérément à ne pas contrôler la majorité** des utilisateurs s'exposeraient à des sanctions ;

– la **prise de décision collégiale de l'Arcom** : la décision de procéder au blocage serait prise par le collège de l'Autorité après échange de vues entre ses membres et appréciation de la proportionnalité de la mesure ;

– la limitation à une **durée maximale de vingt-quatre mois** des mesures de blocage, **sans durée minimale** et avec réévaluation, d'office ou sur demande, de leur nécessité, au minimum tous les douze mois ; celles-ci seraient interrompues sans délai lorsque les faits les ayant justifiées ne seraient plus établis ;

– l'existence d'une **procédure de recours devant le juge administratif**, permettant à l'éditeur du service et aux personnes chargées de mettre en œuvre les mesures de blocage et de déréférencement, de lui demander **l'annulation des mesures**, le juge devant alors statuer sur leur légalité dans un **délai d'un mois à compter de la saisine**. L'appel serait rendu dans les trois mois. Une procédure en référé resterait possible dans les conditions du droit commun[1].

Le dispositif suppose une **convergence de jurisprudence entre le juge judiciaire,** qui aurait à apprécier, dans le cadre d'une procédure pénale, **si les éléments constitutifs de l'infraction pénale sont réunis** au titre de l'article 227-24 du code pénal, **et l'Arcom** qui ne peut en principe ordonner la mesure administrative de blocage que **si elle se situe dans le champ de l'infraction**.

b) La nécessité d'un référentiel obligatoire compte tenu des enjeux

Le Gouvernement a fait le choix de confier un pouvoir normatif à l'Arcom afin de lui laisser une certaine souplesse et capacité d'adaptation pour définir les **caractéristiques requises**, plutôt que de fixer directement les règles par arrêté ou décret, ce qui semble bienvenu. Le référentiel pourrait ainsi faire l'objet de réactualisations pour prendre en compte les nouvelles solutions techniques disponibles sur le marché.

Pour assurer l'opposabilité et l'efficacité de ce référentiel, il a entendu doter l'Arcom d'un **pouvoir de mise en demeure et de sanction spécifique**. Toutefois, à la lecture des sanctions prévues aux articles 1er et 2, il semble difficile de distinguer, s'agissant de l'éditeur, ce qui relève de la l'obligation de conformité au référentiel (article 1er) de ce qui relève de l'obligation de mettre en place toute mesure de nature à empêcher l'accès des mineurs au contenu incriminé (article 2), auquel s'ajouterait la responsabilité pénale au titre de l'article 227-24 du code pénal.

[1] *Articles L. 521-1 et L. 521-2 du code de justice administrative.*

c) Les modifications apportées par la commission spéciale

Afin de mettre plus de cohérence entre les différentes sanctions, et ainsi conforter la solidité du dispositif, la commission spéciale a choisi, à l'initiative du rapporteur, de réorganiser les articles 1er et 2 afin de bien **distinguer la situation des éditeurs et de celle des fournisseurs d'accès à Internet et des moteurs de recherche.**

L'article 1er serait consacré uniquement à la mission de l'Arcom de veiller à la non-accessibilité des contenus pornographiques en ligne aux mineurs et au référentiel. La commission spéciale a souhaité préciser expressément que les personnes dont l'activité est d'éditer un tel service de communication au public en ligne **vérifient préalablement l'âge de leurs utilisateurs** (**amendement COM-91)**. Elle a également adopté l'amendement **COM-37** de Laurence Rossignol précisant que le référentiel devait être établit dans les **six mois de la promulgation de la loi.**

L'article 2 créerait un nouvel article 10-1 dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui rassemblerait l'ensemble des pouvoirs de l'Arcom pour lutter contre l'accessibilité par les mineurs des contenus pornographiques sur Internet.

L'éditeur qui n'aurait pas mis en place de **système de vérification** d'âge ou un **système non conforme** au référentiel pourrait faire l'objet d'une **mise en demeure par l'Arcom** et encourrait une **sanction pécuniaire** à ce titre qui serait **modulée selon son degré de coopération**, la sanction maximale étant encourue lorsque l'éditeur n'a mis en place aucun système de vérification d'âge. Cette mise en demeure serait le préalable nécessaire à une mesure directe de blocage et de déréférencement du site, toujours à l'initiative de l'Arcom, dès lors qu'il est constaté que ce site est accessible aux mineurs.

Le président de la Cnil serait consulté le cas échéant avant une mise en demeure motivée par le déploiement d'un système de vérification d'âge non conforme au référentiel pour analyser l'impact sur la vie privée des utilisateurs. Son avis serait également demandé pour évaluer la sanction.

Cette procédure administrative viendrait ainsi compléter la répression qui pourrait être engagée contre l'éditeur sur le fondement de l'article 227-24 du code pénal, sans empiéter sur son champ.

L'**Arcom serait compétente pour les mises en demeure dans les deux cas, et non plus le seul** président, **pour mettre en demeure un éditeur** dont le site laisse accès aux mineurs à des contenus pornographiques par cohérence avec la mise en demeure relative au référentiel. Les **conclusions du rapporteur public seraient maintenues** dans le cadre de la procédure de recours devant le président du tribunal administratif, le délai d'un mois semblant tout à fait compatible avec cette étape de la procédure qui permet d'éclairer les débats d'un point de vue extérieur.

La commission spéciale a adopté l'amendement **COM-92** à cette fin, complété de l'amendement rédactionnel **COM-61** de Bernard Fialaire.

La commission spéciale a adopté les articles 1er et 2 **ainsi modifiés**.

Section 2

Pénalisation du défaut d'exécution en vingt-quatre heures d'une demande de l'autorité administrative de retrait de contenu pédopornographique

Article 3

Création d'une infraction pénalisant le défaut d'exécution d'une demande de retrait de contenu pédopornographique par un hébergeur

L'article 3 vise à créer une sanction pénale applicable aux hébergeurs qui ne satisferaient pas à la demande émise par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de procéder au retrait en vingt-quatre heures d'un contenu en ligne d'images ou de représentations de mineurs présentant un caractère pédopornographique relevant de l'article 227-23 du code pénal.

Il compléterait ainsi le dispositif de l'article 6-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[1] en s'alignant sur les dispositions déjà applicables en matière de contenus terroristes, par l'application conjointe du règlement européen du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne[2] (« règlement *TCO* ») et des articles 6-1-3 et 6-1-5 de la LCEN.

La création de cette infraction – punie de 1,25 million d'euros d'amende pour les personnes morales et, en cas d'infraction d'habitude, de 4 % du chiffre d'affaires mondial serait accompagnée de diverses garanties pour l'hébergeur : délai de préavis de douze heures avant la première injonction ; possibilité de ne pas y déférer en cas de motifs de force majeure, d'impossibilité de fait, d'erreurs manifestes ou informations incomplètes ; existence d'une procédure de recours accélérée devant le tribunal administratif.

La commission spéciale a été favorable à l'alignement du régime de responsabilité pénale de l'hébergeur avec celui qui existe en matière de terrorisme. Elle y a apporté quelques modifications rédactionnelles et procédurales.

Elle a adopté cet article ainsi modifié.

---

[1] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

[2] *Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.*

1. Aligner la responsabilité pénale des hébergeurs en matière de demandes de retrait de contenus pédopornographique sur celle en matière d'injonctions de retrait de contenus terroristes

a) Les demandes de retrait de contenus pédopornographiques

Depuis 2015, l'OCLCTIC, qui anime la plateforme de signalement Pharos, peut, en application de l'article 6-1 de la LCEN, demander aux **éditeurs et aux hébergeurs** de retirer « *des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal*[1] » - communément appelés « contenus pédopornographiques ».

En cas de non-retrait de ces contenus sous vingt-quatre heures, l'OCLCTIC peut notifier la liste des adresses électroniques permettant l'accès aux contenus illicites aux fournisseurs d'accès Internet afin qu'ils les bloquent sans délai. L'Office peut également notifier ces adresses aux moteurs de recherche aux fins de déréférencement.

Seule la non-exécution de ces notifications aux fournisseurs d'accès Internet et aux moteurs de recherche est pénalement sanctionnée. Les peines encourues sont **de 250 000 euros d'amende** (au lieu de 75 000 euros avant l'entrée en vigueur de la loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet[2], dite loi *Avia*) et **d'un an de prison**. Pour une personne morale, l'amende encourue est égale au **quintuple**, soit **1 250 000 euros**. Les demandes de retrait faites aux éditeurs et aux hébergeurs ne sont quant à elle sujettes à aucune sanction.

Cette procédure administrative s'exerce **sous le contrôle d'une personnalité qualifiée indépendante** placée sous l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) **chargée d'en vérifier le bien-fondé.** Cette dernière peut saisir le tribunal administratif, en référé ou sur requête, en cas de demande de retrait infondée.

La vérification des contenus pornographiques a constitué **82 % de son activité** en 2022 – **67 577 demandes de retrait** sur les 82 754 demandes totales – les 18 % restants étant consacrés aux contenus terroristes. Une séance de visionnage est organisée à peu près chaque semaine ; elle dure au **maximum trois heures** et permet d'examiner, en moyenne, environ 5 000 demandes adressées par l'OCLCTIC.

---

[1] « L'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique ».

[2] *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet.*

b) Une évolution récente en matière d'injonctions de retrait de contenus terroristes

L'article 6-1 de la LCEN est également applicable aux contenus faisant de la provocation ou de l'apologie du terrorisme au sens de l'article 421-2-5 du code pénal. Il a été récemment complété par le règlement européen *TCO*, entré en vigueur le 7 juin 2022, et la loi du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne[1]. Ces nouvelles dispositions permettent à l'OCLCTIC de délivrer une injonction de retrait, dans un **délai d'une heure**, de certains contenus à caractère terroriste **à l'encontre des hébergeurs** (dénommés « fournisseurs de services d'hébergement au public en ligne » dans le règlement).

La violation d'une telle injonction par un hébergeur est **pénalement sanctionnée** d'un an d'emprisonnement et 250 000 euros d'amende.

c) La proposition du Gouvernement : prévoir la même peine pour les hébergeurs en matière de contenus pédopornographiques tout en accordant les mêmes garanties

Le Gouvernement souhaite selon l'étude d'impact « *aligner au maximum* » le régime des hébergeurs en cas de non-respect des demandes de retrait des contenus pédopornographiques sur celui relatif aux contenus terroristes, tant sur le volet répressif que sur le volet procédural. En effet, les deux infractions sont d'une **gravité comparable** – elles sont d'ailleurs les seules à faire l'objet de demande de retrait aussi brève – et il n'y a pas lieu de traiter différemment un hébergeur qui contreviendrait à une demande de retrait selon la nature du contenu. Par ailleurs, il est souhaitable de prévoir **les modalités de recours** en adéquation avec la brièveté des délais qui leur sont imposés.

Dans ce but, l'article 3 du projet de loi introduirait trois nouveaux articles dans la LCEN :

– l'article 6-2 tend à reprendre certaines des **garanties offertes par le règlement *TCO*[2] à l'hébergeur** : information préalable douze heures avant toute première demande de retrait, non-exécution de la demande de retrait en cas de force majeure, d'une impossibilité de fait non imputable au service ou d'une erreur matérielle ; il prévoit également que le **fournisseur de contenus** doit être informé dans les meilleurs délais des motifs du retrait et des voies de recours qui lui sont ouvertes pour contester la demande ;

---

[1] *Loi n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne.*

[2] *Voir les points 2, 7 et 8 de l'article 3 et l'article 11 du règlement.*

– l'article 6-2-1, directement inspiré de l'article 6-1-3, prévoit un **quantum de peines identique à celui applicable en matière de terrorisme** : un an d'emprisonnement et 250 000 euros pour une personne physique, ce qui équivaut à **1 250 000 euros pour une personne morale** ; en cas d'infraction **commise à titre habituel**, l'amende pourrait être **portée à 4 % du chiffre d'affaires mondial** ;

– l'article 6-2-2 a été introduit à l'initiative du Conseil d'État. Il vise à transposer les dispositions procédurales de l'article 6-1-5 et prévoit : un maintien de la possibilité de recourir aux procédures de référés prévus aux articles L. 521-1 et L. 521-2 du code de justice administrative ; l'ouverture d'un **recours au fond aux hébergeurs, aux fournisseurs de contenus, ainsi qu'à la personnalité qualifiée de l'Arcom**, dans un délai de quarante-huit heures, le tribunal administratif disposant de **soixante-douze heures pour statuer** ; un appel possible dans un délai de dix jours à compter de la notification de la décision des juges du fond.

Il est précisé que l'audience serait publique et se déroulerait **sans conclusions du rapporteur public,** ce qui serait justifié par les délais extrêmement resserrés de la procédure. Cette absence de conclusions de rapporteur public n'est pas prévue actuellement en matière de contenus terroristes par l'article 6-1-5, mais elle est proposée par l'article 23 du projet de loi. Elle est actuellement une simple possibilité inscrite à l'article R. 732-1-1 du code de justice administrative par le décret d'application du 3 juin 2023[1].

2. La position de la commission spéciale : accepter l'alignement proposé

a) Un constat préalable : la portée limitée de la disposition apportée

Les sites d'hébergement de contenus, notamment vidéo, en ligne tendent généralement à **retirer rapidement les contenus** dès lorsqu'ils leur sont signalés, ainsi que le relève la personnalité qualifiée de l'Arcom dans son rapport annuel 2022[2].

Compte tenu de cette bonne coopération et du fait que de nombreux hébergeurs sont situés à l'étranger, la pénalisation du non-respect des demandes de retrait relève **plus d'une bonne harmonisation des règles juridiques, que d'un besoin opérationnel.** Elle peut également inciter certains petits acteurs récalcitrants…

---

[1] *Décret n° 2023-432 du 3 juin 2023 relatif au retrait des contenus à caractère terroriste en ligne, pris en application des articles 6-1-1 et 6-1-5 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

[2] *Consultable en ligne sur le site de l'Arcom.*

Tableau récapitulatif de l'activité de contrôle de la personnalité qualifiée du 1er janvier au 31 décembre 2022

	Demandes de retrait	Contenus retirés	Demandes de blocage	Demandes de déréférencement
Contenus à caractère terroriste	**15 177** (18 %)	**11 950** (78 %)	**12** (3 %)	**879** (30 %)
Contenus à caractère pédopornographique	**67 577** (82 %)	**61 135** (90 %)	**381** (97 %)	**2 072** (70 %)
Total	**82 754**	**73 685**	**392**	**2 951**

Extrait du rapport annuel 2022 de la personnalité qualifiée

Par ailleurs, ainsi que l'expose l'étude d'impact, l'article 3 vise à anticiper l'entrée en vigueur du règlement relatif à la lutte contre les abus sexuels sur mineurs publié par la Commission européenne le 11 mai 2022[1]. Ce projet de règlement prévoit la possibilité pour les autorités nationales compétentes d'émettre des injonctions de retrait des contenus à caractère pédopornographique dans un délai de vingt-quatre heures, étant précisé que le non-respect de cette obligation devrait faire l'objet d'une sanction en droit interne.

Toutefois, cette proposition, par ailleurs très discutée, est toujours en débat et **il est plus que probable que de nouveaux ajustements législatifs seront nécessaires prochainement dès son adoption.**

b) La position de la commission spéciale : adopter l'article sous réserve de quelques ajustements

La commission a accepté d'adopter cet article, en y apportant quelques corrections pour mieux aligner sa rédaction sur le règlement TCO (amendement **COM-93**) et rétablir les conclusions du rapporteur public, le pouvoir réglementaire ayant la possibilité de permettre au magistrat de dispenser le rapporteur public de prononcer des conclusions à l'audience (amendement **COM-94**).

La commission spéciale a adopté l'article 3 **ainsi modifié**.

[1] *Proposition de règlement du Parlement européen et du Conseil du 11 mai 2022 établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, COM(2022) 209 final.*

TITRE II
PROTECTION DES CITOYENS DANS L'ENVIRONNEMENT NUMÉRIQUE

Article 4

Protection des citoyens contre les vecteurs de propagande étrangère manifestement destinés à la désinformation et à l'ingérence

L'article 4 étend les compétences de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) pour la mise en œuvre des mesures restrictives européennes visant les médias aux éditeurs et distributeurs de services de communication audiovisuelle, aux opérateurs de réseaux satellitaires et à leurs prestataires techniques et aux services de communication au public en ligne. L'Arcom pourra enjoindre à ces prestataires de respecter les interdictions de diffusion des contenus produits par des médias visés par les sanctions européennes.

1. La législation actuelle

L'Union européenne dispose d'un arsenal juridique lui permettant de décider de sanctions à l'encontre d'États tiers. L'article 29 du traité sur l'Union européenne confère au Conseil de l'Union européenne le droit de prendre des sanctions à l'encontre de gouvernements de pays tiers, d'entités non étatiques et de personnes afin de les inciter à revoir leur politique ou leur activité.

Par ailleurs, l'article 215 du traité sur le fonctionnement de l'Union européenne permet au Conseil d'adopter les mesures nécessaires à la mise en œuvre des décisions prises en vertu de l'article 29 du traité sur l'Union européenne afin d'assurer leur application uniforme dans tous les pays de l'Union européenne.

Les sanctions prises par l'Union européenne dans ce cadre visent des pays non membres de l'Union, des personnes physiques ou morales, des groupes ou des entités non étatiques qui ne respectent pas le droit international ou les droits de l'homme ou mènent des politiques ou des actions contraires à l'État de droit ou aux principes démocratiques.

Différents types de sanctions sont possibles et peuvent être prises graduellement.

Les sanctions diplomatiques prévoient l'expulsion de diplomates, la suspension des visites officielles, la suspension de la coopération bilatérale ou multilatérale avec l'Union européenne et le boycottage d'événements sportifs ou culturels.

Les sanctions économiques et financières permettent l'embargo sur les armes et les équipements militaires figurant dans la liste commune des

équipements militaires de l'Union européenne ainsi que des restrictions à l'importation et l'exportation des biens à usage civil et militaire.

Les mesures restrictives peuvent concerner le gel des fonds et des ressources économiques détenus ou contrôlés par des personnes ou des organisations ciblées, l'interdiction de visa ou de voyage empêchant l'entrée des personnes dans l'Union européenne et les mesures d'interdiction sectorielle, par exemple sur l'importation ou l'exportation de certains biens ou certaines technologies.

Article 215 (ex-article 301 TCE)

1. Lorsqu'une décision, adoptée conformément au chapitre 2 du titre V du traité sur l'Union européenne, prévoit l'interruption ou la réduction, en tout ou en partie, des relations économiques et financières avec un ou plusieurs pays tiers, le Conseil, statuant à la majorité qualifiée, sur proposition conjointe du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et de la Commission, adopte les mesures nécessaires. Il en informe le Parlement européen.

2. Lorsqu'une décision, adoptée conformément au chapitre 2 du titre V du traité sur l'Union européenne, le prévoit, le Conseil peut adopter, selon la procédure visée au paragraphe 1, des mesures restrictives à l'encontre de personnes physiques ou morales, de groupes ou d'entités non étatiques.

3. Les actes visés au présent article contiennent les dispositions nécessaires en matière de garanties juridiques.

À la suite de l'invasion de l'Ukraine par la Fédération de Russie, l'Union européenne a adopté des mesures restrictives, dont des interdictions de diffusion de contenus produits par des médias liés directement ou indirectement au pouvoir russe. Une quinzaine de médias, dont Russia Today et Sputnik, sont concernés par ces interdictions de diffusion sur le territoire de l'Union européenne.

Cependant, les autorités françaises ont pu constater au cours de l'année 2022 la mise en œuvre, en particulier de la part de RT France, de stratégies de contournement des mesures restrictives au travers du recours à des sites Internet et de plateformes domiciliées hors de l'Union européenne comme Odysee et Rumble.

Ces différents cas de contournement ont mis en évidence l'absence de dispositif juridique en France permettant de s'assurer de la mise en œuvre des mesures restrictives européennes visant les médias.

La loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication qui définit les pouvoirs et les compétences de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) ne prévoit ainsi pas de dispositions permettant de mettre en œuvre des sanctions européennes visant les médias.

Par ailleurs, il apparaît également que les dispositions de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

qui permettent le retrait, le blocage et le déréférencement de contenus illicites ne concernent que ceux à caractère terroriste ou pédopornographique diffusés sur Internet.

Les autres modes d'action comme la saisine du juge judiciaire ou le recours aux services douaniers ne permettent pas davantage d'aboutir à faire cesser les infractions constatées faute d'autorité compétente pour arrêter très rapidement la diffusion des contenus visés.

2. Le dispositif proposé

Le dispositif prévu par le présent article 4 vise à élargir l'application des articles 42 et 42-10 de la loi du 30 septembre 1986 précitée aux opérateurs de communication audiovisuelle et aux opérateurs de communication au public en ligne afin de permettre à l'Arcom de mettre en demeure les opérateurs de faire cesser la diffusion des contenus faisant l'objet de sanctions. En cas de réponse insuffisante, l'Arcom pourra prononcer une sanction à l'encontre de l'opérateur concerné ou recourir à la procédure de « référé audiovisuel » prévu par l'article 42-10 qui permet au président de la section du contentieux du Conseil d'État d'ordonner toute mesure permettant de faire cesser un manquement au besoin en prononçant des astreintes.

En ce qui concerne les opérateurs de communication au public en ligne, le nouveau dispositif créé s'inspire des dispositions de l'article 6-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. L'Arcom pourra ainsi délivrer des injonctions aux acteurs qui concourent à la diffusion de contenus sanctionnés afin que cette diffusion cesse dans un délai de soixante-douze heures, délai durant lequel ils pourront lui adresser des observations et saisir le juge des référés du Conseil d'État. En l'absence d'exécution, et lorsque le contenu est en ligne, l'Arcom pourra enjoindre aux fournisseurs d'accès à Internet de bloquer le site diffusant le contenu. En cas de méconnaissance de l'obligation de retirer les contenus ou de faire cesser leur diffusion par les opérateurs, l'Arcom pourra prononcer une sanction pécuniaire à leur encontre, tenant compte de la gravité du manquement ou de la réitération.

Pour les personnes fournissant des services d'hébergement ou d'édition de service de communication au public, le montant de la sanction ne pourra excéder 4 % du chiffre d'affaires ou 250 000 euros ou, en cas de réitération, 6 % du chiffre d'affaires ou 500 000 euros. Pour les fournisseurs d'accès à Internet, le montant de la sanction pourra atteindre 75 000 euros ou 1 % du chiffre d'affaires, et en cas de réitération 150 000 euros ou 2 % du chiffre d'affaires.

Lorsque seront prononcées une amende administrative et une amende pénale en application de l'article 459 du code des douanes (pouvant aller de 450 euros à 225 000 euros) à l'encontre de la même personne,

le montant global des amendes ne pourra pas dépasser le maximum légal le plus élevé des sanctions encourues.

3. La position de la commission spéciale

a) La nécessité de mieux lutter contre les opérations d'ingérence conduites sur Internet

Dès le 24 février 2022, le président de la commission de la culture, de l'éducation et de la communication, Laurent Lafon, a saisi le président de l'Arcom du cas Russia Today afin de lui indiquer qu'il lui semblait « *urgent de nous interroger sur la menace que (faisait) peser cet organe de communication gouvernemental russe sur nos valeurs démocratiques à l'aune de la situation nouvelle créée par le déclenchement des opérations militaires en Ukraine* ». Il interpellait en particulier le régulateur de l'audiovisuel sur le respect par la chaîne russe de sa convention. Toutefois, cette saisine a également mis en évidence l'absence de véritables moyens d'action pour mettre un terme à la diffusion de ce média plus largement sur Internet et à travers les applications et les réseaux sociaux.

Dès le 2 mars 2022, le Conseil de l'Union européenne a décidé de suspendre d'urgence les activités de diffusion de Sputnik et de RT/Russia Today (RT English, RT UK, RT Germany, RT France et RT Spanish) dans l'Union européenne ou en direction de l'Union européenne, jusqu'à ce que l'agression contre l'Ukraine prenne fin et jusqu'à ce que la Fédération de Russie et ses médias associés cessent de mener des actions de désinformation et de manipulation de l'information contre l'Union européenne et ses États membres.

Les dispositions du présent article visent à donner leur pleine efficacité aux décisions prises par le Conseil de l'Union européenne et à se prémunir contre les manœuvres de contournement. Elles ont été élaborées dans le cadre d'un dialogue avec le régulateur de la communication audiovisuelle et numérique afin de tenir compte des contraintes que connaissent les acteurs du secteur.

Dans son avis, le Conseil d'État a considéré que les dispositions prévues à cet article « *ne se heurtent à aucun obstacle d'ordre constitutionnel ou conventionnel, notamment au regard de la liberté d'expression et de communication* »[1].

Le rapporteur souscrit pleinement aux objectifs de cet article. Concernant le régime des sanctions prévu au paragraphe IV du nouvel article 11 de la loi du 21 juin 2004, il remarque qu'il devra être mis en œuvre selon les modalités de l'article 42-7 de la loi n° 86-1067 du 30 septembre 1986 qui prévoit une instruction préalable par un rapporteur nommé par le vice-président du Conseil d'État. Cette procédure qui respecte le principe du

[1] *Considérant n° 19 de l'avis du Conseil d'État n° 406991 du 27 avril 2023.*

contradictoire apportera les mêmes garanties que dans les autres cas où l'Arcom est fondée à envisager de sanctionner des auteurs de manquements.

Par ailleurs, le durcissement des sanctions en cas de réitération des manquements tant par les personnes fournissant des services d'hébergement ou d'édition de service de communication au public que par les fournisseurs d'accès à Internet (FAI) s'inscrit dans la pratique habituelle de l'Arcom de recourir à des sanctions croissantes lorsque la phase de dialogue n'a pu aboutir à faire évoluer des comportements. Pour le régulateur, le recours à la sanction ne doit constituer que l'ultime solution lorsque toutes les autres démarches ont échoué et la récidive dans les manquements est donc particulièrement sanctionnée puisqu'elle marque l'échec d'une approche privilégiant le dialogue et les engagements réciproques.

À noter que le montant des sanctions est plus élevé pour les personnes fournissant des services d'hébergement ou d'édition de service de communication au public que pour les FAI, ce qui s'explique par le fait que ces derniers n'interviennent qu'*ex post* afin de bloquer, à la demande du régulateur, la diffusion des sites incriminés alors que les personnes fournissant des services d'hébergement ou d'édition de service de communication au public sont supposées exercer une veille plus étroite sur les contenus dont ils concourent à la diffusion.

b) Trois amendements visant à compléter le dispositif de l'article 4

La commission spéciale a adopté trois amendements qui modifient et complètent le présent article.

1. Un élargissement des compétences de l'Arcom à l'égard de certains médias extra-européens

L'amendement **COM-95 rectifié** a vocation à donner à l'Arcom une compétence sur les services de télévision et les services de médias audiovisuels à la demande (SMAD) extra-communautaires diffusés en France ne relevant pas de la compétence d'un autre État membre de l'Union européenne (UE), de l'Espace économique européen (EEE) ou de la Convention européenne sur la télévision transfrontière (CETT), quel que soit le mode de diffusion ou de distribution. La modification de l'article 43-2 de la loi du 30 septembre 1986 vient asseoir la compétence de l'Arcom sur ces services, tant pour veiller à l'application des principes de la loi du 30 septembre 1986 (s'agissant notamment de l'ordre public, de la dignité humaine, de l'incitation à la haine) que pour assurer la pleine effectivité des nouvelles dispositions donnant compétence à l'Arcom en matière d'application des sanctions européennes (1° et 2° du I du présent article).

Cet amendement **COM-95 rectifié** donne ainsi compétence à l'Arcom pour :

– mettre en demeure les services visés de respecter les principes de la loi du 30 septembre 1986 et, en cas de non-respect de la mise en demeure,

transmettre les faits au rapporteur mentionné à l'article 42-7 de ladite loi afin qu'il engage une procédure de sanction ;

– et mettre en demeure un distributeur de services mettant à la disposition du public une offre de services de communication audiovisuelle de cesser la diffusion d'un service extra-communautaire distribué par un réseau n'utilisant pas des fréquences assignées par l'Autorité de régulation de la communication audiovisuelle et numérique, à l'instar de ce que l'Arcom peut faire en matière de diffusion par satellite.

Contrairement aux services diffusés par un distributeur ou un opérateur de réseaux satellitaires, l'Arcom ne dispose pas de moyens d'action dans la loi du 30 septembre 1986 permettant d'obtenir la cessation de la diffusion d'une chaîne diffusée en Over-the-top service (OTT)[1]. Les articles 42, 42-1 et 42-10 ne s'appliquent pas aux fournisseurs d'accès Internet (FAI) pourtant en mesure de mettre fin à la diffusion des contenus visés. C'est pourquoi l'amendement **COM-95 rectifié** prévoit de modifier les articles 42 et 42-10 de la loi du 30 septembre 1986 afin de faire entrer les services extra-communautaires pour lesquels l'Arcom serait compétente dans le champ du I et II de l'article 33-1 de la loi du 30 septembre 1986 (pour les services de télévision) et de l'article 33-3 (pour les SMAD) relatifs au conventionnement ou à la déclaration des services.

Cet amendement prévoit également d'ajouter ces services de télévision extra-communautaires dans la dérogation prévue au III de l'article 33-1 de la loi du 30 septembre 1986 afin de leur appliquer le même régime qu'aux services extra-communautaires diffusés par satellite, et de prévoir la même dérogation pour les SMAD extra-communautaires à l'article 33-3 de la même loi. Enfin, il prévoit une modification de l'article 43-7 relatif aux obligations de contribution à la production des services de télévisions et des SMAD qui ne sont pas établis en France, qui ne relèvent pas de la compétence de la France et qui visent le territoire français, afin d'éviter que la modification de l'article 43-2 ait une incidence sur l'application de l'article 43-7.

2. Deux amendements de précision concernant la mise en œuvre de l'article

Alors que l'alinéa 7 prévoit que les fournisseurs d'accès à Internet devront sans délai empêcher l'accès aux sites dont l'Arcom leur aura signalé les adresses, **l'amendement COM-96 confie à l'Arcom le soin de déterminer le délai au terme duquel les FAI devront nécessairement avoir coupé l'accès à ces sites**. Il apparaît, en effet, difficile d'exiger des FAI qu'ils soient en mesure de neutraliser l'accès à des sites « sans délai » notamment à certains moments de la journée ou de la semaine. *A contrario*, il n'apparaît

[1] *Un service par contournement (en anglais over-the-top service ou OTT) est un service de communication ou de livraison de média sans la participation d'un opérateur de réseau traditionnel fournissant la connexion à Internet.*

pas judicieux de fixer dans la loi un délai trop long qui pourrait être mis à profit dans le cadre d'opérations d'ingérence.

Par ailleurs, **l'amendement COM-97 complète le présent article par un paragraphe V qui prévoit que les conditions d'application du présent article seront précisées par un décret en Conseil d'État**. Il reviendra à ce décret de préciser les modalités opérationnelles de mise en œuvre des dispositions prévues au présent article concernant par exemple les modalités d'un éventuel déblocage des sites concernés.

3. La nécessité de prévoir des modalités de prise en charge des coûts engagés par les FAI

Le rapporteur remarque par ailleurs que **le présent article ne prévoit pas les modalités de prise en charge des coûts engagés par les FAI pour assurer un blocage des sites dans un délai très réduit**.

Le rapporteur rappelle à cet égard que l'article 3 de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique a prévu concernant la prise en charge des coûts induits par la lutte contre le piratage des droits sportifs de renvoyer à un accord conclu entre les parties sous l'égide de l'Arcom. Il revient en particulier à cet accord de préciser « *les mesures qu'elles s'engagent à prendre pour faire cesser d'éventuelles violations de l'exclusivité du droit d'exploitation audiovisuelle de la manifestation ou compétition sportive et la répartition du coût des mesures ordonnées (…)* ». Si le recours à ce type d'accord n'est pas envisageable dans le cas présent, **la question de la prise en charge demeure un sujet de préoccupation légitime des acteurs concernés que le rapporteur souhaite mentionner.**

La commission spéciale a adopté les amendements **COM-95 rectifié**, **COM-96** et **COM-97**.

La commission spéciale a adopté l'article 4 **ainsi modifié**.

Article 5

Création d'une peine complémentaire de blocage d'un compte d'accès aux plateformes en ligne

L'article 5 vise à créer une peine complémentaire de blocage du compte d'accès aux plateformes en ligne d'une personne condamnée lorsque ce compte a été utilisé pour la commission de plusieurs délits (harcèlement sexuel, par conjoint ou scolaire ; certains délits portant atteinte à l'ordre public ou à l'intégrité de la personne ; délits de presse graves…) et à sanctionner d'une amende le non-respect, par les plateformes, de cette condamnation.

La commission spéciale a adopté cet article en y apportant des modifications substantielles, visant à la fois à renforcer la portée de la peine complémentaire ainsi instituée (*via*, notamment, un élargissement de son champ matériel d'application à de nouveaux délits) et à permettre l'application du « bannissement » dans le cadre de l'exécution des peines et des alternatives aux poursuites.

1. Le régime des peines complémentaires dans le droit en vigueur

S'ajoutant à une peine principale d'amende ou d'emprisonnement, les peines complémentaires ont vocation, par leur diversité, à contribuer à l'individualisation des peines par le juge pénal.

Principales peines complémentaires prévues par le code pénal en matière délictuelle

Le code pénal, dans sa rédaction actuelle, prévoit les peines complémentaires suivantes en cas de commission d'un délit :

– retrait des droits civiques, civils et familiaux. Ce retrait entraîne notamment l'inéligibilité, la perte du droit de vote et du droit d'être tuteur ;

– retrait de l'autorité parentale ;

– interdiction d'émettre des chèques ;

– suspension du permis de conduire, voire retrait définitif du permis avec interdiction de le repasser pendant un maximum de cinq ans ;

– interdiction de détenir une arme ;

– interdiction de détenir un animal (l'interdiction pouvant se limiter aux chiens dits « dangereux ») ;

– pour les étrangers, interdiction du territoire français ;

– interdiction de séjour (c'est-à-dire de paraître en certains lieux), interdiction de participer à des manifestations sur la voie publique ;

– confiscation d'un animal ou d'un bien ;

– suivi socio-judiciaire ;

– stage de sensibilisation aux drogues, à la sécurité routière, stage de citoyenneté, stage de responsabilisation sur les violences conjugales et sexistes ;

– interdiction d'exercer certaines professions (interdiction d'exercer une certaine profession si l'infraction a été commise dans ce cadre ; interdiction de travailler avec des mineurs, en cas d'infraction sexuelle ; fermeture d'un commerce ou d'une entreprise ; interdiction de gérer une entreprise) ;

– exclusion des marchés publics ;

– affichage de la décision ou diffusion de celle-ci dans certains médias.

On peut, schématiquement, utiliser deux typologies pour établir une catégorisation juridique des peines complémentaires :

– il est tout d'abord possible d'opérer une distinction fondée sur le **caractère obligatoire ou facultatif de la peine complémentaire** : pour les premières, la loi impose au juge, sauf dispense prononcée par celui-ci, d'en assortir la peine principale (à l'instar de l'inéligibilité en cas de condamnation pour un crime ou pour l'un des délits visés à l'article 131-26-2 du code pénal) ; quant aux secondes, elles **constituent une simple faculté à la disposition du juge, qui peut choisir ou non d'y recourir, et doivent être spécialement et expressément prévues pour chaque infraction pour laquelle elles sont encourues** ;

– on peut ensuite les distinguer par **nature** ; la doctrine s'accorde en général pour distinguer les peines complémentaires atteignant une **liberté** (celle d'aller et venir pour l'interdiction du territoire, par exemple) de celles qui atteignent un **droit** (à l'instar du droit de vote pour une privation des droits civiques), de celles qui touchent au **patrimoine** du condamné (c'est-à-dire les confiscations) ou sa **réputation** (l'affichage).

Or, en dépit de leur diversité, les peines complémentaires existantes ne concernent pas le domaine numérique : **si le juge peut prononcer à l'encontre d'un condamné l'interdiction de paraître en certains lieux ou de participer à certaines manifestations publiques, il ne peut pas lui interdire d'accéder à l'espace numérique**[1].

Les communications en ligne sont, à l'inverse, déjà couvertes par certaines modalités d'exécution des peines. Elles sont en effet incluses dans le périmètre des **interdictions d'entrer en relation avec la victime ou avec la partie civile :**

– à l'issue de la peine : ces interdictions, telles qu'elles résultent de l'article 712-16-2 du code de procédure pénale, sont facultatives dans la plupart des cas mais obligatoires pour certains délits – et notamment pour des délits susceptibles d'être commis en ligne (proposition sexuelle faite par un majeur à un mineur de quinze ans[2] ou à une personne se présentant comme telle en utilisant un moyen de communication électronique, pour pédopornographie ; fabrication ou diffusion d'un message pornographique ou violent susceptible d'être vu ou perçu par un mineur ; incitation à commettre un crime ou un délit à l'encontre d'un mineur…) ;

---

[1] *Dans le champ extra-juridique, l'étude d'impact relève que la suspension ou la suppression des comptes d'accès aux plateformes en ligne est prévue par lesdites plateformes en cas de violation de leurs conditions générales d'utilisation (CGU) qui, pour certaines, rejoignent des crimes ou des délits (menaces de violences ou incitations à la violence ; individus, organisations ou réseaux engagés dans des actes de violence « hors ligne » ; contenus tendant à la vente, l'achat ou la commercialisation d'armes ; fraude et tromperie ; exploitation sexuelle des enfants et des majeurs ; harcèlement et intimidation ; atteintes à la vie privée ; discours « haineux »…).*

[2] *Soit une personne âgée de moins de quinze ans.*

– **à la place de l'emprisonnement, ou en même temps que celui-ci** : l'interdiction de contact est, dans ce cas, encourue pour toute condamnation pour un délit puni d'une peine d'emprisonnement (14° de l'article 131-6 du code pénal).

2. La création d'une nouvelle peine complémentaire de blocage du compte d'accès aux plateformes en ligne

L'article 5 du projet de loi crée une peine complémentaire de suspension du compte d'accès à un service de plateforme en ligne : il s'agit donc, dans l'intention, de la **traduction en droit pénal d'une sanction de « bannissement » des réseaux sociaux.**

Aux termes du II de l'article 5, cette nouvelle peine serait applicable dès lors que le compte concerné aura été utilisé pour commettre l'un des délits suivants (qui correspondent, majoritairement mais non exclusivement, aux infractions visées par la loi pour la confiance dans l'économie numérique (LCEN) de 2004) :

– les **délits de harcèlement** prévus aux articles 222-33 (harcèlement sexuel), 222-33-2-1 (harcèlement du conjoint, partenaire de pacte civil de solidarité ou concubin), 222-33-2-2 (harcèlement moral), 222-33-2-3 (harcèlement scolaire) et au deuxième alinéa de l'article 222-33-3 (diffusion de l'enregistrement d'images relatives à la commission d'une atteinte volontaire à l'intégrité de la personne) du code pénal ;

– les délits prévus aux articles 225-4-13 (pratiques visant à modifier ou réprimer l'orientation sexuelle ou l'identité de genre d'une personne), 225-5 et 225-6 (**proxénétisme** et infractions assimilées), 227-23 (diffusion, offre, cession d'images **pédopornographiques**), 227-24 (fabrication, transport, diffusion de **message violent, pornographique ou contraire à la dignité**, lorsqu'il est susceptible d'être vu ou perçu par un mineur) et 421-2-5 du code pénal (**provocation et apologie du terrorisme**) ;

– certains **délits de presse graves**, à savoir ceux prévus aux cinquième, septième et huitième alinéas de l'article 24 (**apologie publique des crimes de guerre, des crimes contre l'humanité**, des crimes de réduction en esclavage ou des crimes et délits de collaboration avec l'ennemi ; **provocation à la discrimination, à la haine ou à la violence** à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée ; **provocation à la haine, aux discrimination ou à la violence** à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap) et à l'article 24 *bis* (**négationnisme**) de la loi du 29 juillet 1881 sur la liberté de la presse.

Cette sanction prendrait la forme d'une peine complémentaire **facultative**, d'une durée maximale de **six mois** (portée à un an en cas de récidive légale).

La condamnation serait transmise au fournisseur du service de plateforme concerné, à charge pour lui de bloquer le compte pendant toute la durée de la peine ; il encourrait à défaut une amende de 75 000 euros.

Le fournisseur serait également tenu de « *[mettre] en œuvre des mesures* » permettant d'éviter l'utilisation par la personne condamnée d'autres comptes (préexistants ou nouveaux), sans que cette obligation soit assortie d'une sanction et sans que la nature des « *mesures* » concernées soit précisée.

3. La position de la commission spéciale : étendre la portée du « bannissement » pour renforcer la protection accordée aux victimes

Sans l'estimer complétement platonique, la commission spéciale n'a pu qu'observer que la nouvelle peine complémentaire aurait un **impact essentiellement symbolique sur les condamnés comme sur les victimes**. Cette analyse est cohérente avec la vocation principale du « bannissement » tel qu'il a été imaginé par le Gouvernement : selon les informations recueillies par le rapporteur Loïc Hervé lors de ses auditions, la peine complémentaire a été, à titre principal, conçue pour toucher les condamnés disposant d'une large audience en ligne et qui font usage de leur notoriété pour assurer une vaste diffusion à des messages délictuels[1], et non pour s'appliquer de manière générale à la délinquance en ligne.

Tout en soutenant l'esprit de cette innovation, puisque la peine complémentaire de blocage du compte pourra concourir à sécuriser l'espace numérique pour les citoyens et à éviter qu'y soient commises des infractions graves, **la commission spéciale a estimé possible de renforcer la portée du « bannissement » en réévaluant son périmètre technique, son champ matériel et sa nature.**

[1] *Cette analyse est corroborée par l'étude d'impact, aux termes de laquelle* « cette peine complémentaire de suspension de compte dissuade les utilisateurs dont les comptes ont déjà été suspendus [de] récidiver et également d'autres utilisateurs qui pourraient être tentés de se livrer à des comportements similaires », *reconnaissant l'impact essentiellement dissuasif de la mesure.*

a) Sur le périmètre technique de la peine complémentaire

La commission spéciale a constaté que la nouvelle peine complémentaire de « bannissement » aurait une portée limitée, **générant un doute sérieux sur l'effectivité de la mesure comme sur la réalité de la protection accordée aux victimes**[1].

Ce constat résulte de plusieurs facteurs.

En premier lieu, la nouvelle peine sera centrée sur le compte utilisé pour commettre l'infraction. **Il restera donc loisible à la personne condamnée de disposer librement des comptes dont elle disposerait (ou qu'elle créerait) sur d'autres plateformes.** Plus encore, la rédaction proposée ne semble pas autoriser la juridiction pénale à étendre le « bannissement » à plusieurs plateformes – y compris dans l'hypothèse, plausible, dans laquelle l'infraction aura été commise en recourant à plusieurs réseaux sociaux ou services en ligne.

En deuxième lieu, l'article 5 ne prévoit de sanctionner les plateformes qu'en cas de défaut de blocage du compte ayant permis la commission de l'infraction, **et non pour les autres comptes (existants ou nouveaux) détenus sur la même plateforme par la personne condamnée**. Cette lacune avait déjà suscité des interrogations de la part du Conseil d'État qui, dans son avis sur le projet de loi, « *sugg[érait au Gouvernement] de ne pas retenir la disposition qui prévoit que le fournisseur du service de plateforme en ligne qui procède au blocage du compte d'accès suspendu met par ailleurs en œuvre des mesures permettant de procéder au blocage des autres comptes d'accès à son service éventuellement détenu par la personne condamnée et d'empêcher la création par celle-ci de nouveaux comptes* », au motif que « *cette obligation présentée comme une obligation de moyens et qui n'est pas pénalement réprimée ne trouve pas sa place dans le code pénal* » (point 23).

En troisième lieu, la peine complémentaire proposée est limitée aux « services de plateforme en ligne ». Or ceux-ci sont définis par le règlement sur les services numériques (RSN) (article 3) comme des « *service[s] d'hébergement qui, à la demande d'un destinataire du service, stocke[nt] et diffuse[nt] au public des informations* », étant rappelé qu'un service d'hébergement est défini comme un service « *consistant à stocker des informations fournies par un destinataire du service à sa demande* ». **Cette caractérisation touche les principaux réseaux sociaux et places de marché mais exclut**, comme l'a relevé la direction des affaires criminelles et des grâces lors de son audition par le rapporteur, **les sites qui ne stockent pas les contenus**. Si, à ce jour, la plupart des plateformes de réseaux sociaux

[1] *L'étude d'impact rappelle, à ce titre, qu'*« il reste relativement aisé pour les détenteurs de comptes supprimés de recréer un compte en utilisant d'autres informations : les auteurs de haine en ligne ou cyber-harcèlement continuent donc d'agir, rendant inopérantes les mesures mises en place par les plateformes » *: ce constat, pleinement valable, n'est pas limité aux fournisseurs privés et risque d'être (au moins partiellement) applicable à la nouvelle peine complémentaire de suspension du compte d'accès.*

ou de partage de vidéos remplissent cette condition, ce critère est susceptible à terme d'exclure des plateformes reposant sur un principe exclusif de diffusion instantanée de contenus.

De même, le rapporteur observe que la notion de « diffusion au public » au sens du RSN s'étend du « *fait de mettre des informations à la disposition d'un nombre potentiellement illimité de tiers, à la demande du destinataire du service ayant fourni ces informations* », ce qui paraît de nature à **empêcher l'application de la peine complémentaire à des services reposant sur une sélection préalable des membres** (par le biais d'un « parrainage » ou de tout autre système de validation) plutôt que sur l'inscription libre.

Limitée dans ses effets pour les personnes physiques, la peine complémentaire pourrait, à l'inverse, ouvrir de larges possibilités aux plateformes en ligne. En effet, au cours d'une table ronde réunissant les régulateurs (Arcom, Arcep et Cnil) et organisée le 13 juin 2023, la présidente de la Cnil, Marie-Laure Denis, a relevé que **l'obligation de moyens imposée aux plateformes pour la gestion des comptes « tiers » du condamné risquait de se traduire par une collecte disproportionnée des données personnelles des utilisateurs**[1] . Cette position est au demeurant cohérente avec la délibération de la Cnil sur le projet de loi, celle-ci ayant souligné que « *les traitements qui seront mis en œuvre par les plateformes en ligne aux fins de blocage ou visant à empêcher une personne d'en créer de nouveaux devront respecter les principes et le droit de la protection des données à caractère personnel* ».

Pour répondre à ces difficultés, la commission spéciale a, à l'initiative de son rapporteur, adopté l'amendement **COM-98** tendant à :

– prévoir que la peine complémentaire conduira au blocage des comptes utilisés pour commettre l'infraction, y compris sur plusieurs services en ligne ;

– clarifier la portée de la peine complémentaire en y **intégrant, de manière explicite, les services de réseaux sociaux en ligne et les services de plateforme de partage de vidéo** au sens du règlement 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, afin de prendre en compte l'ensemble des services de plateforme quelles que soient leurs modalités de fonctionnement technique ;

---

[1] *Marie-Laure Denis a ainsi déclaré :* « Je vous fais part de mes interrogations sur les solutions concrètes qui pourraient être mises en œuvre, afin notamment d'empêcher la création de nouveaux comptes par la personne condamnée. […] Ces dispositions ne devraient pas conduire les réseaux sociaux à collecter des données supplémentaires, ou à mettre en œuvre des traitements intrusifs pour l'ensemble de leurs utilisateurs, alors que ces mesures ne concerneront qu'un nombre limité de ces derniers. En outre, je m'interroge sur la pertinence d'un blocage qui reposerait sur l'adresse IP, dans la mesure où il pourrait être facilement contourné, par exemple avec un VPN, et que cela porterait atteinte aux libertés de toutes les personnes vivant dans le foyer concerné. »

– rappeler que les mesures mises en place par les plateformes pour le blocage des comptes « tiers » des personnes condamnées devront s'inscrire dans le cadre protecteur de l'article 46 la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés », afin notamment **d'éviter la constitution par les plateformes d'un fichier des personnes condamnées** qui serait non seulement choquant dans son principe, mais aussi directement contraire au RGPD.

Le rapporteur n'a, en revanche, pas estimé conforme à la Constitution de prévoir que la peine complémentaire pourrait toucher les comptes existants sur des plateformes autres que celles auxquelles il a été fait recours pour commettre l'infraction ; le « bannissement » instauré en tant que modalité d'exécution de la peine ou dans le cadre des alternatives aux poursuites atteindra cependant un effet analogue (voir *infra*).

b) Sur le champ matériel de la peine complémentaire

En outre, **le champ matériel d'application de cette nouvelle peine complémentaire ne paraît pas couvrir l'ensemble des infractions susceptibles d'être commises par le biais d'une plateforme en ligne** ; elle omet d'ailleurs (logiquement, en l'absence d'adoption définitive de ce texte) de citer plusieurs délits visés, en tant qu'infractions contre lesquelles les acteurs du numérique doivent lutter au titre de la LCEN, par la récente proposition de loi visant à instaurer une majorité numérique et à lutter contre la haine en ligne[1].

Outre qu'il ne concerne pas les crimes, **le périmètre d'application de la peine exclut ainsi un certain nombre de délits pouvant relever de la cybercriminalité**, parmi lesquels :

– des **faits analogues au harcèlement**, cette infraction étant largement mais incomplètement couverte par le dispositif initial, et qui peuvent être commis au moins partiellement par le biais de plateformes, comme l'outrage sexiste et sexuel (article 222-33-1-1 du code pénal) ou le harcèlement au travail (article 222-33-2) ;

– de même, des **faits assimilables au proxénétisme**, comme la tenue d'un établissement de prostitution (article 225-10) dont la publicité peut être assurée en ligne, et des formes aggravées de proxénétisme (articles 225-7 et suivants) ;

– les **atteintes à la vie privée** (articles 226-1 et suivants), cette infraction étant notamment caractérisée par le fait de « *[fixer, enregistrer ou transmettre], sans le consentement de celle-ci, l'image d'une personne se*

[1] *Cette proposition de loi a fait l'objet d'un accord de la commission mixte paritaire chargée de proposer un texte sur celles de ses dispositions restant en discussion ; ses conclusions seront discutées en séance publique au Sénat le 29 juin prochain, ouvrant la voie à une promulgation rapide.*

trouvant dans un lieu privé » **et à la représentation de la personne** (article 226-8) ;

– la **violation d'une interdiction de contact** posée par une ordonnance de protection du juge aux affaires familiales (article 227-4-2) ;

– les **infractions qui consistent à rendre publiques des allégations infondées ou des informations secrètes ou confidentielles**, et qui peuvent par nature être commises sur les réseaux sociaux : diffusion malveillante d'informations personnelles sur une personne afin de l'exposer à un risque d'atteinte à son intégrité (article 223-1-1), dénonciation calomnieuse (article 226-10), détournement et/ou révélation de données à caractère personnel (articles 226-21 et 226-22), révélation d'informations mettant en danger les membres des services ou unités spécialisés (articles 413-13 et 14) ;

– les **faits de chantage** prévus aux articles 312-10 à 312-12 du code pénal ;

– **divers délits de provocation, là encore publics par nature** : provocation publique et directe à commettre un génocide (article 211-2), provocation au suicide (article 223-13), provocation d'un mineur à consommer ou vendre des stupéfiants, à consommer de l'alcool de manière excessive ou à commettre un crime ou un délit (articles 227-18 à 227-21), provocation à s'armer contre l'autorité de l'État (article 412-8), à l'attroupement armé (431-6) ;

– **des délits « voisins » de la pédopornographie** : favorisation de la corruption de mineurs, la corruption elle-même lorsqu'elle est commise ou tentée « *par un moyen de communication électronique* » (articles 227-22 à 227-22-2) ou la sollicitation par un majeur d'images pornographiques d'un mineur (article 227-23-1).

La commission spéciale a souhaité que ces délits soient intégrés au champ matériel de la nouvelle peine complémentaire de « bannissement » et a adopté, pour ce faire, l'amendement **COM-99 rectifié** du rapporteur.

Enfin, **face à la montée en fréquence et en intensité des violences contre les élus locaux, la commission spéciale a estimé nécessaire que ceux qui harcèlent, menacent ou intimident les représentants des collectivités territoriales ou qui entendent porter atteinte au fonctionnement normal de la démocratie soient, eux aussi, passibles de cette nouvelle sanction.** C'est ainsi qu'elle a, par le même amendement **COM-99 rectifié**, intégré au champ matériel de celle-ci l'entrave, par voie de menaces, à l'exercice des libertés publiques et aux débats des assemblées parlementaires ou des organes délibérants des collectivités (article 431-1), ainsi que les **menaces et actes d'intimidation commis contre les personnes exerçant une fonction publique** (articles 433-3 et 433-3-1).

Par cohérence avec ces évolutions, la commission spéciale a estimé nécessaire de **modifier la liste des infractions contre la diffusion desquelles les opérateurs du numérique doivent lutter** en application de l'article 6 de la LCEN, afin qu'y soient intégrés l'ensemble des délits précités. Ce choix se traduit par un amendement à l'article 22 du projet de loi (amendement **COM-134**, exposé ci-après).

c) Sur l'opportunité d'une extension de la nature du « bannissement »

Le projet de loi limite la nature du « bannissement » à celle d'une peine complémentaire. Cette situation soulève deux difficultés.

En premier lieu, le « bannissement » vise à interdire à une personne d'être présente sur un espace numérique public, celui du réseau social, où elle pourrait récidiver et/ou entrer en contact avec ses victimes. **Intellectuellement, il s'apparente donc à l'interdiction de paraître ou à l'interdiction d'entrer en relation avec la victime** ; or ces interdictions, qui ont fait la preuve de leur efficacité, constituent non pas des peines complémentaires, mais des **modalités d'exécution des peines**.

Deuxièmement, **le « bannissement » conçu comme une peine complémentaire sera vraisemblablement réservé aux condamnations les plus légères.** En effet, l'accès à Internet étant *de facto* impossible, si ce n'est légalement proscrit, en prison (ce qui rend la peine complémentaire de « bannissement » inopérante dans le cas d'une condamnation à une peine de prison ferme) et la durée maximale de la peine instituée par le projet de loi (six mois, ou un an en cas de récidive) n'étant pas susceptible en pratique de s'étendre au-delà d'un emprisonnement ferme[1], il est plausible que les magistrats ne prévoiront pas l'application de cette sanction en complément des condamnations les plus lourdes.

Le rapporteur considère que le blocage du compte d'accès à une plateforme est un levier essentiel pour protéger les victimes et prévenir la récidive, ainsi que pour sécuriser l'espace numérique en interdisant son accès aux personnes qui y ont commis des infractions. Sans remettre en cause l'intérêt du « bannissement » en tant que peine complémentaire, il estime donc nécessaire que cette sanction puisse s'appliquer non seulement en parallèle d'une peine principale, mais aussi **en l'absence de poursuites pour les cas les moins graves et à l'issue d'une peine d'emprisonnement dans les hypothèses les plus dramatiques.**

Ainsi conçu, le « bannissement » ne supposerait pas le blocage par une plateforme d'un ou plusieurs comptes d'accès, mais prendrait la forme d'une interdiction qui, si elle n'est pas respectée, expose le contrevenant à

[1] *L'aménagement des peines est obligatoire pour une peine d'emprisonnement inférieure à six mois, et possible (et très fréquent en pratique) pour les peines comprises entre six mois et un an : un juge qui condamnerait une personne à une peine d'emprisonnement effective, donc supérieure à un an, n'aurait donc aucun intérêt à prononcer en parallèle la peine complémentaire de « bannissement » telle qu'elle est proposée par le projet de loi.*

subir une sanction dont l'application avait précédemment été écartée, suspendue ou aménagée. En d'autres termes, **au même titre que pour une interdiction d'entrer en relation avec un tiers, la violation par un condamné d'une interdiction d'accéder à une plateforme pourrait se traduire par une incarcération ou une réincarcération.**

C'est dans cette optique que la commission spéciale a souhaité, sur l'impulsion de son rapporteur (amendement **COM-100**), que **le « bannissement » soit étendu :**

– aux alternatives aux poursuites, en prévoyant que le blocage des comptes d'accès à des plateformes pourra être proposé, avant la mise en mouvement de l'action publique et dans le cadre de la composition pénale de l'article 41-2 du code de procédure pénale, à une personne physique qui reconnaît avoir commis un ou plusieurs délits punis d'une peine d'emprisonnement maximale de cinq ans ;

– aux mesures susceptibles d'être prononcées à la place ou en même temps que l'emprisonnement dans le cadre défini par l'article 131-6 du code pénal, c'est-à-dire pour tous les délits passibles d'une peine d'emprisonnement ;

- aux obligations pouvant être imposées à un condamné par la juridiction de condamnation ou par le juge d'application des peines au titre de l'article 132-45 du code pénal. **Le « bannissement » serait ainsi rendu applicable à de nombreuses hypothèses, y compris après l'exécution d'une peine d'emprisonnement**, puisqu'il pourrait :

- **être décidé dans le cadre de la surveillance judiciaire** (article 723-30 du code de procédure pénale), c'est-à-dire **en cas de risque avéré de récidive**, à l'issue d'une peine privative de liberté d'une durée égale ou supérieure à sept ans (ou, en cas de récidive, à cinq ans)[1] ;
- s'appliquer **en cas de placement d'une personne détenue à l'extérieur ou en semi-liberté, ainsi que lors des permissions de sortie** (article 723-4 du code de procédure pénale) ;
- s'appliquer en cas de **sursis probatoire** (article 739) ;
- être décidé en cas de suspension ou de fractionnement d'une peine d'emprisonnement en matière correctionnelle (article 720-1), ainsi que de **libération sous contrainte ou conditionnelle** (article 721-2) ;
- être prévu dans le cadre d'un **suivi socio-judiciaire** (article 131-36-2 du code pénal).

[1] *L'article 723-25 du code de procédure pénale dispose que* « En cas d'inobservation par le condamné des obligations et interdictions qui lui ont été imposées, le juge de l'application des peines peut […] retirer tout ou partie de la durée des réductions de peine dont il a bénéficié et ordonner sa réincarcération ».

d) La création d'une infraction d'outrage en ligne

Les auditions conduites par le rapporteur et par la commission spéciale en formation plénière ont mis au jour les difficultés posées, en matière de harcèlement en ligne, par la réponse pénale « classique ». En effet, le cyber-harcèlement ne fait pas l'objet d'une définition autonome par le code pénal et se trouve couvert par les infractions existantes de harcèlement (qu'il s'agisse de harcèlement « simple », de harcèlement scolaire ou de harcèlement du conjoint) ; or il s'agit de faits graves, passibles d'une peine d'emprisonnement et qui supposent la tenue d'un procès et, en amont de celui-ci, la conduite d'une enquête, parfois longue, pour garantir le respect des droits de toutes les parties. La sanction pénale, indépendamment de la question du « bannissement », intervient ainsi plusieurs mois, voire plusieurs années après la commission des faits.

Face à ce constat, **certaines personnes auditionnées ont suggéré que le législateur mette en place un système inspiré de la « riposte graduée » applicable en matière de protection des droits d'auteur**, avec l'envoi d'un courrier aux cyber-harceleurs. Cette formule n'a pas semblé suffisante à la commission spéciale au vu de la nature des faits, *a fortiori* dans un contexte où la « riposte graduée » pratiquée par l'Arcom repose, légitimement, sur une procédure longue (deux courriers d'avertissement, suivis d'une réitération, avant transmission au procureur de la République en vue du prononcé d'une amende d'un montant maximal de 1 500 euros) qui ne répond qu'imparfaitement à l'objectif d'une sanction plus rapide des infracteurs.

D'autres ont proposé qu'il soit fait recours à l'amende forfaitaire délictuelle (AFD) pour réprimer plus rapidement le cyber-harcèlement, aujourd'hui traité *de jure* comme le harcèlement de la « vie réelle » et donc soumis à la voie juridictionnelle. Il n'a pas semblé envisageable au rapporteur de suivre cette proposition pour deux raisons principales : d'une part, l'AFD s'applique aujourd'hui à des faits relativement simples et « légers » (conduite sans assurance ou sans permis, usage de stupéfiants, filouterie de carburants, tags, intrusion dans un établissement scolaire, atteintes à la circulation des trains…), dont la gravité ne saurait être comparée à celle des délits existants en matière harcèlement ; d'autre part, elle emporte l'extinction de l'action pénale, c'est-à-dire qu'elle empêche l'engagement de poursuites par le parquet.

Le régime de l'amende forfaitaire délictuelle

Depuis 2016, la procédure de l'amende forfaitaire délictuelle a été intégrée au code de procédure pénale afin d'améliorer la réponse pénale pour certaines infractions. D'abord prévue pour certaines infractions routières, elle a été étendue à l'occupation illicite de terrains puis à certaines infractions de petite délinquance dont l'usage de stupéfiants. Elle a, plus récemment, été prévue par le législateur dans le cadre de la loi d'orientation et de programmation du ministère de l'intérieur du 24 janvier 2023 pour la répression des dégradations ou détériorations légères (tags) prévues et réprimées par les articles 322-1, 322-4 et 322-15 du code pénal, pour la filouterie de carburant prévue et réprimée à l'article 313-5 du code pénal, pour le délit d'entrave à la circulation prévu et réprimé à l'article L. 412-1 du code de la route, pour les atteintes à la circulation des trains, les intrusions non autorisées dans un établissement scolaire prévues et réprimées par l'article 431-22 du code pénal, ou encore pour la détention sans permis de chien d'attaque, ou de garde ou de défense malgré mise en demeure ou incapacité prévue et réprimée par l'article L. 215-2-1 du code rural. Elle s'applique également en cas d'outrage sexiste ou sexuel (communément appelé « harcèlement de rue ») aggravé (article 222-33-1-1 du code pénal).

Les AFD sont mises en œuvre directement par les policiers et gendarmes qui constatent l'infraction ; en pratique, leur application repose sur des modèles de procès-verbaux électroniques. Elles peuvent soit être payées par l'auteur (immédiatement ou dans un délai de quinze jours avec un montant minoré, et dans un délai maximal de 45 jours sans minoration) s'il reconnaît les faits, soit faire l'objet d'un titre exécutoire à montant majoré de plein droit.

Au plan pénal, elles excluent tout recours au juge et leur paiement éteint l'action publique. En revanche, la victime conserve la possibilité de se porter partie civile et d'obtenir réparation lors d'une audience à juge unique statuant sur les seuls intérêts civils.

L'application de l'amende forfaitaire délictuelle est exclue pour les mineurs ou si plusieurs infractions, dont l'une au moins ne peut donner lieu à une amende forfaitaire, ont été constatées simultanément. Sauf disposition contraire de la loi, elle n'est pas non plus applicable en état de récidive légale (article 495-17 du code de procédure pénale).

Source : commission des lois

Pour autant, cette piste de réflexion doit-être écartée ? Le rapporteur considère, à l'inverse, que **le recours à l'AFD en matière de cyber-harcèlement ne manque pas de pertinence.** Il a ainsi pu constater aux côtés de Marc-Philippe Daubresse, en tant que rapporteur du projet de loi d'orientation et de programmation du ministère de l'intérieur examiné par le Parlement en 2022-2023, que l'AFD était un outil efficace dont l'usage avait permis pour certaines infractions (et notamment la consommation de stupéfiants et l'occupation en réunion de halls d'immeuble) une nette amélioration du taux de réponse pénale. En l'espèce, **son application aux faits les plus « simples » de cyber-harcèlement permettrait de sanctionner les auteurs avant que le harcèlement ne s'inscrive dans la durée et de massifier la réponse pénale**, aujourd'hui inadaptée face à la fréquence des comportements déplacés subis en ligne par les citoyens, et en particulier par les plus jeunes.

Le rapporteur mènera, d'ici à la séance publique, des concertations visant à mettre au jour une solution opérationnelle permettant à la fois aux victimes de faire valoir leurs droits et aux agents chargés de la répression d'exercer cette nouvelle mission dans des conditions satisfaisantes.

La commission spéciale a adopté l'article 5 **ainsi modifié**.

Article 6

Déploiement d'un filtre national de cybersécurité grand public

L'article 6 vise à instaurer un « filtre national de cybersécurité grand public » afin de lutter contre les actes de cybermalveillance du quotidien.

La commission a adopté cet article, modifié par l'adoption de 11 amendements dont 10 amendements du rapporteur Patrick Chaize, afin de renforcer le caractère opérationnel du dispositif proposé, de rehausser le niveau de protection des citoyens en ligne et de responsabiliser l'ensemble des intermédiaires techniques et des opérateurs concernés.

1. Le droit en vigueur : une multitude de dispositifs de filtrage de contenus dont aucun ne vise spécifiquement les actes de cybermalveillance

a) Une co-existence de plusieurs dispositifs sectoriels de filtrage des contenus pouvant être ordonnés par voie judiciaire ou administrative

1. Un dispositif judiciaire de portée générale pour filtrer les contenus haineux sur Internet et ceux portant atteinte aux personnes

L'article 6 de la loi pour la confiance dans l'économie numérique (LCEN)[1] dispose que « *le président du tribunal judiciaire, statuant selon la procédure accélérée au fond, peut prescrire à toute personne susceptible d'y contribuer toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ».

En vertu de cet article, les fournisseurs d'accès à un service de communication au public en ligne et les hébergeurs de contenus concourent à la lutte contre la diffusion des contenus faisant :

[1] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

– l'apologie, la négation ou la banalisation des crimes contre l'humanité ;

– de la provocation à la commission d'actes de terrorisme et leur apologie ;

– de l'incitation à la haine raciale, à la haine à l'égard des personnes en raison de leur sexe, de leur orientation sexuelle, de leur identité de genre ou de leur handicap ;

– de la pornographie enfantine ;

– de l'incitation à la violence, notamment aux violences sexistes et sexuelles ;

– des atteintes à la dignité humaine.

2. *Un dispositif judiciaire spécifique de retrait des contenus pédopornographiques ou terroristes*

L'article 6-1 de la LCEN prévoit que l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), rattaché à la direction générale de la police nationale et gestionnaire des plateformes Pharos et Thesee, puisse demander aux éditeurs de contenus ou aux hébergeurs de retirer les contenus pédopornographiques ou terroristes.

En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'OCLCTIC transmet aux offreurs d'accès aux services de communication au public en ligne la liste des adresses électroniques dont l'accès doit être bloqué ou déréférencé sans délai.

Par exemple, pour l'année 2022, la plateforme Pharos a procédé aux demandes figurant dans le tableau ci-dessous[1].

	Retrait	Blocage	Déréférencement
Contenus pédopornographiques	73 925	343	3 201
Contenus terroristes	15 132	11	823

Afin d'éviter toute mesure qui serait disproportionnée, une personnalité qualifiée désignée au sein de l'autorité compétente vérifie le bien-fondé des demandes de retrait de contenus, de blocage et de déréférencement. Jusqu'au 7 juin 2022, cette personnalité qualifiée était membre de la Cnil. Depuis, il s'agit d'une personnalité qualifiée désignée par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), en l'occurrence Laurence Pécaut-Rivolier.

[1] *Contribution écrite transmise par la Direction générale des entreprises.*

S'agissant des seuls contenus à caractère terroriste, ce dispositif a été récemment enrichi. Le règlement européen relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne[1], adapté en droit national par la loi du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne[2], a été l'occasion d'introduire les articles 6-1-1 et suivants au sein de la LCEN, permettant à l'OCLCTIC de délivrer une injonction de retrait, dans un délai d'une heure, de certains contenus à caractère terroriste à l'encontre des fournisseurs de services d'hébergement au public en ligne. Les sanctions prévues sont d'un an d'emprisonnement et 250 000 euros d'amende, les injonctions de retrait étant susceptibles de recours devant le tribunal administratif.

3. Un dispositif judiciaire spécifique pour l'arrêt des services de communication au public en ligne diffusant des contenus terroristes

Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes par l'utilisation d'un service de communication au public en ligne est puni de sept ans d'emprisonnement et de 100 000 euros d'amende[3].

Dans ce cas, l'arrêt du service de communication en ligne concerné peut être prononcé par le juge des référés, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir[4].

4. Un dispositif judiciaire spécifique pour retirer les activités en ligne de nature à altérer la sincérité des scrutins

Le juge des référés peut également, dans un délai de quarante-huit heures à compter de sa saisine, prescrire « *toutes mesures proportionnées et nécessaires* »[5] pour faire cesser la diffusion d'allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir, diffusées de manière délibérée, artificielle ou automatisée ou massive par le biais d'un service de communication au public en ligne.

5. Un dispositif judiciaire de portée générale pour filtrer les contenus portant atteinte aux droits d'auteur et aux droits voisin

L'article L. 336-2 du code de la propriété intellectuelle prévoit un dispositif similaire de filtrage des contenus par voie judiciaire lorsque le contenu d'un service de communication au public en ligne porte atteinte à un droit d'auteur ou à un droit voisin, le président du tribunal judiciaire

---

[1] *Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.*
[2] *Loi n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne.*
[3] *Article L. 421-2-5 du code pénal.*
[4] *Article 706-23 du code de procédure pénale.*
[5] *Article L. 163-2 du code électoral.*

pouvant ordonner, selon la procédure accélérée au fond, toutes mesures propres à prévenir ou à faire cesser une telle atteinte.

Cette procédure peut, par exemple, être utilisée par des organismes de défense professionnelle pour qu'il soit fait injonction aux fournisseurs d'accès à Internet (FAI), mais aussi aux fournisseurs de moteurs de recherche, afin qu'ils prennent les mesures de blocage et de déréférencement de sites offrant aux internautes la possibilité d'accéder à des contenus contrefaisants, en flux continu *(streaming)* ou en téléchargement.

6. Un dispositif administratif de filtrage des pratiques commerciales déloyales, trompeuses ou agressives en ligne

Lorsqu'ils constatent des pratiques commerciales déloyales, trompeuses ou agressives, ou des manquements à la conformité et à la sécurité de produits vendus en ligne, et lorsque l'auteur de ces pratiques ne peut être identifié ou qu'il n'a pas déféré à une injonction de mise en conformité, les agents habilités de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) peuvent, dans un délai d'au moins quarante-huit heures :

– ordonner aux opérateurs de plateforme en ligne d'afficher un message avertissant les consommateurs du risque de préjudice encouru lorsqu'ils accèdent au contenu manifestement illicite ;

– ordonner aux opérateurs de plateforme en ligne ou aux hébergeurs de contenus, pour les infractions les plus graves passibles d'une peine d'au moins deux ans d'emprisonnement, le déréférencement ou la limitation de l'accès aux adresses électroniques des interfaces en ligne dont les contenus sont manifestement illicites, ou le blocage d'un nom de domaine[1].

Ce dispositif a, par exemple, été récemment utilisé pour déréférencer la plateforme Wish à la suite du signalement de la présence, sur cette plateforme, de produits non conformes voire dangereux pour les consommateurs.

b) Une absence de dispositif national de filtrage dédié aux actes de cybermalveillance

1. Un « vide juridique national » dans un contexte de hausse des actes quotidiens de cybermalveillance

Comme le souligne l'étude d'impact du présent projet de loi, la création d'un filtre national de cybersécurité grand public « *s'appuie sur le constat selon lequel* ***il n'existe pas de précédent identifiable en droit français permettant de répondre à la préoccupation de lutter préventivement contre les actes de cybermalveillance*** *visés par le dispositif et de façon aussi rapide et efficace que les modes opératoires standardisés, évolutifs et extrêmement réactifs des cybercriminels* ».

[1] *Article L. 521-3-1 du code de la consommation.*

Or, selon son dernier rapport d'activité, la fréquentation de la plateforme *Cybermalveillance.gouv.fr*, opérée par le groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma), est en hausse avec 3,8 millions de visiteurs en 2022 et plus de 280 000 parcours d'assistance, **la cybermalveillance désignant toute infraction commise par voie numérique. Cette plateforme en recense 48 formes différentes, les plus fréquentes étant** :

– l'hameçonnage *(phishing)* – plus de 100 000 demandes d'assistance en ligne en 2022 – qui consiste à l'envoi de courriel ou de SMS en usurpant l'identité d'un tiers pour l'inciter, par exemple, à communiquer ses données personnelles, professionnelles ou bancaires : faux messages d'infraction, sollicitations concernant le compte personnel de formation (CPF), messages d'escroquerie à la livraison de colis, *etc.* ;

– le piratage de compte en ligne – plus de 20 000 demandes d'assistance en ligne en 2022 – **e**n particulier les comptes de messagerie et les comptes des réseaux sociaux ;

– les arnaques aux faux supports techniques ou fraudes à la réparation informatique afin d'inciter les utilisateurs à payer de faux dépannages ;

– le cyberharcèlement, c'est-à-dire le fait de tenir en ligne, de manière répétée et intentionnelle, des propos ou des comportements ayant pour but ou conséquence une dégradation des conditions de vie de la personne qui en est victime ;

– la violation de données personnelles ;

– les attaques par rançongiciel *(ransomware)* – près de 2 500 demandes d'assistance en ligne en 2022 – qui constituent la première cybermenace pour les entreprises, et qui consistent à bloquer l'accès à un appareil ou à des fichiers et à réclamer le paiement d'une rançon pour en obtenir de nouveau l'accès ;

– les spams électroniques ou téléphoniques, qui sont des communications non sollicitées à des fins publicitaires, commerciales ou malveillantes ;

– les attaques en déni de service, afin de rendre inaccessible un serveur, à provoquer une panne ou un fonctionnement dégradé ;

– les faux ordres de virement ;

– les virus.

2. Des expériences étrangères qui justifient d'autant plus de compléter notre arsenal législatif national

Si la France ne dispose pas encore d'un dispositif national de filtrage des actes de cybermalveillance à destination du grand public, il existe pourtant **une panoplie de diverses solutions techniques dont certaines ont déjà été mises en œuvre dans d'autres pays**. Le tableau ci-dessous, issu de

l'étude d'impact du projet de loi, synthétise les principales solutions en vigueur à l'étranger.

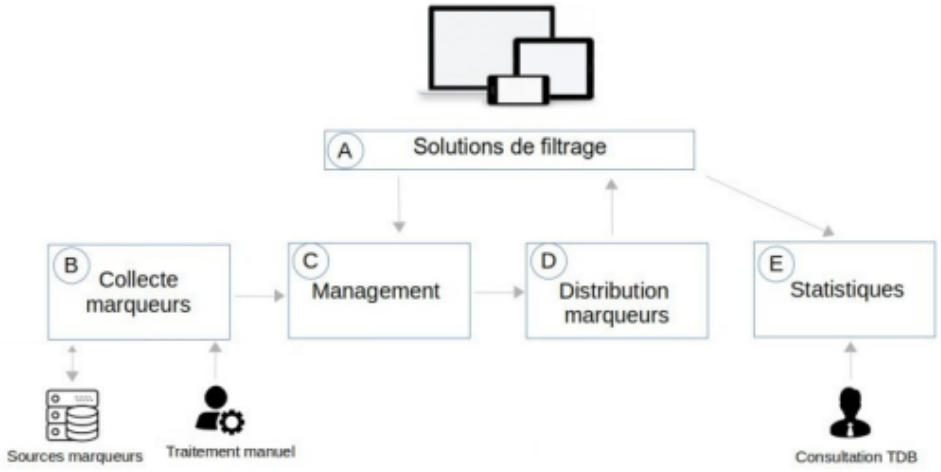
Dispositif	Périmètre	Solutions techniques
Bouclier anti-hameçonnage *(phishing)* (Belgique)	Cybercriminalité, cyber-arnaques, logiciels malveillants *(malware)*	Service informatique distribué de gestion des noms de domaine (DNS) activé par défaut par les fournisseurs d'accès à Internet (FAI) Redirige le site malveillant vers une page d'avertissement hébergée par le Centre pour la Cybersécurité Belge
Canadian Shield (Canada)	Logiciels malveillants, hameçonnage, réseaux zombies *(botnet)*, cyber-arnaques	DNS récursif filtrant les noms de domaine Configuration manuelle du DNS nécessaire
Quad9 (Suisse)	Logiciels malveillants, hameçonnage, réseaux zombies, cyber-arnaques, fraudes financières	DNS récursif filtrant les noms de domaine Configuration manuelle du DNS nécessaire
Protective DNS (États-Unis)	Logiciels malveillants, serveurs de commande et contrôle (C&C)	DNS récursif filtrant les noms de domaine
Protective DNS (Royaume-Uni)	Logiciels malveillants, serveurs de commande et contrôle (C&C)	DNS récursif filtrant les noms de domaine Support dédié *Dashboard* pour l'organisme Existence d'un *plugin* Windows 10
Servicio anti botnet (Espagne)	Réseaux zombies	Scan sur le terminal Extension du navigateur et sur application mobile

2. Le dispositif proposé : le déploiement progressif d'un nouveau dispositif de filtrage dédié aux actes courants de cybermalveillance

a) La désignation d'un opérateur technique pour garantir la mise en œuvre opérationnelle de ce dispositif

Le GIP Acyma s'est proposé pour être l'opérateur technique de ce futur dispositif, en particulier pour permettre aux différentes autorités administratives pressenties d'envoyer aux fournisseurs d'accès à Internet et aux fournisseurs de navigateurs sur Internet les noms de domaines à filtrer.

Selon l'étude d'impact du projet de loi, les autorités administratives pressenties pour constater les infractions sont notamment la DGCCRF, l'Autorité de contrôle prudentiel et de résolution (ACPR), l'Autorité des marchés financiers (AMF), la sous-direction de la lutte contre la cybercriminalité de la police nationale, le commandement de la gendarmerie dans le cyberespace (COMCyberGend) et l'Agence nationale de la sécurité de systèmes d'information (Anssi).



A : solutions de filtrage mises en place par les fournisseurs d'accès Internet et les éditeurs de navigateurs

B : autorités administratives

C : GIP ACYMA

D : GIP ACYMA

E: GIP ACYMA

Source : GIP Acyma

Selon les premières estimations réalisées par le GIP Acyma, **le coût fixe du développement de ce dispositif serait de 1 115 000 euros**, sans inclure les frais de maintenance pour les années à venir.

b) La mise en œuvre d'un dispositif national de cybersécurité pour lutter contre des infractions bien identifiées et de plus en plus courantes

L'article 6 de ce projet de loi réécrit l'article 12 de la LCEN et instaure un dispositif national de cybersécurité grand public ciblant des actes de cybermalveillance bien identifiés et correspondant aux infractions suivantes :

– l'usurpation d'identité, c'est-à-dire « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* »[1] ;

– la collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite[2] ;

– l'accès frauduleux à un système de traitement automatisé de données, y compris s'il en résulte la suppression ou la modification des données contenues dans le système[3] ;

– l'usage frauduleux de moyens de paiement, c'est-à-dire **«** *le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés* »[4] pour :

- contrefaire ou falsifier un chèque ou un autre instrument de paiement ;
- faire ou tenter de faire usage, en connaissance de cause, d'un chèque ou d'un autre instrument de paiement contrefait ou falsifié ;
- accepter, en connaissance de cause, de recevoir un paiement au moyen d'un chèque ou d'un autre instrument de paiement contrefait ou falsifié.

c) Dans un premier temps, l'affichage par les fournisseurs de navigateurs à Internet d'un message d'alerte pendant sept jours

Lorsque l'une des infractions mentionnées ci-dessus est constatée, **l'autorité administrative notifie aux fournisseurs de navigateurs sur Internet** (Google Chrome, Apple Safari, Mozilla Firefox, Microsoft Edge, Samsung Internet, Yahoo, Bing, Qwant, *etc.*) l'adresse de l'éditeur du service

---

[1] *Article L. 226-4-1 du code pénal.*
[2] *Article L. 226-18 du code pénal.*
[3] *Article L. 323-1 du code pénal.*
[4] *Article L. 163-4 du code monétaire et financier.*

de communication au public en ligne en cause afin de prendre sans délai, à titre conservatoire et pendant sept jours « ***toute mesure utile consistant à afficher un message avertissant l'utilisateur du risque de préjudice encouru en cas d'accès à cette adresse*** ».

Simultanément, l'éditeur du service de communication au public en ligne en cause dispose de **cinq jours pour adresser ses observations** à l'autorité administrative.

Si le constat de l'infraction n'est plus valable, l'autorité administrative demande en conséquence aux fournisseurs de navigateurs sur Internet de mettre fin aux mesures conservatoires préalablement mises en place.

d) Dans un deuxième temps, à l'issue d'une procédure de contradictoire, le blocage de l'accès au service en cause par les fournisseurs de navigateurs sur Internet, d'accès à Internet et de systèmes de résolution de nom de domaine

Si le constat de l'infraction est toujours valable, si l'éditeur en cause n'a pas transmis ses observations dans le délai imparti ou s'il n'a pas mis à disposition les informations nécessaires pour le contacter, alors **l'autorité administrative peut demander aux fournisseurs de navigateurs sur Internet, d'accès à Internet (FAI) (Orange, SFR, Bouygues Télécom, Free, *etc.*) ou de systèmes de résolution de nom de domaine (DNS) (Cloudflare, Quad9, NextDNS, CleanBrowsing, *etc.*)** de prendre, pour une durée maximale de trois mois, « ***toute mesure utile destinée à empêcher l'accès à l'adresse de ce service, et d'afficher un message avertissant les utilisateurs du risque de préjudice encouru lorsqu'ils tentent d'y accéder*** ».

Cette mesure peut être prolongée pour une durée de six mois, renouvelable une fois pour la même durée, sur avis conforme de la personnalité qualifiée au sein de la Commission nationale pour l'informatique et les libertés (Cnil). Toutefois, si le constat de l'infraction n'est plus valable, l'autorité administrative peut, à tout instant, demander la fin des mesures de blocage.

e) Un mécanisme de garantie du caractère justifié et proportionné des mesures prises, sous l'égide de la Commission nationale pour l'informatique et les libertés

Au regard des différents dispositifs nationaux et existants de filtrage des contenus, le dispositif proposé par l'article 6 de ce projet de loi s'inspire et se rapproche du dispositif de la DGCCRF actuellement en vigueur pour les pratiques commerciales déloyales, trompeuses ou agressives en ligne.

Toutefois, **des précautions supplémentaires sont prises afin de ne pas porter une atteinte disproportionnée ou injustifiée à la liberté d'expression et à la liberté de communication**. C'est pourquoi une **personnalité qualifiée au sein de la Cnil** est chargée de s'assurer

« *du* ***caractère justifié des mesures*** *et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste des adresses électroniques concernées* ».

Par conséquent, cette personnalité peut, à tout moment, « *enjoindre à l'autorité administrative de mettre fin aux mesures qu'elle a prises* ».

Par ailleurs, les éditeurs des services de communication au public en ligne en cause peuvent saisir d'un recours cette personnalité qualifiée, le blocage de l'accès aux services concernés étant suspendu pendant le temps de l'instruction : **le recours est suspensif**.

3. La position de la commission spéciale : un dispositif ordonné par voie administrative justifié et proportionné mais dont la mise en œuvre opérationnelle doit encore être précisée

a) Un dispositif qui s'inscrit dans la continuité d'une première initiative sénatoriale visant à renforcer l'information des consommateurs sur le niveau de cybersécurité des plateformes

La mise en place d'un filtre national de cybersécurité grand public, destiné à mieux lutter contre les infractions quotidiennes de cybersécurité et les escroqueries en ligne, poursuit **un même objectif de protection des citoyens en ligne**, à l'instar de la loi du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[1], dite « loi Cyberscore ».

Cette loi, portée par l'actuel président de la commission de la culture du Sénat, Laurent Laffont, part du constat qu'aucune disposition ne garantit l'information du consommateur quant à la sécurité informatique de la solution numérique qu'il utilise. C'est pourquoi il a été mis en place un véritable « Cyberscore » des solutions numériques, accessible de façon claire et lisible, à l'aide d'un système de couleurs, pour les internautes[2].

Ce dispositif devrait entrer en vigueur à compter du 1er janvier 2024[3] et constituer une nouvelle étape dans la protection des citoyens en ligne, avant l'entrée en vigueur de ce projet de loi et le déploiement opérationnel du filtre anti-arnaques.

b) Un dispositif ordonné par voie administrative justifié et proportionné

À l'issue des différentes auditions menées, **la commission a estimé que le nouveau dispositif de filtrage des contenus proposé était justifié**, y compris son déclenchement ordonné par voie administrative.

---

[1] *Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public*

[2] *Rapport n° 503 (2021-2022) d'Anne-Catherine Loisier, fait au nom de la commission des affaires économiques du Sénat, déposé le 16 février 2022.*

[3] *Rapport d'information n° 636 (2022-2023),* Bilan annuel de l'application des lois, *déposé le 24 mai 2023.*

En effet, il est indispensable, au regard de la hausse des actes quotidiens de cybermalveillance, de disposer d'un dispositif souple et réactif face aux menaces que ces actes de cybermalveillance représentent pour notre vie privée et nos données à caractère personnel.

La mise en œuvre d'un dispositif ordonné par voie administrative est ainsi de nature à répondre à cet objectif de souplesse et de réactivité.

La commission a également considéré que les précautions et les procédures mises en œuvre sont de nature à garantir le caractère proportionné du dispositif et la bonne conciliation des exigences de protection de l'ordre public dans l'espace numérique d'une part, et de préservation des libertés d'expression et de communication d'autre part, notamment :

– la désignation d'une personnalité qualifiée au sein de la Cnil, dont les modalités d'information des décisions prises par les autorités administratives ont été renforcées par l'adoption de l'amendement **COM-108** du rapporteur. Le choix de la Cnil est principalement justifié par la nature des infractions visées, les arnaques en ligne ayant pour principale conséquence d'usurper notre identité ou d'obtenir des données à caractère personnel telles que des données bancaires ou d'identité ;

– la mise en œuvre d'une procédure de contradictoire pendant laquelle les éditeurs de sites frauduleux peuvent contester le constat de l'infraction effectué par l'autorité administrative ;

– la mise en œuvre de mesures conservatoires préalablement à toute demande de blocage ;

– la possibilité de lever, à tout moment, les mesures conservatoires et les mesures de blocage ordonnées par l'autorité administrative ;

– la possibilité, pour la personnalité qualifiée au sein de la Cnil, d'enjoindre l'autorité administrative de mettre fin aux mesures qu'elle a prises ;

– la possibilité, pour les éditeurs de services de communication en ligne en cause, de bénéficier d'une **procédure de recours administratif pourvu d'un effet suspensif** ;

– la publication d'un rapport annuel d'activité sur la mise en œuvre de ce nouveau dispositif de blocage, dont le contenu a été enrichi par l'adoption de l'amendement **COM-109** du rapporteur.

c) Une responsabilisation souhaitable de l'ensemble des acteurs face à l'absence de solution technique unique, auto-suffisante et satisfaisante

À l'issue des différentes auditions menées, **la commission a également estimé que le dispositif proposé présentait l'avantage de mobiliser les principaux intermédiaires techniques concernés, en fonction de la mesure que l'autorité administrative souhaite prendre et des**

informations dont elle dispose sur les éditeurs de services de communication en ligne en infraction :

– si les éditeurs de sites malveillants sont identifiables, alors la mobilisation des fournisseurs de navigateur Internet est préférée ;

– si les éditeurs de sites malveillants ne sont pas identifiables, alors la mobilisation des FAI et des fournisseurs de résolution de noms de domaine est préférée. Dans la mesure où les auteurs d'actes de cybermalveillance recherchent souvent l'anonymat, leur mobilisation est indispensable, même si les mesures prises par ces acteurs sont moins précises.

Afin d'éviter une éventuelle confusion, l'amendement **COM-105** du rapporteur Patrick Chaize prévoit ainsi que l'autorité administrative compétente qui émet une injonction de blocage précise quelle catégorie de fournisseurs met en œuvre la mesure.

Favorable à une mobilisation et à une responsabilisation de l'ensemble des acteurs techniques, la commission a également adopté l'amendement **COM-8** de Sylviane Noël, avec un avis favorable du rapporteur, laissant la **possibilité aux autorités administratives compétentes de notifier aux annuaires et aux moteurs de recherche les adresses électroniques permettant d'accéder à des sites dont l'accès a été empêché. En effet, les mesures de blocage peuvent efficacement être couplées avec les mesures de déréférencement que peuvent prendre les moteurs de recherche**.

d) Une mise en œuvre opérationnelle qui mériterait d'être précisée afin de renforcer la protection des citoyens en ligne

La commission remarque que le dispositif de filtrage proposé s'inspire à la fois des dispositifs de filtrage déjà existants, des dispositifs mis en œuvre à l'étranger, mais aussi des solutions gratuites déjà mises en œuvre par les principaux navigateurs sur Internet depuis plusieurs années, en particulier l'outil *Safe Browsing* de Google et *Smart Screen* de Microsoft, qui sont d'ailleurs utilisables sur d'autres navigateurs tels que Mozilla Firefox. Le dispositif proposé va toutefois plus loin que ce que le marché offre actuellement, en permettant le blocage de l'accès aux sites frauduleux.

Afin de rendre ce dispositif plus opérationnel, plus facilement compréhensible par les opérateurs qui seront chargés de sa mise en œuvre et de renforcer le niveau de protection des citoyens en ligne, **la commission spéciale a adopté les amendements du rapporteur suivants** :

– l'amendement **COM-101**, qui facilite la constatation des infractions visées, et donc le déclenchement du filtre anti-arnaques par les autorités administratives compétentes ;

– l'amendement **COM-102**, qui prévoit une procédure de mise en demeure des éditeurs de services de communication en ligne considérés

comme frauduleux au lieu d'une procédure d'information, car le déclenchement du dispositif fait suite à la constatation d'une ou plusieurs infractions ;

– l'amendement **COM-103**, qui précise que ce sont les adresses électroniques qui doivent être notifiées ;

– l'amendement **COM-104**, qui précise que le message d'avertissement à l'attention des internautes doit être claire, lisible, compréhensible, unique et permettre le renvoi vers la plateforme Cybermalveillance.gouv.fr, dans un double objectif de sensibilisation accrue aux escroqueries en ligne et d'harmonisation de l'information présenté aux internautes ;

– l'amendement **COM-105**, qui prévoit également que les mesures de blocage ordonnées par voie administrative doivent être prises sans délai ;

– l'amendement **COM-106**, qui oblige les autorités administratives compétentes à tenir une liste des adresses électroniques permettant l'accès à des sites ayant fait l'objet d'une mesure de blocage, afin qu'elles puissent évaluer, à l'issue de la durée de blocage, si un nouvelle mesure de blocage est nécessaire ;

– l'amendement **COM-107**, de précision rédactionnelle ;

– l'amendement **COM-110**, qui applique la peine d'un an d'emprisonnement et de 250 000 euros d'amende à l'ensemble des intermédiaires techniques mobilisés dans le déploiement du dispositif, afin qu'ils soient tous responsabilisés de la même façon.

La commission spéciale a adopté l'article 6 **ainsi modifié**.

TITRE III
RENFORCER LA CONFIANCE ET LA CONCURRENCE DANS L'ÉCONOMIE DE LA DONNÉE

CHAPITRE IER
Pratiques commerciales déloyales entre entreprises sur le marché de l'informatique en nuage

Article 7
Encadrement des frais de transfert et des crédits d'informatique en nuage

L'article 7 vise à définir et à encadrer l'octroi d'avoirs d'informatique en nuage, ainsi qu'à supprimer les frais de transfert sortant de données et les frais de changement de fournisseur de services d'informatique en nuage, par anticipation de l'adoption prochaine du *Data Act*.

La commission a adopté cet article modifié par l'adoption de six amendements, dont quatre du rapporteur, visant à :

– actualiser la définition du service d'informatique en nuage ;

– compléter la définition d'un avoir d'informatique en nuage ;

– plafonner à un an la durée pendant laquelle de tels avoirs peuvent être octroyés, en interdisant toute condition d'exclusivité auprès d'un seul fournisseur lors de l'octroi de ces avoirs ;

– soumettre au contrôle de l'Arcep la facturation des frais liés à un changement de fournisseur de services d'informatique en nuage afin d'éviter les facturations abusives ;

– interdire les pratiques de vente liée sur le marché de l'informatique en nuage dès lors qu'elles constituent une pratique commerciale déloyale.

1. Le droit en vigueur : une régulation du marché de l'informatique en nuage qui se concentre sur les frais de transfert sortant de données

a) Une timide régulation européenne du marché des services d'informatique en nuage

Le marché de l'informatique en nuage est aujourd'hui en forte croissance et à forte valeur ajoutée. Selon l'étude d'impact du projet de loi, il représentait 65 milliards d'euros en 2021 en Europe, dont 16 milliards d'euros en France, et pourrait dépasser les 1 200 milliards d'euros de valorisation au niveau mondial d'ici à 2025.

La particularité de ce marché est d'être fortement concentré autour d'un nombre restreint d'acteurs qui captent environ 70 % des parts de marché, les acteurs dominants étant notamment Amazon Web Services et Microsoft Azure. S'il existe des acteurs français et européens, leur taille et

leur internationalisation étant plus modestes même s'ils connaissent une forte croissance, ces derniers dénoncent, depuis plusieurs années déjà, des pratiques anticoncurrentielles qui tendent à ralentir leur développement.

L'absence d'interopérabilité sur ce marché et l'imbrication des technologies, en particulier des logiciels développés avec les plateformes et les infrastructures utilisées, conduisent à des pratiques commerciales déloyales de vente liée et à « verrouiller » le marché, limitant la capacité des fournisseurs alternatifs à offrir d'autres services d'informatique en nuage que ceux proposés par les acteurs dominants.

L'adoption du règlement européen sur les marchés numériques (RMN), ainsi que les négociations européennes en cours de finalisation pour adopter la proposition de règlement européen sur les données *(Data Act)*, devraient permettre une meilleure régulation du marché de l'informatique en nuage afin de **rendre ce marché plus interopérable et plus contestable**.

b) Une régulation inédite des frais de transfert sortant de données prévue par le règlement européen sur les données

Parmi les pratiques anticoncurrentielles les plus contestées sur le marché de l'informatique en nuage, figurent notamment **les frais de transfert sortant de données**, dont la légitimité de la facturation est décriée.

En effet, il s'agit d'une **pratique d'enfermement propriétaire qui constitue une barrière commerciale au développement d'un environnement qui permet aux utilisateurs de recourir à plusieurs fournisseurs de services d'informatique en nuage de manière simultanée**. Les utilisateurs sont donc captifs du premier fournisseur d'informatique en nuage utilisé, ce qui entraîne des situations de dépendance technologique, pénalisant ainsi nos entreprises françaises et européennes.

Selon une enquête menée en 2022 par l'autorité de la concurrence néerlandaise sur le marché de l'informatique en nuage[1], **ces « frais de sortie » sont dix fois plus importants chez les trois principaux fournisseurs d'informatique en nuage** (Amazon Web Services, Microsoft Azure, Google Cloud) que chez les autres fournisseurs, sachant que certains fournisseurs français ne facturent aucun frais. L'étude d'impact du projet de loi précise par exemple que « *AWS, Azure et Google facturent respectivement 4300 $, 3450 $ et 3392 $ pour l'extraction de 50 tera-bits de données en dehors de leurs écosystèmes, contre aucun frais facturé par Scaleway et OVH* ».

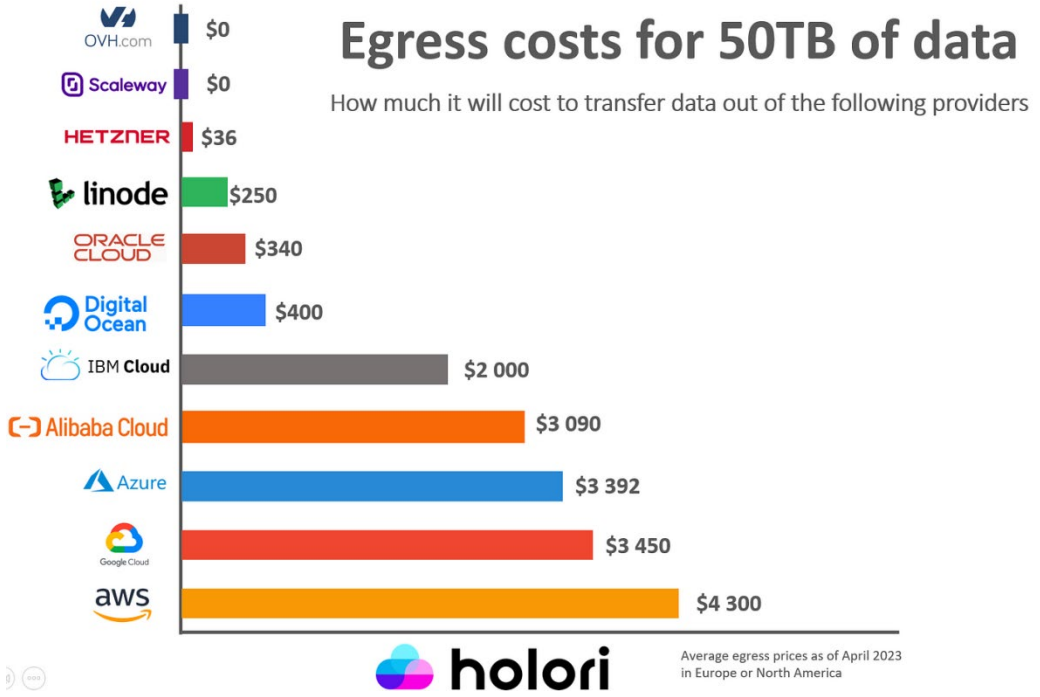
Cette **pratique anti-concurrentielle** est aujourd'hui largement documentée, et l'ensemble des auditions menées par le rapporteur à ce sujet ont confirmé la nécessité d'encadrer et d'interdire les frais de transfert de données qui ne sont pas justifiés.

[1] *Public Market study cloud services DEF (acm.nl)*

Récemment, l'office britannique chargé des communications a publié une étude sur le marché de l'informatique en nuage, considérant que **ces frais sont additionnels aux charges incompressibles relatives au changement de fournisseur**, ayant pour but de dissuader les utilisateurs de transférer leurs données vers un autre fournisseur ou même vers leurs propres infrastructures.

En France, l'Autorité de la concurrence (ADLC) devrait publier son étude sur l'état concurrentiel sur le marché de l'informatique en nuage au mois de juillet 2023.

Par exemple, selon une récente étude menée par l'entreprise *Cloudflare*, **le montant de ces frais facturés par certains fournisseurs représentait jusqu'à 80 fois le coût réel de ces derniers**.



Source : Holori

Dans ce contexte et au regard du consensus qui se dessine sur ce sujet, **il est apparu urgent de supprimer les frais liés à un changement de fournisseur de services d'informatique en nuage : c'est l'objet de l'article 25 du *Data Act***, toujours en cours de négociation à l'échelle européenne. Cet article prévoit la suppression progressive des frais de changement de fournisseur pendant une période de trois ans à compter de l'application du *Data Act*, la date estimée étant le 15 février 2027.

L'article 7 du projet de loi traduit en partie et par anticipation les dispositions prévues à l'article 25 du *Data Act*.

c) Une absence de régulation spécifique à la pratique de l'octroi de crédits d'informatique en nuage

En l'état actuel du *Data Act*, il n'y a pas de dispositions relatives à l'encadrement de l'octroi des crédits *cloud*. Pourtant, il s'agit également d'une pratique dont les effets anticoncurrentiels sont désormais bien documentés.

Dans son rapport de l'an dernier sur la souveraineté économique, la commission des affaires économiques alertait déjà sur une stratégie qui « ***permet principalement à une entreprise de capter des parts de marché dès la création de l'entreprise cliente et de se constituer un avantage par rapport à ses concurrents***. *En raison de la durée d'octroi de ces crédits, des montants distribués et* ***des conditions restrictives imposées par les grandes entreprises américaines du numérique pour transférer les données*** *qu'elles hébergent vers d'autres infrastructures et logiciels, ces pratiques sont* ***jugées anticoncurrentielles*** *par de nombreux acteurs et spécialistes des marchés numériques : il existe en effet* ***un risque de dépendance technologique des jeunes pousses*** »[1].

Au regard des informations transmises au rapporteur Patrick Chaize lors des travaux de la commission spéciale, les offres suivantes de crédits *cloud* ont par exemple été identifiées :

- jusqu'à 100 000 dollars par an de crédits octroyés par Google et Amazon Web Services, avec parfois en plus un accès temporaire et gratuit à certaines fonctionnalités ;

- jusqu'à 36 000 dollars sur un an pour 50 start-up sélectionnées par Scalway ;

- jusqu'à 500 dollars offerts et 70 % de réduction pendant deux ans pour les start-up chez Oracle ;

- jusqu'à 10 000 euros pour les start-up et 100 000 euros pour les *scale-up* pendant deux ans maximum et sans renouvellement chez OVH Cloud.

En l'état actuel du marché, la durée d'octroi des crédits *cloud* par les acteurs dominants, tout comme le montant attribué et l'association éventuelle de fonctionnalités supplémentaires gratuites ne permettent pas aux acteurs français et européens de l'informatique en nuage de rivaliser de façon loyale.

Bien que le sujet ne fasse pas suffisamment consensus au niveau européen pour pouvoir être intégré au *Data Act*, le Gouvernement français a souhaité, à l'article 7 de ce projet de loi, prévoir un encadrement national et spécifique à l'octroi de tels crédits, dont les effets anticoncurrentiels sont également bien documentés aujourd'hui.

---

[1] *Cinq plans pour reconstruire la souveraineté économique, Rapport d'information n° 755 (2021-2022) de Sophie Primas, Amel Gacquerre et Franck Montaugé, déposé au nom de la commission des affaires économiques le 6 juillet 2022.*

2. Le dispositif envisagé : un double encadrement des avoirs d'informatique en nuage et des frais de transfert sortant de données

L'article 7 du projet de loi crée **un nouvel article L. 442-12 au sein du code de commerce**, au sein de la section 2 « Autre pratiques prohibées » du chapitre II « Des pratiques commerciales déloyales entre entreprises » du titre IV « De la transparence, des pratiques restrictives de concurrence et d' autres pratiques prohibées » du livre IV « De la liberté des prix et de la concurrence ».

a) Une première proposition d'encadrement de la durée d'octroi des avoirs d'informatique en nuage

Premièrement, l'article 7 codifie la définition existante d'un service d'informatique en nuage, entendu comme « *un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées* ».

Deuxièmement, est proposée, pour la première fois en droit, une définition d'un « *avoir d'informatique en nuage* », entendue comme « *un montant de crédits offert par un fournisseur de services d'informatique en nuage à ses utilisateurs et utilisables sur différents services* ».

Troisièmement, **n'est autorisé l'octroi d'avoirs d'informatique en nuage que pour une durée limitée** aux personnes exerçant des activités de production, de distribution ou de services, un décret en Conseil d'État devant déterminer les modalités de renouvellement et de validité.

b) Une première proposition de suppression de certains frais de transfert sortant de données par anticipation de l'application du règlement européen sur les données

L'article 7 du projet de loi **interdit, avec effet immédiat, les frais de transfert sortant de données *(egress fees)* facturés lorsqu'un client souhaite transférer ses données vers ses propres infrastructures ou vers les infrastructures d'un autre fournisseur au sein d'une architecture *multi-cloud***.

Par contre, dans la lignée de ce qui est prévu à l'article 25 du *Data Act*, il est prévu **une exception pour les « frais de migration » liés à un changement de fournisseur**, ces frais pouvant être justifiés par les coûts incompressibles que peuvent représenter un processus de migration de données.

Les dispositions de l'article 7 du projet de loi relatives aux frais de transfert sortant de données ne sont valables que jusqu'au 15 février 2027, date estimée d'entrée en vigueur du *Data Act*, conformément aux dispositions prévues à l'article 36 du projet de loi.

3. La position de la commission : un double encadrement nécessaire qui mériterait toutefois de mieux prendre en compte la réalité des pratiques anticoncurrentielles sur le marché de l'informatique en nuage

a) Un encadrement indispensable des effets anticoncurrentiels des crédits d'informatique en nuage déjà mis en évidence par les travaux de la commission des affaires économiques du Sénat

Au regard des travaux précédemment menés sur ce sujet par le Sénat et de ceux conduits par le rapporteur, dans le cadre de l'examen de ce projet de loi, **la commission spéciale tient à saluer l'initiative française d'encadrement des avoirs d'informatique en nuage**.

Toutefois, la commission a considéré que l'encadrement proposé était encore trop timide et méritait d'être clarifié dès maintenant pour les opérateurs économiques, afin de préciser l'intention du législateur poursuivie par ce nouvel encadrement.

Ainsi, **l'amendement COM-112** du rapporteur **clarifie la définition proposée d'un avoir d'informatique en nuage**, précisant qu'il s'agit d'un avantage octroyé par un fournisseur de services d'informatique en nuage à titre temporaire.

En définissant, par nature, un avoir d'informatique en nuage comme un avantage octroyé à une entreprise, cette définition ouvre également la voie à une prise en compte d'autres formes d'avoirs ayant des effets anticoncurrentiels. Si l'octroi de crédits offerts est la principale pratique commerciale visée, d'autres pratiques, telle que la mise à disposition gratuites de fonctionnalités techniques, ont par exemple été relevées par l'Autorité de la concurrence dans son avis sur le projet de loi[1].

L'amendement **COM-111** du rapporteur **actualise par ailleurs la définition d'un service d'informatique en nuage**, au regard de la dernière définition retenue par la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « directive NIS 2 ».

Au regard des différentes auditions menées, la commission spéciale a également adopté **l'amendement COM-113** du rapporteur **afin de limiter davantage les phénomènes de verrouillage ou de dépendance** sur le marché de l'informatique en nuage. Pour cela :

– est fixée à une année la durée maximale d'octroi des avoirs d'informatique en nuage, ce qui laisse suffisamment de souplesse pour octroyer des avoirs de durées différentes, permet d'autoriser l'octroi de tels avoirs pour une courte période car correspondant à des offres d'essai gratuit,

---

[1] *Autorité de la concurrence, Avis sur certaines dispositions du projet de loi, 20 Avril 2023.*

tout en interdisant l'octroi de tels avoirs pour une période plus longue qui serait préjudiciable d'un point de vue concurrentiel ;

– est précisé que l'utilisation d'un avoir d'informatique en nuage ne peut pas être assortie de conditions d'exclusivité vis-à-vis du fournisseur, ce qui permet de ne pas préjuger du choix final du fournisseur par l'utilisateur et d'inciter à recourir à des offres d'essai gratuit.

b) Un encadrement indispensable des effets anticoncurrentiels des frais de transfert sortant de données afin de favoriser l'interopérabilité des services d'informatique en nuage

Afin de clarifier l'articulation entre les frais de transfert de données qui sont supprimés et les frais liés au changement de fournisseur qui sont temporairement autorisés jusqu'à l'application des dispositions dédiées du *Data Act*, toujours en cours de négociation à l'échelle européenne, la commission spéciale a adopté l'amendement **COM-114** du rapporteur.

Concernant les frais liés à un changement de fournisseur de services d'informatique en nuage, **cet amendement précise notamment, pour éviter la surfacturation régulièrement mise en évidence par différentes autorités européennes chargées de la concurrence, que la facturation doit s'effectuer aux coûts réels et doit être communiquée de façon transparente aux utilisateurs, sous le contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) dans le cadre de ses nouvelles attributions en matière de régulation de l'informatique en nuage**.

La commission spéciale a considéré que cette disposition constituait une avancée majeure de ce projet de loi, répondant ainsi aux préoccupations exprimées par les acteurs français de l'informatique en nuage, la commission spéciale souhaitant soutenir leur développement.

c) Un encadrement indispensable des autres effets anticoncurrentiels identifiés sur le marché de l'informatique en nuage

La commission spéciale a également adopté, sur l'avis favorable du rapporteur, les deux amendements identiques COM-51 et COM-88 relatifs aux pratiques de vente liée sur le marché de l'informatique en nuage.

Si pendant longtemps la vente liée a été considérée, par principe, comme illicite en France, elle est désormais autorisée, mais encadrée. La vente liée consiste à subordonner la vente d'un produit ou d'une prestation de service à l'achat d'un autre produit ou d'un autre service. Cette pratique est aujourd'hui très répandue sur le marché de l'informatique en nuage, par exemple en obligeant une entreprise à transférer ses données sur son architecture de *cloud* afin de pouvoir utiliser son logiciel.

Ces deux amendements sont conformes à l'encadrement actuel de la vente liée, puisque l'interdiction est subordonnée à la qualification de

pratique commerciale déloyale au sens de l'article L. 121-1 du droit de la consommation.

La commission spéciale, sur l'avis de son rapporteur, a donc considéré que ces deux amendements étaient de nature à limiter les pratiques anticoncurrentielles sur le marché de l'informatique en nuage.

La commission spéciale a adopté l'article 7 **ainsi modifié**.

CHAPITRE II
Interopérabilité des services d'informatique en nuage

Article 8
Obligations d'interopérabilité et de portabilité à la charge des services d'informatique en nuage

L'article 8 vise à prévoir, par anticipation de l'adoption du *Data Act*, les obligations d'interopérabilité, de portabilité et d'équivalence fonctionnelle que devront respecter les fournisseurs de services d'informatique en nuage.

La commission spéciale a adopté cet article modifié par l'adoption d'un amendement du rapporteur Patrick Chaize visant à préciser la définition choisie de l'équivalence fonctionnelle.

1. Le droit en vigueur : une régulation du marché de l'informatique en nuage qui se concentre sur les frais de transfert sortant de données

a) Une série de barrières techniques qui rendent le marché de l'informatique en nuage difficilement contestable pour les acteurs émergents

Le marché de l'informatique en nuage est aujourd'hui un marché en forte croissance et à forte valeur ajoutée. Selon l'étude d'impact du projet de loi, ce marché représentait 65 milliards d'euros en 2021 en Europe, dont 16 milliards d'euros en France, et pourrait dépasser les 1 200 milliards d'euros de valorisation au niveau mondial d'ici à 2025.

En plus des pratiques anticoncurrentielles décrites précédemment et pour lesquelles l'article 7 du projet de loi prévoit un encadrement spécifique, voire une interdiction, **il existe aujourd'hui un grand nombre de barrières techniques**, souvent instaurées à l'initiative des acteurs dominants, qui rendent le marché de l'informatique en nuage difficilement contestable pour les entreprises françaises et européennes.

Il est ainsi constaté un **fort manque d'interopérabilité à tous les niveaux du marché de l'informatique en nuage**, que ce soit au niveau des

infrastructures (Iaas), des plateformes (Paas) ou des logiciels (Saas). Autrement dit, il y a **un manque de langage commun** sur ce marché, notamment pour décrire les modalités d'accès, de stockage et de traitement des données.

Ce manque d'interopérabilité incite par exemple les vendeurs de logiciels indépendants à développer leurs services sur des infrastructures qui appartiennent aux fournisseurs de services d'informatique en nuage les plus utilisés, afin de toucher une large clientèle. Or, cela **accentue les phénomènes d'enfermement des clients et l'exclusivité en faveur des acteurs dominants du marché**.

b) Des avancées significatives qui seront permises par l'adoption du règlement européen sur les données

Face à ces constats et dans une volonté de rééquilibrer le marché de l'informatique en nuage, **la proposition de règlement européen sur les données, le *Data Act*, toujours en négociation à l'échelle européenne, consacre un chapitre entier aux mesures d'interopérabilité, en particulier ses articles 28 et 29**.

Il y est notamment précisé que les spécifications d'interopérabilité ouvertes et les normes européennes pour l'interopérabilité des services de traitement des données couvrent :

– les aspects de l'interopérabilité de l'informatique en nuage pour l'interopérabilité du transport de données, l'interopérabilité syntactique, l'interopérabilité sémantique des données, l'interopérabilité comportementale et l'interopérabilité stratégique ;

– les aspects de la portabilité des données en nuage pour la portabilité syntactique des données, la portabilité sémantique des données et la portabilité stratégique des données.

L'article 8 du projet de loi traduit donc en partie les dispositions du *Data Act* relatives aux exigences d'interopérabilité, dans un souci de faciliter le choix et le changement de fournisseur par les utilisateurs, afin qu'ils puissent choisir ce qui correspond le mieux à leurs besoins.

2. Le dispositif envisagé : des objectifs généraux d'interopérabilité et de portabilité des services d'informatique en nuage

a) L'introduction de nouvelles définitions en droit

L'article 8 du projet de loi propose **une nouvelle définition des actifs numériques adaptée au marché de l'informatique en nuage**, ces actifs étant entendus comme « *tous les éléments en format numérique sur lesquels l'utilisateur d'un service d'informatique en nuage a un droit d'utilisation, y compris des actifs qui ne sont pas inclus dans le champ de sa relation contractuelle avec le service d'informatique en nuage. Ces actifs comprennent notamment les données, les*

applications, les machines virtuelles et les autres technologies de virtualisation, telles que les conteneurs ».

Une première définition de l'équivalence fonctionnelle est également proposée, s'inspirant de celle figurant à l'article 2 du *Data Act*, sans être strictement identique. L'équivalence fonctionnelle est ainsi définie comme « *un niveau minimal de fonctionnalité assurée dans l'environnement d'un nouveau service d'informatique en nuage après la migration, de manière à garantir aux utilisateurs un usage des éléments essentiels du service aux mêmes niveaux de performance, de sécurité, de résilience opérationnelle et de qualité que le service d'origine au moment de la résiliation du contrat* ».

b) La fixation de nouvelles obligations d'interopérabilité et de portabilité pour les fournisseurs de services d'informatiques en nuage

Enfin, l'article 8 déclare, sans plus de précisions, que les fournisseurs de services d'informatique en nuage assurent la conformité de leurs services avec les exigences essentielles d'interopérabilité et de portabilité, dans des conditions sécurisées, vers les services des utilisateurs ou à l'égard d'autres fournisseurs couvrant le même type de fonctionnalités.

Par conséquent, ces fournisseurs doivent mettre à disposition les **interfaces de programmation d'application** (API) nécessaires pour assurer ces exigences de portabilité et d'interopérabilité.

3. La position de la commission : des premières précisions rédactionnelles qui annoncent des ajustements plus significatifs une fois le *Data Act* définitivement adopté

La commission spéciale souhaite attirer l'attention du Gouvernement et de l'Assemblée nationale sur la nécessité, une fois le *Data Act* définitivement adopté, d'effectuer un travail d'harmonisation important des définitions des actifs numériques et de l'équivalence fonctionnelle.

Dans l'attente de l'adoption définitive du *Data Act*, la commission spéciale a adopté l'amendement **COM-115** du rapporteur visant à modifier la rédaction de la définition de l'équivalence fonctionnelle en remplaçant les termes « *aux mêmes niveaux* » par les termes « *à des niveaux équivalents* ». Il s'agit d'**éviter un effet indésirable d'harmonisation de l'ensemble des offres proposées sur le marché des infrastructures d'informatique en nuage**, ce qui n'est pas l'objectif poursuivi par la fixation d'une obligation d'équivalence fonctionnelle.

La commission spéciale a adopté l'article 8 **ainsi modifié**.

Article 9

Obligations d'interopérabilité et de portabilité à la charge des services d'informatique en nuage

L'article 9 confie à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) le soin d'édicter les spécifications d'interopérabilité et de portabilité que devront respecter les fournisseurs de services d'informatique en nuage.

La commission spéciale a adopté cet article modifié par l'adoption d'un amendement du rapporteur Patrick Chaize visant à préciser que les spécifications d'interopérabilité et de portabilité édictées par l'Arcep tiennent compte des différences de nature entre les services d'informatique en nuage, ainsi que des règles édictées en la matière par les autres autorités européennes.

1. L'anticipation des dispositions du futur règlement européen sur les données afin de débuter dès aujourd'hui l'important travail de normalisation en matière d'interopérabilité et de portabilité

a) La désignation de l'Arcep comme autorité chargée d'édicter les spécifications d'interopérabilité et de portabilité des fournisseurs de services d'informatique en nuage

L'article 9 du projet de loi confie à l'Arcep le soin de préciser les règles techniques d'interopérabilité et de portabilité que devront respecter les fournisseurs de services d'informatique en nuage, conformément aux obligations définies à l'article 8 de ce projet de loi.

Pour effectuer ce délicat travail d'édiction des règles techniques, l'Arcep peut **recourir à un ou plusieurs organismes de normalisation**, ce qui est conforme à ce qui est prévu par la proposition de règlement européen sur les données, ou *Data Act*.

L'Arcep fixera ainsi le délai de mise en conformité des opérateurs concernés à ces nouvelles règles, sachant que le travail de normalisation est estimé à plusieurs années, surtout qu'il sera concerté à l'échelle européenne.

b) L'obligation d'assurer l'équivalence fonctionnelle au niveau des infrastructures d'informatique en nuage

L'article 9 du projet de loi précise également que l'obligation d'équivalence fonctionnelle, telle que définie à l'article 8 du projet de loi, concerne seulement les services d'infrastructures d'informatique en nuage. En effet, il est précisé que cette obligation s'applique « *à des ressources informatiques modulables et variables limitées à des éléments d'infrastructure tels que les serveurs, les réseaux et les ressources virtuelles nécessaires à l'exploitation de l'infrastructure* ».

2. La position de la commission : une nécessaire adaptation des spécifications d'interopérabilité et de portabilité aux particularités du marché de l'informatique en nuage

La commission spéciale salue le choix de l'Arcep pour édicter ces nouvelles spécifications d'interopérabilité et de portabilité, tout en étant consciente que ce travail représente un défi conséquent et nouveau pour cette Autorité. La commission remarque ainsi que, par cet article, le Gouvernement positionne l'Arcep comme autorité administrative indépendante chargée de la mise en œuvre du futur *Data Act*. Ainsi, le rapporteur sera particulièrement vigilant à ce que l'Arcep bénéficie, dès le prochain projet loi de finances, **des moyens budgétaires et humains nécessaires à l'accomplissement de ses nouvelles missions**.

Par ailleurs, au regard des différentes auditions menées dans le cadre de la commission spéciale et des inquiétudes des opérateurs économiques exprimées à cette occasion, l'amendement **COM-116** du rapporteur a été adopté afin de rendre le travail d'édiction des obligations d'interopérabilité et de portabilité plus opérationnel et d'éviter de le rendre « aveugle » des spécificités du marché de l'informatique en nuage, en :

– demandant à l'Arcep de tenir compte des différences existantes entre les infrastructures, les plateformes et les logiciels de services d'informatique en nuage ;

– précisant que ces différences doivent être prises en compte lors de l'édiction des spécifications techniques, plutôt que dans la définition des exigences d'interopérabilité et de portabilité, afin de laisser davantage de souplesse à l'Arcep et aux opérateurs économiques concernés ;

– prévoyant un délai d'édiction de ces spécifications techniques et, par conséquent, un délai de mise en conformité des opérateurs économiques concernés à ces spécifications, qui sera fixé par décret, après consultation de l'Arcep.

La commission spéciale a adopté l'article 9 **ainsi modifié**.

Article 10

Contrôle des obligations des fournisseurs de services d'informatique en nuage par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse

L'article 10 vise à préciser les prérogatives de l'Autorité de la régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) en matière de contrôle des obligations des fournisseurs de services d'informatique en nuage.

La commission a adopté cet article modifié par deux amendements du rapporteur Patrick Chaize, dont l'un crée notamment une procédure de saisine de l'Autorité de la concurrence (ADLC) par l'Arcep lorsque cette dernière a connaissance d'abus de position dominante et de pratiques entravant le libre exercice de la concurrence dans le secteur de l'informatique en nuage.

1. L'extension des pouvoirs d'enquête, de sanction et du mécanisme de règlement des différends aux fournisseurs de services d'informatique en nuage

a) L'application des pouvoirs d'enquête aux fournisseurs de services d'informatique en nuage

Pour mener à bien ses nouvelles missions et s'assurer du respect des obligations d'interopérabilité et de portabilité par les fournisseurs de services d'informatique en nuage, l'article 10 du projet de loi dispose que **l'Arcep puisse faire usage de son pouvoir de recueil des informations et des documents, ainsi que de son pouvoir d'enquête**.

Ces pouvoirs s'apparentent déjà aux moyens dont dispose l'Arcep dans les autres secteurs économiques où elle assure la régulation, en particulier le secteur des communications électroniques. C'est pourquoi il est précisé que les enquêtes menées le sont dans les conditions prévues aux II à IV de l'article L. 32-4 et à l'article L. 32-5 du code des postes et des communications électroniques (CPCE).

b) L'application du mécanisme de règlement des différends aux fournisseurs de services d'informatique en nuage

Dans l'éventualité d'un désaccord sur les conditions de recueil des documents nécessaires pour faire respecter aux fournisseurs de services d'informatique en nuage leurs nouvelles obligations en matière d'interopérabilité et de portabilité, **l'Arcep peut également recourir à son mécanisme de règlement des différends**, dans les conditions prévues à l'article L. 36-8 du CPCE.

c) L'application des pouvoirs de sanction aux fournisseurs de services d'informatique en nuage

Enfin, l'article 10 du projet de loi prévoit également que **l'Arcep puisse sanctionner les manquements des fournisseurs de services d'informatique en nuage** à leurs obligations en matière d'interopérabilité, de portabilité et d'équivalence fonctionnelle.

Si l'Arcep peut se saisir d'office, elle peut également faire usage de son pouvoir de sanction à la demande du ministre chargé de l'économie, d'une organisation professionnelle, d'une association agréée d'utilisateurs ou de toute personne physique ou morale concernée, sous réserve que la constatation de l'infraction soit avérée.

Le cas échéant, l'Arcep peut prononcer à l'encontre du prestataire de services d'informatique en nuage en cause **une sanction pécuniaire** dont le montant est proportionné à la gravité du manquement et aux avantages qui en sont tirés, sans pouvoir excéder 3 % du chiffre d'affaires hors taxes du dernier exercice clos, taux porté à 5 % en cas de réitération du manquement dans un délai de cinq ans à compter de la date à laquelle la première décision de sanction est devenue définitive.

2. La position de la commission : un renforcement bienvenu des missions et des pouvoirs de l'Arcep qui doit toutefois s'accompagner d'une hausse des moyens qui lui sont alloués

Si la commission spéciale salue le renforcement des pouvoirs de l'Arcep, qui a vocation à devenir le régulateur du marché de l'informatique en nuage ou « gendarme du *cloud* », le rapporteur veillera à ce que l'Arcep **bénéficie, dès le prochain projet loi de finances, des moyens budgétaires et humains nécessaires à l'accomplissement de ses nouvelles missions**.

Par ailleurs, la commission a adopté deux amendements du rapporteur :

- l'amendement **COM-117**, de nature rédactionnelle ;

- l'amendement **COM-118**, qui **instaure une procédure de saisine de l'Autorité de la concurrence (ADLC) par l'Arcep lorsque cette dernière a connaissance d'abus de position dominante et de pratiques entravant le libre exercice de la concurrence dans le secteur de l'informatique en nuage**, à l'instar de la procédure existante en matière de communications électroniques.

La commission spéciale a adopté l'article 10 **ainsi modifié**.

CHAPITRE II *BIS*
Transparence sur le marché de l'informatique en nuage
(Division nouvelle)

Article 10 bis (nouveau)
Obligations de transparence sur le marché de l'informatique en nuage

La commission spéciale a adopté, sur l'avis favorable de son rapporteur Patrick Chaize, deux amendements identiques de Florence Blatrix Contat et plusieurs de ses collègues et de Vanina Paoli Gagin et plusieurs de ses collègues portant création d'un article additionnel après l'article 10 du projet de loi.

Cet article fixe des obligations de publicité et de transparence aux fournisseurs d'informatique en nuage, ainsi qu'à leurs intermédiaires, notamment en matière de risque d'accès gouvernemental aux données des utilisateurs, ce qui s'inscrit dans la continuité des travaux de la commission des affaires économiques et de la commission d'enquête sur TikTok du Sénat.

La commission spéciale a adopté le chapitre II *bis* et l'article 10 *bis* ainsi rédigés.

1. Le dispositif envisagé : l'obligation de publier des informations relatives à la localisation des infrastructures informatiques et aux risques d'accès gouvernemental des données des utilisateurs

Ces amendements visent à insérer, après l'article 10 de ce projet de loi, **un chapitre II *bis*, intitulé « *Transparence sur le marché de l'informatique en nuage* »**, constitué de l'article 10 *bis*. Le dispositif consiste à obliger les fournisseurs de services d'informatique en nuage, ainsi que leurs intermédiaires, à publier sur leur site Internet des informations :

– relatives à l'emplacement physique de toute l'infrastructure informatique déployée pour le traitement des données de leurs services individuels ;

– sur l'existence d'un risque d'accès gouvernemental aux données de l'utilisateur du service d'informatique en nuage ;

– concernant les mesures techniques, juridiques et organisationnelles adoptées par le fournisseur d'informatique en nuage afin d'empêcher l'accès gouvernemental aux données lorsque ce transfert ou cet accès créerait un conflit avec le droit de l'Union ou le droit national de l'État membre concerné.

2. La position de la commission : des obligations de transparence bienvenues qui s'inscrivent dans la continuité des préoccupations du Sénat sur l'extra-territorialité des données

La commission spéciale a adopté, sur l'avis favorable de son rapporteur, les deux amendements identiques **COM-52** et **COM-157 rectifié *bis*** portant création de ce chapitre et cet article additionnels.

La commission spéciale a considéré que le renforcement des obligations de publicité et de transparence des fournisseurs de services d'informatique en nuage, ainsi que de leurs intermédiaires, était **un prérequis indispensable pour contribuer à rééquilibrer le marché de l'informatique en nuage**, le rendre plus contestable par les acteurs émergents, et surtout pour renforcer l'information des utilisateurs, particuliers comme entreprises, quant à l'utilisation de leurs données.

Par ailleurs, la commission spéciale a également constaté que ces deux amendements s'inscrivaient **dans la continuité des travaux de la commission des affaires économiques du Sénat sur la souveraineté économique[1], et font écho aux travaux actuels de la commission d'enquête sur TikTok, ces deux instances sénatoriales critiquant fortement la soumission de nos données aux législations extra-territoriales**.

La commission spéciale relève toutefois que des ajustements rédactionnels éventuels pourraient être nécessaires une fois le règlement européen sur les données, ou *Data Act*, définitivement adopté.

La commission spéciale a adopté le chapitre II *bis* et l'article 10 *bis* **ainsi rédigés**.

[1] Cinq plans pour reconstruire la souveraineté économique, *Rapport d'information n° 755 (2021-2022) de Sophie Primas, Amel Gacquerre et Franck Montaugé, déposé au nom de la commission des affaires économiques le 6 juillet 2022.*

CHAPITRE III
Régulation des services d'intermédiation de données

Article 11
Désignation de l'Arcep comme autorité compétente en matière de régulation des services d'intermédiation de données

L'article 11 procède à la désignation de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) en tant qu'autorité de régulation des prestataires de services d'intermédiation de données (SID), une nouvelle catégorie d'acteur créée par le règlement européen sur la gouvernance des données, qui ne pourra procéder ni à la collecte, ni au traitement des données, mais seulement servir de plateforme d'échange pour des entreprises, particuliers ou administrations.

Le rapporteur Patrick Chaize salue la désignation de l'Arcep dans la régulation de cette nouvelle activité, pour laquelle elle semblait la plus qualifiée, mais veillera avec un soin particulier à la mise en cohérence de ses moyens humains et budgétaires avec cette mission supplémentaire.

La commission spéciale a adopté cet article sans modification.

1. L'institution de services d'intermédiation de données doit s'accompagner de la désignation d'une autorité compétente pour la régulation de ce nouveau champ d'activité, avant le 24 septembre 2023

Issu d'une initiative de la Commission européenne en date du 25 novembre 2020, le **règlement européen sur la gouvernance des données**[1] **(en anglais, *Data Governance Act*),** est entré en vigueur le 23 juin 2022. Il contribue à la consolidation d'un **marché européen unifié de la donnée,** par l'harmonisation des règles nationales, en vue d'établir un cadre équitable pour l'accès aux données, leur partage et leur réutilisation.

Il **s'inscrit dans le cadre d'un effort plus large de l'Union européenne pour la régulation de son espace numérique**, en complément du règlement sur les services numériques (en anglais, *Digital Services Act – DSA*) qui lutte contre la haine et la désinformation en ligne, du règlement sur les marchés numériques (en anglais, *Digital Markets Act – DMA*), qui vise à diminuer la concentration du secteur numérique, et du règlement sur les données (en anglais, *Data Act*) à venir.

Institués par le règlement sur la gouvernance européenne des données, les « **services d'intermédiation de données** » sont de nouveaux acteurs de l'économie numérique, qui auront pour mission de permettre

[1] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.*

l'échange de données, en particulier non personnelles, de façon transparente, concurrentielle et fiable entre acteurs économiques, administrations aux particuliers, au sein de l'Union européenne.

Ce règlement met en place **un cadre pour l'échange volontaire de données, gratuit ou à titre onéreux, en particulier dans les domaines industriel et commercial, des données peu encadrées jusqu'à présent.**

L'Union européenne prévoit en effet une augmentation de 530 % du volume mondial de données en sept ans, passant, ce qui devrait démultiplier le potentiel d'innovation fondée sur les données.

Ce nouveau service pourra par exemple trouver des applications dans les domaines de la santé – médecine personnalisée –, et de la transition écologique. Il bénéficiera en particulier aux opérateurs de l'intelligence artificielle, renforçant les positions européennes dans ce secteur en plein essor.

Source : Commission européenne

Parmi les acteurs positionnés sur ce créneau, on peut d'ores et déjà signaler Hub One dans le domaine aéroportuaire et Agdatahub[1], qui entrevoit dans les SID l'opportunité de **mieux maîtriser l'usage qui est fait des données commerciales des agriculteurs** mais également de **mieux les monétiser**, et de **corriger des asymétries d'information** avec de grands groupes fournisseurs d'intrants (Syngenta, John Deere…). La commission des affaires économiques du Sénat avait identifié un point faible de la souveraineté agricole française dans le manque de maîtrise des données commerciales des agriculteurs [2].

Ce règlement sera pleinement applicable à partir du 24 septembre 2023. Son article 13, paragraphe 1, dispose que « *chaque État membre désigne* ***une ou plusieurs autorités compétentes*** *pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données* ». Aux termes de cet article, la France a jusqu'à cette même date pour procéder à cette désignation et la notifier à la Commission européenne.

L'autorité désignée devra assurer ses fonctions dans le respect de l'article 26 de ce règlement européen.

L'article 11 du présent projet de loi est la traduction de cette obligation européenne.

2. Le Gouvernement a choisi l'Arcep plutôt que la Cnil comme régulateur de ce nouveau type d'acteurs de l'économie de la donnée, en raison de la visée pro-concurrentielle du règlement européen sur la gouvernance des données

Le premier alinéa de l'article 11 de ce projet de loi désigne l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) comme autorité compétente, en France, pour la régulation des services d'intermédiation de données.

Sur le fondement de cette attribution de compétence, le deuxième alinéa prévoit un avis simple de l'Arcep sur l'ensemble des projets de lois et des décrets relatifs aux services d'intermédiation de données, ainsi que, sur ces sujets, si le ministre chargé du numérique le demande, une association à la préparation de la position française dans les négociations internationales et une participation à la représentation française dans les organisations internationales et au sein de l'Union européenne.

---

[1] *Une société contrôlée à 55 % par le monde agricole (Chambres d'agriculture France, instituts techniques, éditeurs de logiciels, Unigrain, Sofiprotéol, marché du porc) et à 45 % par le secteur public (Caisse des dépôts et consignations, Imprimerie nationale).*

[2] *Rapport de Sophie Primas, Amel Gacquerre et de Franck Montaugé, «* Cinq plans pour reconstruire la souveraineté économique *», adopté par la commission des affaires économiques le 6 juillet 2022.*

Le troisième et dernier alinéa de cet article rappelle que l'Arcep devra, dans de ce but s'assurer d'une application coordonnée et cohérente de la réglementation, **collaborer** avec ses homologues des vingt-six autres États membres de l'Union européenne, avec la Commission européenne, ainsi qu'avec un groupe d'experts, **le comité européen de l'innovation dans le domaine des données**[1], créé par l'article 29 du même règlement auprès de la Commission.

Cette précision est d'une portée juridique limitée**, la coopération étant dans la nature même des autorités de régulation européennes**. Elle n'en constitue pas moins un **signal bienvenu**, dans le sens d'un renforcement de l'harmonisation des règles et des pratiques au sein de l'Union, qui est, au demeurant, l'objet même du règlement européen sur la gouvernance des données.

3. La commission spéciale salue la désignation de l'Arcep comme autorité de régulation des services d'intermédiation de données et appelle à lui donner les moyens de sa nouvelle mission

a) Bien qu'aucune solution ne soit complètement évidente, la désignation de l'Arcep constitue la solution la plus satisfaisante

Le rapporteur observe qu'aucune autorité de régulation n'a été créée spécialement pour la régulation des services d'intermédiation de données.

Si le règlement européen sur la gouvernance des données impose de désigner une autorité pour la régulation des SID au plus tard le 24 septembre 2023, il n'impose pas l'identité de cette autorité, laissant aux États membres le choix de l'architecture institutionnelle qui leur semble la plus efficace.

Des justifications relatives à la typologie des données – il s'agit en effet essentiellement de données d'entreprises, *a priori* non personnelles – et à la dimension pro-concurrentielle du cadre réglementaire ont présidé au choix de l'Arcep, plutôt que de la Cnil, pour superviser les dispositions relatives aux prestataires de services d'intermédiation des données (étude d'impact).

Si le rapporteur n'a pas disposé de suffisamment de temps pour vérifier que d'autres États membres effectuaient ou manifestaient l'intention d'effectuer un autre choix que la désignation de leur autorité de régulation

[1] *Groupe d'experts, présidé par la Commission européenne, qui se compose de représentants des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'ENISA, de la Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière.*

des télécommunications, il lui semble que l'Arcep était la mieux placée pour exercer ces fonctions, en raison de son expertise dans la régulation de l'économie numérique.

b) Un calendrier législatif tardif au regard des obligations européennes de la France, qui ne doit pas empêcher l'Arcep de se préparer dès aujourd'hui

Sur le papier, cette désignation intervient trop tard car il paraît désormais impossible, au regard de l'ordre du jour du Parlement français, que la nomination de l'Arcep ait lieu avant la date du 24 septembre 2023[1], correspondant à la date de pleine application du règlement européen sur la gouvernance des données.

Pour autant, l'intention exprimée par le Gouvernement à travers cet article 11, et celle qu'exprime également la commission spéciale en adoptant cet article sans modification, devraient donner à l'Arcep la prévisibilité dont elle a besoin pour anticiper l'entrée en vigueur du règlement européen et monter en compétences, en lien avec les premiers opérateurs déclarés (Agdatahub, Hub One, *etc.*).

c) L'émergence d'une véritable économie de la donnée nécessite une mise en adéquation des moyens de régulation

De simple composante de secteurs économiques établis, les données sont en train de devenir un secteur à part entière, donnant lieu à l'émergence d'une véritable « économie de la donnée ». Il devient urgent, selon le rapporteur, de calibrer les moyens à la hauteur de l'enjeu énorme que ce nouveau secteur représente pour la société.

À l'instar de l'ensemble des autres missions créées au titre III du présent projet de loi, les nouvelles missions de régulation des SID devront aller de pair avec des moyens budgétaires et humains renforcés pour les autorités chargées de les contrôler.

Cela vaut évidemment au premier chef pour l'Arcep, dont les besoins humains pourraient s'élever, **au minimum** à trois équivalents temps plein dès 2024, et un quatrième en 2025, pour un montant budgétaire associé de 80 000 euros par ETP (soit **320 000 euros par an d'ici deux ans**), pour la seule **montée en compétences dans la régulation des services d'intermédiation de données (SID[2]). Il s'agit, du reste, d'une obligation résultant du paragraphe 5 de l'article 26 du règlement européen sur la gouvernance des données** (« *Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données disposent des ressources humaines et*

[1] *Fixée à l'article 13 (1) du règlement européen sur la gouvernance des données.*

[2] *Auxquels il faut ajouter au minimum trois équivalents temps plein dès 2014, et trois supplémentaires en 2025, pour un montant identique par ETP (soit 480 000 euros par an d'ici deux ans) pour mettre en œuvre l'interopérabilité et la portabilité des services d'informatique en nuage.*

financières suffisantes, y compris des connaissances et ressources techniques nécessaires, pour mener à bien les tâches qui leur sont assignées »).

Le rapporteur veillera tout spécialement, dès le prochain projet loi de finances, à la mise en adéquation des moyens budgétaires et humains avec les nouvelles missions confiées à l'Arcep et autres autorités.

La commission spéciale a adopté l'article 11 **sans modification**.

Article 12

Champ de compétences et pouvoirs de l'Arcep en matière de régulation des services d'intermédiation de données

L'article 12 du projet de loi établit les pouvoirs de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) en matière d'enquête et d'accès aux données, dans le cadre de sa nouvelle mission de régulation des prestataires de services d'intermédiation de données (SID). Si ces pouvoirs sont étendus, ils sont justifiés par la nature stratégique des données échangées et par la nécessité de garantir la confiance des opérateurs publics et privés sur le nouveau marché européen de la donnée.

La commission a adopté cet article 12 sans modification.

1. Le règlement sur la gouvernance européenne des données consacre en même temps qu'il régule un nouvel acteur de l'économie de la donnée, les services d'intermédiation de données (SID)

Les prestataires de services d'intermédiation de données sont un nouveau type d'acteurs du marché européen numérique, institué par le règlement européen sur la gouvernance des données[1] dans le but d'établir une concurrence équitable sur le marché des données, en particulier industrielles et commerciales.

Il s'agit de plateformes ne pouvant **ni collecter, ni traiter** de données, **mais jouant le rôle de tiers de confiance pour l'échange**, monétisé ou non, de données brutes entre offreurs – opérateurs en particulier économiques pouvant disposer, par exemple, de fichiers clients – et demandeurs – acteurs procédant à du traitement de données pour leur activité propre ou pour offrir des prestations de service à d'autres opérateurs.

[1] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.*

La réglementation encadrant l'activité de ces services d'intermédiation de données (SID) étant intégralement nouvelle et entrant en application le 24 septembre 2023, **aucune autorité n'est à ce jour compétente pour leur contrôle.**

Le présent projet de loi prévoit qu'en France, c'est à l'**Arcep** que revient le soin de contrôler cette activité, en raison de son expertise dans la régulation de l'économie numérique.

La **base juridique** des sanctions pouvant être prononcées à l'encontre des prestataires de SID qui ne respecteraient par les obligations résultant du chapitre III du règlement européen sur la gouvernance des données (« Exigences applicables aux services d'intermédiation de données[1] ») figure à **l'article 14 dudit règlement**.

Cet article confère aux autorités de régulation des prestataires de SID trois pouvoirs, à savoir ceux :

« *a) d'imposer, par le biais de procédures* ***administratives, des sanctions financières dissuasives****, pouvant comporter des astreintes et des sanctions avec effet rétroactif, d'engager des procédures* ***judiciaires*** *en vue d'infliger des* ***amendes****, ou les deux ;*

b) d'exiger un ***report du début de la fourniture*** *du service d'intermédiation de données ou une* ***suspension*** *de cette fourniture jusqu'à ce que les modifications des conditions demandées par l'autorité compétente en matière de services d'intermédiation de données aient été réalisées ;*

c) d'exiger la ***cessation de la fourniture*** *du service d'intermédiation de données dans le cas où il n'a pas été remédié à des* ***infractions graves ou répétées*** *malgré l'envoi d'une notification préalable conformément au paragraphe 3.* »

2. L'Arcep se voit dotée de pouvoirs d'enquête et d'accès aux données étendus, sur le modèle de ceux dont elle dispose déjà pour d'autres champs de sa compétence

Le I de l'article 12 établit les pouvoirs de l'Arcep dans le cadre de la nouvelle compétence qui lui est attribuée à l'article 11 en matière de régulation des prestataires de services d'intermédiation des données (SID)

Il est ainsi prévu que l'Arcep puisse **recueillir**, auprès de ces prestataires de SID, **tout document ou toute information « *nécessaires*** *pour s'assurer [du] respect [par ces acteurs] des exigences du chapitre III du règlement sur la gouvernance européenne des données ou dans les actes délégués pris pour son application*[2] ». En pratique, il pourrait s'agir, selon l'Arcep, « *des conditions*

[1] *En pratique, cela concerne en particulier la notification que ces prestataires de SID doivent envoyer à l'autorité compétente avant de pouvoir opérer sur ce marché (article 11 du règlement), et les quinze conditions fixées par l'article 12 du même règlement à leur activité.*

[2] *Aucun acte délégué n'est prévu pour l'heure, selon la Direction générale des entreprises.*

générales d'utilisation, des offres de référence, ou encore des certifications du niveau de sécurité des serveurs exploités par ces acteurs ».

Il est également prévu que l'Arcep puisse diligenter des enquêtes, aux mêmes conditions que pour ses pouvoirs d'enquête administrative actuels et pour ceux du ministre chargé des communications électroniques dans le secteur des communications électroniques, c'est-à-dire :

– par des agents habilités, assermentés, pouvant pénétrer dans les locaux d'une entreprise ou dans un véhicule professionnel entre 8 heures et 20 heures, et pouvant accéder aux logiciels, programmes informatiques et aux données stockées, et ne pouvant se voir opposer le secret professionnel[1] – l'autorité devant toutefois veiller à ce que ne soient pas divulguées les informations couvertes par ce secret ;

– et, lorsque les locaux ou une partie de ceux-ci constituent un domicile, après ordonnance du juge des libertés et de la détention du tribunal compétent et sous son autorité, en présence de l'occupant des lieux, de son représentant ou d'au moins deux témoins[2].

Enfin, ce même I définit également les limites des nouvelles compétences de l'Arcep, l'autorité ne pouvant faire usage de ses prérogatives que « ***de manière proportionnée aux besoins liés à l'accomplissement de ses missions, et sur la base d'une décision motivée*** », sur le modèle de ce qui existe pour ses pouvoirs de régulation dans d'autres domaines[3], ce qui revient en pratique à lui confier un pouvoir important.

Le II du présent article prévoit que l'Arcep peut se saisir d'office de tout manquement d'un prestataire de SID au chapitre III du règlement sur la gouvernance des données. Il est également prévu que « toute personne concernée » peut saisir l'Arcep, ce qui inclut « *notamment le ministre chargé des communications électroniques, une organisation professionnelle ou une association agréée d'utilisateurs* », par cohérence avec le droit existant[4], liste les personnes susceptibles de saisir l'Arcep.

Les sanctions sont les mêmes que celles pouvant actuellement être prononcées par l'Autorité[5], à l'exception de deux points, pour rester conforme au règlement européen sur la gouvernance des données[6] :

– le délai de mise en conformité par le prestataire de SID est fixé à trente jours (au lieu d'être librement déterminé par l'Arcep) ;

– les trois derniers alinéas se contentent de reprendre la typologie des sanctions prévue par l'article 14 du règlement européen, en précisant que

---

[1] *Article L. 32-4 du code des postes et des communications électroniques.*
[2] *Article L. 32-5 du même code.*
[3] *Article L. 32-4 du même code.*
[4] *Article L. 36-11 du même code.*
[5] Idem.
[6] *Article 14, paragraphes 4 à 6 du règlement.*

la sanction pécuniaire ne peut excéder 3 % du chiffre d'affaires mondial hors taxes du dernier exercice clos (5 % en cas de nouvelle violation de la même obligation), ou 150 000 euros en cas d'absence de chiffre d'affaires (375 000 euros en cas de nouvelle violation de la même obligation dans les cinq ans).

3. Des pouvoirs étendus se justifiant par la nécessité de garantir la confiance dans les données échangées

Le rapporteur Patrick Chaize constate que l'article 12 du projet de loi institue **un large champ de compétences pour l'Arcep dans l'exercice de ses nouvelles missions**, lui laissant des marges de manœuvre importantes, gage d'une régulation efficace.

Pour autant, ces larges pouvoirs apparaissent justifiés par la nécessité de garantir la confiance dans ce nouveau type d'acteurs, par des moyens effectifs de constater des manquements et des sanctions suffisamment dissuasives.

Du reste, le cadre prévu pour la régulation des prestataires de SID ne diffère pas de celui déjà en vigueur pour les autres missions de l'Arcep. Les sanctions sont même davantage encadrées (trois derniers alinéas de l'article 12) dans ce contexte, afin de respecter les termes du règlement européen sur la gouvernance des données.

En outre, la majoration des sanctions en cas de « récidive » n'est encourue que pendant un délai de cinq ans à compter du premier manquement pour les prestataires de SID sans chiffre d'affaires et donc sans activité. Ce délai de cinq ans, sorte de « remise à zéro » pour des prestataires non encore professionnalisés, est institué pour ne pas pénaliser un secteur encore balbutiant, dans une logique de « droit à l'erreur ».

Le rapporteur rappelle enfin **l'exigence de proportionnalité** de la sanction à la gravité du manquement et au regard du cas d'espèce, à laquelle l'Arcep reste soumise, en ce domaine comme en d'autres.

Il **se félicite donc de ces larges pouvoirs conférés à l'Arcep** et rappelle qu'ils supposent, pour avoir un effet utile, une mise à niveau des moyens budgétaires et humains de l'autorité, de nature à permettre une mise en œuvre complète du règlement européen sur la gouvernance des données.

La commission spéciale a adopté l'article 12 **sans modification**.

Article 13

Articulation des compétences de l'Arcep et de la Cnil, s'agissant des données à caractère personnel, dans le cadre de la régulation par l'Arcep des services d'intermédiation de données

L'article 13 établit les modalités de consultation de la Commission national de l'informatique et des libertés (Cnil) par l'Autorité de Régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), dans le cadre de la nouvelle mission de celle-ci en matière de régulation des services d'intermédiation de données (SID).

Suivant l'analyse du rapporteur Patrick Chaize, la commission spéciale a souhaité maintenir une coopération souple entre l'Arcep et la Cnil, consacrant la première comme seule autorité compétente pour la régulation des SID. Le règlement européen sur la gouvernance des données s'applique en effet sans préjudice du règlement général sur la protection des données (RGPD), duquel la Cnil tient directement ses pouvoirs.

La commission spéciale a adopté cet article 13 après avoir adopté deux amendements du rapporteur de nature rédactionnelle, clarifiant la nature de la consultation de la Cnil, sans modifier l'économie générale de l'article.

1. Le règlement européen sur la gouvernance des données s'applique sans préjudice du règlement général sur la protection des données, duquel la Cnil directement ses pouvoirs

Les services d'intermédiation de données sont des services nouveaux, créés par le règlement européen sur la gouvernance des données[1], et pour lesquels le droit européen ne prévoit pas d'autorité de régulation *ad hoc*.

Le Gouvernement a donc fait le choix, à travers l'article 11 du présent projet de loi, de confier ce rôle de régulation à l'Arcep, en raison de la proximité de ses missions actuelles avec celles découlant du règlement, et de sa fine connaissance de l'économie numérique. Si la désignation d'une autorité est une obligation, le choix de l'Arcep ne résultait pas d'une obligation européenne, et l'étude d'impact révèle qu'il a également été envisagé de confier cette mission à la Cnil.

Le règlement européen sur la gouvernance des données, et le choix retenu pour son application, **ne privent pas les autres autorités administratives existantes de leurs compétences**, que ce soit l'Autorité de la concurrence et la Commission européenne en matière de droit de la concurrence, ou la Cnil s'agissant de protection des données à caractère

[1] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.*

personnel. Cela est rappelé à de multiples reprises, dans les considérants et dans le dispositif dudit règlement :

– « *le présent règlement ne devrait pas être lu comme créant une nouvelle base juridique pour le traitement des données à caractère personnel dans le cadre de l'une des activités réglementées, ni comme modifiant les exigences en matière d'information prévues par le [RGPD]*[1] » ;

– « *lorsque les prestataires de services d'intermédiation de données traitent des données à caractère personnel, le présent règlement ne devrait pas avoir d'incidence sur la protection de ces données*[2] » ;

– « *le présent règlement est* ***sans préjudice*** *des règlements (UE) 2016/679 et (UE) 2018/1725 et des directives 2002/58/CE et (UE) 2016/680, y compris en ce qui concerne les pouvoirs et compétences des autorités de contrôle.* ***En cas de conflit*** *entre le présent règlement et les dispositions du droit de l'Union en matière de protection des données à caractère personnel ou du droit national adopté conformément audit droit de l'Union,* ***les dispositions pertinentes du droit de l'Union ou du droit national en matière de protection des données à caractère personnel prévalent****. Le présent règlement ne crée pas de base juridique pour le traitement des données à caractère personnel et ne modifie pas les droits et obligations énoncés dans le règlement (UE) 2016/679 ou (UE) 2018/1725 ou dans la directive 2002/58/CE ou (UE) 2016/680*[3]*. »*

Cette articulation est rappelée de la façon la plus explicite et la plus exhaustive à l'article 13 du règlement, qui dispose que « *les pouvoirs des autorités compétentes en matière de services d'intermédiation de données sont sans préjudice des* ***pouvoirs des autorités chargées de la protection des données, des autorités nationales de la concurrence, des autorités chargées de la cybersécurité et des autres autorités sectorielles concernées****. Dans le respect de leurs compétences respectives au titre du droit de l'Union et du droit national, ces autorités* ***établissent une coopération solide et échangent les informations qui sont nécessaires à l'accomplissement de leurs tâches en rapport avec les prestataires de services d'intermédiation de données, et visent à assurer la cohérence des décisions prises en application du présent règlement*** ».

2. Une institutionnalisation souple de la coopération entre l'Arcep et la Cnil s'agissant de la régulation des prestataires de services d'intermédiation de données

L'article 13 prévoit une saisine **obligatoire** de la Cnil par l'Arcep (« *avant* ***toute décision*** »), dès lors que certaines pratiques des SID sont « *de nature à soulever des questions liées à la protection des données personnelles* ».

---

[1] *Considérant 4 du règlement européen sur la gouvernance des données.*
[2] *Considérant 35 du même règlement.*
[3] *Article 1, paragraphe 3 du même règlement.*

Les alinéas 2 à 4 renvoient par ailleurs à un décret le soin de préciser les conditions dans lesquelles l'Arcep « *recueille, **le cas échéant**, les observations **éventuelles** de la Cnil* », qui doivent être formulées dans un délai de quatre semaines, dans deux circonstances particulières, qui résultent de la saisine de SID ou d'utilisateurs de SID :

– la Cnil peut d'abord être consultée **dans la procédure de reconnaissance officielle des opérateurs respectant les articles 11 et 12 du règlement européen sur la gouvernance des données**, qui se traduira concrètement par le droit d'utiliser la qualification « *prestataires de services d'intermédiation de données reconnu dans l'Union* » et d'arborer un logo commun attestant de cette qualité, créé par actes d'exécution de l'Union[1] ;

– elle peut ensuite être consultée **dans le cas où des utilisateurs de SID introduiraient une réclamation relative au champ d'application du règlement**[2] – par exemple, si un utilisateur souhaite limiter l'usage de données aux finalités consenties ou faire valoir son droit à l'accès de données à des conditions équitables et transparentes, comme le règlement le prévoit.

Les alinéas 5 et 6 formalisent les procédures d'information mutuelle entre la Cnil et l'Arcep :

– ainsi la Cnil est-elle en tout état de cause informée par l'Arcep, en cas de demande de labellisation par un SID ou de recours sur le champ d'application du règlement par un utilisateur ;

– dans ces deux mêmes cas, l'Arcep communique à la Cnil, dans des conditions fixées par décret, « *toute information utile [lui] permettant de formuler ses observations éventuelles sur les questions liées à la protection des données à caractère personnel* » dans le délai imparti de quatre semaines. Elle tient obligatoirement informée la Cnil des suites données à la procédure, le cas échéant ;

– en sens inverse, il est prévu que la Cnil communique « des faits » dont elle a connaissance et qui pourraient constituer des manquements à l'une des quatorze obligations de l'article 12 du règlement (tenue d'un journal d'activité, information en cas de transfert, d'accès ou d'utilisation non autorisés, prévention des pratiques frauduleuses, interopérabilité…).

3. Maintenir une coopération souple entre l'Arcep et la Cnil, consacrant l'Arcep comme seule autorité compétente pour la régulation des SID

Le rapporteur observe que l'attribution de compétences à l'Arcep en matière de régulation des prestataires de SID, avec simple consultation facultative de la Cnil, se justifie par la **nature essentiellement industrielle et**

---

[1] *Article 11, paragraphe 9 du règlement européen sur la gouvernance des données.*

[2] *Cette disposition vient préciser l'article 27 du règlement, qui prévoit la possibilité de telles réclamations.*

commerciale des données échangées *via* ces nouvelles plateformes. Le choix a été fait de laisser à l'Arcep le soin de déterminer si certaines pratiques de prestataires de SID « *sont de nature à soulever des questions liées à la protection des données personnelles* », une qualification relativement souple et laissée à l'appréciation de cette autorité.

Bien que la Cnil souligne la difficulté qui peut se faire jour au sujet de certaines données à caractère personnel indissociables de données industrielles ou commerciales, l'Arcep a indiqué dans sa contribution écrite être « *attachée à la pleine mise en œuvre des mécanismes de coopération institués dans le texte […], dans le respect des prérogatives de chacune* » et avoir pour objectif de « *retenir une interprétation large de cette disposition, en n'excluant de la transmission que des documents qui seraient manifestement sans impact sur la question des données personnelles* ».

Surtout, le règlement européen sur la gouvernance des données, d'application directe, prévoit déjà explicitement que les activités des SID devront, en tout état de cause, respecter le règlement général sur la protection des données (RGPD). La Cnil tient ses pouvoirs en matière de protection des données personnelles, indépendamment du présent article, directement du RGPD, qui introduit, du reste, un régime de responsabilisation des détenteurs de données et non un régime de contrôle *a priori*.

Une saisine systématique ou un avis conforme pourraient même produire des situations fâcheuses dans lesquelles il serait considéré, à tort, que la position de la Cnil serait révélée par son avis rendu à l'Arcep.

Le rapporteur souhaite en outre rappeler les possibilités offertes à la Cnil, par l'article 1er de la loi pour une République numérique[1], de demander à d'autres administrations la communication de documents utiles à l'accomplissement de ses missions.

Pour ces différentes raisons, si **le rapporteur salue dans cet article l'institutionnalisation d'un principe de bonne coopération entre autorités administratives** – qui va au-delà des obligations européennes et aurait pu faire l'objet de simples lignes directrices –, **il ne juge pas opportun d'alourdir davantage la procédure de consultation de la Cnil par l'Arcep.**

Une surrèglementation pourrait en effet pénaliser les prestataires de SID français par rapport à leurs concurrents européens.

Le rapporteur préfère donner toute ses chances en France à un modèle de partage des données original et, en soi, protecteur de la vie privée – en ce qu'il constitue un contre-modèle à l'intégration verticale du marché de la donnée par des acteurs cumulant la collecte, l'échange et le traitement des données.

---

[1] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.*

Afin de lever toute ambiguïté sur la nature de la consultation de la Cnil prévue au présent article, et sans remettre en cause l'économie générale de l'article 13, le rapporteur a toutefois souhaité proposer quelques clarifications rédactionnelles par l'amendement **COM-119**, adopté par la commission :

– il a d'abord jugé indispensable de préciser que l'Arcep devra non seulement « recueillir », mais « tenir compte » des éventuelles observations de la Cnil, lorsqu'elles ont été rendues, Cette formulation n'introduit pas un avis conforme, la saisine restant facultative, et laisse des marges de manœuvre importantes à l'Arcep ;

– le rapporteur souhaite que l'ensemble des faits (« *les* faits » et non « *des* faits ») dont la Cnil a connaissance et qui pourraient constituer des manquements de SID à leurs obligations au regard du règlement européen sur la gouvernance des données, soient communiqués à l'Arcep, afin de permettre à cette dernière d'exercer sa compétence en pleine connaissance de cause.

Dans les deux cas, la clarification ne fait que rappeler le droit européen applicable et consacrer la compétence des deux autorités, chacune dans le domaine qui la concerne.

Enfin, l'amendement **COM-120** du rapporteur, procédant à des précisions purement rédactionnelles, a été adopté par la commission spéciale.

La commission spéciale a adopté l'article 13 **ainsi modifié**.

Article 14

Coordinations juridiques au sein du code des postes et des communications électroniques

L'article 14 procède à de simples coordinations au sein du code des postes et des communications électroniques, afin de permettre la bonne articulation des nouvelles dispositions résultant du titre III du présent projet de loi, avec le droit existant.

La commission spéciale a adopté cet article 14 après avoir adopté l'amendement **COM-121** du rapporteur Patrick Chaize de précision juridique.

1. La nécessité de rattacher les nouvelles sanctions que l'Arcep pourra prendre en application de sa nouvelle compétence sur l'informatique en nuage et les SID à une formation existante de l'autorité

L'article L. 130 du code des postes et des communications électroniques définit le statut d'autorité administrative indépendante de l'Arcep, établit la composition de ses différentes formations (plénière et restreinte), énumère les compétences échues à l'une ou l'autre de ces formations, ainsi que les possibles sanctions qu'elles peuvent respectivement prononcer.

Le cinquième alinéa de cet article prévoit que **la formation restreinte de l'Arcep** « *est chargée de prononcer les sanctions dans les conditions prévues* » à trois articles existants (articles L. 5-3 et L. 36-11 du code des postes et des communications électroniques et article 24 de la loi sur la distribution de la presse[1]).

Cela ne couvre donc pas les nouvelles sanctions instituées par ce projet de loi, résultant des règles européennes relatives à l'informatique en nuage et du règlement sur la gouvernance des données.

Les modalités de ces sanctions, essentielles pour assurer l'effectivité de ces textes européens, doivent donc être clairement fixées en droit interne.

2. Un renvoi juridique manifestement erroné

Dans la version déposée par le Gouvernement sur le bureau du Sénat, l'unique alinéa de l'article 14 prévoit de rattacher à la formation restreinte de l'Arcep les sanctions « *prévues au deuxième alinéa du II de l'article 10* » du présent projet de loi, qui **en réalité ne portent pas sur des sanctions, mais sur le règlement des litiges**.

3. Un amendement de précision juridique pour corriger cette erreur et réparer un oubli

Le rapporteur a proposé l'amendement **COM-121** de précision juridique à la commission spéciale, qu'elle a adopté.

Cet amendement permet de bien viser, à l'alinéa établissant les pouvoirs de la formation de l'Arcep, les conditions prévues au deuxième alinéa du III de l'article 10 du présent projet de loi, c'est-à-dire celui qui porte sur les sanctions dans le cadre de la régulation de l'informatique en nuage.

Il permet en outre de viser, au même alinéa de l'article L. 130 du code des postes et des communications électroniques, les sanctions prévues aux

[1] *Loi n° 47-585 du 2 avril 1947 relative au statut des entreprises de groupage et de distribution des journaux et publications périodiques.*

huitième à onzième alinéas de l'article 12 du présent projet de loi, c'est-à-dire celles prévues pour l'application du règlement européen sur la gouvernance des données.

Le rapporteur n'a pas d'autres observations à formuler sur cet article de simple coordination juridique.

La commission spéciale a adopté l'article 14 **ainsi modifié**.

TITRE IV
ASSURER LE DÉVELOPPEMENT EN FRANCE DE L'ÉCONOMIE DES JEUX NUMÉRIQUES MONÉTISABLES DANS UN CADRE PROTECTEUR

Article 15
Encadrement des jeux à objets numériques monétisables

L'article 15 a pour objectif d'habiliter le Gouvernement à légiférer par voie d'ordonnance afin de définir et de fixer le cadre de contrôle et de régulation des jeux à objets numériques monétisables (Jonum).

La commission a adopté un amendement du rapporteur Patrick Chaize supprimant l'habilitation à légiférer par voie d'ordonnance. Ainsi amendé, cet article propose, pour la première fois en droit, une définition des Jonum et ainsi qu'une autorisation, à titre expérimental, de ce nouveau type de jeux, tout en s'assurant que cette expérimentation soit suffisamment protectrice contre les effets de bord et les risques pour l'ordre public et social, la santé des usagers et les mineurs.

1. Le droit en vigueur : les Jonum, nouveaux jeux en ligne à la croisée des jeux de loisirs et des jeux d'argent et de hasard, ne sont pour le moment pas définis juridiquement ni régulés en droit français

a) Les Jonum, de nouveaux jeux hybrides entre les jeux vidéo et les jeux d'argent et de hasard en ligne

1. Des jeux en ligne issus des technologies du Web 3…

Les évolutions numériques sont sources de nombreuses innovations : le Web 3 et son organisation décentralisée ont ainsi permis l'émergence de la *blockchain*, des crypto-actifs et des jetons non fongibles, et sont un levier de développement pour le secteur des jeux vidéo et des jeux en ligne et, plus largement, pour l'économie toute entière.

Un nouveau type de jeux en ligne se fondant sur ces technologies s'est ainsi développé, dans lesquels est proposé l'achat d'objets numériques, nécessaires à la participation et à la progression dans le jeu. Ces objets numériques ont la particularité d'être identifiés par un certificat attestant de leur authenticité et d'être monétisables. Ces jeux à objets numériques monétisables (Jonum), aussi dénommés jeux *Play to earn* (jouer pour gagner de l'argent) offrent en effet la possibilité de revendre ces objets à des tiers, sur la plateforme de l'éditeur du jeu ou sur une place de marché secondaire.

De très nombreux jeux *Play to earn* sont en cours de développement en France et dans le monde. L'autorité nationale des jeux (ANJ) estime qu'entre 1 200 et 2 500 jeux *Play to earn* sont en phase de développement, sachant que douze milliards de dollars ont été investis en 2022 dans ces technologies. S'agissant du secteur français, l'ANJ recense quinze jeux de ce type développés ou en cours d'élaboration en 2022.

Glossaire

Web 3 : Troisième génération d'Internet succédant au Web 1.0 et 2.0, avec une organisation décentralisée reposant sur la *blockchain*.

Blockchain : La *blockchain* – chaîne de blocs – est une technologie de stockage et de transmission d'informations sous forme de blocs liés les uns aux autres et protégés contre toute modification.

Actif numérique : actif constitué par des données numériques, dont la propriété ou le droit d'usage est un élément du patrimoine d'une personne physique ou morale. Les actifs numériques sont définis par la loi à l'article L. 54-10-1 du code monétaire et financier.

Jeton non fongible (JNF) : un jeton non fongible – *non fongible token (NFT)* en anglais – est un fichier numérique auquel est attaché un certificat d'authenticité numérique. Ce jeton est stocké sur une *blockchain* et représente un actif unique, qui ne peut être échangé par un autre, il est ainsi non fongible.

2 … à la croisée des jeux d'argent et des jeux vidéo…

Les Jonum empruntent des caractéristiques à la fois aux jeux vidéo, définis à l'article 220 *terdecies* du code général des impôts, et aux jeux d'argent et de hasard, définis aux articles L. 320-1 et suivants du code de la sécurité intérieure.

Les jeux vidéo sont définis comme tout « *logiciel de loisir mis à la disposition du public sur un support physique ou en ligne intégrant des éléments de création artistique et technologique, proposant à un ou plusieurs utilisateurs une série d'interactions s'appuyant sur une trame scénarisée ou des situations simulées et se traduisant sous forme d'images animées, sonorisées ou non.* ». Ainsi, dès lors qu'un Jonum répond à ces caractéristiques, il peut être légitimement assimilé à un jeu vidéo.

Toutefois, les Jonum peuvent également réunir plusieurs des caractéristiques des jeux d'argent et de hasard, définis à l'article L. 320-1 du code de la sécurité intérieure comme : « *toutes* ***opérations offertes au public****, sous quelque dénomination que ce soit, pour faire naître* ***l'espérance d'un gain*** *qui serait* ***dû, même partiellement, au hasard*** *et pour lesquelles* ***un sacrifice financier est exigé*** *de la part des participants*. ».

En France, l'encadrement des jeux d'argent et de hasard est très strict : ces jeux sont interdits, sauf s'ils figurent sur la liste des dérogations à l'interdiction inscrite à l'article L. 320-6 du code de la sécurité intérieure. Si un Jonum est assimilé à ces jeux, il sera dès lors interdit et considéré comme illégal.

3 … et qui présentent des risques similaires

Les Jonum sont susceptibles de présenter des risques similaires aux risques associés aux jeux d'argent et de hasard et, dans une moindre mesure, à ceux associés aux jeux vidéo, tant pour la société que pour les usagers.

Ces jeux peuvent présenter des risques de jeu excessif ou pathologique, au même titre que les jeux d'argent et de hasard, les paris financiers et les jeux vidéo. Ces risques ont été documentés par plusieurs études : le taux de prévalence du jeu d'argent et de hasard problématique est de 6 % en France, et s'élève à 33 % pour les jeux en ligne selon les études de l'observatoire des jeux (ODJ)[1] et de l'observatoire français des drogues et des tendances addictives (OFDT)[2]. Les jeux de *fantasy* présentent également un taux important de jeu problématique selon une étude du *Rutgers Center (New Jersey)*[3], estimé à 41,4 %.

En deuxième lieu, ces jeux peuvent également entraîner des risques de fraude, dès lors que les objets numériques sont cédés à titre onéreux : *hacking* des porte-monnaie numériques stockant les objets numériques monétisables, manipulation artificielle de la valeur d'un JNF en créant l'illusion d'une forte demande *(wash trading)*, blanchiment d'argent ou encore risques de financement du terrorisme en raison du caractère décentralisé de la *blockchain* et de l'absence de vérification de l'identité des parties.

En dernier lieu, **ces nouveaux jeux, sans encadrement adéquat, peuvent aussi présenter des risques de contournement des interdictions de jeux d'argent et de hasard en proposant une offre détournée de casino en ligne sous forme de Jonum**.

---

[1] *Costes, J-M., Richard, J-B. et Eroukmanoff, V., Les problèmes liés aux jeux d'argent en France en 2019, Les notes de l'Observatoire des Jeux n°12, Juin 2020.*

[2] *Eroukmanoff, V., Brissot, A., Philippon, A. et Spilka, S., Pratiques de jeux d'argent et de hasard sur Internet, Tendance n°152 de l'Observatoire français des drogues et des conduites addictives, Octobre 2022.*

[3] *Nower, L., Volberg, R.A., Caler, K.R , The Prevalence of Online and Land-Based Gambling in New Jersey., 2017.*

b) Il n'existe actuellement pas d'encadrement de ces jeux

Actuellement il n'existe pas de définition juridique ni de cadre de régulation pour ces nouveaux types de jeux. S'ils réunissent les quatre critères constitutifs d'un jeu d'argent et de hasard, alors ils doivent être considérés comme des jeux d'argent et de hasard en ligne illégaux, sauf si les éditeurs de ces jeux justifient de l'une des dérogations prévues à l'article L. 320-6 du code la sécurité intérieure. À ce jour, aucune entreprise de jeu proposant une offre de Jonum ne justifie d'une de ces dérogations.

Certains éditeurs de jeu, alertés par l'ANJ du risque de voir leur offre de jeu considérée comme une offre illégale de jeu en ligne, ont fait évoluer leur offre en faisant soit disparaître le sacrifice financier en renforçant leur offre gratuite, soit en supprimant le caractère patrimonial du gain.

Il n'existe pas de cadre européen pour ces jeux d'un nouveau genre. En effet, le droit des jeux d'argent et de hasard est régi par le principe de subsidiarité en l'absence de droit dérivé, et il n'existe pas de règles spécifiques applicables aux Jonum. L'Espagne et Malte suivent la même démarche que le France et ont annoncé vouloir encadrer ces jeux.

2. Le dispositif envisagé : une habilitation à légiférer par ordonnance

L'article 15 du projet de loi contient une habilitation du Gouvernement à légiférer par voie d'ordonnance dans un délai de quatre mois à compter de la promulgation de la loi. Cet habilitation ne comporte ni définition, ni ébauche du cadre de régulation et de contrôle des Jonum.

La commission spéciale et son rapporteur considèrent qu'en l'état cet article est une « coquille vide ».

3. La position de la commission : les caractéristiques des Jonum imposent de soumettre leur définition et la construction de leur cadre réglementaire à l'examen parlementaire

a) La nécessité de se saisir du sujet

L'émergence des Jonum et la multiplication de l'offre est source d'inquiétude pour les secteurs du jeu en ligne et du jeu vidéo. Faute de définition juridique claire, l'assimilation actuelle des Jonum à des jeux d'argent et de hasard laisse craindre une paralysie de l'innovation du secteur, au détriment des acteurs du jeu français. **Ce cadre très restrictif n'est pas conçu pour ces Jonum encore en cours de développement. De même, le cadre de régulation des jeux vidéo, très souple, n'est pas adapté à ces nouveaux jeux** qui peuvent présenter des risques pour l'ordre public, la santé et les mineurs.

Le rapporteur, considérant comme inacceptable le recours à une habilitation à légiférer par ordonnance sur un tel sujet, a décidé de s'en saisir. La première étape consiste à définir les Jonum et à les autoriser dans un cadre expérimental, afin d'évaluer la nécessité d'une tierce régulation dédiée aux Jonum.

Le cadre expérimental est ainsi adapté, car permettant de favoriser l'innovation d'un secteur particulièrement dynamique en France – le jeu vidéo représente par exemple plus de cinq milliards d'euros de chiffre d'affaires en France et 18 000 emplois – tout en évitant les effets de contournement que peuvent constituer ces jeux ainsi que les risques identifiés pour l'ordre public, la santé et les mineurs.

b) Une première définition inédite des Jonum et un cadre expérimental d'autorisation

La commission a ainsi adopté l'amendement COM-122 du rapporteur, qui supprime l'habilitation à légiférer par ordonnance, définit pour la première fois en droit les Jonum et pose la première pierre d'un éventuel nouveau cadre de régulation dédié à ces jeux, qui ne sera ni le cadre des jeux d'argent et de hasard, ni celui des jeux vidéo.

Cette nouvelle rédaction autorise les Jonum à titre expérimental pour une durée de trois ans à compter de la promulgation du projet de loi.

Les Jonum sont définis comme « *des jeux proposés par l'intermédiaire d'un service de communication au public en ligne qui permettent l'obtention, reposant sur un mécanisme faisant appel au hasard, par les joueurs ayant consenti un sacrifice financier, d'objets numériques monétisables, à l'exclusion de tout gain monétaire* ».

Il est ainsi considéré que les Jonum réunissent trois des quatre critères de définition d'un jeu d'argent et de hasard : l'offre au public, le sacrifice financier, et la présence d'un mécanisme faisant appel au hasard.

Les objets numériques monétisables visés doivent conférer aux joueurs des droits associés au jeu et être cessibles ou échangeables : **les jeux vidéo comportant des objets numériques ne pouvant être cédés ou échangés à titre onéreux, c'est-à-dire évoluant dans une « boucle fermée » dans le jeu vidéo sans possibilité de monétisation à l'extérieur du jeu, ne sont pas concernés par cette tierce législation**.

Afin d'éviter un contournement des interdictions de jeux d'argent et de hasard en ligne – notamment l'interdiction des jeux de casino en ligne – la définition précise que ces objets numériques monétisables ne peuvent être cédés à toute entreprise de jeu, et ce directement ou indirectement. De plus, ces objets numériques ne peuvent constituer des cryptoactifs au sens du 2° de l'article L. 54-10-1 du code monétaire et financier, c'est-à-dire des crypto monnaies.

L'amendement du rapporteur précise que les entreprises de jeu poursuivent, en grande partie, des objectifs similaires à ceux de l'État en matière de jeux d'argent et de hasard (inscrits à l'article L. 320-3 du code de la sécurité intérieure), à savoir : prévenir le jeu excessif ou pathologique et protéger les mineurs, assurer l'intégrité, la fiabilité et la transparence des opérations de jeu, prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment de capitaux et le financement du terrorisme.

Enfin, un rapport rendant compte des conclusions de l'expérimentation et de la pertinence de sa poursuite devra être remis au Parlement six mois avant la fin de l'expérimentation.

La commission spéciale a adopté l'article 15 **ainsi modifié**.

TITRE V
PERMETTRE À L'ÉTAT D'ANALYSER PLUS EFFICACEMENT L'ÉVOLUTION DES MARCHÉS NUMÉRIQUES

Article 16

Élargissement des pouvoirs de collecte des données par le Pôle d'expertise de la régulation du numérique pour des activités de recherche publique

L'article 16 vise à renforcer les capacités de collecte de données du Pôle d'expertise de la régulation numérique (PEReN) pour ses activités de recherche publique, notamment à des fins de détection des risques systémiques au sein de l'Union européenne.

La commission a adopté l'article, modifié par trois amendements du rapporteur Patrick Chaize, afin de sécuriser l'accès du PEReN aux données des très grandes plateformes et des très grands moteurs de recherche en ligne et d'étendre la durée de conservation de ces données.

1. Une extension nécessaire des compétences du PEReN en matière de collecte de données à des fins de recherche publique

a) Les compétences du PEReN

Le pôle d'expertise de la régulation numérique est un service à compétence nationale institué par le décret n° 2020-1102 du 31 août 2020 portant création d'un service à compétence nationale dénommé Pôle d'expertise de la régulation numérique (PEReN). Placé sous l'autorité conjointe des ministres chargés de l'économie, de la communication et du

numérique, le PEReN est administrativement rattaché à la direction générale des entreprises (DGE) du ministère de l'économie, des finances et de la souveraineté industrielle et numérique.

Ce service est chargé d'«*appuyer les services de l'État intervenant dans la régulation des plateformes numériques, dans leurs travaux de conception, de mise en œuvre et d'évaluation de cette régulation* ». Le PEReN met ainsi à disposition de l'État une expertise et une assistance technique générales et fournit une contribution et une expertise techniques dans le cadre de contrôles, enquêtes ou études menés sur les plateformes numériques.

Les compétences du PEReN sont précisées à l'article 36 de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique. Le PEReN est ainsi investi de deux missions principales : d'une part, la conduite d'expérimentations visant à utiliser, concevoir ou évaluer des outils techniques portant sur la régulation des opérateurs de plateforme en ligne et, d'autre part, la conduite d'activités de recherche publique.

Le PEReN collabore également avec huit autorités administratives indépendantes, dont la liste est fixée par décret du 21 avril 2022. Il s'agit de l'Autorité de la concurrence (ADLC), l'Autorité des marchés financiers (AMF), l'Autorité nationale des jeux (ANJ), l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), l'Autorité de régulation des transports (ART), la Commission nationale de l'informatique et des libertés (Cnil) et du Défenseur des droits.

Selon le directeur adjoint du PEReN entendu par la commission spéciale le 12 juin[1], il n'existe pas, à l'heure actuelle, de service similaire dans les autres pays membres de l'Union européenne, mais un centre européen pour la transparence algorithmique devrait prochainement ouvrir à Séville. La mutualisation des compétences du PEReN avec les services de l'État et les autorités administratives indépendantes est inédite au sein de l'Union européenne, et source d'inspiration pour la Commission européenne.

b) Le dispositif envisagé

L'article 16 du projet de loi modifie l'article 36 de la loi du 25 octobre 2021 fixant les compétences du PEReN pour la poursuite de ses activités d'expérimentation et de recherche publique.

Comme pour ses activités d'expérimentation, **le PEReN agira désormais en *qualité* de responsable de traitement au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pour ses activités de recherche publique, ce qui étend ses**

[1] https://www.senat.fr/compte-rendu-commissions/20230612/cs_num.html#toc3

compétences de collecte de données. Dès lors, il ne pourra se voir refuser l'accès aux données publiquement accessibles à des fins de recherche publique, déjà garanti pour ses activités d'expérimentation au cinquième alinéa de l'article 36.

Les activités de recherche du PEReN sont également spécifiées. En effet, le PEReN conduira ses activités « *notamment à des fins de recherches contribuant à la détection, à la détermination et à la compréhension des risques systémiques dans l'Union* ». Ces risques systémiques découlant de la conception ou du fonctionnement des services des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne sont précisés à l'article 34, paragraphe 1 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (RSN). Il s'agit de :

– la diffusion de contenus illicites par l'intermédiaire des services de ces plateformes ;

– tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, en particulier du droit fondamental à la dignité humaine, au respect de la vie privée et familiale, à la protection des données à caractère personnel, à la liberté d'expression et d'information, des droits fondamentaux relatifs aux droits de l'enfant et du droit fondamental à un niveau élevé de protection des consommateurs ;

– tout effet négatif réel ou prévisible sur le discours civique, les processus électoraux et la sécurité publique ;

– tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes.

La spécification des activités de recherche publique du PEReN est essentielle afin de lui donner accès au statut de chercheur au sens de l'article 40, paragraphe 2, du RSN (voir *infra*) et de lui assurer l'accès aux données publiques des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne prévu à ce même article. Cet accès – qui porte uniquement sur les activités de recherche publique du PEReN – est formalisé par une inscription au sixième alinéa de l'article 36 de la loi du 25 octobre 2021 afin de le sécuriser juridiquement. Selon l'article 40, paragraphe 12, du RSN, ces plateformes en ligne devront donner accès au PEReN « *sans retard injustifié, aux données, y compris, lorsque cela est techniquement possible, aux données en temps réel, à condition que ces données soient publiquement accessibles sur leur interface en ligne* ».

Le PEReN est-il considéré comme chercheur agrée au sens du RSN ?

Si le PEReN est enregistré au registre national des services de recherche (RNSR), le service ne peut obtenir le statut de chercheur agréé au sens de l'article 40 paragraphe 4 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (RSN).

Ce statut de chercheur agréé permet d'avoir un accès étendu aux données (publiques ou non) des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne. Ce statut de chercheur est attribué projet par projet par le coordinateur pour les services numériques, si sept conditions cumulatives listées à l'article 40, paragraphe 8, du RSN sont remplies. Le PEReN ne remplit cependant pas l'une des conditions, imposant d'être affilié « *à un organisme de recherche tel qu'il est défini à l'article 2, point 1), de la directive (UE) 2019/790* », c'est-à-dire une « *entité ayant pour objectif premier de mener des recherches scientifiques, ou d'exercer des activités éducatives comprenant également des travaux de recherche scientifique* ». Le PEReN ne menant pas de recherches scientifiques ou d'activités éducatives comprenant de tels travaux, il ne peut bénéficier de ce statut de chercheur agréé.

Le PEReN est toutefois considéré comme un chercheur pouvant bénéficier d'un accès aux données publiques des plateformes au titre de l'article 40, paragraphe 12, du RSN. Ces chercheurs ne doivent répondre qu'à certaines conditions listées à l'article 40, paragraphe 8, du RSN : être indépendant de tout intérêts commerciaux, respecter les exigences spécifiques en matière de sécurité et de confidentialité des données et protéger les données à caractère personnel, démontrer que leur accès aux données et les périodes d'accès demandées sont nécessaires et proportionnés aux fins poursuivies par leur recherche et que les résultats escomptés de cette recherche contribueront à la détection, au recensement et à la compréhension des risques systémiques dans l'Union et indiquer la source de financement de leur recherche.

2. La position de la commission : une volonté de lever les limites restantes à la transmission et à la conservation des données des très grandes plateformes et des très grands moteurs de recherche en ligne afin de renforcer notre compréhension et notre régulation de l'économie numérique

Afin de garantir un accès total du PEReN aux données publiques détenues par les plateformes et qui sont rendues accessibles aux chercheurs par le RSN, il est nécessaire de lui donner accès aux données de ces mêmes plateformes lorsqu'elles sont stockées sur les terminaux mobiles par les systèmes d'exploitation. En effet, certaines plateformes en ligne ne disposent pas d'un accès sur Internet, mais uniquement sur une application *via* un appareil mobile. L'accès à ces données provenant initialement de très grandes plateformes et moteurs de recherche en ligne, pourtant garanti par le RSN, peut dès lors être dénié par un tiers, le fournisseur du système d'exploitation du terminal.

De plus, la nouvelle rédaction de l'article 36 de la loi du 25 octobre 2021 issue du présent article 16 vient soumettre les activités de recherche publiques du PEReN à une limitation de la durée de conservation des données similaire à celle applicable pour ses activités d'expérimentation.

En l'état, les données doivent être détruites à l'issue des travaux et au plus tard dans un délai de neuf mois. Le PEReN a fait état des limitations que représente cette restriction de la conservation des données pour la conduite de ses travaux.

En conséquence, **la commission a adopté l'amendement COM-124 du rapporteur visant à obliger les fournisseurs de système d'exploitation à transmettre au PEReN les données publiques des très grandes plateformes et des très grands moteurs de recherche en ligne visées à l'article 40, paragraphe 2, du RSN stockées sur les terminaux mobiles pour ses activités de recherche publique**.

En second lieu, **cet amendement élargit la période de conservation des données collectées dans le cadre des activités de recherche publique du PEReN à cinq ans** ; ce qui demeure en conformité avec les exigences du RGPD.

La commission spéciale a également adopté les deux amendements de précision rédactionnelle **COM-123** et **COM-125** présentés par le rapporteur.

La commission spéciale a adopté l'article 16 **ainsi modifié**.

Article 17

Dispositif de centralisation des données devant être transmises aux communes par les opérateurs de plateformes numériques en matière de location de meublés de tourisme

L'article 17 vise à créer une plateforme unique, intermédiaire entre les plateformes et les communes, centralisant les données relatives aux meublés de tourisme mis en location dans chaque commune. Cette plateforme sera gérée par un organisme unique désigné par décret en Conseil d'État.

La commission salue ce dispositif dont elle a souhaité renforcer encore davantage le caractère opérationnel pour les communes. Elle a ainsi adopté un amendement du rapporteur Patrick Chaize qui permet de garantir que les communes qui le souhaitent pourront disposer d'un accès à ces données via le portail unique, sans avoir à formuler à chaque fois une demande ponctuelle explicite de transmission de données.

La commission spéciale a adopté l'article ainsi modifié.

1. La situation actuelle : une difficulté des communes à contrôler le bon respect des obligations des loueurs de meublés de tourisme

a) La location de meublés de tourisme est encadrée par la loi afin que son développement puisse être maîtrisé par les communes

1. La location de meublés de tourisme est soumise au cadre juridique du changement d'usage et à une déclaration préalable

Depuis la loi dite *Alur* de 2014[1], il est précisé à l'article L. 631-7 du code de la construction et de l'habitat que « *le fait de louer un local meublé destiné à l'habitation de manière répétée pour de courtes durées à une clientèle de passage qui n'y élit pas domicile constitue un changement d'usage* ». Ainsi, dans les communes mentionnées à cet article, le changement d'usage d'un local d'habitation – sauf d'une résidence principale – est soumis à une **autorisation préalable**. Le même régime **peut** être appliqué dans les communes situées en zones tendues sur décision du conseil municipal ou de l'établissement public de coopération intercommunale[2] et dans les autres communes après autorisation du préfet.

Toujours hors résidence principale, ces locations font l'objet d'une **déclaration préalable auprès de la commune** en vertu de l'article L. 324-1-1 du code du tourisme.

2. Une procédure de déclaration préalable avec enregistrement auprès de la commune complète ce cadre pour certaines communes depuis 2016

Depuis la loi pour une République numérique de 2016[3], dans les communes dans lesquelles le changement d'usage des locaux d'habitation est soumis à autorisation préalable, le conseil municipal **peut** soumettre à **déclaration préalable avec enregistrement auprès de la commune** toute location d'un meublé de tourisme, résidences principales incluses. La déclaration mène à la délivrance d'un **numéro** obligatoirement affiché sur l'annonce de location.

Depuis lors, les plateformes de location comme Airbnb ont l'obligation d'informer **les loueurs de leurs obligations** de déclaration ou d'autorisation préalable et d'obtenir une **déclaration sur l'honneur** attestant de leur conformité avec la loi. Ils ont l'interdiction d'offrir à la location des meublés de tourisme déclarés comme résidence principale dont ils ont connaissance qu'ils ont été loués par leur entremise **plus de 120 jours au**

---

[1] *Loi n° 2014-366 du 24 mars 2014 pour l'accès au logement et un urbanisme rénové.*
[2] *Annexe du décret n°2013-392 10 mai 2013 relatif au champ d'application de la taxe annuelle sur les logements vacants instituée par l'article 232 du code général des impôts.*
[3] *Loi n°2016-1321 du 7 octobre 2016 pour une République numérique*

cours d'une année. La loi dite *Élan* de 2018[1] a appliqué cette obligation aux loueurs[2].

Dans les faits, selon l'Union nationale pour la promotion de la location de vacances (UNPLV), à la fin de l'année 2022, 193 communes appliqueraient une procédure de déclaration préalable avec enregistrement. D'autres sources privées évoquent plus de 700 communes, le Gouvernement retenant quant à lui une estimation de 350 communes.

b) Pour contrôler le bon respect de ces obligations, une transmission numérique de données aux communes est prévue depuis 2018

1. La transmission de données par les loueurs

Depuis la loi *Élan* de 2018[3], les communes ont la possibilité de demander **au loueur**, jusqu'au 31 décembre de l'année suivant la location d'un meublé, **la transmission d'informations** sur le nombre de jours pendant lesquels ce dernier a été loué. Ces informations, transmises sous un mois, incluent l'adresse du meublé et son numéro de déclaration. Toutefois, ces demandes individualisées ne sont pas propices au contrôle effectif du bon respect des obligations des loueurs dans un contexte où la location de meublés de tourisme s'opère en large partie ***via*** **des plateformes numériques**.

2. La transmission de données par les plateformes de location

Depuis 2018 également, **toute commune ayant mis en œuvre la procédure d'enregistrement** peut, jusqu'au 31 décembre de l'année suivant la location du meublé, demander **à la plateforme** de location de lui transmettre sous un mois le nombre de jours au cours desquels ce meublé a été loué par son intermédiaire. Les données incluent le nom du loueur, l'adresse du bien, le numéro de déclaration et s'il s'agit d'une résidence principale. Elles sont transmises par la plateforme lorsque cette dernière « *en a connaissance* », ce qui implique que les transactions doivent se dérouler sur la plateforme.

c) Un dispositif administrativement lourd pour les communes

En théorie, ce dispositif de transmission de données permet aux communes de contrôler le bon respect des obligations suivantes :

– l'obtention par le meublé proposé à la location du **numéro de déclaration** mentionné dans l'annonce ;

– s'il s'agit d'une résidence secondaire, le bon respect du cadre juridique sur le **changement d'usage** ;

---

[1] *Loi n°2018-1021 du 23 novembre 2018 portant évolution du logement, de l'aménagement et du numérique*
[2] *Article 324-1-1 du code de tourisme*
[3] *Article L. 324-1 du code du tourisme.*

– s'il s'agit d'une résidence principale, le bon respect de la **limitation à 120 jours** de location par an.

En pratique, les communes doivent adresser une demande à chaque plateforme sur laquelle les meublés de tourisme de son territoire peuvent être proposés à la location – si Airbnb est la plateforme de location la plus connue et la plus populaire, il en existe plusieurs autres concernées par cette procédure. Les données sont transmises annuellement[1] par les opérateurs de plateforme sous un format tableur modifiable informatiquement, entraînant des pics d'activité saisonniers sans pour autant que toutes les communes ne formulent cette demande au même moment. Les **échanges bilatéraux** sont multiples et concernent souvent les mêmes meublés de tourisme présents sur plusieurs plateformes, **nuisant à la lisibilité et à la rapidité** du traitement des données collectées. Le **foisonnement d'interlocuteurs** rend le processus administratif lourd pour les communes et difficilement automatisable.

Entre février et septembre 2022, **l'expérimentation de la plateforme** « ***API meublé*** » a permis de tester une solution facilitant les échanges de données entre cinq opérateurs numériques de location de meublés de tourisme et cinq communes. Sans supprimer les échanges bilatéraux entre communes et opérateurs de plateformes, ce dispositif mis en œuvre par voie contractuelle a permis aux acteurs de disposer d'un outil unique de contrôle des données, proposant un fichier consolidé.

2. Le dispositif envisagé : la création d'une plateforme unique de centralisation des données devant être transmises aux communes

Le dispositif envisagé prévoit de tirer les enseignements de l'expérience positive d'*API meublé* en confiant à un **organisme unique** désigné par décret en Conseil d'État la gestion d'un **guichet centralisant les données** collectées auprès des plateformes intermédiaires de location.

Chaque commune n'aura ainsi plus à s'adresser à chaque plateforme pour obtenir des informations sur les meublés de tourisme loués sur son territoire, mais pourra consulter ces données en se connectant sur un portail unique en ligne. L'objectif est **d'alléger la charge administrative des communes** et de leur permettre de mieux contrôler le respect de la loi par les loueurs via l'étude des données consolidées dont elles disposeront. Le Gouvernement estime ainsi que pour 350 communes, le déploiement du nouveau dispositif centralisé réduirait de 3500 actuellement à 370 le nombre de démarches administratives réalisées.

---

[1] *En vertu de l'article R. 324-2 du code du tourisme, la commune peut adresser au plus une demande d'information par année civile à l'opérateur de plateforme.*

Le II de l'article L.324-2-1 du code du tourisme est donc modifié afin de :

– disposer que la commune **demande** non plus à la plateforme de lui mettre à disposition les données relatives aux meublés loués par son intermédiaire, mais à un **organisme unique** chargé de recueillir ces données par voie électronique auprès des plateformes numériques ;

– prévoir qu'un décret en Conseil d'État désigne l'organisme unique en question et détermine la nature des données, leur durée de conservation, les délais de réponse, la fréquence et les modalités techniques de leur transmission.

3. La position de la commission : le renforcement du caractère opérationnel du dispositif afin de faciliter le travail des communes

La commission spéciale est favorable à un dispositif unique et centralisé de transmission des données, qui serait de nature à alléger la charge administrative des communes et faciliter leur contrôle des obligations des loueurs. Seule disposition du présent projet de loi intéressant les collectivités territoriales, elle a retenu toute l'attention de la commission spéciale qui rappelle que le bon respect du cadre juridique relatif à la location de meublés de tourisme permet aux communes d'éviter de potentiels effets indésirables du développement non maîtrisé de ces locations sur leur territoire, comme la hausse de prix de l'immobilier, la pénurie de logements destinés à l'habitation, la modification de l'offre commerciale ou des besoins en équipements.

En effet, le dispositif actuel est loin de permettre le bon respect de la loi par les loueurs : selon l'étude d'impact du projet de loi, le taux de **non-conformité du parc de locations de meublés de tourisme** est estimé à **34** % à Paris et **46** % à Lyon. La complexité du dispositif actuel de transmission des données et sa lourdeur administrative pèsent sur les communes, dont certaines ont pu être découragées d'exercer leur faculté à formuler cette demande aux plateformes.

Ainsi, selon les chiffres communiquées par Airbnb au rapporteur, sur l'année 2022, seules 90 communes lui ont adressé une demande de transmission des données, alors que 192 auraient été fondées à le faire.

L'amélioration du dispositif est donc bienvenue aux yeux de la commission spéciale, qui souligne toutefois plusieurs incertitudes. Dans sa rédaction initiale, l'article prévoit la **possibilité** pour les communes de **demander la transmission de données** à l'organisme unique, ce qui en pratique leur donnerait accès au portail unique. Pour la commission spéciale, cela revient à **limiter considérablement** le champ du dispositif, certaines communes risquant de ne pas exercer cette faculté, ou alors de manière irrégulière, ce qui limiterait leur capacité à contrôler les obligations des loueurs. D'autres incertitudes devront être levées lors de la prise du décret

en Conseil d'État, notamment en ce qui concerne la fréquence de la transmission des données aux collectivités. Il serait en effet souhaitable que les données soient collectées par l'organisme unique auprès des plateformes à un **intervalle régulier** permettant aux communes qui le souhaitent d'y avoir accès *via* une simple connexion sur le portail unique, sans avoir à réitérer leur demande. La commission insiste donc sur l'importance de la **concertation** des acteurs préalablement à la prise de ce décret afin de déterminer les modalités de mise en œuvre de cette interface.

La commission spéciale attire également l'attention sur le fait que l'organe qui sera désigné par un décret en Conseil d'État devra être doté des **moyens humains et financiers nécessaires à la réalisation de ses missions**. Les moyens attribués à cet organisme feront l'objet d'une attention particulière lors de l'examen du projet de loi de finances.

Elle signale enfin que le présent article est une anticipation par rapport au règlement européen proposé en novembre 2022 sur la collecte et le partage des données relatives aux services de location de courte durée qui, **au-delà des seuls meublés de tourisme, concernera toutes les locations de courte durée**. Cette proposition en cours de négociation prévoit en effet que les États membres mettent en place un « **point d'entrée numérique unique** » pour la transmission de données relatives aux locations de courte durée entre les opérateurs de plateforme et les autorités publiques. La loi française devra donc être à nouveau adaptée une fois ce règlement adopté.

Afin de renforcer le caractère opérationnel du dispositif, la commission spéciale a adopté l'amendement **COM-126** du rapporteur précisant que les communes qui le souhaitent disposent, *via* une simple connexion au portail unique, d'un accès aux données relatives aux meublés de tourisme, sans avoir à formuler à chaque fois une demande ponctuelle de transmission de données. En effet, conditionner chaque accès à ces données à une demande de transmission adressée par la commune emporte le risque de limiter considérablement le champ du dispositif.

La commission spéciale a adopté l'article **17 ainsi modifié.**

TITRE VI
RENFORCER LA GOUVERNANCE DE LA RÉGULATION DU NUMÉRIQUE

Article 18

Coopération du coordinateur pour les services numériques avec le Pôle d'expertise de la régulation numérique

L'article 18 désigne le Pôle d'expertise de la régulation numérique (PEReN) comme soutien technique au coordinateur des services numériques.

La commission a adopté cet article sans modification.

1. Désignation du PEReN comme soutien technique au coordinateur des services numériques

a) Le coordinateur des services numériques

Le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques (RSN) prévoit à son article 49, paragraphe 2, la désignation d'un coordinateur des services numériques dans chaque État membre « *responsable de toutes les questions en lien avec la surveillance et l'exécution du présent règlement* ».

b) Le dispositif envisagé

L'article 18 crée un nouvel article 7-1 dans la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, au sein d'une nouvelle section créée par l'article 25 du présent projet de loi et intitulée « Coordinateur pour les services numériques et coopération entre les autorités compétentes ».

Cet article met à disposition du coordinateur pour les services numérique les services du PEReN, notamment pour toute question liée aux analyses de données, aux codes sources, aux programmes informatiques, aux traitements algorithmiques ou à l'audit des algorithmes. Cet article prévoit également que le PEReN puisse proposer de lui-même son assistance technique au coordinateur pour les services numériques afin de mener les travaux relevant de son expertise, mentionnés à l'article 36 de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique.

Le PEReN sera aussi associé par le coordinateur pour les services numériques aux missions de coopération relatives au développement de l'expertise et des capacités de l'Union européenne en matière d'évaluation des questions systémiques et émergentes, mentionnées à l'article 64 du RSN.

Cette évaluation des questions systémiques est par ailleurs, en vertu de l'article 16 du présent projet de loi, l'une des compétences du PEReN au sein de ses activités de recherche publique.

Enfin, l'article 18 prévoit des garanties d'indépendance du PEReN et de confidentialité des données et informations recueillies, limitées aux seules fins nécessaires à ses missions.

2. La position de la commission : un appui technique bienvenu de nature à renforcer notre compréhension et notre régulation de l'économie numérique

L'article 25 du présent projet de loi prévoit de nommer l'Arcom comme coordinateur des services numériques. Si les services du PEReN travaillent déjà de concert avec l'Arcom – celle-ci étant l'une des huit autorités administrative indépendantes bénéficiant du soutien technique du PEReN – sécuriser la mise à disposition du PEReN pour la conduite des missions de l'Arcom en tant que coordinateur des services numériques est essentiel. En effet, la mission de coordinateur des services numériques nécessite une expertise technique à laquelle les services de l'Arcom ne peuvent répondre seuls. Au regard de ses compétences inscrites à l'article 36 de la loi du 25 octobre 2021, le PEReN apparaît donc comme un appui naturel de l'Arcom dans l'accomplissement de sa mission de coordinateur.

Le PEReN a toutefois émis un point d'attention sur la charge que constituerait cette nouvelle compétence, considérant les effectifs nécessaires à l'accomplissement de ces nouvelles missions.

La commission spéciale et son rapporteur Patrick Chaize se montreront particulièrement vigilants, dès le prochain projet de loi de finances, à ce que le PEReN dispose des moyens budgétaires et humains nécessaires à la mise en œuvre de ces nouvelles missions.

La commission spéciale a adopté l'article 18 **sans modification**.

TITRE VII
CONTRÔLE DES OPÉRATIONS DE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL EFFECTUÉES PAR LES JURIDICTIONS DANS L'EXERCICE DE LEUR FONCTION JURIDICTIONNELLE

Articles 19, 20 et 21

Création d'une autorité de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions au sein du Conseil d'État, de la Cour de cassation et de la Cour des comptes

Les articles 19, 20 et 21, qui forment le titre VII du projet de loi, visent à combler un vide juridique en confiant respectivement au Conseil d'État, à la Cour de cassation et à la Cour des comptes une nouvelle mission de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions et leurs ministères publics, dans l'exercice de leurs fonctions juridictionnelles.

Ce contrôle serait exercé sous la forme d'une « autorité » respectivement constituée, pour chacun des ordres, d'un membre du Conseil d'État élu par son assemblée générale, d'un conseiller à la Cour de cassation désigné par son premier président et d'un magistrat de la Cour des comptes élu par la chambre du conseil. À l'exception du prononcé de sanctions pécuniaires, ils disposeraient, pendant une durée de trois ans renouvelable une fois, des mêmes pouvoirs que ceux dont disposent actuellement le président et la formation restreinte de la commission nationale de l'informatique et des libertés (Cnil) en matière d'enquête et d'adoption de mesures correctrices.

Estimant ces mesures pertinentes dans la mesure où elles garantiront aux justiciables une meilleure protection de leurs données personnelles, la commission spéciale a adopté ces trois articles en y apportant des clarifications rédactionnelles et en étendant le principe de l'élection à l'autorité de contrôle de la Cour de cassation, à l'instar des autorités de contrôle compétentes pour les juridictions administratives et financières.

1. Le droit en vigueur ne prévoit pas de compétence de la Cnil en matière de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle

a) Au motif de la préservation de l'indépendance de l'autorité judiciaire, aussi bien le RGPD que le droit national excluent des compétences de la Cnil le contrôle des opérations de traitement des données personnelles effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle

En vertu de l'article 55 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit règlement général sur la protection des données (RGPD)[1], **les autorités de contrôle de l'utilisation des données personnelles** – c'est-à-dire, en France, la Cnil – « ***ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle*** ». L'incompétence des autorités de contrôle en matière juridictionnelle est imposée également, dans les mêmes termes, par l'article 45 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016[2], dite *directive police-justice*, qui régit le traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

La justification de l'incompétence des autorités de contrôle est précisée au sein du considérant n° 20 dudit RGPD, qui met en avant le souhait du législateur européen « *de **préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires**, y compris lorsqu'il prend des décisions* ».

En application de ces deux textes européens, le droit interne a été modifié, par le biais de l'ordonnance n° 2018-1125 du 12 décembre 2018[3], afin d'exclure du domaine de compétences de la Cnil les opérations en lien direct avec l'activité juridictionnelle. Ainsi, le V de l'article 19 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose

---

[1] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*

[2] *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.*

[3] *Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.*

désormais que « *dans l'exercice de son pouvoir de contrôle portant sur les traitements* [de données à caractère personnel], *la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions* ».

Interrogée par le rapporteur Loïc Hervé, **la Cnil a confirmé qu'elle n'exerçait aucun contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions** dans l'exercice de leurs fonctions juridictionnelles, aussi bien depuis la modification du cadre législatif en 2018 qu'avant l'entrée en vigueur des mesures d'adaptation au RGPD.

La Cnil contrôle en revanche les opérations de traitement des données concernant le ministère de la justice mais qui ne relèvent pas de l'exercice des activités juridictionnelles. À ce titre, des contrôles ont ainsi été menés sur le traitement du fichier judiciaire automatisé des auteurs d'infractions sexuelles et violentes (Fijais), de la plateforme nationale des interceptions judiciaires (PNIJ) ou encore du fichier de suivi des bracelets électroniques.

b) En l'absence de cadre législatif clair, un contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle confié à des « délégués à la protection des données »

L'incompétence de la Cnil ne signifie pas pour autant que les opérations de traitement des données à caractère personnel effectuées par les juridictions et leur ministère public dans l'exercice de leurs fonctions juridictionnelles ne font l'objet d'aucun contrôle.

En premier lieu, la jurisprudence de la Cour de justice de l'Union européenne (CJUE) a précisé l'interprétation qui devait être faite de l'article 55 du RGPD. Par son arrêt C-245/20 du 24 mars 2022[1], **la CJUE a jugé que l'article 55 précité n'a pas entendu soustraire à tout contrôle les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle**, mais a seulement exclu que le contrôle de ces opérations soit confié à l'autorité de contrôle de droit commun.

En second lieu, **les ordres juridictionnels ont chacun pris des mesures, de façon hétérogène, afin de respecter aussi bien le RGPD que la jurisprudence de la CJUE**.

Ainsi, le Conseil d'État tout comme la Cour des comptes ont chacun désigné **un délégué à la protection des données**, chargé de veiller à l'application du RGPD et de traiter d'éventuelles réclamations. Par ailleurs,

[1] *Affaire C-245/20: Arrêt de la Cour de justice de l'Union européenne (première chambre) du 24 mars 2022 (demande de décision préjudicielle du Rechtbank Midden-Nederland – Pays-Bas) – X, Z / Autoriteit Persoonsgegevens*

pour le cas spécifique des juridictions financières, il est demandé à chaque chambre de la Cour, à chaque chambre régionale et à chaque direction de nommer un référent RGPD pour suivre les traitements de données à caractère personnel de leur périmètre, faire remonter les alertes et diffuser les bonnes pratiques. L'animation de ce réseau est à la charge du délégué à la protection des données. En revanche, le délégué à la protection des données du Conseil d'État n'effectue aucun contrôle sur les traitements des juridictions administratives spécialisées autres que la Cour nationale du droit d'asile (CNDA).

S'agissant des juridictions judiciaires, le contrôle des opérations de traitement des données à caractère personnel prend des formes variées.

S'il existe un contrôle *a priori* de la Cnil, qui doit être saisie de tout projet de texte portant création de traitement, y compris donc sur des textes relatifs à des opérations de traitement relevant de l'activité juridictionnelle, le parquet général de la Cour de cassation a indiqué au rapporteur qu'à l'exception de certains fichiers sensibles pour lesquels il a été expressément prévu un contrôle par le législateur, tels que Cassiopée[1], la plateforme nationale des interceptions judiciaires (PNIJ)[2] ou le fichier de suivi des bracelets électroniques et anti-rapprochement[3], **les autres fichiers ne font l'objet d'aucune disposition spécifique et d'aucun contrôle particulier *a posteriori***. Pour le siège, une fonction de délégué à la protection des données est assurée par un conseiller de la Cour de cassation qui est destinataire de toutes les requêtes des particuliers. Cette fonction de délégué à la protection des données ne s'applique cependant qu'à la Cour de cassation et non aux autres juridictions judiciaires.

En parallèle de ces contrôles internes, **tout particulier dispose des voies de droit commun contre l'État, dont la responsabilité peut être recherchée au titre de ses activités juridictionnelles**, comme l'a récemment illustré l'ordonnance n° 2304177 du 19 mai 2023 par laquelle le juge des référés du tribunal administratif de Lille a ordonné l'effacement des données à caractère personnel contenues dans le fichier des manifestants contre la réforme des retraites placés en garde à vue.

---

[1] *Le fichier Cassiopée, qui contient des informations relatives aux plaintes et aux dénonciations reçues par les magistrats dans le cadre de procédures judiciaires, est placé sous le contrôle d'un magistrat du parquet hors hiérarchie assisté d'un comité de trois personnes qui peut ordonner toute mesure nécessaire telles que les saisies ou copies d'information ainsi que l'effacement d'enregistrements illicites.*

[2] *La plateforme nationale des interceptions judiciaires relève du contrôle d'une personnalité qualifiée assistée d'un comité de cinq personnes dont un député et un sénateur qui peut ordonner toutes mesures nécessaires à l'exercice de son contrôle et dispose d'un accès permanent au lieu où se trouve la plateforme.*

[3] *Les traitements relatifs aux bracelets électroniques et anti-rapprochement sont placés sous le contrôle d'un magistrat du parquet hors hiérarchie, nommé par arrêté du garde des sceaux qui peut procéder à toute vérification sur place et obtenir du responsable de traitement tout renseignement utile.*

2. Les articles 19, 20 et 21 du projet de loi harmonisent le contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions et leur ministère public dans l'exercice de leur fonction juridictionnelle en créant, pour chaque ordre juridictionnel, une autorité de contrôle spécifique

Si le droit européen exclut des compétences de la Cnil le contrôle les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle, **il impose cependant aux États membres de mettre en place un dispositif spécifique pour assurer ce contrôle**, lequel n'est pas prévu par le droit en vigueur.

En conséquence, et compte tenu de l'hétérogénéité des mécanismes de contrôle actuellement mis en œuvre, les articles 19, 20 et 21 visent à combler ce vide juridique et à harmoniser les pratiques existantes en confiant respectivement au Conseil d'État, à la Cour de cassation et à la Cour des comptes une nouvelle mission de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions et leur ministère public, dans l'exercice de leur fonction juridictionnelle.

Ce contrôle serait exercé sous la forme d'une « autorité » respectivement constituée, pour chacun des ordres, d'un membre du Conseil d'État élu par son assemblée générale, d'un conseiller à la Cour de cassation désigné par son premier président, et d'un magistrat de la Cour des comptes, élu par la chambre du conseil.

Ces autorités seraient compétentes pour l'ensemble des juridictions dépendant de leur ordre, ce qui permettra, d'une part, d'inciter davantage les responsables des opérations de traitement à veiller à la bonne application du RGPD et, d'autre part, d'unifier aussi bien les modalités de contrôles que la jurisprudence. À ce titre, l'article 19 précise que le Conseil d'État sera chargé du contrôle des opérations de traitement des données à caractère personnel effectuées par le tribunal des conflits.

À l'exception du prononcé de sanctions pécuniaires, **ces trois autorités disposeraient, pendant une durée de trois ans renouvelable une fois, des mêmes pouvoirs que ceux dont disposent actuellement le président et la formation restreinte de la Cnil en matière de conseil, d'enquête et d'adoption de mesures correctrices**, qui peuvent aller jusqu'à la rectification ou l'effacement des données à caractère personnel n'ayant pas été traitées convenablement ou encore une interdiction, à destination de la personne morale ou physique fautive, du traitement des données à caractère personnel.

L'article 20, relatif à l'ordre judiciaire, comporte des dispositions supplémentaires par rapport aux articles 19 et 21 afin, d'une part, de confier le contrôle des opérations de traitement des données à caractère personnel effectuées par le Conseil supérieur de la magistrature à l'autorité de contrôle formée au sein de la Cour de cassation et, d'autre part, de préciser que

les recours contre les décisions de cette même autorité de contrôle relèvent de la compétence de la Cour de cassation. Les articles 19 et 21 ne mentionnent pas les modalités de recours contre les décisions prises par les autorités de contrôle instituées auprès du Conseil d'État et de la Cour des comptes, car celles-ci relèvent du domaine du règlement et seront donc précisées par le biais du décret en Conseil d'État que prévoit chacun de ces articles.

Par coordination, le II de l'article 20 modifie le V de l'article 19 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin **d'exclure de la compétence de la Cnil le contrôle des opérations de traitement des données à caractère personnel effectuées par le ministère public dans l'exercice de ses fonctions juridictionnelles**.

Afin de garantir la pleine indépendance de ces autorités, il est précisé aux articles 19, 20 et 21 du projet de loi que celles-ci disposent « *des ressources humaines, matérielles et techniques nécessaires à l'exercice de* [leur] *fonction* », fournies respectivement par le Conseil d'État, la Cour de cassation et la Cour des comptes. Cette précision a son importance compte tenu de la charge de travail que risque de représenter la fonction de ces autorités. Interrogés par le rapporteur, aussi bien le Conseil d'État que la Cour des comptes et la Cour de cassation ont estimé que cette autorité, composée d'un membre unique, devra être assistée d'un service pour assurer ses fonctions et gérer l'éventuel flux régulier des requêtes.

Si le Conseil d'État et la Cour des comptes jugent la charge de travail reposant sur l'autorité de contrôle relativement modeste, du moins ne nécessitant vraisemblablement pas une occupation à temps plein, **la Cour de cassation a alerté le rapporteur sur l'étendue « *considérable* »[1] du domaine d'action de l'autorité créée au sein de ladite Cour**, qui sera compétente pour toutes les juridictions judiciaires et leur ministère public. Outre que cela représente un nombre très conséquent d'entités à contrôler, le nombre de fichiers concernés est également significatif, au moins une vingtaine d'après un recensement non exhaustif réalisé par le parquet général de la Cour de cassation.

Le premier président de la Cour de cassation a ainsi exprimé son « *scepticisme* »[2] sur l'affirmation contenue dans l'étude d'impact établie par le Gouvernement qui indique que les conséquences sur les services administratifs de la Cour de cassation seront « *limitées, compte tenu du nombre très faible de réclamations qui est attendu* ».

---

[1] *Réponses écrites d'Audrey Prodhomme, secrétaire générale du parquet général de la Cour de cassation, représentant François Molins, procureur général, au questionnaire du rapporteur.*

[2] *Réponses écrites de Christophe Soulard, premier président de la Cour de cassation, au questionnaire du rapporteur.*

Enfin, il est entendu que **les opérations de traitement effectuées hors des fonctions juridictionnelles demeureront soumises au contrôle de la Cnil**, comme c'est le cas en l'état actuel du droit. S'il reviendra à la jurisprudence de résoudre d'éventuels conflits de compétence, il est clair dans l'esprit du législateur qu'une fois la loi promulguée, la Cnil conservera son pouvoir de contrôle lorsqu'un fichier litigieux est aussi utilisé dans un cadre administratif, ou dans un cadre de police judiciaire mais extérieur à une activité juridictionnelle.

3. Des mesures bienvenues afin de garantir aux justiciables une meilleure protection de leurs données personnelles

La commission spéciale a approuvé le principe de création d'une autorité de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions au sein du Conseil d'État, de la Cour de cassation et de la Cour des comptes.

Elle souligne que ces mesures permettront, d'une part, de combler un vide juridique et d'assurer la pleine conformité du droit français au RGPD et, d'autre part, d'harmoniser le régime de contrôle des opérations de traitement des données à caractère personnel en instaurant un même modèle pour chacun des ordres juridictionnels.

En fin de compte, ces mesures participeront à rendre plus lisible et plus accessible, pour les justiciables, le dispositif de protection des données personnelles par les juridictions. En outre, l'instauration d'une autorité disposant d'un pouvoir de sanction, plutôt que d'un « *délégué à la protection des données* », devrait inciter les responsables de traitements des données à la vigilance et au respect des obligations qui leur incombent en application du RGPD.

Sans remettre en cause les lignes directrices de ces trois articles, **la commission spéciale a adopté dix amendements**, présentés par son rapporteur Loïc Hervé ainsi que par Vanina Paoli-Gagin et Jérôme Durain.

Outre les amendements rédactionnels **COM-82**[1] et **COM-127** à l'article 19 ainsi que l'amendement **COM-129** à l'article 20, **la commission spéciale a adopté les amendements COM-128, COM-131 et COM-132**, modifiant de façon identique les articles 19, 20 et 21 du projet de loi afin de lever une ambiguïté au sein du texte initial quant aux compétences de ces autorités de contrôle.

En effet, la définition des pouvoirs dont disposeront ces autorités de contrôle est renvoyée à l'article 58 du RGPD et aux articles 20 à 22 de la loi du 6 janvier 1978. Or, ces derniers opèrent des distinctions entre les pouvoirs du président de la Cnil et ceux de sa formation restreinte. Ces distinctions apparaissent inappropriées au cas des autorités de contrôle instituées par les

[1] *Cet amendement a été présenté par Vanina Paoli-Gagin.*

articles 19 à 21 du projet de loi, puisqu'il est proposé que ces autorités ne soient composées que d'un membre unique (*cf. supra*).

Les amendements **COM-128**, **COM-131** et **COM-132** clarifient par conséquent l'étendue des compétences de ces autorités de contrôle, **en précisant qu'elles exerceront, pour l'application des articles 19, 20 et 22 de la loi du 6 janvier 1978, aussi bien celles président de la Cnil que celle de sa formation restreinte**.

La commission spéciale a également adopté les amendements COM-53 rectifié, COM-54 rectifié et COM-55 rectifié. présentés par Jérôme Durain, modifiant les articles 19, 20 et 21. Ces amendements prévoient, sur le modèle de l'article L. 143-8 du code des juridictions financières relatif au rapport annuel d'activité de la Cour des comptes, que les autorités de contrôle précitées établissent chaque année, rendu public et adressé au Parlement. Outre un bilan de son activité annuelle, ce rapport pourra comporter des observations et des recommandations relatives au domaine d'intervention de l'autorité de contrôle.

Enfin, **la commission spéciale a adopté l'amendement COM-130** portant sur l'article 20, afin d'harmoniser sa rédaction avec celle des articles 19 et 21 du projet de loi, en prévoyant que l'autorité de contrôle compétente pour les juridictions judiciaires soit élue, à l'instar des autorités de contrôle dédiées aux juridictions administrative et financière.

L'élection apparaît en effet mieux à même de garantir l'indépendance de cette autorité de contrôle vis-à-vis, notamment, du premier président de la Cour de cassation, qui est le responsable final des opérations de traitement des données personnelles effectuées par la Cour de cassation.

C'est pourquoi **l'amendement COM-130 prévoit que le conseiller de la Cour de cassation ne soit plus désigné par le premier président de la Cour, mais soit élu par l'assemblée des magistrats du siège hors hiérarchie**, comme c'est le cas pour la désignation des magistrats membres de la formation du Conseil supérieur de la magistrature compétente à l'égard des magistrats du siège.

La commission spéciale a adopté les articles 19, 20 et 21 **ainsi modifiés**.

TITRE VIII
ADAPTATIONS DU DROIT NATIONAL

CHAPITRE IER
Mesures d'adaptation de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Article 22
Adaptations de la loi pour la confiance dans l'économie numérique

L'article 22 du projet de loi vise à adapter la loi du 21 juin 2004 pour la confiance dans l'économie numérique afin de tirer les conséquences de l'application du règlement européen sur les services numériques.

La commission a adopté cet article modifié par l'adoption de deux amendements des rapporteurs, de nature rédactionnelle ou de coordination juridique.

1. Le droit en vigueur : une nécessaire mise à jour de la loi du 21 juin 2004 pour la confiance dans l'économie numérique

La loi française du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) a été adoptée afin de **transposer les dispositions de la directive 2000/31 sur le commerce électronique**, dite *directive e-commerce*, à une période où le développement de l'économie numérique n'était pas aussi abouti qu'aujourd'hui.

Cette législation pose les **grands principes applicables à la régulation de l'économie numérique, qui demeurent encore valables aujourd'hui**. En particulier, le principe de la responsabilité des hébergeurs de services de communication au public en ligne, l'absence de surveillance générale des données et le principe dit « du pays d'origine » selon lequel les prestataires de services de la société de l'information doivent se conformer à la législation de leur pays d'établissement.

Or, depuis cette directive, au regard des évolutions du marché, des innovations technologiques et des priorités politiques des Gouvernements successifs, la LCEN a été modifiée à de nombreuses reprises, ***sans pour autant permettre*** **de s'adapter au mieux aux nouvelles pratiques et aux nouveaux risques inhérents au développement d'une société et d'une économie de plus en plus numériques**.

La directive e-commerce ayant atteint ses limites, et face aux risques de fragmentation durable des législations nationales des États membres au sein de l'Union européenne, de nouveaux règlements européens ont été adoptés, en particulier le règlement sur les services numériques (RSN) ou *Digital Services Act (DSA)* et le règlement sur les marchés numériques (RMN) ou *Digital Markets Act (DMA)*.

Ces deux règlements européens sont des **règlements horizontaux d'harmonisation maximale**, c'est-à-dire que les États membres ne devraient pas adopter ou maintenir des exigences nationales supplémentaires dans les domaines relevant du champ d'application de ces deux règlements, sauf si cela est expressément prévu.

L'article 22 du projet de loi vise à modifier plusieurs dispositions de la LCEN afin de tirer les conséquences de l'application du RSN, prévue au 17 février 2024. Toutefois, pour les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, les dispositions du RSN s'appliqueront à compter du 25 août 2023, la Commission européenne ayant récemment publié la liste des entreprises concernées : AliExpress, Amazon Store, App Store, Booking, Facebook, Google Maps, Google Play, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipédia, YouTube, Zalando, Bing et Google Search.

2. Le dispositif envisagé : une restructuration de la loi pour la confiance dans l'économie numérique afin de tirer les conséquences de l'entrée en vigueur du règlement sur les services numériques

La nécessaire adaptation de la LCEN est l'occasion à la fois de restructurer son contenu, de mettre à jour les définitions retenues, d'abroger les dispositions redondantes avec le RSN ou devenues obsolètes, et d'ajouter des dispositions supplémentaires qui nécessitent une adaptation de notre droit national.

a) La création des articles 1-1 et 1-2

Afin de disposer, au sein du titre Ier « De la liberté de communication en ligne », d'un chapitre Ier « La communication au public en ligne » plus cohérent, sont insérés deux articles supplémentaires après l'article 1er.

Premièrement, **un article 1-1 qui reprend les dispositions des III, IV et V de l'article 6 de la LCEN**, dans sa version actuelle. Ces dispositions sont respectivement relatives à la mise à disposition du public de certaines informations dans un standard ouvert, à l'exercice du droit de réponse auprès du directeur de la publication d'un éditeur ainsi qu'à l'application des dispositions de la loi du 29 juillet 1881 sur la liberté de la presse.

Deuxièmement, **un article 1-2 qui reprend les dispositions du VI de l'article 6 de la LCEN** dans sa version actuelle. Ces dispositions sont relatives à la sanction de la méconnaissance des obligations prévues au nouvel article 1-1 par un éditeur de service de communication au public en ligne.

b) La création de l'article 5-1 au sein de la LCEN

L'article 22 du projet de loi prévoit également une réorganisation du chapitre II du titre Ier, qui concerne les articles 5 à 9.

Premièrement, **l'intitulé de ce chapitre II est modifié pour devenir « Les fournisseurs de services intermédiaires »** plutôt que « Les prestataires techniques ».

Deuxièmement, **une section 1 est créée au sein de ce chapitre, intitulée « Définitions et obligations relatives aux fournisseurs de services intermédiaires »**.

Troisièmement, **un article 5-1 est créé afin de définir les services de la société de l'information** conformément à la définition retenue par la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des services de la société de l'information.

Il est également **institué une définition des services intermédiaires**, conformément à la définition retenue par l'article 3 du RSN. Ces services comprennent les services de simple transport, les services de mise en cache et les services d'hébergement.

c) La réécriture de l'article 6 au sein de la LCEN

L'article 22 du projet de loi procède à une **restructuration importante de l'article 6 de la LCEN**, qui suit désormais la structure suivante :

– définitions ;

– obligations des services d'accès à Internet et sanctions associées aux manquements ;

– obligations des hébergeurs et sanctions associées aux manquements ;

– obligations applicables à la fois aux services d'accès à Internet et aux hébergeurs, ainsi que leurs sanctions ;

– obligations applicables aux services de plateforme en ligne ;

– obligations applicables aux réseaux sociaux ;

– sanction pour signalement abusifs.

L'exercice de restructuration de l'article 6 de la LCEN a conduit à **l'abrogation des dispositions suivantes, considérées comme obsolètes, contraires ou redondantes avec les dispositions du RSN** :

– les conditions dans lesquelles la connaissance des faits litigieux est présumée acquise, dans le cadre du régime de responsabilité des hébergeurs, ont été abrogées car allant au-delà du RSN ;

– l'interdiction des obligations générales de surveillance, qui est redondante avec le RSN ;

– les obligations de transparence et de mise en place d'un système de signalement, redondantes avec le RSN ;

– les dispositions relatives au signalement des activités illicites de jeux d'agent, abrogées car devenues obsolètes par la réforme 2019/2020 sur la régulation des jeux d'argent en ligne, qui prévoit un pouvoir d'intervention direct de l'Autorité nationale des jeux sur les opérateurs.

2. La position de la commission – Une adaptation souhaitable de la loi pour la confiance dans l'économie numérique

La commission spéciale a adopté deux amendements des rapporteurs, de nature rédactionnelle ou de coordination :

- l'amendement **COM-133** du rapporteur Patrick Chaize, de nature rédactionnelle ;

- l'amendement **COM-134** du rapporteur Loïc Hervé, qui effectue les coordinations nécessaires aux modifications adoptées à l'article 5 du projet de loi.

La commission spéciale a adopté l'article 22 **ainsi modifié**.

Article 23

Adaptations relatives à la lutte contre les contenus terroristes et pédopornographiques

L'article 23 procède à diverses coordinations et à une réorganisation des articles 6-1 à 6-2-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Sur le fond, l'article prévoit de relever le plafond maximal de l'amende pénale – de 4 à 6 % du chiffre d'affaires mondial – encourue par un hébergeur en cas de méconnaissance habituelle de l'obligation d'informer immédiatement les autorités compétentes de contenus terroristes présentant une menace imminente pour la vie.

Il tend également à supprimer les conclusions du rapporteur public dans le cadre d'un recours exercé devant le tribunal administratif contre une injonction de retrait de contenus à caractère terroriste.

La commission spéciale a adopté cet article en rétablissant les conclusions du rapporteur public.

1. Des mesures de réorganisation et de coordination des dispositions de la LCEN relatives à la lutte contre les contenus terroristes et pédopornographiques

À l'instar des articles 22, 24 et 25 du présent projet de loi, l'article 23 prévoit une réorganisation de certaines dispositions de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

Il créerait une section 2 intitulée « Dispositions relatives à la lutte contre les contenus terroristes et pédopornographiques » qui regrouperait les articles 6-1 à 6-2-1. Les dispositions de l'actuel article 6-5 de la LCEN, consacré à l'information du mineur et des titulaires de l'autorité parentale sur l'utilisation civique et responsable des réseaux sociaux, seraient intégrées à l'article 6 par l'article 22 du projet de loi, tandis que l'article 6-2 actuel, sur le contrôle du respect des obligations d'agrément préalable et de déclaration encadrant les enfants influenceurs, serait renuméroté 6-5.

Sur proposition du rapporteur, la commission spéciale a adopté un amendement **COM-135** de clarifications rédactionnelles.

La commission spéciale a également noté qu'aucune des mesures d'harmonisation – recommandées par André Reichardt, dans son rapport[1] sur la loi du 16 août 2022[2], s'agissant des procédures nationale et européenne de retrait de contenus terroristes –, n'a été prévue. La prochaine adoption du règlement en vue de prévenir et de combattre les abus sexuels sur les enfants (CSAM)[3] en créera peut-être de nouveau l'occasion.

2. Le rehaussement de l'amende encourue par les hébergeurs en cas de méconnaissance habituelle de l'obligation d'information de la présence de contenus terroristes en ligne

Le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (règlement *TCO*) a imposé de prévoir une sanction à l'encontre des hébergeurs qui, de manière habituelle, ne respecterait pas une injonction de retrait dans l'heure dont le **montant maximal était fixé à 4 %** du chiffre d'affaires mondial. C'est ce qui a été inscrit à l'article 6-1-3 de la LCEN créé par la loi du 16 août 2022 précitée.

Ce même montant maximal de 4 % du chiffre d'affaires mondial a été choisi en cas de méconnaissance habituelle par un hébergeur de son obligation d'informer immédiatement les autorités lorsqu'il prend

---

[1] *Rapport n° 752 (2021-2022) d'André Reichardt, fait au nom de la commission des lois sur la proposition de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne.*

[2] *Loi n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne.*

[3] *Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants - COM/2022/209 final.*

connaissance d'un **contenu à caractère terroriste présentant une menace imminente pour la vie,** bien qu'aucun montant maximal n'ait été fixé dans le règlement européen.

L'article 23 du projet de loi prévoit de rehausser ce montant à 6 % du chiffre d'affaires mondial en cohérence avec l'article 52 du RSN, qui fixe ce plafond pour toutes les infractions à ce règlement.

Ce rehaussement ne paraît pas de nature à améliorer la cohérence d'ensemble des sanctions pécuniaires prévues dans le cadre de la LCEN ; toutefois il semble **légitime** de prévoir **la sanction maximale autorisée au regard du risque réel pour les citoyens en cas de non-notification de soupçon de préparation d'un attentat**.

3. Le maintien des conclusions du rapporteur public en cas de recours contre une injonction de retrait de contenus à caractère terroriste

L'article 23 prévoit également la **suppression des conclusions du rapporteur public** en cas de recours exercé devant le tribunal administratif contre une injonction de retrait de contenus à caractère terroriste, ce qui se justifierait du fait des délais de jugement resserrés pour ce contentieux.

Or, l'article R. 732-1-1 du code de justice administrative[1] prévoit d'ores et déjà la possibilité pour le magistrat statuant seul de dispenser le rapporteur public, sur sa proposition, de prononcer des conclusions à l'audience pour ce contentieux.

Comme elle l'a déjà fait aux articles 2 et 3, la commission spéciale a adopté l'amendement **COM-135** précité afin de conserver le caractère facultatif de cette dispense de conclusions du rapporteur public et laisser le soin aux magistrats de décider de l'opportunité de cette dispense.

La commission spéciale a adopté l'article 23 **ainsi modifié**.

[1] *Décret n° 2023-432 du 3 juin 2023 relatif au retrait des contenus à caractère terroriste en ligne.*

Article 24

Adaptations au RSN de la loi du 21 juin 2004 pour la confiance dans l'économie numérique

L'article 24 déplace, sans modification substantielle, les dispositions relatives au blocage judiciaire de l'accès aux contenus illicites pour tenir compte de la restructuration de la loi pour la confiance de l'économie numérique du 21 juin 2004. Par ailleurs, il abroge l'actuel article 6-4 de la même loi, où étaient inscrites depuis 2021, par « pré-transposition » du RSN, les obligations qui s'imposent aux opérateurs en matière de lutte contre la diffusion de contenus illicites.

La commission spéciale a adopté cet article sans modification.

L'article 24 du projet de loi poursuit deux objectifs, tous deux liés à la restructuration de la LCEN.

En premier lieu, **il déplace, sans les modifier, les dispositions relatives à l'intervention du président du tribunal judiciaire et à la portée de ses décisions en matière de lutte contre les contenus illicites.**

Ces dispositions, qui figurent actuellement au I du 8 de l'article 6 et à l'article 6-3 de la LCEN, se trouveraient ainsi intégrées à une nouvelle section « Dispositions relatives à l'intervention de l'autorité judiciaire » regroupant :

– l'article 6-3, désormais relatif à la **compétence du président du tribunal judiciaire pour prescrire en procédure accélérée** « *toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* » ;

– l'article 6-4, correspondant à l'actuel article 6-3 et qui concerne la portée des décisions judiciaires ainsi rendues, c'est-à-dire **la possibilité pour l'autorité administrative, sur le fondement de la décision judiciaire, d'obtenir la mise hors d'accès des sites « miroirs » ou le déréférencement de ceux-ci** ;

– l'article 6-5 (correspondant à l'actuel article 6-2 et dont le déplacement est prévu par l'article 23 du présent projet de loi), qui **autorise l'administration à saisir le juge judiciaire lorsqu'elle constate qu'un contenu fait apparaître un mineur** en violation des obligations d'agrément posées par le code du travail ou des obligations déclaratives posées par la loi n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants âgés de moins de seize ans sur les plateformes en ligne.

Ces déplacements n'emportent pas de changement de fond des dispositions concernées.

Le même article 24 abroge l'article 6-4 actuel de la LCEN, où figure la **liste des obligations qui s'imposent aux plateformes en ligne en matière de lutte contre les contenus illicites**. Ces obligations, qui sont largement couvertes par le RSN s'agissant des « *très grandes* » plateformes (donc celles qui atteignent le seuil de 45 millions de connexions mensuelles à l'échelle européenne), concernent dans notre droit national les plateformes dépassent le seuil fixé par décret[1] de 10 millions de visiteurs uniques par mois sur le territoire français.

Plus en détail, ces obligations concernent :

– la mise en œuvre de procédures et de moyens humains et technologiques proportionnés permettant une **coopération efficace avec les autorités judiciaires ou administratives compétentes** (information sur les suites données aux injonctions ; traitement des réquisitions visant à identifier les utilisateurs ; conservation temporaire des contenus signalés et qui ont été rendus inaccessibles ou retirés à des fins de recherche, de constatation et de poursuite des infractions pénales)[2] ;

– la **désignation d'un point de contact unique**, personne physique chargée de la communication avec les autorités publiques ;

– la mise à la disposition du public, de façon accessible, des **conditions générales d'utilisation de leur service**, cette obligation étant assortie de règles de transparence en matière de modération des contenus et de lutte contre les contenus illicites ;

– l'obligation de **rendre compte au public** des moyens mis en œuvre pour lutter contre les contenus illicites, selon des modalités et une périodicité fixées par l'Arcom ;

– la mise en place d'un **dispositif de signalement des contenus illicites aisément accessible et facile d'utilisation** ;

– le traitement en priorité des signalements soumis par les tiers de confiance ;

– la mise en œuvre de procédures et de moyens humains et technologiques proportionnés permettant le **traitement effectif des signalements de contenus illicites** (accusé de réception ; examen rapide ;

---

[1] *Décret n° 2022-32 du 14 janvier 2022 pris pour l'application de l'article 42 de la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République et relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne concourent à la lutte contre la diffusion publique des contenus illicites.*

[2] *Seule est reprise, à l'article 22 du présent projet, l'obligation faite aux plateformes de* «met[tre] en œuvre des procédures et des moyens humains et technologiques proportionnés permettant, lorsqu'elle a une activité de stockage de contenus, de conserver temporairement les contenus qui lui ont été signalés comme contraires aux dispositions [de la LCEN] et qu'elle a retirés ou rendus inaccessibles, aux fins de les mettre à la disposition de l'autorité judiciaire pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

information de l'auteur sur les suites données à son signalement et sur les voies de recours à sa disposition ; information de l'utilisateur en cas de retrait d'un contenu, en l'informant (notamment) de l'existence de sanctions civiles et pénales en cas de publication de contenus illicites ; *etc.*) ;

– la mise en œuvre de dispositifs de **recours interne** ;

– l'exposition, dans les conditions générales d'utilisation, des procédures conduisant par exemple à la suspension ou à la résiliation d'un compte ;

– l'obligation de **rendre compte à l'Arcom** des procédures et moyens mis en œuvre pour l'application des dispositions précitées.

Pour les opérateurs atteignant un nombre de visiteurs uniques mensuels encore plus important (15 millions de visiteurs uniques mensuels sur le territoire français), des obligations complémentaires s'appliquent. Ils doivent ainsi, aux termes du II de l'actuel article 6-4, procéder chaque année à une évaluation des risques systémiques liés au fonctionnement et à l'utilisation de leurs services en matière de diffusion des contenus illicites et d'atteinte à la liberté d'expression, mettre en œuvre des mesures raisonnables, efficaces et proportionnées pour atténuer les risques de diffusion de ces contenus, et rendre compte au public de l'évaluation de ces risques et de la nature des mesures d'atténuation prises.

L'article 6-4 avait été inséré dans la LCEN au cours des débats sur la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République ; comme le rappelait le rapport établi, lors de l'examen de ce texte, par Jacqueline Eustache-Brinio et Dominique Vérien[1] au nom de la commission des lois, cet ajout avait vocation, à l'initiative du Gouvernement, à « *anticiper et "pré-transposer" [le RSN]* » alors que débutaient seulement les négociations sur ce texte. Dans ce contexte, **il est regrettable que le Gouvernement n'ait pas fourni, pour permettre la juste évaluation de cette évolution, des éléments chiffrés permettant de mesurer l'écart entre les seuils figurant dans la loi actuelle (10 ou 15 millions de visiteurs uniques par mois sur le territoire français) et le nouveau seuil issu du RSN** (c'est-à-dire un « *nombre mensuel moyen de destinataires actifs du service dans l'Union égal ou supérieur à 45 millions* »), *a fortiori* alors que ces seuils sont fondés sur un ensemble de personnes (visiteurs uniques d'un côté, destinataires actifs de l'autre) et un périmètre géographique (la France d'un côté, l'Union européenne de l'autre) différents.

En dépit de cette lacune, il n'a pas paru raisonnable au rapporteur Loïc Hervé de maintenir dans la loi des dispositions qui prétendaient anticiper le RSN alors que celui-ci va entrer en application. Pour cette raison, **il n'a pas proposé à la commission spéciale de revenir sur l'abrogation de l'article 6-4**.

---

[1] *Rapport n° 454 (2020-2021) déposé le 18 mars 2021.*

La commission spéciale a adopté l'article 24 **sans modification**.

Article 25

Adaptations de la loi pour la confiance dans l'économie numérique

L'article 25 du projet de loi vise également à adapter la loi du 21 juin 2004 pour la confiance dans l'économie numérique afin de tirer les conséquences de l'application du règlement européen sur les services numériques, notamment concernant les missions et compétences du coordinateur national pour les services numériques : l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom).

La commission a adopté cet article modifié par l'adoption de trois amendements du rapporteur Patrick Chaize, de nature rédactionnelle ou de coordination entres les procédures d'enquêtes domiciliaires attribuées à l'Arcom et à la Commission nationale pour l'informatique et les libertés (Cnil).

1. Une adaptation nécessaire des missions et pouvoirs de l'Arcom, désignée coordinateur national pour les services numériques

a) La réécriture de l'article 7

Tirant les conséquences de l'article 49 du règlement européen sur les services numériques, l'article 25 de ce projet de loi réécrit l'article 7 de la LCEN pour **désigner l'Arcom comme coordinateur des services numériques**. Ce coordinateur « *est responsable de toutes les questions en lien avec la surveillance et l'exécution du présent règlement dans cet État membre, sauf si l'État membre concerné a assigné certaines missions ou certains secteurs spécifiques à d'autres autorités compétentes. Le coordinateur pour les services numériques a, en tout état de cause, la responsabilité d'assurer la coordination au niveau national vis-à-vis de ces questions et de contribuer à une surveillance et une exécution efficaces et cohérentes du présent règlement dans toute l'Union* ».

L'article 25 du projet de loi **désigne également la Direction générale chargée de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et la Cnil comme autorités administratives chargées de la mise en œuvre de ce règlement européen**.

Par conséquent, l'article 25 insère une section 4, intitulée « Coordinateur pour les services numériques et coopération entre les autorités compétentes » au sein du chapitre II de la LCEN relatif aux fournisseurs de services intermédiaires.

b) L'insertion des articles 7-2 et 7-3

Tirant les conséquences de l'article 57 du règlement européen sur les services numériques, l'article 25 de ce projet de loi insère un nouvel article 7-2 au sein de la LCEN pour **préciser que les autorités chargées de la mise en œuvre du RSN coopèrent étroitement et se prêtent mutuellement assistance, ce qui inclut notamment la libre communication d'informations dont elles disposent**. Les modalités de coopération et d'assistance entre les autorités désignées seront précisées par la signature de conventions de coopération.

Tirant les conséquences de l'article 61 du règlement européen sur les services numériques, l'article 25 de ce projet de loi insère un nouvel article 7-3 au sein de la LCEN pour **préciser que l'Arcom siège au comité européen des services numériques**, sachant que l'Arcom peut être accompagnée, en fonction de l'ordre du jour, d'une autre autorité désignée comme compétente pour la mise en œuvre du RSN.

Il est également précisé que l'Arcom assure **une mission de veille et d'analyse des risques systémiques** mentionnées à l'article 34 du RSN, c'est-à-dire :

- la diffusion de contenus illicites par l'intermédiaire des services de ces plateformes ;

– tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, en particulier le droit fondamental à la dignité humaine, au respect de la vie privée et familiale, à la protection des données à caractère personnel, à la liberté d'expression et d'information, des droits fondamentaux relatifs aux droits de l'enfant et du droit fondamental à un niveau élevé de protection des consommateurs ;

– tout effet négatif réel ou prévisible sur le discours civique, les processus électoraux et la sécurité publique ;

– tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes.

c) L'insertion d'un article 8-1

Alors que l'Arcom n'était jusqu'à présent compétente que pour certains des acteurs visés par le RSN, par exemple les services de plateforme de partage de vidéo ou les opérateurs de plateforme en ligne – cette dénomination étant abrogée par le présent projet de loi –, **l'article 25 consacre les compétences de l'Arcom à l'égard de l'ensemble des fournisseurs de services intermédiaires**.

d) L'insertion d'un article 9-1

Tirant les conséquences de l'article 51 du RSN, l'article 25 du projet de loi insère un nouvel article 9-1 au sein de la LCEN afin de préciser que l'Arcom **peut bénéficier de pouvoirs d'enquête et d'exécution** afin de contraindre les fournisseurs de services intermédiaires à respecter leurs obligations.

À cet égard, l'Arcom peut recueillir, auprès de tout fournisseur de service intermédiaire qui a une activité sur le territoire national, les informations nécessaires à son travail de contrôle.

Surtout, l'article 25 du projet de loi **dote les agents habilités et assermentés de l'Arcom d'un pouvoir de visites domiciliaires au sein des locaux des fournisseurs de services intermédiaires, sur le modèle de celui dont bénéficie la Cnil auprès des responsables de traitement de données à caractère personnel**. L'Arcom pourra également émettre des injonctions provisoires à l'égard des fournisseurs mis en cause afin de les contraindre, avant la prononciation d'une éventuelle sanction, à se conformer aux griefs de la mise en demeure prononcée à leur égard.

e) L'insertion d'un article 9-2

L'article 25 du projet de loi insère un nouvel article 9-2 au sein de la LCEN afin de **préciser les pouvoirs de sanction dont bénéficie l'Arcom à l'égard des fournisseurs de services intermédiaires** qui ne respectent pas leurs obligations et pour lesquels le manquement a été constaté**.**

Les sanctions que l'Arcom peut prononcer sont **de nature pécuniaire, et peuvent être assorties d'astreintes, d'injonctions de mise en conformité et de mesures de publicité**.

La sanction pécuniaire prononcée ne peut ainsi excéder 6 % du chiffre d'affaires mondial hors taxe de l'exercice qui précède la sanction et le montant maximal de l'astreinte ne peut excéder 5 % des revenus ou du chiffre d'affaires mondial hors taxe journalier de l'exercice précédent l'astreinte.

2. La position de la commission – Un renforcement bienvenu des pouvoirs et missions de l'Arcom qui doit toutefois s'accompagner d'une hausse des moyens qui lui sont alloués

Si la commission spéciale salue le renforcement des pouvoirs de l'Arcom, qui a vocation à devenir le coordinateur national pour les services numériques, le rapporteur Patrick Chaize veillera à ce que l'Arcom **bénéficie, dès le prochain projet loi de finances, des moyens budgétaires et humains nécessaires à l'accomplissement de ses nouvelles missions**.

Sur ce point, l'étude d'impact du projet de loi insiste sur l'**élargissement significatif des missions de l'Arcom permis par ce projet de loi**. Si la dernière loi de finances a fixé un plafond d'emplois à 370 équivalents temps plein, un renforcement supplémentaire des effectifs et des moyens de l'Arcom sera nécessaire.

S'il est encore difficile d'évaluer précisément ces besoins, l'étude d'impact de la Commission européenne sur la mise en œuvre du RSN estime que les coûts engendrés par les autorités de contrôle devraient fluctuer entre 50 000 et 300 000 euros par contrôle ou audit. En outre, la Commission européenne estime qu'en termes d'effectifs, les coûts directs varieront de 0,5 ETP à 25 ETP, en fonction de la taille des services établis dans chaque État membre.

Afin de compléter la rédaction de l'article 25 du projet de loi, la commission spéciale a également adopté les trois amendements suivants du rapporteur :

– l'amendement **COM-136** précisant que le rôle attribué à l'Arcom en matière de coordination ne porte pas atteinte aux compétences et attributions des autorités administratives et des autorités de régulation qui concourent, par leurs activités et leurs missions, à mettre en œuvre le règlement européen sur les services numériques ;

– l'amendement **COM-137**, qui apporte des précisions juridiques et rédactionnelles ;

– l'amendement **COM-138** qui vise à harmoniser davantage la procédure d'enquêtes domiciliaires confiée à l'Arcom avec celle dont dispose déjà la Cnil conformément à l'article 19 de la loi relative à l'informatique, aux fichiers et aux libertés ainsi qu'à l'article 32 du projet de loi.

La commission spéciale a adopté l'article 25 **ainsi modifié**.

CHAPITRE II
Modification du code de la consommation

Article 26
Adaptation du code de la consommation en cohérence avec la mise en œuvre du règlement sur les services numériques

L'article 26 vise à adapter certaines dispositions du code de la consommation au règlement sur les services numériques (RSN) afin d'harmoniser les définitions et obligations des plateformes en ligne et donner à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) les pouvoirs lui permettant de contrôler le bon respect de ces obligations.

La commission spéciale a adopté cet article modifié par l'adoption de deux amendements de précision juridique du rapporteur Patrick Chaize.

1. La nécessaire adaptation du code de la consommation au règlement européen sur les services numériques

a) L'harmonisation des différentes définitions

La définition de la **plateforme en ligne** présente dans le RSN repose sur le stockage et la diffusion au public d'informations par un service d'hébergement, à la demande du bénéficiaire d'un service. Cette définition inclut donc les réseaux sociaux ou les fournisseurs de places de marché en ligne, mais pas les **moteurs de recherche**.

Le code de la consommation encadre les **plateformes dans un sens plus large**, incluant les moteurs de recherches, les places de marché en ligne ou encore les comparateurs en ligne :

– l'article L. 111-7 définit **l'opérateur de plateforme en ligne**, en incluant, selon l'avis du Conseil d'État, les moteurs de recherche et les services d'intermédiation en ligne ;

– son article liminaire définit notamment la **place de marché en ligne** comme un service utilisant un logiciel qui permet aux **consommateurs de conclure des contrats à distance avec d'autres professionnels ou consommateurs.** Cette définition est issue de la directive dite « *Omnibus* »[1] mais n'apparaît pas dans le RSN, qui considère toutefois les places de marchés en ligne comme une catégorie de plateformes en ligne.

[1] *Article 3 de la directive (UE) 2019/2161 du Parlement Européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs*

Afin de mettre en cohérence ces définitions, le présent article procède aux adaptations suivantes :

– la définition d'une « **plateforme en ligne** » présente à l'article L. 111-7 du code de consommation est remplacée par la définition présente au sein du RSN et est placée à l'article liminaire du code de la consommation ;

– l'article liminaire du code est enrichi d'une définition du « **moteur de recherche en ligne** » puisque ce dernier n'entre pas dans le champ de la définition selon le RSN ;

– enfin, les comparateurs en ligne ne rentrant pas dans le champ du RSN, la définition en droit français peut être maintenue. Elle est toutefois placée à l'article liminaire.

b) L'harmonisation des obligations afférentes aux plateformes en ligne

Le RSN édicte des mesures **d'harmonisation totale**. Les dispositions nationales imposant des exigences supplémentaires aux opérateurs visés par le RSN doivent donc être abrogées, à l'exception de celles qui transposent des actes juridiques de l'Union européenne. En l'occurrence, la directive dite « *Omnibus* »[1] prévoit une obligation d'information des consommateurs applicable aux contrats conclus sur des **places de marché en ligne** et précise que les États membres peuvent leur imposer des obligations supplémentaires si elles sont proportionnées et non discriminatoires.

Les obligations de transparence et de loyauté des contenus sont donc aménagées dans le respect du droit européen de la consommation :

– l'article L. 111-7 impose aux **plateformes** d'informer le consommateur sur les modalités de référencement et de déréférencement des contenus des biens ou des services proposés ou mis en ligne. Ces obligations sont désormais réservées aux **fournisseurs de places de marché** et aux comparateurs – ces derniers n'étant pas visés par le RSN ;

– l'article 111-7-1 prévoit quant à lui que les opérateurs de plateformes en ligne qui dépassent un seuil de nombre de connexions défini par décret (en l'occurrence, cinq millions) élaborent et diffusent aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, transparence et loyauté, tandis que le RSN fixe un seuil à 45 millions de connexions par mois. Il est donc abrogé ;

– l'article L. 111-7-3 est modifié pour que l'obligation de réaliser un audit de cybersécurité s'applique aux fournisseurs de plateformes en ligne, de moteurs de recherche en ligne et de comparateurs en ligne.

[1] *Article 4, 5) de la même directive.*

c) La désignation de la DGCCRF pour contrôler le bon respect des obligations incombant aux opérateurs des places de marché en ligne

L'article 26 crée un régime de sanctions à l'encontre des fournisseurs de plateforme en ligne à l'article L. 133-1 du code de la consommation, dans un nouveau chapitre III intitulé « Obligations des fournisseurs de plateformes en ligne ».

Il habilite les agents de la DGCCRF pour rechercher et constater les infractions des **fournisseurs de places de marché en ligne** à leurs obligations de **traçabilité des professionnels**[1], de **conformité des interfaces dès leur conception**[2], de **droit d'information des consommateurs**[3] et en termes **d'interdiction** de **concevoir des *dark patterns*** – des interfaces conçues de façon à tromper, manipuler ou entraver la capacité des consommateurs à prendre des décisions libres et éclairées[4].

Bien que les articles 30 à 32 du RSN visent les fournisseurs de plateforme en ligne « *permettant aux consommateurs de conclure des contrats à distance avec des professionnels* », il est possible pour le droit national de cibler plus largement les **fournisseurs de places de marché en ligne**, en vertu de la directive « *Omnibus* » mentionnée plus haut.

Les infractions sont punies d'une peine de deux ans d'emprisonnement et d'une amende de 300 000 euros pouvant atteindre 6 % du chiffre d'affaires mondial pour une personne morale. Il est donné à la DGCCRF la possibilité de demander au juge civil d'enjoindre à l'auteur d'un manquement de se mettre en conformité, injonction qui peut être assortie d'une astreinte pouvant atteindre 5 % du chiffre d'affaires hors taxes journalier moyen réalisé au cours du dernier exercice clos. Des peines complémentaires sont créées pour les personnes physiques ainsi que pour les personnes morales dès lors qu'elles sont déclarées pénalement responsables.

d) L'adaptation des pouvoirs d'enquête et de sanction

Il est inséré une nouvelle section 4 au sein du chapitre II du titre I^er^ du livre V du code de la consommation, intitulée « Dispositions spécifiques aux plateformes en ligne », afin de régir de manière spécifique les pouvoirs des agents de la DGCCRF pour rechercher et constater les infractions au RSN :

– un article L. 512-66 dispose que la recherche et la constatation de ces infractions par la DGCCRF s'effectuent dans les mêmes conditions d'indépendance que celles qui régissent le coordinateur pour les services numériques[5] ;

[1] *Article 30 du RSN.*
[2] *Article 31 du RSN.*
[3] *Article 32 du RSN.*
[4] *Article 25 du RSN.*
[5] *Articles 49 et 50 du RSN.*

– un article L. 512-7 confère aux agents de la DGCCRF un pouvoir d'accès aux données de certaines plateformes nécessaires au contrôle de la bonne application du RSN, dans les mêmes conditions que le coordinateur national pour les services numériques[1] ;

– un article L. 512-68 prévoit la coopération entre les agents de la DGCCRF et les agents du coordinateur des services numériques, l'Arcom.

Il est aussi créé un article L. 531-7 pour sanctionner les **entraves à l'enquête** comme la fourniture d'informations inexactes ou le refus de se soumettre à une opération de visite et une saisie.

Enfin, l'article L. 521-3-1 est adapté pour élargir les cas où la DGCCRF peut avoir recours à la réquisition des plateformes en ligne :

– aux cas de manquement ou d'infraction aux règles relatives à la conformité et à la sécurité non seulement des produits, mais aussi des services ;

– lorsque le professionnel n'a pas déféré à une injonction en matière de sécurité des produits et des services ;

– aux cas d'infraction mettant en jeu la sécurité ou la santé des consommateurs lorsque l'auteur n'a pas déféré à une injonction.

2. La position de la commission : une adaptation du droit de la consommation qui doit s'accompagner d'une hausse indispensable des moyens alloués à la DGCCRF

La commission spéciale est favorable à une adaptation du droit national au droit de l'Union européenne permettant la bonne mise en œuvre du RSN sans contrariété juridique. Elle est également favorable à l'élargissement des missions et des pouvoirs de la DGCCRF qui découle de sa désignation comme autorité contrôlant la bonne application des obligations des fournisseurs de plateformes numériques prévues au RSN.

Toutefois, elle rappelle que l'élargissement, certes bienvenu, des missions de la DGCCRF doit aller de pair avec une **augmentation de ses moyens, budgétaires et humains**, et ce dès le prochain projet de loi de finances. Ce constat fait suite à plusieurs alertes de la commission des affaires économiques sur l'inadéquation entre les missions et les moyens de la DGCCRF. Au cours du dernier quinquennat, plus d'une trentaine de lois et ordonnances lui ont confié de nouvelles missions ainsi que des outils d'actions modernisés, sans que le Gouvernement ne mette ses moyens en adéquation avec ses nouveaux objectifs. Dans le cadre de l'examen du projet de loi de finances pour 2023, la commission des affaires économiques avait ainsi adopté un amendement visant à octroyer à la DGCCRF cinq millions d'euros supplémentaires en autorisation d'engagement.

---

[1] *Article 40 du RSN.*

Dès l'examen du prochain projet de loi de finances, la commission des affaires économiques se montrera donc attentive à la poursuite de la hausse des effectifs de la DGCCRF afin que ses moyens soient cohérents avec l'étendue de ses missions, notamment au vu des orientations qui seront précisées dans le prochain programme national d'enquête.

La commission spéciale a adopté deux amendements du rapporteur :

- l'amendement **COM-139** de précision rédactionnelle visant à déterminer l'amende maximale pouvant être prononcée pour sanctionner des manquements aux obligations des fournisseurs de plateformes en ligne en fonction du chiffre d'affaires mondial hors taxes de la personne morale contrôlée ;

- l'amendement **COM-140** de précision juridique visant à rappeler que les pouvoirs de contrôle de la DGCCRF des fournisseurs de plateforme en ligne au regard de leurs obligations s'exercent conformément au principe du pays d'origine.

La commission spéciale a adopté l'article 26 **ainsi modifié**.

CHAPITRE III
Modification du code de commerce

Article 27
Adaptation du code de commerce au règlement sur les marchés numériques

L'article 27 vise à adapter le code de commerce au règlement sur les marchés numériques (RMN) pour donner aux autorités françaises les moyens de conduire des investigations et de coopérer avec la Commission européenne sur les pratiques des contrôleurs d'accès.

La commission spéciale a adopté cet article sans modification.

1. Des mesures nécessaires d'adaptation du code de commerce au règlement européen sur les marchés numériques

a) La désignation des juridictions spécialisées

L'article 26 du projet de loi précise à l'article L. 420-7 du code de commerce que les litiges relatifs à l'application du RMN sont attribués aux **juridictions civiles et commerciales spécialisées actuellement compétentes pour les litiges en matière de pratiques anticoncurrentielles**, dont le siège et le ressort sont fixés par décret en Conseil d'État.

Il est également procédé à une actualisation des références aux articles des traités européens mentionnés au sein de cet article L. 420-7.

b) La désignation des autorités compétentes

Le code de commerce est complété d'un article L. 450-11 qui précise que l'Autorité de la concurrence (ADLC), le ministère chargé de l'économie et les fonctionnaire qu'il a désignés ou habilités - en pratique, à la Direction générale de la consommation, de la concurrence et de la répression des fraudes (DGCCRF) – **sont les autorités nationales chargées de faire appliquer** les règles mentionnées à l'article 1er, paragraphe 6 , du RMN, c'est-à-dire les règles de concurrence européennes et nationales concernant le contrôle des concentrations, les accords anticoncurrentiels, les décisions d'association, les pratiques concertées et les abus de position dominante.

En effet, le RMN ne se substitue pas à la régulation existante aux niveaux national et européen mais la complète avec **un cadre de régulation *ex ante* applicable à certains acteurs – les contrôleurs d'accès – sans priver ni les autorités nationales ni la Commission européenne de la possibilité d'intervenir en vertu d'autres règles existantes, éventuellement *ex post***.

c) Les pouvoirs reconnus à ces autorités

Le RMN rappelle que les autorités nationales coopèrent et échangent avec la Commission européenne dans le cadre d'un « **Réseau européen de concurrence** ». Ainsi, le code de commerce est complété par des articles précisant les compétences du ministre chargé de l'économie ainsi que de l'ADLC :

– un article L. 450-12 précise qu'ils disposent des pouvoirs reconnus par le code de commerce pour mener des **auditions et recueillir des déclarations**, pour effectuer des **inspections et des enquêtes de marché** en soutien à la commission et **pour ouvrir et conduire des investigations** sur un cas **de non-respect éventuel des obligations** imposées aux contrôleurs d'accès par le RMN ;

– un article L. 462-9-2 les rend compétents pour **recevoir les renseignements en provenance de tiers** sur toute pratique ou comportement des contrôleurs d'accès relevant du champ d'application du RMN, sans être tenus de donner suite aux renseignements reçus. En cas de non-respect au RMN, ils transmettent ces informations à la Commission européenne.

Enfin, le code de commerce est complété d'un article L. 490-9 qui précise que le ministre chargé de l'économie ou son représentant est habilité à adresser à la Commission européenne, conjointement avec au moins trois autres États membres, une **demande d'ouverture d'enquête de marché** lorsqu'il existe des motifs raisonnables de soupçonner qu'une entreprise est « contrôleur d'accès », en application de l'article 41 du RMN.

Ces articles actualisent également les références aux articles des traités européens mentionnés.

2. La position de la commission : une adaptation du code du commerce qui doit s'accompagner d'un renforcement indispensable des moyens alloués aux autorités administratives chargées de la concurrence

La commission spéciale est favorable à l'adaptation effective du droit national afin de permettre aux autorités nationales chargées de l'application du droit de la concurrence d'élargir leurs compétences actuelles en coordination avec la Commission européenne au bénéfice de la mise en œuvre du RMN.

En revanche, la commission note que ces nouvelles missions importantes nécessiteront un **renforcement significatif des moyens, notamment humains, de la DGCCRF et de l'ADLC.** Ces moyens n'ont pour l'instant pas été objectivés par le Gouvernement, même si l'étude d'impact mentionne des demandes de hausses d'équivalents temps plein portées par ces autorités. Lors de l'examen des prochains projets de loi de finances, la commission des affaires économiques sera donc très vigilante à l'octroi de moyens suffisants à l'ADLC et à la DGCCRF.

La commission spéciale a adopté l'article 27 **sans modification.**

CHAPITRE IV
Mesures d'adaptation de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication

Article 28
Adaptations au RSN de la loi n° 86-1087 du 30 septembre 1986 sur la liberté de communication

L'article 28 apporte diverses modifications à la loi du 30 septembre 1986 sur la liberté de communication afin de tirer les conséquences des nouvelles responsabilités dévolues à l'Arcom par le RSN et d'y intégrer les terminologies issues du « paquet numérique » européen.

La commission spéciale a adopté cet article en y apportant des modifications visant à clarifier sa rédaction.

1. Les mesures d'adaptation de la loi du 30 septembre 1986 relative à la liberté de communication

L'article 28 du projet de loi comporte diverses mesures d'adaptation de la loi du 30 septembre 1986 relative à la liberté de communication, dite « loi *Léotard* », pour tenir compte des nouvelles règles instaurées par le RSN. En particulier, il :

– opère des **actualisations terminologiques**, notamment pour substituer à la notion d'« opérateurs de plateforme en ligne », les notions similaires découlant du RSN. Ce faisant, il est cependant porteur de **divergences de rédaction peu compréhensibles, une même notion dans les textes en vigueur pouvant se trouver traduite de plusieurs manières différentes sans justification apparente**. C'est ainsi, par exemple, qu'alors que la loi de 1986 renvoie à la même notion d'« opérateurs de plateforme en ligne » au sens de l'article L. 111-7 du code de la consommation en ses articles 14 (contrôle de l'Arcom sur la programmation des émissions publicitaires) et 58 (recommandations de l'Arcom en matière lutte contre la manipulation de l'information en période électorale), le projet de loi ne rend que le premier de ces articles, mais non le second, applicable aux plateformes de partage de vidéos ;

– **met à jour des références législatives** ou procède à des abrogations, par coordination avec les autres dispositions du projet de loi ;

– réécrit, afin d'en prévoir l'articulation avec les nouveaux outils issus du RSN, les dispositions relatives à la publication, par l'Arcom, d'un **bilan périodique des actions entreprises par les plateformes au titre de la lutte contre la désinformation** ;

– confirme la compétence de l'Arcom pour superviser, y compris en utilisant ses pouvoirs d'enquête et d'injonction, le respect par les **plateformes de partage de vidéos** de leurs obligations.

Par ailleurs, l'article 28 maintient en vigueur, jusqu'au 17 février 2024 (au lieu du 31 décembre 2023), les dispositions transitoires issues de la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République et relatives aux **obligations des plateformes en ligne en matière de lutte contre les contenus haineux** : plus en détail, ces dispositions confient au Conseil supérieur de l'audiovisuel (donc aujourd'hui à l'Arcom) la mission de veiller au respect par les plateformes des obligations issues de l'article 6-4 de la LCEN s'agissant de la lutte contre les contenus illicites[1] et d'établir, à cet égard, des lignes directrices pour l'application de ces mêmes obligations. Il donne également au régulateur des pouvoirs d'accès aux données des plateformes, y compris avec une collecte automatisée, et le charge de définir les informations et indicateurs chiffrés que les opérateurs sont tenus de publier comme de publier lui-même, chaque année, un rapport établissant le bilan de ce mécanisme. Il le dote enfin d'un pouvoir de mise en demeure lui permettant

[1] *Il s'agit, plus précisément, des contenus visés par le troisième alinéa du 7 du I de l'article 6 de la LCEN (apologie, négation ou banalisation des crimes contre l'humanité ; provocation à la commission d'actes de terrorisme et leur apologie ; incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation sexuelle, de leur identité de genre ou de leur handicap ; pornographie enfantine ; incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes ; atteintes à la dignité humaine, y compris les faits de harcèlement en ligne…).*

de faire respecter, à peine de sanction pécuniaire, les obligations de l'article 6-4 ainsi que ses demandes d'accès aux données des opérateurs.

Ces dispositions avaient vocation à s'appliquer dans l'attente de l'entrée en vigueur du RSN, initialement prévue le 1er janvier 2024 ; la modification de la date d'échéance de ce régime provisoire est donc le reflet du report de cette entrée en application.

2. La position de la commission spéciale

La commission spéciale a adopté cet article, enrichi de plusieurs modifications adoptées à l'initiative du rapporteur Loïc Hervé pour :

– clarifier des rédactions ambiguës (amendement **COM-142**) ;

– consacrer la compétence de l'Arcom en matière de régulation des plateformes de partage de vidéo, cette notion n'étant pas absolument équivalente à celle de « plateforme en ligne » au sens du RSN (amendements **COM-141** et **COM-143**).

La commission spéciale a adopté l'article 28 **ainsi modifié**.

CHAPITRE V
Mesures d'adaptation de la loi relative à la lutte contre la manipulation de l'information

Article 29
Abrogation de trois articles de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (loi *Infox*)

L'article 29 du présent projet de loi tend à abroger les articles 11, 13 et 14 de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, dite loi *Infox*, dont plusieurs dispositions apparaissent couvertes par le règlement sur les services numériques (RSN).

Ces trois articles imposent aux plateformes en ligne un devoir de coopération en matière de lutte contre la diffusion de fausses informations, prenant la forme d'un dispositif de signalement spécifique aux fausses informations (article 11), la désignation d'un représentant légal exerçant les fonctions d'interlocuteur référent pour l'application des mesures relatives à la lutte contre la désinformation en ligne (article 13) et la publication de statistiques agrégées sur le fonctionnement des algorithmes de recommandation, classement ou référencement de contenus d'information se rattachant à un débat d'intérêt général (article 14).

La commission spéciale a adopté cet article en maintenant, dans le droit national, l'obligation, pour les plateformes en ligne, de mettre en place un dispositif de signalement des fausses informations.

1. Dans un objectif de « responsabilisation » des opérateurs de plateformes en ligne, la loi *Infox* de 2018 a imposé à ces derniers un devoir de coopération en matière de lutte contre la diffusion de fausses informations

a) Jusqu'en 2018, aucun dispositif spécifiquement dédié à la lutte contre la diffusion de fausses informations ne s'appliquait aux opérateurs de plateformes en ligne

Conformément à la directive 2000/31/CE du 8 juin 2000[1], dite directive sur le commerce électronique, le principe d'ensemble régissant l'écosystème numérique repose sur **un régime de responsabilité limitée des hébergeurs et des intermédiaires techniques**, **qui n'ont pas une obligation générale de surveillance des contenus** publiés sur leur plateforme en ligne.

Cette obligation s'imposant à l'échelle européenne a été transposée en droit interne à l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique[2] (LCEN), lequel dispose, en son point 7, que les hébergeurs et les intermédiaires techniques « *ne sont pas soumis à une obligation générale de surveiller les informations qu'[ils] transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites*. »

Cependant, si les hébergeurs n'ont pas d'obligation de surveillance, ils doivent tout de même **mettre en place des dispositifs de signalement** pour certains types de contenus, définis par la loi.

Ce dispositif doit être « *facilement accessible et visible* » et permettre « *à toute personne de porter à [la] connaissance* » des hébergeurs les « *activités illicites* » définies par la loi. Une fois ces activités illicites signalées aux hébergeurs, **ces derniers sont sommés d'en « *informer promptement les autorités publiques compétentes* »**. Ces signalements sont alors traités par le portail officiel de signalement des contenus illicites de l'Internet, Pharos, géré par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Les hébergeurs doivent en outre « *rendre publics les moyens qu'[ils] consacrent à la lutte contre [ces] activités illicites* »[3].

---

[1] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.*

[2] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*

[3] *Article 6 de la loi du 21 juin 2004 précitée.*

En l'état actuel du droit[1], les contenus illicites mentionnés à l'article 6 de la LCEN, pour lesquels les hébergeurs doivent mettre en place des dispositifs de signalement, appartiennent à deux catégories :

– les activités illégales de jeux d'argent ;

– **les activités en lien avec la sécurité et la dignité humaine**, à savoir « l'apologie, la négation ou la banalisation des crimes contre l'humanité, la provocation à la commission d'actes de terrorisme et leur apologie, l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation sexuelle, de leur identité de genre ou de leur handicap ainsi que la pornographie enfantine, l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que les atteintes à la dignité humaine »[2].

Ainsi, le cadre général régissant les obligations de mise en place de dispositifs de signalement s'appliquant aux opérateurs de plateformes en ligne n'inclut pas les fausses informations, lesquelles sont définies par l'article L. 163-2 du code électoral comme « *toute allégation ou imputation d'un fait inexacte ou trompeuse […] diffusée de manière délibérée* ».

La diffusion délibérée de fausses informations est cependant sanctionnée par plusieurs textes, depuis au moins la loi du 29 juillet 1881 sur la liberté de la presse qui a instauré un délit de « fausses nouvelles », sans pour autant que ces dispositions, souvent anciennes, ne prévoient de mesures spécifiques à la désinformation en ligne.

Synthèse des principales dispositions législatives réprimant la désinformation, hors dispositions liées au numérique

Fondements	Qualifications/Principe	Peines encourues/actions
Article 27 de la loi du 29 juillet 1881	Délit de fausses nouvelles	45 000 € d'amende (135 000 € en cas de faits de nature à « *ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation* »)
Articles 29, 30, 31 et 32 de la loi du 29 juillet 1881	Délit de diffamation publique	12 000 € d'amende (45 000 € si la personne visée est un élu par exemple)
Article L. 97 du code électoral	Délit de fausses nouvelles ayant altéré un scrutin	Un an d'emprisonnement et 15 000 € d'amende
Article 9 du code civil	Droit au respect de la vie privée	Action en référé possible Action en réparation

[1] *L'article 22 du présent projet de loi procède à une nouvelle rédaction de l'article 6 de la loi du 21 juin 2004 précitée.*

[2] Ibid.

Fondements	Qualifications/Principe	Peines encourues/actions
Article 226-8 du code pénal	Délit de photomontage ou montage sonore sans le consentement et sans consentement et sans précision qu'il s'agit d'un montage	Un an d'emprisonnement et 15 000 € d'amende

Source : commission spéciale

b) La loi Infox *de 2018 a soumis les opérateurs de plateformes en ligne à de nouvelles obligations de transparence des algorithmes et de signalement des fausses informations*

Le législateur français a récemment cherché à remédier à l'absence de dispositif dédié à la lutte contre les fausses informations en ligne **en instaurant un mécanisme *ad hoc* régi par la loi dite *Infox*** du 22 décembre 2018[1], et donc distinct du cadre général porté par l'article 6 de la loi pour la confiance dans l'économie numérique.

L'un des objectifs de la loi *Infox*, selon les termes de la rapporteure du texte pour la commission de la culture, de l'éducation et de la communication du Sénat, Catherine Morin-Desailly, consistait à **confier aux opérateurs de plateformes en ligne « *de nouvelles responsabilités* »[2] en matière de lutte contre la désinformation**, tout en respectant les principes généraux définis par la directive européenne relative à l'économie numérique (*cf. supra*).

Pour atteindre cet objectif, le titre III de la loi *Infox* impose aux opérateurs de plateformes en ligne **un devoir de coopération en matière de lutte contre la diffusion de fausses informations**.

Ce devoir de coopération se matérialise par leur assujettissement à de nouvelles règles, définies notamment aux articles 11, 13 et 14 de la loi *Infox* :

– l'article 11 leur impose, d'une part, **de mettre en place un dispositif de signalement,** « *facilement accessible et visible* », **spécifique aux fausses informations** susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un scrutin et, d'autre part, de prendre des « *mesures complémentaires* » pouvant « *notamment* » porter sur « *la transparence des algorithmes* », « *la promotion de certains contenus d'entreprises et d'agences de presse et d'éditeurs audiovisuels* », « *la lutte contre certains comptes qui propagent des fausses informations* », « *la transparence vis-à-vis de l'identité des personnes pour le compte desquelles les contenus sont diffusés* » ou encore « *l'éducation aux*

[1] *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation en ligne.*

[2] *Rapport n° 677 (2017-2018) de Catherine Morin-Desailly, fait au nom de la commission de la culture, de l'éducation et de la communication, sur la proposition de loi relative à la lutte contre la manipulation de l'information, déposé le 18 juillet 2018.*

médias et à l'information ». Ces mesures doivent être rendues publiques et donnent lieu à « *une déclaration* » adressée à l'Arcom ;

– l'article 13 impose aux mêmes opérateurs de plateformes **la désignation d'un représentant légal exerçant les fonctions « d'interlocuteur référent »** sur le territoire français pour l'application des mesures relatives à la lutte contre la désinformation en ligne et contre les « activités illicites » mentionnées au point 7 de l'article 6 de la LCEN (*cf. supra*) ;

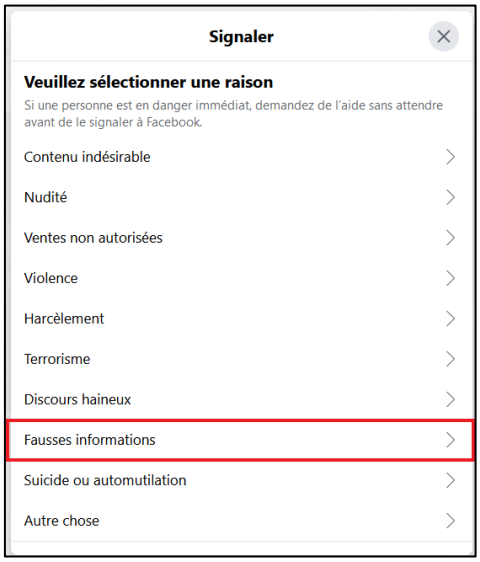
– enfin, l'article 14 prévoit **la publication** en format libre et ouvert, par chaque opérateur de plateforme en ligne, **de statistiques agrégées sur le fonctionnement des algorithmes de recommandation, classement ou référencement** de contenus d'information se rattachant à un débat d'intérêt général.

Aucune sanction n'est passible en cas de manquement aux obligations résultant de ces trois articles, à l'exception de la publicité négative qui pourrait advenir de la publication du bilan annuel de l'Arcom en matière de lutte contre la désinformation en ligne (*cf. infra*).

En application de l'article D. 111-15 du code de la consommation, ces obligations concernent les opérateurs dont les plateformes dépassent un seuil de cinq millions de connexions de visiteurs uniques par mois.

À titre d'illustration, cela inclut le groupe Meta, auquel appartient la plateforme Facebook. Celle-ci a rassemblé au sein d'un onglet unique les divers motifs pour lesquels la LCEN et la loi *Infox* lui imposent de mettre à la disposition de l'utilisateur un dispositif de signalement, incluant les fausses informations.

Dispositif de signalement de la plateforme Facebook



Source : Commission spéciale d'après une capture d'écran issue de la plateforme Facebook

c) Une application « globalement satisfaisante » *des mesures de lutte contre les fausses informations*

Aussi bien dans son bilan annuel des moyens et mesures mis en œuvre par les opérateurs de plateforme en ligne sur l'année 2021[1] qu'en réponses aux interrogations formulées par le rapporteur Loïc Hervé, **l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) a indiqué que les opérateurs concernés se soumettaient désormais de façon « *globalement satisfaisante* » à l'obligation de mise en place d'un outil de signalement des fausses informations** susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un des principaux scrutins.

L'Autorité estime néanmoins que **l'accessibilité et la visibilité de cet outil demeurent « *inégales* » d'une plateforme à l'autre**, en particulier pour les moteurs de recherche. De plus, l'Arcom déplore « *un manque flagrant* » d'indicateurs et de données chiffrées relatives aux signalements et à l'efficacité de leur traitement, empêchant une évaluation de la pertinence et l'efficacité des mesures au regard des risques associés à chacun des services.

Si la mise en place d'un dispositif de signalement des fausses informations est obligatoire, les « *mesures complémentaires* » que prévoit, de façon moins contraignante, l'article 11 de la loi *Infox* (*cf. supra*) ont également été déployées par tous les opérateurs concernés. L'Arcom a cependant constaté que le déploiement de ces mesures a été « *plus ou moins approfondi* » selon les opérateurs, certains ayant instauré volontairement des dispositifs allant au-delà de leurs obligations légales, comme par exemple des outils de lutte contre les publicités comportant de la désinformation ou de lutte contre les hypertrucages[2] à visée de désinformation. Ces mêmes disparités entre opérateurs ont été identifiées en matière d'éducation aux médias et à l'information, la quantité d'actions engagées par les opérateurs en direction des utilisateurs variant fortement.

Toujours selon l'Arcom, **l'article 13 de la loi *Infox***, imposant aux opérateurs de plateformes en ligne de désigner un référent national en matière de lutte contre la désinformation, **a été respecté par l'ensemble des opérateurs concernés**, à l'exception de Wikipédia. Toutefois, l'Arcom a noté qu'à la suite de départs des référents de deux opérateurs (Snapchat et Twitter), aucun nouveau référent n'a pas été désigné, malgré ses demandes.

Ce bilan plutôt favorable est néanmoins nuancé par les efforts de transparence qui pourraient, selon l'Arcom, être encore accrus, notamment en termes de transmission de données chiffrées et d'informations concernant les modèles de vente et d'enchères et le ciblage publicitaire.

---

[1] *Bilan annuel (2021) des moyens et mesures mis en œuvre par les opérateurs de plateforme en ligne pour lutter contre la manipulation de l'information en application de la loi du 22 décembre 2018, publié en novembre 2022 par l'Arcom.*

[2] *Les* « deepfakes ».

2. L'article 29 procède à l'abrogation de trois articles traitant de la lutte contre la désinformation, qui ne sont que partiellement couverts par le RSN

L'article 29 du projet de loi tend à abroger les articles 11, 13 et 14 de la loi *Infox*, décrits ci-dessus.

Cette abrogation serait justifiée par leur redondance avec le règlement sur les services numériques, qui est d'application directe et dont certains articles couvrent des sujets similaires.

a) Le signalement des fausses informations

L'article 16 du RSN, qui s'applique aux fournisseurs de services d'hébergement, y compris les plateformes en ligne, prévoit **l'instauration obligatoire de « *mécanismes permettant à tout particulier ou à toute entité de leur signaler la présence au sein de leur service d'éléments d'information spécifiques que le particulier ou l'entité considère comme du contenu illicite* »**. Ce dispositif de signalement doit être « *facile d'accès et d'utilisation et permettent la soumission de notifications exclusivement par voie électronique* ».

Ce dispositif de signalement est présenté dans l'étude d'impact du projet de loi comme une obligation similaire à celle qui résulte de l'article 11 de la loi *Infox*. Il convient cependant de noter que la définition juridique des « contenus illicites » est imprécise, ce qui pourrait entraîner des divergences d'interprétation quant à l'intégration ou non des fausses informations au sein du dispositif de signalement.

En effet, bien que le considérant n° 12 du RSN dispose qu'il faille « ***donner une définition large de la notion de contenu illicite*** », il ne mentionne par la suite que « *les informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales* ». Outre que les fausses informations ne sont pas nommément incluses au sein du considérant n° 12, l'absence, en droit interne, de définition des fausses informations plus claire que celle qui résulte de l'article L. 163-2 du code électoral rend incertaine l'intégration de celles-ci parmi le nouveau régime d'obligations issu du RSN s'appliquant aux opérateurs de plateformes en ligne.

Ainsi, interrogée par le rapporteur, l'Arcom confirme ces inquiétudes en considérant que « *si le législateur a précisé le type de phénomènes contre lequel les plateformes doivent lutter, la manipulation de l'information et les fausses informations ne font pas l'objet d'une définition légale* » faisant consensus. C'est pourquoi les fausses informations ne semblent ainsi relever des « *contenus illicites* » mentionnés par le RSN « *que dans l'hypothèse où leur diffusion permet par ailleurs de caractériser une infraction prévue en droit français* ». La Direction générale des entreprises (DGE) estime quant à elle sans ambiguïté que « ***les fausses informations mentionnées à l'article 11 de***

la loi* Infox *ne sont pas des contenus illicites »[1] tels que mentionnés à l'article 16 du RSN, puisque le signalement de ces informations ne déclenchera pas le régime de responsabilité limité des services d'hébergement. La DGE considère que ces éléments restrictifs maintiennent néanmoins la possibilité, pour l'utilisateur, de signaler malgré tout une fausse information par le biais du mécanisme de signalement des contenus illicites prévu à l'article 16 du RSN.

En parallèle du RSN, les fausses informations font l'objet de plusieurs mesures au sein du code européen renforcé de bonnes pratiques contre la désinformation du 16 juin 2022, notamment **l'engagement n° 23 qui prévoit la mise en place d'un dispositif de signalement relatif aux « *informations fausses et/ou préjudiciables* ». Ce code de conduite n'est toutefois soumis qu'à la bonne volonté des opérateurs de plateformes en ligne**, lesquels ne sont pas obligés d'y souscrire : d'après la Commission européenne, seuls 34 d'entre eux y ont adhéré lors de la présentation de ce code de bonnes pratiques[2], dont Twitter qui s'en est depuis retiré.

En outre, dans le cadre de l'évaluation des risques systémiques mentionnés à l'article 34 du RSN, les très grandes plateformes en ligne et les très grands opérateurs de recherche en ligne doivent « *recenser, analyser et évaluer* » les risques liés « *à la diffusion de contenus illicites par l'intermédiaires de leurs services* ». **La commission spéciale appelle à ce que soit adoptée une acception « *large* », pour reprendre le terme du considérant n° 12, de ces contenus illicites afin d'y inclure les fausses informations**, notamment au regard de l'article 35 qui mentionne également les « *risques systémiques* » ayant un « *effet négatif réel ou prévisible sur le discours civique, les processus électoraux et la sécurité publique* ».

b) Les mesures « complémentaires » de lutte contre la désinformation

Plusieurs articles du RSN traitent des « mesures complémentaires » que peuvent mettre en place les opérateurs de plateformes en ligne, conformément à l'article 11 de la loi *Infox* précitée :

– la transparence des algorithmes et des modalités de diffusion des contenus est régie par l'article 27 du RSN ;

– la transparence sur l'identité des commanditaires de contenus publicitaires est imposée par l'article 26 du RSN.

En revanche, **certaines dispositions n'ont aucun équivalent dans le RSN ou vont au-delà des obligations que ce règlement impose**, ce qui signifie que leur abrogation ne serait pas compensée par celui-ci. Il s'agit :

– de l'éducation aux médias et à l'information (aucun équivalent dans le RSN) ;

---

[1] *Source : réponse écrite de la DGE au questionnaire du rapporteur.*

[2] *Commission européenne, Bâtir l'avenir numérique de l'Europe.*

– de la promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle (aucun équivalent dans le RSN) ;

– et de la lutte contre les comptes qui propagent des fausses informations. Ce dernier point va au-delà de l'article 23 du RSN, qui impose aux opérateurs de plateformes en ligne de suspendre les utilisateurs qui « *fournissent fréquemment des contenus manifestement illicites* », sans qu'il ne soit fait mention particulière des fausses informations.

c) La désignation d'un référent

L'article 13 de la loi *Infox* impose aux opérateurs de plateformes en ligne la désignation d'un représentant légal sur le territoire français, exerçant les fonctions d'interlocuteur référent en matière de lutte contre la désinformation et de contenus illicites.

Cette obligation n'est que partiellement couverte par l'article 13 du RSN, qui impose certes la désignation d'un représentant légal pour tous les fournisseurs de services intermédiaires proposant des services dans l'Union sans avoir d'établissement au sein de l'Union européenne, mais **sans pour autant confier à ce représentant une mission particulière concernant la lutte contre la désinformation**. Tout au plus est-il précisé que « *le représentant légal désigné peut être tenu pour responsable du non-respect des obligations prévues par le règlement [sur les services numériques]* ».

d) La transparence des algorithmes

Enfin, comme évoqué précédemment, **le RSN comporte un article dédié à la transparence du système de recommandation, lequel, sans être aussi exigeant en termes de transparence, recouvre en partie l'article 14 de la loi *Infox***. L'article 27 du RSN dispose ainsi que « *les fournisseurs de plateformes en ligne qui utilisent des systèmes de recommandation établissent dans leurs conditions générales, dans un langage simple et compréhensible, les principaux paramètres utilisés dans leurs systèmes de recommandation, ainsi que les options dont disposent les destinataires du service pour modifier ou influencer ces principaux paramètres* ».

L'article 14 de la loi *Infox* allait cependant plus loin puisqu'il imposait aux opérateurs de plateformes en ligne de publier des statistiques agrégées sur le fonctionnement des algorithmes de recommandation, classement ou référencement de contenus d'information se rattachant à un débat d'intérêt général. Ces statistiques devaient notamment faire apparaître la part d'accès direct, sans recours aux algorithmes de recommandation, classement ou référencement, à ces contenus, ainsi que les parts d'accès indirects imputables, d'une part, à l'algorithme du moteur de recherche interne de la plateforme le cas échéant et, d'autre part, aux autres algorithmes de recommandation, classement ou référencement de la plateforme qui sont intervenus dans l'accès aux contenus.

3. L'indispensable maintien d'un dispositif de signalement des fausses informations

Contrairement à ce qu'énonce l'étude d'impact du projet de loi, **le règlement sur les services numériques (RSN) ne couvre pas l'obligation, pour les opérateurs de plateformes en ligne, de mettre en place un dispositif de signalement des fausses informations**, présentement imposée par l'article 11 de la loi *Infox*, puisqu'aussi bien l'Arcom que le Gouvernement ont indiqué au rapporteur que les « *contenus illicites* » mentionnés à l'article 16 du RSN n'incluent pas les fausses informations (*cf. supra*).

L'abrogation, non compensée par le RSN, de l'article 11 de la loi *Infox* signifierait **un net recul en matière de lutte contre la désinformation en ligne**.

C'est pourquoi **la commission spéciale a adopté l'amendement COM-144**, présenté par son rapporteur, afin **de conserver, dans le droit national, l'obligation, pour les plateformes en ligne, de mettre en place un dispositif de signalement des fausses informations**. Ce faisant, la Commission invite le Gouvernement à défendre auprès des instances européennes « *une définition large de la notion de contenu illicite* », conformément aux termes du considérant n° 12 du RSN.

La commission spéciale a cependant maintenu l'abrogation des articles 13 et 14 de la loi *Infox*, ainsi que la suppression des dispositions de l'article 11 relatives aux « *mesures complémentaires* » que peuvent prendre les plateformes en matière de lutte contre la désinformation, lesquels apparaissent *in globo* couverts par le RSN.

La commission spéciale a adopté l'article 29 **ainsi modifié**.

CHAPITRE VI
Mesures d'adaptation du droit électoral

Article 30
Rehaussement du seuil de connexions à partir duquel s'appliquent certaines règles de transparence relatives à la propagande en ligne en période électorale

L'article 30 tend à modifier l'article L. 163-1 du code électoral, lequel impose aux opérateurs de plateforme en ligne des obligations de transparence renforcée en matière de propagande numérique pendant les périodes électorales. Alors que ces obligations s'appliquent, en l'état actuel du droit, à toutes les plateformes dont le nombre de connexions mensuelles de visiteurs uniques dépasse le seuil national de cinq millions, l'article 30 n'imposerait désormais ces obligations qu'aux seules plateformes dépassant un seuil européen de 45 millions de visiteurs uniques par mois.

La commission spéciale a adopté cet article sans modification, tout en invitant le Gouvernement à veiller à ce que l'adoption future du règlement européen relatif à la transparence et au ciblage de la publicité à caractère politique n'entraîne pas à nouveau un recul par rapport au droit national en matière d'encadrement de la publicité politique en ligne.

1. Afin de veiller à la sincérité des scrutins, les opérateurs de plateformes en ligne sont soumis, depuis la loi *Infox* de 2018, à des obligations de transparence renforcée en matière de propagande lors des périodes électorales

Bien que de nombreuses règles régissent déjà les abus de propagande électorale[1] et que le code de la consommation encadre l'usage de la publicité en ligne, en imposant notamment, en son article L. 111-7, à tout opérateur de plateforme en ligne de délivrer au consommateur « *une information loyale, claire et transparente* » sur « *l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne* » et sur « *la qualité de l'annonceur* », **le législateur a souhaité instaurer des obligations supplémentaires, ne s'appliquant qu'en période électorale**. L'objectif mis en avant était d'assurer

[1] *Sans être exhaustif, peuvent être citées l'interdiction, pour tout agent de l'autorité publique ou municipale de distribuer des bulletins de vote, profession de foi et circulaires des candidats (art. L. 50 du code électoral), l'interdiction, pour un candidat d'utiliser directement ou indirectement pour sa campagne les indemnités et les avantages en nature mis à disposition de leurs membres par les assemblées parlementaires pour couvrir les frais liés à l'exercice de leur mandat (article L. 52-8-1 du même code), ou encore l'interdiction de l'utilisation à des fins de propagande électorale de tout procédé de publicité commerciale par la voie de la presse ou par tout moyen de communication audiovisuelle dans les six mois précédant un scrutin (article L. 52-1 dudit code).*

« *l'intérêt général attaché à l'information éclairée des citoyens en période électorale* » et de garantir « *la sincérité du scrutin* »[1].

Ainsi, la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information[2], dite loi *Infox*, a inséré un nouvel article L. 163-1 au sein du code électoral, afin de règlementer la promotion de contenus d'information se rattachant à un débat d'intérêt général.

Depuis 2018, **les opérateurs de plateformes en ligne dépassant le seuil**, défini par décret[3], **de cinq millions de connexions** mensuelles de visiteurs uniques, **sont donc tenus de fournir « *une information loyale, claire et transparente* » sur les personnes morales ou physiques « *versant à la plateforme des rémunérations* *en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général* »**, sur « *l'utilisation* » qui est faite « *des données personnelles* » de l'utilisateur « *dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général* » et, enfin, sur « *le montant des rémunérations reçues en contrepartie de la promotion de tels contenus* ».

Toutes ces informations sont agrégées en format ouvert au sein d'un « *registre* » mis à la disposition du public sur un support électronique.

Cet effort de transparence accentuée n'est exigé des opérateurs de plateforme en ligne **que lors des trois mois précédant le premier jour du mois d'élections générales** et jusqu'à la date du tour de scrutin où celles-ci sont acquises. Ces obligations s'appliquent donc pour les élections législatives, les élections sénatoriales[4], les élections européennes[5], les opérations référendaires[6] et l'élection du Président de la République[7]. *A contrario*, elles ne sont pas exigibles lors d'élections partielles et pour les scrutins locaux.

Il appert cependant qu'en imposant des obligations de transparence concernant tout « *contenu d'information se rattachant à un débat d'intérêt général* », l'article L. 163-1 du code électoral a **un périmètre d'application plus large que les seules informations de nature à altérer la sincérité d'un scrutin**.

En application de l'article L. 112 du code électoral, **les personnes ne satisfaisant pas aux règles fixées à l'article L. 163-1 précité encourent une peine d'un an d'emprisonnement et de 75 000 euros d'amende, pouvant être portée au quintuple lorsqu'il s'agit d'une personne morale**. Le juge pénal peut, en outre, prononcer l'interdiction, pour une durée de cinq ans au

---

[1] *Selon les termes employés par le premier alinéa de l'article L. 163-1 du code électoral.*
[2] *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.*
[3] *Article D. 111-15 du code de la consommation.*
[4] *Par le renvoi figurant à l'article L. 306 du code électoral.*
[5] *Par le renvoi figurant à l'article 14-2 de la loi n° 77-729 du 7 juillet 1977 relative à l'élection des représentants au Parlement européen.*
[6] *Par le renvoi figurant à l'article L. 558-46 du code électoral.*
[7] *Par le renvoi figurant à l'article 3 de la loi organique n° 62-1292 du 6 novembre 1962.*

plus, d'exercer directement ou indirectement l'activité professionnelle en lien avec l'infraction. Le juge peut également ordonner l'affichage de la décision de justice ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

2. L'article 30 du projet de loi rehausse significativement le seuil de connexions à partir duquel s'appliqueraient les obligations de transparence renforcée en matière de propagande électorale en ligne

a) L'article 30 du projet de loi vise à adapter le code électoral au RSN

Tel que déposé au Sénat, l'article 30 du projet de loi apporte deux modifications principales à l'article L. 163-1 du code électoral :

– il restreint le nombre de plateformes concernées par les obligations de transparence précitées, en remplaçant la référence aux opérateurs de plateforme en ligne mentionnés à l'article L. 111-7 du code de la consommation par une référence aux « *très grandes plateformes en ligne et les très grands moteurs de recherches en ligne* » définis à l'article 33 du règlement européen sur les services numériques (RSN). **Le seuil à partir duquel les plateformes appartiennent à cette catégorie a été fixé à 45 millions d'utilisateurs européens par mois**, soit 10 % de la population européenne, contre, pour mémoire, cinq millions de connexions mensuelles uniques en l'état actuel du droit interne. La Commission européenne n'a, pour l'instant, désigné que **17 plateformes catégorisées comme « *très grandes* »**, à savoir Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube et Zalando, et **deux « *très grands* » moteurs de recherche**, à savoir Bing et Google Search. À titre d'exemple, parmi les opérateurs soumis, en droit actuel, aux obligations de transparence issues de l'article L. 163-1 du code électoral, Twitch, Yahoo Search et Dailymotion en seraient exemptés du fait de ce rehaussement du seuil d'application ;

– il remplace l'actuel registre recensant les données relatives à la propagande numérique par un registre, issu de l'article 39 du RSN, qui concerne de façon plus large la publicité en ligne (*cf. infra*).

Ces deux modifications sont présentées par le Gouvernement comme une nécessaire adaptation au règlement sur les services numériques[1].

[1] Cf. *l'étude d'impact annexée au présent projet de loi.*

b) Le RSN prévoit un régime de transparence publicitaire plus exigeant pour les « très grandes plateformes en ligne » *et les* « très grands moteurs de recherche »

Concernant la transparence du caractère publicitaire des contenus numériques, **le règlement sur les services numériques distingue deux régimes d'obligations, le premier s'imposant à tous les fournisseurs de plateformes en ligne, le second s'appliquant cumulativement pour les seuls « *très grandes plateformes en ligne* » et « *très grands moteurs de recherche* »**.

1. Une obligation de présentation « non ambiguë » des contenus publicitaires pour tous les fournisseurs de plateformes en ligne

L'article 26 du RSN, qui s'applique à tous les fournisseurs de plateformes en ligne, constitue le cadre normatif minimal en matière de transparence des contenus publicitaires.

Il impose aux fournisseurs de plateformes en ligne qui affichent de la publicité sur leur interface **de « *veiller à ce que, pour chaque publicité spécifique* » présentée à chaque utilisateur individuel, celui-ci puisse « *de manière claire, précise et non ambiguë et en temps réel* » identifier le caractère publicitaire du contenu**.

Plus précisément, l'utilisateur doit être en mesure :

– de se rendre compte que les informations sont de la publicité, y compris au moyen de marquages bien visibles ;

– d'identifier la personne physique ou morale pour le compte de laquelle la publicité est présentée ou, le cas échéant, qui a payé pour la publicité ;

– de déterminer les informations utiles, qui doivent être directement et facilement accessibles à partir de la publicité, concernant les principaux paramètres utilisés pour cibler l'utilisateur auquel la publicité est présentée et, le cas échéant, la manière dont ces paramètres peuvent être modifiés.

2. La publication d'un « registre » *contenant des informations détaillées sur les contenus publicitaires pour les* « très grandes » *plateformes et les* « très grands » *moteurs de recherche*

En parallèle des obligations de transparence imposées par l'article 26 du RSN, **les très grandes plateformes et les très grands moteurs de recherche sont soumis à la publication d'un « *registre* »,** qu'ils doivent mettre à la disposition du public, dans une section spécifique de leur interface. Cette responsabilité supplémentaire résulte de **l'article 39 du RSN**, qui précise par ailleurs que ce registre comporte un outil de recherche « *fiable* » permettant d'effectuer des recherches multicritères.

Ce registre doit présenter avec « *exactitude* » :

– le contenu de la publicité, y compris le nom du produit, du service ou de la marque, ainsi que l'objet de la publicité ;

– la personne physique ou morale pour le compte de laquelle la publicité est présentée ou, le cas échéant, qui a payé pour la publicité ;

– la période au cours de laquelle la publicité a été présentée ;

– le fait que la publicité était ou non destinée à être présentée spécifiquement à un ou plusieurs groupes particuliers de destinataires du service et, dans l'affirmative, les principaux paramètres utilisés à cette fin, y compris, s'il y a lieu, les principaux paramètres utilisés pour exclure un ou plusieurs de ces groupes particuliers ;

– le nombre total de destinataires du service atteint et, le cas échéant, les nombres totaux ventilés par État membre pour le ou les groupes de destinataires que la publicité ciblait spécifiquement.

La liste des informations que doit contenir ce registre n'est cependant pas limitée par l'article 39 du RSN, puisque le premier alinéa du paragraphe 2 de ce même article dispose que ce registre **contient « *au moins* » les informations susmentionnées**. Cette précision est d'importance puisque les articles 26 et 39 du RSN n'évoquent pas, contrairement à l'article L. 163-1 du code électoral, le montant des rémunérations reçues en contrepartie de la promotion des contenus publicitaires.

3. Le maintien d'obligations de transparence renforcée pour les plus grandes plateformes approuvé par la commission spéciale

La commission spéciale a adopté l'article 30 sans modification, en se félicitant que le Gouvernement soit revenu sur son projet initial d'abrogation de l'article L. 163-1 du code électoral, comme l'a conseillé le Conseil d'État dans son avis public[1] sur le projet de loi.

Au demeurant, le rehaussement du seuil à partir duquel s'appliqueront les exigences de transparence renforcée en matière de publicité politique en ligne constitue malgré tout un recul par rapport à l'état actuel du droit, puisque certains opérateurs, à l'instar de Twitch, Yahoo Search et Dailymotion, s'en verraient exemptés.

La commission spéciale prend cependant acte que **le RSN sera bientôt complété par un règlement européen relatif à la transparence et au ciblage de la publicité à caractère politique**, actuellement en phase de trilogue. **Elle invite par conséquent le Gouvernement à être particulièrement vigilant lors des négociations autour de ce futur**

[1] *Consultable en ligne sur le site du Sénat.*

règlement européen, afin de maintenir un cadre normatif ambitieux, qui garantira la sincérité et la qualité du débat démocratique en ligne.

La commission spéciale a adopté l'article 30 **sans modification**.

CHAPITRE VII
Mesures d'adaptation de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Article 31
Adaptations de la loi n° 78-17 « Informatique et libertés » au règlement européen sur la gouvernance des données (*Data Governance Act* – altruisme en matière de données)

L'article 31 apporte diverses modifications à la loi « Informatique et libertés » du 6 janvier 1978 afin d'adapter celle-ci aux règles issues du règlement européen sur la gouvernance des données dit *Data Governance Act (DGA)* et de consacrer les nouvelles compétences de la Cnil dans le domaine de l'altruisme en matière de données.

La commission spéciale a adopté un **amendement de réécriture globale de cet article** afin de faciliter l'insertion de ces dispositions au sein de la loi « Informatique et libertés » et de combler les lacunes du texte initial s'agissant des modalités de mise en œuvre par la Cnil de ses nouvelles prérogatives.

1. Les apports du règlement *DGA* : de nouvelles règles pour garantir l'altruisme en matière de données sous le contrôle de la Cnil

Lié à la volonté de l'Union européenne de faire face à l'utilisation des données par les GAFAM et d'éviter une distorsion de concurrence préjudiciable aux entreprises européennes, le règlement européen sur la gouvernance des données, ou règlement *DGA*, vise à fixer un cadre commun pour faciliter le partage de données tout en créant des mécanismes de gouvernance afin de limiter les atteintes apportées à la vie privée des Européens et de garantir une souveraineté de l'Union sur les données qu'elle produit. C'est ainsi que ce règlement entend créer un marché de l'intermédiation de la donnée fondé sur une conception alternative à celle qui prévaut actuellement : en effet, alors que les données sont aujourd'hui largement vendues ou achetées par les entreprises qui les utilisent, le *DGA* vise à mettre en place un modèle reposant sur la commercialisation des données par des « tiers de confiance » qui ne les utilisent pas eux-mêmes.

Concrètement, le règlement :

– crée un Comité européen de l'innovation dans le domaine des données et **prévoit la désignation, dans chaque État, d'une autorité nationale compétente** ;

– définit les conditions de réutilisation des données, en particulier afin d'exclure d'une telle réutilisation certaines données sensibles par destination ou par nature (données détenus par des entreprises publiques, des établissements culturels ou d'enseignement, *etc.* ; données à la défense, à la sécurité, *etc.*), ou encore d'interdire les transferts internationaux hors de l'Union dès lors que ces transferts sont contraires aux réglementations européennes ou internationales. Le règlement vient également limiter la possibilité d'octroyer des droits d'exclusivité aux données partagées aux cas où cette exclusivité est nécessaire à la fourniture d'un service public ou d'un produit d'intérêt général. Dans les cas où la réutilisation sera possible, **il est prévu que l'accès aux données puisse se faire en contrepartie du versement d'une redevance** ;

– pose le cadre applicable aux services d'intermédiation de données, c'est-à-dire aux services visant à établir des relations commerciales à des fins de partage des données entre les détenteurs et les utilisateurs. Le règlement prévoit ainsi que les personnes souhaitant exercer une telle activité devront notifier leur intention (sans que cette procédure s'apparente à une autorisation préalable) à l'autorité nationale compétente[1] et se soumettre au respect de diverses règles, notamment en matière de sécurité des données stockées, de traçabilité des usages et de prévention des pratiques frauduleuses ou abusives ;

– définit le cadre de collecte et de traitement des données à des fins « altruistes », c'est-à-dire sans contrepartie financière : le *DGA* permet ainsi la mise à disposition volontaire de données pour des motifs d'intérêt général (ces motifs devant être définis par le droit national). Les données concernées seront **remises à des organisations dites « *altruistes* », inscrites sur un registre tenu par l'autorité nationale compétente**, et qui ne pourront être reconnues comme telles que si elles poursuivent un objectif d'intérêt général et respectent, de manière effective, les obligations énumérées par le règlement (entités à but non lucratif, recueil du consentement des personnes concernées, garantie de la sécurité des données, établissement d'un rapport d'activité rendant compte de leur action…).

Enfin, en matière de données personnelles, le *DGA* pose lui-même le principe de son **infériorité normative par rapport au RGPD** : en d'autres termes, en cas de difficultés d'articulation (voire de rivalité ou de contradiction de règles) entre ces deux textes, le RGPD primera.

---

[1] *L'autorité nationale compétente sur ce volet du* DGA *est l'Arcep (voir ci-avant, article 11 du présent projet de loi).*

2. Le dispositif prévu par le projet de loi

L'article 31 vient restructurer la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés (dite « informatique et libertés ») afin de consacrer le rôle de la Cnil comme autorité compétente pour l'application des dispositions du *DGA* sur l'altruisme en matière de données et de lui reconnaître les prérogatives associées à ce nouveau statut.

Le projet de loi crée, à cette fin, une nouvelle section V, intitulée « Dispositions relatives à l'altruisme en matière de données », au sein de la loi « Informatique et libertés » qui :

– affirme la compétence de la Cnil pour le traitement des demandes d'enregistrement des organisations « altruistes » et la tenue à jour du registre national associé, étant souligné qu'il est prévu que la procédure d'enregistrement soit définie par un décret en Conseil d'État ;

– définit les pouvoirs de la Cnil pour faire respecter les règles fixées par le règlement *DGA* : ses agents habilités pourraient ainsi constater des manquements et solliciter, par une demande motivée, les organisations altruistes afin de vérifier qu'elles respectent les obligations posées par le *DGA*, sans que cette prérogative soit particulièrement encadrée. **Quant au président de la Cnil, il disposerait de plusieurs pouvoirs spécifiques** : il pourrait en effet prononcer des mises en demeure pour les manquements « *susceptible[s] de faire l'objet d'une mise en conformité* » (cette notion n'étant pas définie par le texte mais paraissant renvoyer à l'ensemble des obligations issues du *DGA* (article 24) sur l'altruisme en matière de données) et, en l'absence de mise en conformité, saisir la formation restreinte de la Commission afin que soient prononcées une ou plusieurs sanctions : perte du droit d'utiliser le label d'«*organisation altruiste en matière de données reconnue dans l'Union*» dans toute communication et/ou radiation du registre national des organisations altruistes et/ou amende administrative tenant compte de critères divers fixés par le règlement *DGA* et inférieure aux plafonds prévus par le règlement général pour la protection des données (RGPD) ;

– rend la Cnil compétente pour recevoir et traiter des réclamations, conformément aux dispositions du *DGA*. L'article 31 est, en revanche, **muet sur les voies de recours possibles contre les décisions prises à l'issue de ces réclamations**, alors même qu'un tel recours, avec traitement par une entité autre que celle qui est compétente en matière d'altruisme (c'est-à-dire par une autre autorité administrative indépendante ou par voie contentieuse), est rendu obligatoire par la réglementation européenne.

Plus généralement, l'article 31 se distingue par le **périmètre inhabituel des décrets en Conseil d'État qu'il prévoit : chaque disposition nouvelle est, en effet, adossée à un tel acte réglementaire** sans que le contenu précis de ce dernier ne soit défini.

Il est, corrélativement, **caractérisé par une rédaction relativement floue qui, en particulier, ne permet pas de saisir clairement l'articulation et le périmètre des prérogatives confiées à la Cnil ou à son président** – comme en témoignent les réponses contradictoires apportées, sur ce sujet, par la Cnil et le Gouvernement aux questionnaires établis par le rapporteur Loïc Hervé, le Gouvernement estimant que ces nouveaux outils devront être utilisés de manière successive, selon une logique de gradation, tandis que la Commission considère qu'elle pourra en faire un usage alternatif et recourir sans attendre aux leviers les plus coercitifs en cas de manquement grave.

3. La position de la commission spéciale : une réécriture globale du texte proposé

Afin de corriger les imperfections du texte telles qu'elles ont été exposées ci-avant, la commission spéciale a adopté un amendement **COM-145 rectifié** du rapporteur réécrivant intégralement l'article 31 afin de garantir l'insertion harmonieuse des nouvelles règles d'altruisme en matière de données au sein de la loi « informatique et libertés ». Outre ses apports rédactionnels et légistiques, cet amendement permet de **préciser les conditions dans lesquelles les agents de la Cnil pourront solliciter des observations** de la part des organisations dites « altruistes » ainsi que les **modalités d'exercice, par le président de la Cnil, de ses nouvelles prérogatives**.

Ce même amendement prévoit que **les requérants seront informés de la possibilité de former un recours juridictionnel contre les décisions prises par la Cnil à l'issue d'une réclamation**, conformément aux mécanismes prévus par le *DGA*.

La commission spéciale a adopté l'article 31 **ainsi modifié**.

Article 32

Adaptations de la loi n° 78-17 « Informatique et libertés » au règlement européen sur les services numériques

L'article 32 adapte la loi « Informatique et libertés » du 6 janvier 1978 afin de tenir compte des compétences dévolues à la Cnil dans l'application du règlement européen sur les services numériques (RSN). Il crée, ce faisant, des pouvoirs d'enquête particuliers, limités à la mise en œuvre de ce règlement, et un régime spécifique de sanctions.

Cette évolution, de nature à complexifier l'action des contrôleurs de la Cnil et à dégrader la lisibilité de la loi, ne semble pas la mieux adaptée pour garantir l'efficacité et l'accessibilité du droit.

C'est pourquoi la commission spéciale a adopté divers amendements visant, en particulier, à mieux encadrer les nouveaux pouvoirs conférés à la Cnil (pouvoir de saisie et possibilité d'émettre des injonctions à caractère provisoire) tout en l'autorisant à en faire usage non seulement pour garantir la bonne application du RSN, mais aussi pour veiller au respect des autres obligations inscrites dans la loi de 1978, quelle qu'en soit la source. Elle a ensuite adopté l'article ainsi modifié.

1. Le rôle de la Cnil dans la mise en œuvre du RSN et le contenu de l'article 32

Le Gouvernement a fait le choix, judicieux, de rendre la Cnil compétente pour l'application des dispositions du RSN qui portent sur les données personnelles. En pratique, cette thématique concerne :

– l'obligation faite aux fournisseurs de plateforme en ligne **d'informer les destinataires des principaux paramètres de ciblage des publicités** (article 26 du RSN, *d* du paragraphe 1) ;

– l'interdiction faite aux fournisseurs de plateformes en ligne de présenter aux destinataires de leurs services des **publicités reposant sur du profilage fait à partir des données à caractère personnel les plus sensibles**[1] (article 26, paragraphe 3) ;

– l'interdiction faite aux fournisseurs de plateformes en ligne de **présenter aux destinataires, dès lors qu'ils ont la certitude raisonnable qu'ils sont mineurs, des publicités reposant sur du profilage**, quelle que soit la nature des données personnelles utilisées (article 28, paragraphe 2).

L'article 32 du projet de loi prévoit qu'il appartiendra à la Cnil de veiller au respect de ces obligations par les fournisseurs de plateforme en ligne et qu'elle **disposera, pour ce faire, des pouvoirs qu'elle tire du droit en vigueur en matière de visite de locaux, d'injonction, de sanctions** (hors les sanctions spécifiques au RGPD résultant de l'article 21 de la loi « Informatique et libertés ») **et d'engagement de poursuites selon une procédure simplifiée.**

[1] *Il s'agit des données à caractère personnel visées au 1 de l'article 9 du RGPD, soit celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ; les données génétiques et biométriques permettant d'identifier une personne physique de manière unique ; données concernant la santé ; les données concernant la vie sexuelle ou l'orientation sexuelle.*

Les pouvoirs d'enquête de la Cnil dans le droit en vigueur

Aux termes de l'article 19 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les membres de la Cnil et ses agents habilités disposent, pour l'exercice de leurs missions, de diverses prérogatives.

Ils peuvent, en premier lieu, **accéder aux lieux locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel, de 6 heures à 21 heures**. Ce droit de visite s'exerce sur information préalable du procureur de la République territorialement compétent ou, si tout ou partie des lieux visités est affecté à un domicile privé, sur autorisation du juge des libertés et de la détention.

Le responsable des lieux dispose d'un droit d'opposition à la visite dont il est informé ; lorsqu'il exerce ce droit, la visite suppose l'autorisation du juge des libertés et de la détention (JLD). **Cette autorisation est également requise lorsque « *l'urgence, la gravité à des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents* » impose que le responsable des lieux ne soit pas informé de la visite** ; dans cette hypothèse, il ne dispose pas non plus du pouvoir de s'opposer au contrôle.

Lorsque la visite a été autorisée par le JLD (donc dans tous les cas où le responsable des lieux n'a pas donné, fût-ce par son silence, son assentiment), elle se déroule sous son contrôle (ce qui implique qu'il peut, à tout moment, être saisi d'une demande de suspension ou d'arrêt de la visite), **en présence de l'occupant des lieux ou de son représentant qui peut se faire assister par le conseil de son choix** ; à défaut de présence de l'occupant, les personnes chargées du contrôle font appel à deux témoins qui ne sont pas placés sous leur autorité.

L'ordonnance du JLD ayant autorisé la visite, de même le déroulement des opérations de visite, est susceptible d'un recours devant le premier président de la cour d'appel.

Au cours de la visite, les agents de la Cnil peuvent :

– **demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie** ;

– recueillir tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission ;

– **accéder**, dans des conditions préservant la confidentialité à l'égard des tiers, **aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié** dans des documents directement utilisables pour les besoins du contrôle.

Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, dans certaines conditions, par le secret médical.

Par ailleurs, **pour toute visite, un procès-verbal contradictoire est dressé.**

Outre l'hypothèse d'un contrôle sur place, les agents de la Cnil peuvent procéder à des constatations de toute nature, y compris en source « ouverte » : la loi « Informatique et libertés » les autorise ainsi à « *consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations* ». Ils peuvent également, pour contrôler les services de communication au public en ligne, faire recours à une identité d'emprunt.

Pour l'ensemble de ces missions, les membres et agents habilités de la Cnil peuvent être assistés par des experts.

Source : commission spéciale

L'article 32 instaure également des prérogatives nouvelles, limitées au contrôle du respect du RSN ; elles consistent en un pouvoir de saisie et en la possibilité pour la Cnil d'entendre les membres du personnel du fournisseur et de ses sous-traitants sur une infraction présumée et d'enregistrer leurs réponses avec leur consentement. Ce nouveau pouvoir de saisie, légitime dans son principe et expressément prévu par le RSN, soulève toutefois une difficulté juridique : le projet de loi ne prévoit pas d'en limiter l'exercice aux documents ayant un lien avec l'infraction ou le manquement dont la preuve est recherchée, alors même que cette exigence est reconnue comme substantielle par le Conseil constitutionnel dans des cas analogues[1]. L'article 32 se heurte, en outre, à une difficulté opérationnelle, puisqu'il **ne fixe pas le régime de restitution des documents saisis**.

Plus généralement, et comme le relevait Marie-Laure Denis, présidente de la Cnil, lors de son audition par la commission spéciale au cours d'une table ronde des régulateurs le 13 juin 2023, la limitation de ces nouvelles prérogatives à l'application du RSN n'est pas de nature à faciliter l'exercice par les contrôleurs de leurs missions, le principe d'efficacité plaidant à l'inverse pour une harmonisation des procédures d'enquête quelle que soit la source réglementaire du manquement dont la preuve est recherchée.

En l'espèce, le rapporteur Loïc Hervé constate en effet qu'il n'y a pas de raison évidente pour justifier que le pouvoir de saisie et la possibilité d'enregistrer les réponses du personnel soient limités aux infractions au RSN et exclus pour les autres infractions, y compris les manquements aux règles essentielles fixées par le RGPD.

Corrélativement, l'article précité **fixe un régime de sanctions spécifique au RSN** permettant au président de la Cnil d'émettre des avertissements en cas de soupçon de manquement (l'application de tels « *avertissements* » à des manquements déjà réalisés – ou, à tout le moins, dont la commission est déjà soupçonnée – étant une innovation qui ne correspond à aucune disposition existante de la loi de 1978) ainsi que d'accepter des engagements de mise en conformité des fournisseurs et de les rendre contraignants.

Si ces outils s'avéraient insuffisants, le projet de loi **autorise le président de la Cnil à saisir la formation restreinte de ladite Commission afin que soient prononcées une ou plusieurs sanctions** : rappel à l'ordre ; injonction de mise en conformité avec astreinte (plafonnée à 5 % des revenus ou du chiffre d'affaires mondial journalier moyen du fournisseur concerné), sans que le délai d'exécution de cette injonction soit adossé à un « plancher » et/ou amende administrative (dont le plafond sera fixé à 6 % du chiffre d'affaires mondial de l'exercice précédent). Il crée également des sanctions

[1] *Pour un exemple sur les saisies en matière fiscale : décision n° 2021-908 QPC du 11 mars 2022, « Société H. et autres ».*

en cas d'opposition à fonctions, le fait de faire obstacle aux pouvoirs d'enquête de la Cnil ou de transmettre à ses contrôleurs des informations erronées étant désormais passible de l'injonction ou de l'amende administrative mentionnées ci-avant[1].

L'article 32 permet enfin au président de la Cnil d'adopter des **injonctions à caractère provisoire** en cas de manquement aux règles issues du RSN susceptibles de « *créer un dommage grave* », sans toutefois que la notion de « *dommage grave* » soit définie par le texte ou par une norme applicable dans un domaine similaire. En outre, renvoyant à un décret en Conseil d'État, **le projet de loi ne définit ni la nature des mesures qui pourront être prises dans ce cadre, ni leur durée maximale d'application** – ce qui, s'agissant d'un pouvoir coercitif, soulève des interrogations quant au respect de la compétence que le Parlement tire de l'article 34 de la Constitution.

Comme l'article 31, **l'article 32 comporte un nombre étonnant de renvois généraux à un décret en Conseil d'État, chaque disposition ou presque en étant assortie** : ce parti pris, outre qu'il pourrait laisser penser que le Gouvernement n'a pas encore défini les contours précis des modalités d'exercice par la Cnil de ses nouvelles missions, nuit à la bonne compréhension des mécanismes proposés et ne permet pas d'appréhender intégralement leur pertinence.

Par ailleurs, **de manière surprenante, la rédaction prévue pour la Cnil diffère sensiblement de celle proposée pour l'Arcom sur les mêmes sujets** (acceptation d'engagements des fournisseurs, pouvoir de saisie, *etc.*) dans d'autres articles du projet de loi, sans que cette divergence apparaisse fondée sur des facteurs objectifs.

2. La position de la commission spéciale : modifier la rédaction proposée dans un double objectif de clarification et de sécurité juridique

Outre divers amendements rédactionnels et de coordination (**COM-146**, **COM-152**), la commission spéciale a adopté des amendements de son rapporteur tendant à :

– aligner, dans toute la mesure du possible, la rédaction retenue pour la Cnil sur celle proposée pour l'Arcom ;

– clarifier et préciser les modalités d'exercice par la Cnil de ses nouvelles missions (fixation de délais « plancher » dès que nécessaire et insertion de précisions procédurales sur la mise en œuvre des pouvoirs coercitifs : amendements **COM-149**, **COM-150**, **COM-151**, **COM-153**) ;

---

[1] *Le montant de l'amende serait toutefois plafonné, dans une telle hypothèse, à 1 % du chiffre d'affaires.*

– **encadrer le recours aux décrets en Conseil d'État**, soit en supprimant les renvois qui paraissent inutiles, soit en encadrant le champ des futurs actes d'application ;

– **mieux définir les cas et modalités de recours aux nouvelles injonctions à caractère provisoire**, en précisant que celles-ci pourront être utilisées lorsque la formation restreinte a été saisie (c'est-à-dire lorsqu'une procédure de sanction a été engagée, témoignant de l'existence d'éléments concordants et sérieux quant à la réalité du manquement) et en cas de « *risque élevé d'atteinte aux droits et libertés des personnes physiques* » – notion qui, contrairement à celle de « *dommage grave* », correspond à une terminologie préexistante dans la loi de 1978 et bien maîtrisée par la Cnil (**COM-154 rectifié**). Le même amendement permet, de plus, **d'utiliser ces nouvelles injonctions pour tout type de manquement, quelle qu'en soit la source**, plutôt que pour les seules infractions au RSN ;

– généraliser la possibilité donnée à la Cnil **d'interroger les personnels des entités contrôlées** et d'enregistrer leurs réponses avec leur consentement (**COM-148**) ;

– **sécuriser le nouveau pouvoir de saisie de la Cnil** en prévoyant que seuls pourront être saisis les documents qui se rapportent à l'infraction ou au manquement dont la preuve est recherchée et qu'un inventaire des documents saisis sera annexé au procès-verbal établi à l'issue de la visite, et en fixant les modalités de restitution des pièces saisies (**COM-147 rectifié**). Le même amendement permet d'**homogénéiser les pouvoirs d'enquête de la Cnil en rendant le nouveau pouvoir de saisie applicable non seulement en cas de manquement au RSN, mais aussi en cas de non-respect des autres obligations énumérées par la loi « informatique et libertés »**.

L'harmonisation des pouvoirs d'enquête et de sanction de la Cnil, conforme aux souhaits exprimés par la présidente de la Commission lors de son audition, facilitera l'exercice par ses agents de leurs prérogatives et permettra de **disposer d'outils plus performants pour garantir le respect non seulement du RSN, mais aussi des règles nationales, du *DGA* et du RGPD**.

La commission spéciale a adopté l'article 32 **ainsi modifié**.

CHAPITRE VIII
Mesures d'adaptation de la loi n° 47-585 du 2 avril 1947 relative au statut des entreprises du groupage et de distribution des journaux et publications périodiques

Article 33
Mesures d'adaptation de la loi n° 47-585 du 2 avril 1947 relative au statut des entreprises de groupage et de distribution de journaux et publications périodiques

L'article 33 vise à adapter la législation nationale au règlement du 19 octobre 2022 relatif à un marché unique des services numériques (RSN) au regard en particulier de la suppression de la définition des opérateurs de plateformes et de ses conséquences sur les agrégateurs de presse mentionnés à l'article 15 de la loi n° 47-585 du 2 avril 1947 relative au statut des entreprises de groupage et de distribution de journaux et publications périodiques.

1. La législation actuelle

L'article 15 de la loi n° 47-585 du 2 avril 1947 relative au statut des entreprises de groupage et de distribution de journaux et publications périodiques porte sur la diffusion numérique de la presse.

Le paragraphe I concerne les « kiosques », soit les services par abonnement proposant l'accès à un ensemble de publications. Il prévoit que ces services ne peuvent refuser la diffusion d'un titre d'information politique et générale dès lors qu'elle serait réalisée dans des conditions techniques et financières raisonnables et non discriminatoires.

Le paragraphe II du même article vise les opérateurs de plateformes en ligne mentionnés au I de l'article L. 111-7 du code de la consommation qui proposent le classement ou le référencement de contenus extraits de publications de presse ou de services de presse en ligne d'information politique et générale afin de prévoir qu'il leur revient de fournir à leurs utilisateurs une information loyale, claire et transparente sur l'utilisation de de leurs données personnelles dans le cadre du classement ou du référencement de ces contenus.

Du fait de l'abrogation du paragraphe I de l'article L. 111-7 du code de la consommation où se trouve la définition des *« opérateurs de plateformes en ligne »*, il est devenu nécessaire de préciser à nouveau le champ des acteurs couverts par ces dispositions, le champ de l'article L. 111-7 n'étant pas identique à celui de la définition des « services de plateformes en ligne » issue du règlement européen sur les services numériques *(RSN)*.

2. Le dispositif proposé

Le présent article vise donc à introduire une définition des agrégateurs de presse à l'article 15 de la loi « Bichet » du 2 avril 1947 en s'inspirant de la définition des opérateurs de plateformes désormais abrogée. Un agrégateur de presse sera ainsi défini comme **un service de communication au public en ligne reposant sur le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus extraits de publications de presse ou de services de presse en ligne d'information politique et générale**.

Plus précisément, le présent article 33 supprime la référence aux *« opérateurs de plateformes en ligne mentionnés au I de l'article L. 111-7 du code de la consommation »* dans le paragraphe II de l'article 15 de la loi du 2 avril 1947 et précise la définition des agrégateurs de presse en ajoutant la référence aux algorithmes informatiques dans la définition déjà en vigueur qui visait plus généralement les opérateurs de plateformes en ligne. Il prévoit également deux modifications de renvois par coordination.

3. La position de la commission spéciale

Les dispositions prévues par le présent article visent à adapter la réglementation relative aux agrégateurs de presse afin de la mettre en conformité avec le règlement européen sur les services numériques *(DSA)*.

La commission spéciale a adopté l'article 33 **sans modification**.

CHAPITRE IX

Mesures d'adaptation de la loi n° 2017-261 du 1er mars 2017 visant à préserver l'éthique du sport, du code de la propriété intellectuelle, de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles et du code pénal

Article 34

Mesures d'adaptation de la loi n° 2017-261 du 1er mars 2017 visant à préserver l'éthique du sport, du code de la propriété intellectuelle, de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles et du code pénal

Cet article vise, tout comme le précédent article 33, à mettre en conformité le droit national avec le droit de l'Union européenne tel qu'il résulte de l'adoption du DSA afin de remplacer la référence faite aux opérateurs de plateforme en ligne par une référence aux services de plateforme en ligne.

Il procède pour ce faire à des adaptations de la loi n° 2017-261 du 1er mars 2017 visant à préserver l'éthique du sport, du code de la propriété intellectuelle, de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles et du code pénal.

1. La législation actuelle

Le présent article vise à réaliser des coordinations dans plusieurs articles législatifs afin de tenir compte, en particulier, de la suppression de la catégorie des opérateurs de plateforme en ligne par le règlement européen relatif à un marché unique des services numériques *(DSA)* du 19 octobre 2022.

L'article 24 de la loi n° 2017-261 du 1er mars 2017 visant à préserver l'éthique du sport, à renforcer la régulation et la transparence du sport professionnel et à améliorer la compétitivité des clubs, vise à prévoir que les détenteurs de droits d'exploitation sur des contenus audiovisuels, parmi lesquels peuvent figurer les opérateurs de plateformes en ligne définis à l'article L. 111-7 du code de la consommation, peuvent conclure un ou plusieurs accords relatifs aux mesures et bonnes pratiques qu'ils s'engagent à mettre en œuvre en vue de lutter contre la promotion, l'accès et la mise à la disposition au public en ligne, sans droit ni autorisation, de contenus audiovisuels dont les droits d'exploitation ont fait l'objet d'une cession.

L'article L. 137-2 du code de la propriété intellectuelle précise les modalités d'exploitation d'œuvres par les fournisseurs de services de partage de contenus en ligne tandis que l'article L. 219-2 comprend des dispositions relatives à l'exploitation des objets protégés par un droit voisin par les fournisseurs de services de partage de contenus en ligne.

L'article 36 de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique comprend des dispositions visant à permettre aux autorités administratives indépendantes et aux autorités publiques indépendantes qui interviennent dans la régulation des opérateurs de plateforme en ligne définis à l'article L. 111-7 du code de la consommation, de recourir, dans le cadre de conventions, à l'expertise et à l'appui d'un service administratif de l'État désigné par décret en Conseil d'État.

Enfin, l'article 323-3-2 du code pénal vise pour sa part à sanctionner un opérateur de plateforme en ligne mentionné à l'article L. 111-7 du code de la consommation qui permettrait des transactions manifestement illicites.

2. Le dispositif proposé

Le présent article modifie l'article 24 de la loi du 1er mars 2017 afin de remplacer la référence faite à cet article aux opérateurs de plateforme en ligne par une référence aux services de plateforme en ligne au sens du règlement sur les services numériques, aux moteurs de recherche au sens du même règlement et aux plateformes de partage de vidéos au sens de l'article 2 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

De même, à l'article 323-3-2 du code pénal, la référence faite aux opérateurs de plateforme en ligne est remplacée par une simple référence aux services de plateforme en ligne au sens du règlement sur les services numériques.

De façon similaire, la référence au régime de responsabilité limitée des services d'hébergement au II de l'article L. 137-2 et au II de l'article L. 219-2 du code de la propriété intellectuelle est remplacée par une référence aux dispositions du *DSA*.

3. La position de la commission

Les dispositions prévues par le présent article constituent des coordinations rendues nécessaires par l'adoption du *DSA*.

La commission a adopté un amendement **COM-79** de Julien Bargeton qui crée un paragraphe II *bis* modifiant l'article L. 131-4 du code de la propriété intellectuelle afin de faire référence à une rémunération « appropriée » des auteurs cédant leurs droits exclusifs pour l'exploitation de leurs œuvres. Cette modification s'inscrit dans le prolongement de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et permet de réaffirmer la nécessité de défendre les créateurs.

La commission spéciale a adopté l'article 34 **ainsi modifié**.

CHAPITRE X
Dispositions transitoires et finales

Article 35
Habilitation à légiférer par ordonnance pour l'application dans les territoires ultramarins du projet de loi et de plusieurs règlements européens

L'article 35 prévoit une habilitation du Gouvernement à légiférer par ordonnance dans un délai d'un an pour l'application dans les territoires ultramarins du projet de loi et des règlements européens sur la gouvernance des données (RGD), les marchés du numérique (RMN) et les services numériques (RSN) dans les territoires ultramarins.

La commission spéciale a adopté cet article en réduisant le délai d'habilitation à six mois.

L'article 35 du projet de loi prévoit, en vertu de l'article 38 de la Constitution, de permettre au Gouvernement de légiférer par ordonnance afin de procéder à l'application de la présente loi en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, soumises au principe de spécialité législative, et de permettre les adaptations nécessaires à chacun de ces territoires ainsi qu'aux collectivités de Saint-Barthélemy, Saint-Martin et Saint-Pierre et Miquelon.

L'article 35 prévoit également de rendre applicable trois règlements européens aux pays et territoires d'outre-mer (PTOM), à savoir la Nouvelle-Calédonie, la Polynésie française et les îles Wallis et Futuna. En effet, à l'inverse des autres collectivités d'outre-mer françaises, qui disposent du statut de régions ultrapériphériques (RUP) et sont soumises au droit européen, les PTOM ne font pas partie intégrante de l'Union européenne et bénéficient d'un régime spécial d'association, prévu aux articles 198 à 204 du traité sur le fonctionnement de l'Union européenne (TFUE). Ce faisant, ils ne sont pas soumis de plein droit à la législation européenne, à l'exception de certaines dispositions qui le prévoient expressément. Par conséquent, une mention expresse, ainsi que de potentielles adaptations doivent être prises pour l'application à ces trois territoires :

– du règlement (UE) 2022/868 du 30 mai 2022 portant sur la gouvernance des données (RGD) ;

– du règlement (UE) 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur du numérique (RMN) ;

– et du règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques (RSN).

Le projet de loi fixe au Gouvernement un délai de douze mois suivant sa publication pour la prise des ordonnances, puis un délai de trois mois pour le dépôt d'un projet de loi de ratification devant le Parlement.

Si les mesures d'adaptation et d'application de la loi et des règlements numériques aux outre-mer sont pleinement nécessaires, la commission spéciale a toutefois déploré le fait que le Gouvernement propose de recourir à une ordonnance et ne prévoie pas l'application des diverses dispositions directement dans la loi. Elle a appelé de ses vœux une modification de cet article au cours de la navette, notamment à l'occasion de la discussion en séance publique au Sénat.

Dans l'attente, et sur proposition du rapporteur Loïc Hervé, elle a adopté l'amendement **COM-155** afin de réduire le délai de l'habilitation demandé par le Gouvernement, en le portant à six mois au lieu d'un an. Non seulement ce délai de six mois paraît amplement suffisant pour adapter l'ensemble de des mesures du projet de loi aux territoires ultra-marins mais, en outre, les trois règlements européens précités étant d'application directe, l'attente d'un délai d'un an pour prendre les mesures nécessaires à leur adaptation dans les territoires d'outre-mer semble excessive.

La commission spéciale a adopté l'article 35 **ainsi modifié**.

Article 36
Dispositions d'entrée en vigueur

L'article 36 vise à détailler les dispositions d'entrée en vigueur du projet de loi.

La commission a adopté cet article modifié par l'adoption de deux amendements, dont l'un du rapporteur Patrick Chaize, et d'un sous-amendement, du rapporteur également.

1. Des modalités d'entrée en vigueur différenciées selon les dispositions du projet de loi, au regard des impératifs de sécurité juridique et des exigences d'articulation avec le calendrier européen

a) Sur l'entrée en vigueur de la procédure administrative de blocage et de déréférencement confiée à l'Arcom

L'**article 2 du projet de loi**, qui transforme la procédure judiciaire de blocage et de déréférencement des sites ne respectant pas la restriction d'accès aux mineurs en procédure administrative ordonnée par l'Autorité de

régulation de la communication audiovisuelle et numérique (Arcom), **entre en vigueur à compter du 1er janvier 2024**. Toutefois, **par souci de sécurité juridique, les procédures déjà engagées au 31 décembre 2023 demeurent régies par la procédure judiciaire de blocage**, y compris si les décisions sont rendues après le 1er janvier 2024.

b) Sur l'entrée en vigueur des dispositions relatives aux frais de transfert sortant de données

Les dispositions du III de l'article 7 du projet de loi, relatives à la suppression progressive des frais de transfert sortant de données, restent en vigueur jusqu'à trois ans à compter de la date d'application du futur règlement européen sur les données (*Data Act*), c'est-à-dire jusqu'à une date estimée être le **15 février 2027**.

c) Sur l'entrée en vigueur des dispositions relatives à l'interopérabilité des services d'informatique en nuage

Les dispositions des articles 8, 9 et 10 relatives à l'interopérabilité des services d'informatique en nuage restent en vigueur jusqu'au 15 février 2026, ce qui correspond également à la date d'entrée en vigueur anticipée des dispositions correspondantes du *Data Act*.

d) Sur l'entrée en vigueur des dispositions prises en application du règlement européen sur la gouvernance des données

L'article 11 désigne l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) comme autorité compétente en matière de régulation des services d'intermédiation de données à compter du 24 septembre 2023, date d'application du règlement européen sur la gouvernance des données (*Data Governance Act - DGA*).

L'article 31, qui apporte diverses modifications à la loi dite « informatique et libertés » du 6 janvier 1978 afin d'adapter celle-ci aux règles issues du *DGA* et de consacrer les nouvelles compétences de la Commission nationale pour l'informatique et les libertés (Cnil) dans le domaine de l'altruisme en matière de données, entre également en vigueur au 24 septembre 2023.

e) Sur l'entrée en vigueur des dispositions d'adaptation de notre droit au droit de l'Union européenne

En l'état de la rédaction, les articles 23, 24, 26, 28, 29, 30, 31, 32, 34, 35, 36 du projet de loi entrent entièrement en vigueur à compter du 17 février 2024, soit la date d'application du règlement européen sur les services numériques (RSN).

Les dispositions du C du III de l'article 22, qui réécrit intégralement l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN), entrent en vigueur à des dates différées. Jusqu'au 16 février 2024, pour les dispositions relatives au régime de responsabilité des hébergeurs et à compter du 17 février 2024 pour l'application du régime de sanction en cas d'absence de notification de soupçons d'infractions pénales.

Les dispositions des I, II et III de l'article 25 entrent en vigueur à compter de la promulgation du présent projet de loi. Par contre, les autres dispositions de l'article 25 entrent en vigueur à compter du 17 février 2024, soit le nouvel article 8-1 inséré dans la LCEN relatif aux missions confiées à l'Arcom en matière de régulation des fournisseurs de services intermédiaires, le nouvel article 9-1 inséré dans la LCEN relatif au pouvoir d'enquêtes domiciliaires de l'Arcom vis-à-vis des fournisseurs de services intermédiaires, ainsi qu'au nouvel article 9-2 inséré dans la LCEN relatif aux pouvoirs d'injonction et de sanction de l'Arcom vis-à-vis de ces mêmes fournisseurs.

f) Sur l'entrée en vigueur du dispositif de centralisation des données de location de meublés de tourisme

L'article 17, relatif à la mise en œuvre d'un nouveau dispositif de centralisation des données de location de meublés de tourisme, entre en vigueur à une date fixée par décret, l'étude d'impact du projet de loi justifiant cette procédure par la prise en compte des délais de développement informatique.

2. Une nécessaire prudence quant à l'articulation avec le calendrier européen

De façon générale, **la commission spéciale regrette le manque de transparence du Gouvernement quant à la procédure de notification des dispositions de ce projet de loi à la Commission européenne**, conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information.

Seuls les articles 1er à 10, ainsi que les articles 17 et 36, ont été notifiés[1], sans qu'aucune justification ne soit apportée, malgré les demandes répétées de la commission spéciale, sur l'absence de notification des autres articles.

[1] https://technical-regulation-information-system.ec.europa.eu/en/notification/23874

La commission spéciale regrette l'adaptation tardive de notre droit national aux dispositions du *Data Governance Act*, qui s'applique à compter du 24 septembre 2023, c'est-à-dire pendant la phase d'examen parlementaire du projet de loi.

La commission spéciale appelle à davantage de prudence quant à l'anticipation de l'adaptation de notre droit national aux propositions de règlements européens toujours en cours de négociation, ce qui est le cas du *Data Act* : de nombreuses adaptations au projet de loi devront être effectuées, en particulier aux articles 7 à 10, en fonction du texte qui sera définitivement adopté.

La commission a également adopté l'amendement **COM-156** du rapporteur Patrick Chaize, visant à **préciser que la suppression des frais liés à un changement de fournisseur de services d'informatiques en nuage s'effectue en bonne coordination avec les dispositions prévues par le *Data Act***, dont la date d'application n'est pas encore connue car toujours en cours de discussion à l'échelle européenne : une « date glissante » a été préférée à une « date fixe » afin d'éviter toute incertitude pour les opérateurs économiques concernés dans l'éventualité d'une adoption retardée du *Data Act*.

La commission spéciale regrette également la complexité de certains délais de mis en œuvre choisis par le Gouvernement, certains délais s'appliquant parfois seulement pour quelques semaines.

Par conséquent, elle a adopté l'amendement **COM-69 rectifié** de Nathalie Delattre, sur un avis favorable du rapporteur, visant à harmoniser les dates d'entrée en vigueur du nouvel article 6 de la LCEN tel qu'il résulte de sa nouvelle rédaction à l'article 22 du présent projet de loi avec la date d'application du RSN fixée au 17 février 2024. La nécessité d'appliquer, pour quelques semaines seulement, un régime transitoire pour les fournisseurs de services d'hébergement concernés par le RSN mais non couverts par le droit national actuel n'est pas avérée.

Enfin, la commission a également adopté le **sous-amendement COM-164** du rapporteur, modifiant la rédaction de l'amendement **COM-69 rectifié** précité, afin de supprimer la seconde occurrence à l'article 31, qui avait pour conséquence de prévoir deux délais d'entrée en vigueur distincts pour le même article.

La commission spéciale a adopté l'article 36 **ainsi modifié**.

.

EXAMEN EN COMMISSION

_____

MARDI 27 JUIN 2023

Mme Catherine Morin-Desailly, présidente. – Messieurs les rapporteurs, mes chers collègues, nous voici réunis au terme de trois semaines d'un marathon législatif couru à la vitesse d'un sprint !

La commission spéciale a organisé, lors de ses trois semaines utiles de travail, cinq auditions plénières et trois tables rondes. Nous aurions souhaité en conduire davantage, mais le temps imparti était beaucoup trop restreint. Les rapporteurs, que je remercie très sincèrement pour leur investissement et leur mobilisation exceptionnels sur ce texte, ont pour leur part mené vingt et une auditions. Nous avons par ailleurs reçu des dizaines de courriels et d'appels téléphoniques. Nous avons invité tous ceux qui le souhaitaient à apporter des contributions, qui ont été lues et étudiées de manière approfondie pour nourrir la réflexion des rapporteurs.

Comme je vous l'indiquais lors de la réunion constitutive, ce projet de loi est technique, parfois difficile à appréhender et complexe, comme les participants à la table ronde sur l'informatique en nuage se le rappellent, mais il traite d'enjeux considérables et aura un impact très fort sur nos concitoyens et nos entreprises.

Avant de commencer l'examen des amendements, je souhaite brièvement replacer le projet de loi et ses ambitions dans le contexte plus large du combat que nous menons depuis des années, au Sénat, en France et en Europe, pour un monde numérique sûr, régulé, et respectueux de notre souveraineté. À cet égard, la souveraineté ne doit pas être entendue comme un repli sur soi ou une forme de protectionnisme, mais comme la capacité à décider de notre destin.

Rappelons-nous, c'était hier : internet débarquait, et avec lui les promesses d'un monde ouvert, où l'information circulerait à la vitesse de la lumière, où les entreprises gagneraient en efficacité et en agilité, où la connaissance serait partagée et où des communautés pourraient se constituer par-delà les frontières autour d'intérêts communs. C'était l'internet des années 2000, celles des modems qui se connectaient avec ce petit bruit si caractéristique. C'est de cette époque que date la grande loi européenne dite « e-commerce » du 8 juin 2000, d'ailleurs très inspirée du droit américain, qui reste le cadre de référence pour le numérique. Cette loi est avant tout conçue pour le développement des usages plus que pour l'encouragement des acteurs et d'une économie souveraine.

En 2023, internet est devenu omniprésent dans nos loisirs et nos vies. Les enfants nés après 2000 ont du mal à imaginer un monde sans Google, comme nos parents avaient du mal à imaginer un monde sans

téléphone. Pourtant, on ne peut se satisfaire de la situation actuelle. Le Sénat, en de multiples occasions, a alerté sur les dérives d'internet. Je n'en cite que quelques-unes : multiplication de contenus pornographiques librement diffusés, cyberharcèlement, menaces à l'encontre d'élus, atteintes massives à la vie privée, piratage de contenus culturels, contrefaçons multiples, interférence dans les processus démocratiques, criminalité en ligne, mainmise de quelques géants sur l'accès et les contenus.

Les auditions de la plateforme Pharos ou des associations de protection de l'enfance ont marqué les esprits. Nous avions également tenu avec les rapporteurs à proposer un éclairage européen, en auditionnant Europol la semaine dernière.

Je ne veux cependant pas donner de notre assemblée une image passéiste, bien au contraire. Si internet a déçu, c'est aussi et surtout parce qu'il a su séduire. Soyons honnêtes et reconnaissons que nous passons tous du temps en ligne, parfois trop, et que nous en tirons aussi bien des bénéfices. Soyons pragmatiques et réalistes : telle doit être notre ligne de crête, si l'on souhaite conserver pour demain un internet non pas fragmenté, mais ouvert et sécurisé.

Comme souvent, l'Europe – elle n'était pas seule au demeurant – a mis du temps à identifier les dérives, même quand elles étaient pointées du doigt, à les soumettre au débat et à prendre des décisions. C'est d'ailleurs la crise sanitaire, avec l'accélération de la digitalisation de notre économie et de nos pratiques, puis la guerre en Ukraine, qui a dessillé les yeux des Européens en démontrant la dangerosité d'une dépendance trop forte envers des acteurs extraeuropéens. Trop souvent, le sujet a d'ailleurs été traité sous un angle purement économique, avec l'idée sous-jacente, toujours portée par certains pays, que réguler internet briderait les chances des entreprises européennes. Cet état d'esprit était également présent en France : il ne fallait surtout pas entraver l'innovation. Or la réalité n'est pas que matérielle : ce qui se joue, c'est l'avenir de nos enfants, de nos sociétés, de nos modèles démocratiques, culturels et sociaux – bref, le monde que nous voulons construire.

Le projet de loi que nous allons examiner est l'héritier de ces renoncements et de ces hésitations qui perdurent depuis vingt ans. Pour l'essentiel, il porte des mesures d'adaptation de notre droit aux règlements européens débattus dans le cadre du trilogue ces vingt-quatre derniers mois. Certains ont été votés, d'autres pas encore : je pense notamment au *Data Act*. Ces règlements, d'application directe, portent sur les services et les marchés numériques, adoptés de haute lutte sous la présidence française de l'Union européenne et grâce à la négociation, l'ensemble des États ne partageant pas le même état d'esprit sur ces sujets. Le règlement sur la gouvernance des données – *Data Governance Act* (DGA) – sera par ailleurs complété par le futur règlement sur les données, le *Data Act*.

Comme je le soulignais lors de notre réunion constitutive, le Sénat, avec sa commission des affaires européennes, a su pousser pour obtenir des avancées significatives. En effet, grâce à Jean-François Rapin, nous avons pu conduire des travaux dont certains ont contribué à alimenter ces textes, alors que l'ensemble des parlements des différents États membres n'a pas démontré une telle force de proposition sur ces sujets. Il est vrai que le Sénat s'attache à émettre des avis sur chaque texte. Il nous faut en convenir, l'Europe, avec ce nouvel arsenal, se dote d'une législation ambitieuse, même si nous aurions souhaité aller plus loin, et qui sera observée partout dans le monde, comme l'a été en son temps le règlement général sur la protection des données (RGPD).

Je me réjouis également que le projet de loi s'inspire très ouvertement, comme l'a plusieurs fois souligné le ministre lors de son audition, des travaux de notre délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes pour apporter des réponses à la question cruciale de l'accès des mineurs à la pornographie, dont un récent rapport de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) publié depuis lors a une nouvelle fois souligné le caractère massif.

Cependant, nous ne participons qu'à une étape d'un combat qui se poursuivra aussi longtemps que les technologies évolueront – d'autres suivront, comme celui de l'intelligence artificielle. Dans ce sens, je crois primordial de convenir que le niveau européen est le seul pertinent pour traiter ces sujets, mais qu'il doit être complété par des mesures vigoureuses auxquelles doit s'intéresser l'Europe sur notre souveraineté économique et culturelle. Avec les rapporteurs, nous avons ainsi eu à cœur de concilier le strict respect du cadre européen, des libertés publiques, avec les prémisses de cette souveraineté à construire, notamment par des politiques industrielles.

C'est dans cet esprit que nous avons travaillé.

M. Patrick Chaize, rapporteur. – Le projet de loi que nous examinons aujourd'hui est essentiellement un projet de loi d'adaptation de notre droit national au droit de l'Union européenne. Sous couvert d'un vernis médiatique et de l'ajout de quelques mesures nouvelles spécifiques à la France, ce texte est en réalité un projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne (Ddadue) qui ne dit pas son nom !

Il s'agit en effet d'adapter la quasi-totalité de nos lois nationales traitant des questions numériques à plusieurs règlements européens d'application directe qui entreront en vigueur très prochainement dans l'ensemble des pays de l'Union européenne. C'est pourquoi nous devons être prudents : il s'agit de rester fidèles à leur lettre comme à leur esprit, car ces textes sont issus de négociations et de compromis difficiles, de plusieurs

années, entre les différents États membres et les opérateurs économiques ; il s'agit également d'éviter d'adopter des dispositions qui seraient trop contraignantes et qui risqueraient de pénaliser injustement nos opérateurs économiques. À l'inverse, lorsque nos lois françaises se sont montrées particulièrement ambitieuses, protectrices et avant-gardistes, il nous faut éviter que l'adoption de ce projet de loi ne se traduise par des dispositions moins-disantes par rapport aux règles existantes.

Vous l'aurez compris, la protection est au cœur des préoccupations de ce projet de loi. Afin de mieux protéger nos citoyens en ligne, l'article 6 entend créer un nouveau dispositif national de filtrage des sites internet frauduleux qui commettent des actes de cybermalveillance.

Ici, nous parlons d'usurpation de notre identité en ligne, de piratage de nos comptes, de réception de messages d'arnaques par SMS ou par mail, de vol de données à caractère personnel ou encore d'usage détourné de nos coordonnées bancaires et de nos moyens de paiement.

Les actes de cybermalveillance font désormais partie de notre quotidien : c'est une réalité à laquelle nous nous sommes tristement habitués, mais nous ne devrions pas !

Selon les chiffres communiqués par la plateforme Cybermalveillance, 3,8 millions de personnes ont consulté ce site l'an dernier, et 280 000 ont fait l'objet d'un parcours d'assistance en raison d'une arnaque ou d'une escroquerie en ligne.

Partant du constat qu'il n'existe pas en France, au contraire d'autres pays européens, de dispositif de filtrage des contenus cybermalveillants, l'article 6 entend créer un tel dispositif, avec une activation en plusieurs étapes.

Sur ce point, je vous proposerai d'adopter plusieurs amendements visant à clarifier les modalités du message d'avertissement qui s'affichera sur nos écrans, à responsabiliser l'ensemble des intermédiaires techniques mettant en œuvre une mesure de blocage et à améliorer le contrôle qui sera effectué par la Commission nationale de l'informatique et des libertés (Cnil).

Derrière l'annonce médiatique du Gouvernement, il s'agit de rendre le dispositif plus opérationnel, plus protecteur, plus facile à déclencher, afin d'apaiser la vie en ligne de nos concitoyens.

Ce projet de loi s'intéresse aussi à la vie en ligne des entreprises dans l'économie numérique : les problématiques concurrentielles sont également au cœur des préoccupations de ce projet de loi, en particulier sur le marché de l'informatique en nuage.

Ce marché est très fortement concentré autour d'un nombre restreint d'acteurs, essentiellement américains, qui captent environ 70 % des parts d'un marché qui, à l'échelle mondiale, pourrait représenter plus de 1 200 milliards d'euros d'ici à 2025.

Pour nos entreprises et nos start-up innovantes, « l'entrée sur ce marché » est gratuite et facile grâce à l'octroi de « crédits *cloud* ». Déjà, l'an dernier, dans son rapport sur la souveraineté économique et numérique, la commission des affaires économiques alertait sur les effets anticoncurrentiels de ces pratiques qui « captent » les entreprises, « verrouillent » le marché, surtout lorsque la durée d'octroi de ces crédits est importante.

L'article 7 de ce projet de loi prévoit – c'est une initiative française que je tiens à saluer – d'encadrer l'octroi de ces crédits. Je vous proposerai d'adopter un amendement visant à plafonner cette durée à un an et à interdire toute condition d'exclusivité, afin de limiter les effets anticoncurrentiels sur ce marché.

Si « l'entrée » sur le marché est facile, la « sortie » l'est beaucoup moins, les acteurs dominants ayant mis en place de véritables péages qui prennent la forme de facturation abusive de frais sortant de données. C'est pourquoi le règlement européen sur les données, le *Data Act*, entend supprimer ces frais artificiels, ainsi que les frais de changement de fournisseur de services d'informatique en nuage, pour plus d'interopérabilité et de liberté.

Je vous proposerai également d'adopter un amendement visant à autoriser de façon transitoire ces frais, sous réserve qu'ils soient facturés à des coûts réels, sous le contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) – c'est une demande quasi unanime de nos entreprises.

Les articles 7 à 10 anticipant l'adaptation de notre droit national au *Data Act*, il faudra veiller, dans la suite de la navette parlementaire, à ce que les bonnes définitions soient reprises, notamment en matière d'interopérabilité, de portabilité et d'équivalence fonctionnelle. Sur ce point, je pense que le projet de loi peut encore évoluer afin de mieux prendre en compte la distinction entre plateformes, infrastructures et logiciels d'informatique en nuage : évitons d'adopter un cadre réglementaire aveugle de la réalité du marché.

En matière d'économie de la donnée, l'Arcep se voit attribuer de nouvelles missions importantes et, comme pour les autres autorités administratives chargées de la mise en œuvre de ces nouveaux règlements européens, nous devrons être attentifs à ce qu'elles disposent des moyens budgétaires et humains supplémentaires nécessaires dès le prochain projet de loi de finances.

En plus de devenir « gendarme du *cloud* », l'Arcep se voit également, en application du règlement européen sur la gouvernance des données, attribuer par les articles 11 à 14 du projet de loi de nouvelles missions pour encadrer et accompagner l'émergence d'un nouveau secteur d'activité : les services d'intermédiation des données. Il s'agit de faciliter les échanges de données entre entreprises, administrations et particuliers, de façon plus

transparente et plus concurrentielle, l'Union européenne prévoyant d'ici à sept ans une hausse de plus de 500 % du volume de données échangées, notamment en raison de l'arrivée de l'intelligence artificielle.

Si l'espace numérique doit être mieux sécurisé et mieux régulé, nous ne devons pas non plus empêcher les innovations permises par l'économie numérique. Au contraire, nous devons anticiper ces innovations, afin d'identifier au plus vite les risques qu'elles peuvent représenter pour les citoyens et les internautes que nous sommes, afin de ne tirer que le meilleur et d'assurer des retombées économiques favorables à notre pays.

C'est pour cela que j'ai souhaité réécrire intégralement l'article 15 relatif aux jeux à objets numériques monétisables (Jonum). En l'état, cet article est une coquille vide, et le recours à une habilitation à légiférer par ordonnance est inadmissible. Je vous proposerai donc un amendement visant, d'une part, à introduire pour la première fois en droit une définition des Jonum, qui ne sont ni des jeux d'argent et de hasard ni des jeux vidéo, mais des jeux hybrides à la croisée de ces deux mondes. Ils ne sont donc couverts par aucune législation. D'autre part, cet amendement vise à autoriser les Jonum à titre expérimental, pour une durée de trois ans, et sous le contrôle de l'Autorité nationale des jeux (ANJ). Plusieurs précautions sont prises pour répondre aux inquiétudes, légitimes, des acteurs traditionnels du secteur, mais nous y reviendrons.

Avec plusieurs milliers de Jonum en développement dans le monde entier dont une quinzaine en France, je suis convaincu que nous devons anticiper cette évolution technologique, afin de lui permettre, si cela est jugé nécessaire à l'issue de l'expérimentation, de croître dans un cadre réglementaire protecteur pour les joueurs et les citoyens.

Les évolutions technologiques étant rapides et difficilement prévisibles, ce projet de loi vise aussi à permettre à l'État d'analyser plus efficacement l'évolution de certains marchés numériques, en renforçant notamment les pouvoirs du pôle d'expertise de la régulation numérique (PEReN). Je vous proposerai ainsi plusieurs amendements visant à renforcer la capacité de collecte de données ainsi que leur durée de conservation.

Ce service est aujourd'hui une singularité française saluée et enviée par de nombreux autres pays, ce qui permet à nos autorités de régulation de mieux comprendre les logiques de fonctionnement des plateformes numériques et des moteurs de recherche : nous devons ainsi le soutenir !

Telles sont les grandes lignes de ma feuille de route. Vous l'aurez compris, ce sont à la fois la sécurisation de l'espace numérique, la restauration de la confiance de nos concitoyens dans l'économie numérique et le soutien à l'innovation et au développement de nos entreprises du numérique qui sont en jeu.

M. Loïc Hervé, rapporteur. – Trois semaines après notre réunion constitutive, nous voici de nouveau réunis pour l'établissement du texte de

la commission spéciale. Trois semaines, c'est un délai court pour un projet de loi – trop court, à plusieurs égards, mais nous n'avons pas sombré dans la précipitation. Nous avons en effet pu aller au fond des sujets et mener une réflexion aboutie. Cette qualité de travail, nous la devons notamment à la forte mobilisation des membres de cette commission, nombreux lors des auditions plénières comme lors des auditions des rapporteurs. Je remercie Patrick Chaize et Catherine Morin-Desailly pour leur esprit de cohésion : les propositions que je vais vous soumettre sont le fruit d'un travail commun, mené dans une volonté de cohérence avec les travaux déjà conduits par le Sénat, notamment par notre commission des affaires européennes.

Je ne reviens pas sur le contenu du projet de loi, que j'ai eu l'occasion d'évoquer en détail lors de notre réunion constitutive. Comme vous le savez, il poursuit trois objets : sécuriser les échanges en ligne, réguler l'intervention des acteurs du numérique et adapter notre droit au « paquet numérique » européen.

La régulation concerne principalement mon collègue Patrick Chaize ; je me concentrerai donc sur la sécurisation et l'adaptation.

Tout d'abord, sur l'axe de la sécurisation, il me semble que nous devons protéger davantage les citoyens face aux dangers qui existent en ligne.

Les articles 1er et 2 visent à donner à l'Arcom la mission d'établir un référentiel obligatoire pour les systèmes de vérification d'âge qui doivent être déployés sur les sites pornographiques et ensuite de veiller, grâce à des pouvoirs de mise en demeure et de sanction, à l'effectivité de cette vérification d'âge ou, à défaut, au blocage des sites.

Je suis favorable à cette transformation de la procédure judiciaire actuelle – nous le devons à la pugnacité de Marie Mercier – en procédure administrative toujours confiée à l'Arcom. Je crois que nous devons essayer de rendre les choses plus rapides afin de massifier notre réponse face à la prolifération de contenus pornographiques en accès libre sur internet. Il faut arriver à bloquer ces sites sans attendre qu'une procédure judiciaire aboutisse. Certes, nous ne pourrons empêcher les éditeurs de ces sites de faire des recours – ils seront dans leur droit – ; mais je pense qu'une fois franchis ces obstacles la procédure sera d'autant plus efficace.

Pour renforcer la solidité du dispositif, je vous proposerai de fusionner les deux procédures de mise en demeure et de sanction prévues à l'encontre de l'éditeur, car je trouve qu'elles se recouvrent partiellement et empiètent également sur une éventuelle procédure pénale. Le système que j'ai imaginé est plus simple : il y aurait une mise en demeure de l'éditeur de se conformer au référentiel avec une sanction pécuniaire plus ou moins importante à la clé selon que l'éditeur n'a mis en place aucun contrôle d'âge ou un dispositif non conforme au référentiel. Après cette mise en demeure de l'éditeur et si l'Arcom constate que le site est accessible aux mineurs, elle

pourrait alors demander des mesures de blocage et de déréférencement directement aux fournisseurs d'accès à internet (FAI) et aux moteurs de recherche. Je vous suggérerai également d'intégrer l'ensemble de ces dispositions dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

L'article 4 continue à avoir un écho particulier puisqu'il vise à donner les moyens à l'Arcom, le régulateur de l'audiovisuel et du numérique, de mieux mettre en œuvre les sanctions européennes décidées à l'encontre de la Russie à la suite de l'invasion de l'Ukraine. Je vous proposerai des amendements d'importance variable sur cet article.

Le premier amendement vise à combler un « trou dans la raquette » en donnant à l'Arcom une compétence sur les services de télévision et les services de médias audiovisuels à la demande (Smad) extracommunautaires diffusés en France ne relevant pas de la compétence d'un autre État membre de l'Union européenne. L'absence de support juridique avait pour conséquence l'impossibilité de bloquer la diffusion de certains médias étrangers.

Le deuxième amendement vise à confier à l'Arcom le soin de déterminer le délai au terme duquel les FAI devront avoir coupé l'accès aux sites considérés. Il apparaît difficile, en effet, de considérer que cette action puisse être réalisée « sans délai », comme le prévoit la rédaction actuelle ; pour autant, il va de soi que ce délai devra être restreint au strict minimum.

J'ai également déposé des amendements sur l'article 5, qui crée une nouvelle peine complémentaire de « bannissement ». Cette peine semble avoir été conçue pour s'appliquer à titre principal non pas au cyberharcèlement ou à la pédocriminalité, mais aux délits de presse graves : il s'agit donc d'une sanction qui concernera, en pratique, peu de condamnés. Je ne crois pas que nous puissions nous en satisfaire. C'est pourquoi je vous propose, en premier lieu, un travail sur cette peine complémentaire afin d'en étendre le champ. Le Sénat sera pleinement dans son rôle en prévoyant l'application du bannissement à ceux qui utilisent les services en ligne pour menacer et intimider les élus de la République. Déjà en 2020, 20 % des maires se disaient victimes de cyberharcèlement ; ce phénomène délétère n'a fait que s'amplifier depuis lors. Nous devons agir résolument contre cette forme de violence, qui abîme la démocratie et fragilise nos territoires, en réservant à ceux qui harcèlent les élus sur internet des sanctions exemplaires.

Nous ne devons pas en rester là, et il est possible de faire du bannissement un outil plus ambitieux. La nature même des peines complémentaires les expose à certaines limites juridiques et pratiques ; je crains que le bannissement tel qu'il est proposé par le Gouvernement ne reste relativement symbolique. Nous devons lui donner une portée plus opérationnelle : aussi vous proposerai-je que l'interdiction de se rendre sur certaines plateformes puisse être prévue dans le cadre des alternatives aux

poursuites, pour les infractions les moins lourdes, et dans le cadre de l'exécution des peines, pour les condamnations les plus graves.

À terme, je suis convaincu que nous devons trouver le moyen de sanctionner immédiatement tous ceux qui diffusent sur internet des contenus dégradants, indignes ou humiliants, et qui échappent actuellement à toute répression pénale. À l'évidence, le bannissement ne répondra pas à cet objectif d'immédiateté, mais je travaille activement sur ce sujet pour pouvoir porter une solution lors de la séance publique.

À l'inverse, la création d'une autorité de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions dans l'exercice de leurs fonctions juridictionnelles fait consensus parmi les personnes que nous avons auditionnées, à commencer par les principaux concernés – le Conseil d'État, la Cour de cassation et la Cour des comptes. J'estime, pour ma part, que la création de ces autorités garantira aux justiciables une meilleure protection de leurs données personnelles. Par conséquent, je ne vous proposerai que des amendements de clarification rédactionnelle sur les articles 19, 20 et 21 du projet de loi.

J'en viens au deuxième axe : celui de l'adaptation de notre droit au « paquet numérique » européen.

Cet axe nécessite de la part des législateurs que nous sommes une certaine retenue, puisque les trois règlements que transpose ce projet de loi sont d'application directe. Nous devons cependant demeurer vigilants afin d'éviter que l'adaptation en droit interne de ces règlements n'aboutisse à un recul disproportionné dans certains domaines. Je suis notamment en désaccord avec certaines interprétations qui ont été faites par le Gouvernement et qui résultent en l'abrogation « sèche » et non compensée par le règlement sur les services numériques (RSN) – ou *Digital Services Act* (DSA) – de dispositifs qu'il me semble nécessaire de maintenir. C'est pourquoi je vous proposerai, à l'article 29, de conserver, dans le droit interne, l'obligation pour les opérateurs de plateformes en ligne de mettre en place un dispositif de signalement des fausses informations, lequel n'est pas couvert par le RSN qui ne mentionne que les « contenus illicites ». Le considérant 12 du RSN invite les États membres à adopter une définition « large » de ces contenus illicites : dont acte !

Le projet de loi comporte aussi un volet relatif à la Cnil ; les articles 31 et 32 reconnaissent la compétence de celle-ci pour l'application, respectivement, du DGA et du RSN. L'adaptation de la loi Informatique et libertés à ces textes n'est pas un choix : c'est un impératif, dont la nécessité n'est pas contestable. Pour autant, l'adaptation du droit ne doit pas être le synonyme d'une fragmentation de la loi, et nous ne pouvons pas continuer à adapter nos textes au coup par coup, sans cohérence d'ensemble. Je vous proposerai en conséquence, en plein accord avec mon collègue Patrick Chaize qui est confronté aux mêmes difficultés pour l'Arcom, de permettre à

la Cnil d'utiliser les nouveaux pouvoirs qu'elle tire du RSN non seulement pour assurer le bon respect de ce texte, mais aussi pour veiller à la bonne application des autres obligations issues des textes nationaux ou du RGPD.

Mme Catherine Morin-Desailly, présidente. – Avant de débuter l'examen des amendements, je vais vous préciser le champ retenu pour l'article 45 de la Constitution que nous avons défini avec les deux rapporteurs. Je vous rappelle en effet qu'en application des articles 17 bis et 44 *bis* de notre Règlement, il revient à la commission saisie au fond – en l'occurrence, notre commission spéciale – de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

Nous vous proposons donc de considérer que sont susceptibles de présenter un lien, même indirect, avec le texte déposé, les dispositions relatives à l'actualisation du droit interne au règlement relatif à un marché unique des services numériques, au règlement sur les marchés numériques (RMN), au règlement portant sur la gouvernance européenne des données ainsi qu'à la proposition de règlement sur les données (*Data Act*) ; aux mesures de contrôle et de blocage mis en œuvre pour prévenir l'accès des mineurs à des services de communication en ligne qui mettent à disposition du public des contenus pornographiques ; à la pénalisation du défaut d'exécution par un hébergeur d'une demande de retrait de contenus pédopornographiques émanant de l'autorité administrative compétente ; au respect des interdictions de diffusion de contenus produits par des médias visés par des sanctions européennes ; à la prévention et à la répression du cyberharcèlement et des infractions pénales graves susceptibles d'être commises en ligne ; à la mise en place d'un dispositif national de filtrage des contenus constituant des actes de cybermalveillance ; à la régulation du marché dit de « l'informatique en nuage » et aux conditions économiques et techniques applicables aux opérateurs de ce marché ; à la régulation du marché des services d'intermédiation de données et aux conditions économiques et techniques applicables aux opérateurs de ce marché ; à la définition et à la régulation des jeux à objets numériques monétisables ; aux missions du pôle d'expertise pour la régulation de l'économie numérique ; à la centralisation et à la mise à disposition des données permettant de contrôler le respect des mesures encadrant la location de meublés de tourisme ; au contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle ; à la bonne articulation des autorités indépendantes, juridiques et administratives pour la mise en œuvre des règlements européens précités et pour la prise en compte dans le droit français des prérogatives qu'ils tirent de ces règlements ; aux délais et aux modalités d'entrée en vigueur des dispositions de ce projet de loi.

En revanche, nous vous proposons de considérer que ne présentent pas un lien, même indirect avec le texte, les dispositions relatives à la lutte contre les

violences pornographiques et l'éducation à la vie sexuelle et affective ; à la régulation du marché de la publicité en ligne ; à la lutte contre le piratage des programmes sportifs et des œuvres cinématographiques, musicales et audiovisuelles ; à la sécurité des systèmes d'information et au hacking éthique ; à la régulation de l'activité d'influence commerciale et d'agent d'influenceur ; à la réduction de l'empreinte environnementale du numérique et à la sobriété numérique ; aux considérations d'ordre général sur la régulation des jeux d'argent et de hasard ainsi qu'à la modification de la loi du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ; à la couverture numérique des territoires ; aux mesures prises pour lutter contre l'exclusion numérique et favoriser l'inclusion numérique ; à la modification des obligations applicables aux loueurs de meublés de tourisme et à la lutte contre le surtourisme.

Il en est ainsi décidé.

EXAMEN DES ARTICLES

Article 1er

M. Loïc Hervé, rapporteur. – S'agissant de l'amendement COM-26, je rappelle que le règlement du 19 octobre 2022 relatif à un marché unique des services numériques est d'application directe. Il n'est donc pas nécessaire d'en prévoir une transposition dans le projet de loi. L'objet de l'article 1er est bien d'aller au-delà du RSN au nom de la protection des mineurs dans le cadre permis par la directive e-commerce ; je souscris à cet objectif. Avis défavorable.

M. Loïc Hervé, rapporteur. – L'amendement COM-91 vise à clarifier le fait que l'obligation de vérifier l'âge des utilisateurs repose sur les éditeurs de service de communication au public en ligne permettant l'accès à un contenu pornographique.

Il supprime également la procédure de mise en demeure et sanction en cas de non-conformité au référentiel obligatoire, prévue à l'article 1er, pour l'intégrer à l'article 2 et mieux la coordonner avec le dispositif prévu en cas d'accès aux mineurs à un site à caractère pornographique.

Cet amendement, qui procède également à des améliorations rédactionnelles, forme un tout avec l'amendement que j'ai déposé à l'article 2.

L'amendement COM-26 n'est pas adopté. L'amendement COM-91 est adopté. En conséquence, l'amendement COM-36 *devient sans objet.*

M. Loïc Hervé, rapporteur.– L'amendement COM-37 pose un délai maximal à la publication du référentiel. Le délai proposé de six mois semble

cohérent avec le délai annoncé par la direction générale des entreprises lors de son audition. Avis favorable.

L'amendement COM-37 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-64 rectifié porte sur l'avis conforme de la Cnil.

Nous en avons eu la confirmation lors de l'audition commune de la Cnil, de l'Arcom et de l'Arcep, nos autorités administratives indépendantes travaillent main dans la main sur ce dispositif. Il ne me semble pas nécessaire de créer plus de contraintes qu'il n'y en a. La Cnil, que nous avons consultée, ne semble pas demandeuse de ce type de mesure.

Je vous proposerai à l'article 2 un amendement qui ajoute une consultation du président de la Cnil en cas de procédure de mise en demeure et de sanction pour non-respect du référentiel. Il améliorera, davantage que cet amendement, la coopération entre ces deux autorités indépendantes. Avis défavorable.

L'amendement COM-64 rectifié n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-21 prévoit la prise en compte l'empreinte empreinte environnementale du numérique par le référentiel élaboré par l'Arcom.

Le principal objectif poursuivi est d'avoir un système de contrôle d'âge fiable et respectueux des données personnelles. L'aspect environnemental doit être pris en compte, mais une fois cette étape franchie.

Par ailleurs, je rappelle que la fréquentation des sites de vidéos pornographiques consomme énormément de bande passante – et donc d'énergie. Cela nous a été confirmé par la présidente de l'Arcep. C'est donc plutôt sur cette question qu'il s'interroger en premier et non sur l'empreinte environnementale des systèmes de contrôle d'accès. Avis défavorable.

L'amendement COM-21 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-23 prévoit l'ajout de la garantie de la protection des données personnelles des utilisateurs. Cet amendement me semble satisfait : c'est bien ce que recouvre la notion de respect de la vie privée des utilisateurs et ce qui justifie l'intervention de la Cnil. Demande de retrait ; à défaut, mon avis sera défavorable.

M. Thomas Dossus. – Je le retire.

L'amendement COM-23 est retiré.

M. Loïc Hervé, rapporteur. – L'amendement COM-22 exclut l'utilisation de technologies de reconnaissance biométriques. Laissons la Cnil jouer son rôle et poser les limites qu'elle estime utiles aux systèmes de vérification d'âge : c'est bien l'objet de son intervention dans la mise au point du référentiel.

Certes, les dispositifs ne s'appuieront pas sur la reconnaissance faciale à proprement parler, puisqu'il ne s'agira pas d'établir un lien avec son identité, mais sur la reconnaissance des traits des utilisateurs pour distinguer majeurs et mineurs. En votant cet amendement, nous limiterions peut-être trop les technologies qui nous permettraient de procéder au contrôle de l'âge. Je préfère donc laisser l'autorité administrative indépendante, dont c'est la mission, faire son travail de vérification lorsqu'elle sera amenée à rendre un avis sur le référentiel, plutôt que d'inscrire des interdits dans la loi qui pourraient limiter son efficacité. Avis défavorable.

M. Thomas Dossus. – Ces amendements ont pour objet la définition du référentiel. En tant que législateurs, il me paraît important que nous nous saisissions pleinement de ce texte et que nous définissions davantage ce référentiel.

L'amendement COM-22 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-24 prévoit d'ajouter le respect de l'anonymat. C'est tout l'objet du référentiel que de protéger la vie privée des utilisateurs.

C'est d'ailleurs la direction dans laquelle ont travaillé l'Arcom, la Cnil et le PEReN, qui suggèrent un système de double anonymat.

L'anonymat sera globalement respecté, mais il sera nécessaire qu'un tiers de confiance ait accès à l'identité pour vérifier l'âge. La formule utilisée ne convient donc pas. Avis défavorable.

L'amendement COM-24 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-25 concerne l'accessibilité des systèmes de vérification d'âge sous un format ouvert et librement réutilisable. Il me semble que l'objectif poursuivi avec cet amendement est d'assurer l'information des utilisateurs quant à l'utilisation de leurs données personnelles.

Cette transparence est déjà prévue par le RGPD qui dispose, dans son article 15, que le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement.

S'agissant du format des logiciels utilisés pour le contrôle d'âge, il me semble qu'il faut déjà regarder les solutions disponibles sur le marché. Il est trop tôt pour imposer un format plutôt qu'un autre. Avis défavorable.

L'amendement COM-25 n'est pas adopté.

L'article 1er est adopté dans la rédaction issue des travaux de la commission.

Article 2

M. Loïc Hervé, rapporteur. – Les amendements COM-92, COM-31 et COM-32 concernent les sanctions.

D'abord, l'amendement COM-92 réécrit largement l'article 2, et vise à mieux coordonner les procédures initialement prévues aux articles 1er et 2. L'ensemble des dispositions seraient par ailleurs intégrées dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique pour en garantir une meilleure accessibilité.

Une première procédure de mise en demeure et de sanction concernerait l'éditeur qui ne respecte pas le référentiel, soit parce qu'il ne met pas en œuvre le contrôle d'âge, soit parce que le système mis en place n'est pas conforme à celui fixé par l'Arcom. Après une phase contradictoire d'échange d'observations, l'Arcom pourrait mettre en demeure l'éditeur et, sans réponse au bout de quinze jours, mettre en œuvre une procédure de sanction susceptible d'aboutir à une sanction pécuniaire pouvant aller jusqu'à 6 % du chiffre d'affaires mondial en cas d'absence de contrôle d'âge et de réitération. Le président de la Cnil pourrait être consulté par l'Arcom dès lors que la non-conformité serait relative à la protection de la vie privée des utilisateurs.

Parallèlement, une seconde procédure serait ouverte en cas de mise en demeure de l'éditeur restée sans effet et de constat qu'un accès des mineurs aux contenus pornographiques est possible en violation de l'article 227-24 du code pénal : l'Arcom aurait la possibilité de mettre en œuvre la procédure de blocage et de déréférencement à l'égard des FAI et des moteurs de recherche ; seraient reprises les mesures déjà proposées dans le texte initial – soit le blocage en 48 heures par les FAI et 5 jours pour les moteurs de recherche pour une durée maximale de 24 mois, accompagné d'une publicité des mesures. Les FAI et les moteurs de recherche qui ne se conformeraient pas à ces obligations encourraient des sanctions pécuniaires identiques à l'éditeur qui mettrait en œuvre un système de vérification d'âge qui ne serait pas conforme au référentiel : c'est le régime prévu dans le texte initial. Une information du public serait opérée *via* un renvoi sur une page de l'Arcom expliquant les raisons du blocage.

Concernant l'amendement COM-31, qui deviendrait sans objet en cas d'adoption de mon amendement, M. Dossus et moi nous rejoignons partiellement sur le fond. Mon amendement ajoute une consultation du président de la Cnil, plus souple qu'une consultation du collège, à deux moments de la procédure. Premièrement, en cas de mise en demeure d'un éditeur pour non-respect du référentiel, il semble utile qu'à la demande de l'Arcom, le président de la Cnil puisse être consulté dans les hypothèses où le système de contrôle d'âge utilisé pourrait ne pas être respectueux de la vie privée des utilisateurs ; en revanche lorsqu'il n'y a pas du tout de contrôle d'âge, je n'en vois pas l'intérêt. Deuxièmement, il pourrait être consulté au moment de prononcer une sanction afin que les jurisprudences des deux autorités soient cohérentes.

Il ne me semble pas nécessaire d'aller plus loin et de prévoir un avis systématique à chaque étape, notamment avant une demande de blocage.

Ce n'est d'ailleurs pas le souhait de la Cnil ; il me semble qu'une jurisprudence assez robuste se construirait assez rapidement. Demande de retrait.

Les auteurs de l'amendement COM-32, qui deviendrait également sans objet, souhaitent maintenir la compétence du juge judiciaire pour ordonner à l'éditeur de prendre toute mesure de nature à empêcher l'accès des mineurs aux sites pornographiques. Ils maintiendraient en revanche les demandes directes de blocage et de déréférencement vis-à-vis des intermédiaires techniques.

Outre le fait qu'il est proposé que le juge judiciaire prononce une amende administrative – cela n'est pas possible en droit –, il ne me semble pas qu'un tel panachage soit efficace. Soit on choisit de maintenir le système actuel, soit il faut basculer vers un système d'ordre administratif : c'est le choix du Gouvernement, auquel je vous propose de souscrire. Avis défavorable.

L'amendement COM-31 est retiré.

L'amendement COM-92 est adopté. En conséquence, l'amendement COM-32 devient sans objet.

M. Loïc Hervé, rapporteur. – L'amendement COM-1 restreint le champ des demandes de blocages aux seuls fournisseurs de système de résolution de nom de domaine. Il correspond à une demande explicite de la Fédération française des télécoms. Toutefois, il ne me semble pas opportun de réduire le champ des personnes auxquelles peut être demandée une mesure de blocage.

L'article 2 est calqué sur l'article 23 de la loi du 20 juillet 2020 et sur l'article 6-1 de la LCEN. Il prévoit par ailleurs qu'en cas d'impossibilité matérielle d'agir, aucune sanction ne peut être imposée. Il n'y a donc pas de difficulté.

Je souligne que l'article 32 de la loi de programmation militaire en cours de discussion auquel il est fait référence correspond à une autre hypothèse puisqu'il s'agit de répondre à des agissements malveillants qui passent par le système de noms de domaine (DNS – *Domain Name System*), et non à des contenus illicites ou illicitement rendus accessibles à des mineurs. Avis défavorable.

L'amendement COM-1 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-2 renvoie à l'Arcom la définition du délai de blocage. Il émane également de la Fédération française des télécoms et de l'opérateur Free.

Il s'agirait de laisser à l'Arcom le soin de fixer le délai d'exécution des mesures de blocage et de déréférencement, en imposant des délais minimaux de deux jours ouvrés et d'aligner le sort des moteurs de recherche sur celui des fournisseurs d'accès à internet.

Le délai de 48 heures semble suffisamment clair : les fournisseurs d'accès ont des services spécialisés pour traiter ce type de demande. L'Arcom n'a signalé aucune difficulté en la matière. Avis défavorable.

L'amendement COM-2 n'est pas adopté.

L'amendement rédactionnel COM-61 rectifié est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-67 rectifié supprime les planchers de sanction pécuniaire exprimés en euros. Il semble nécessaire de conserver un plancher exprimé en euros, étant bien précisé que c'est le montant le plus élevé qui est retenu. Avis défavorable.

L'amendement COM-67 rectifié n'est pas adopté.

L'article 2 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 2

M. Loïc Hervé, rapporteur. – L'amendement COM-43 rectifié *bis* vise le retrait des contenus zoophiles par l'Arcom.

Le dispositif de cet amendement n'est pas opérant dans la mesure où il ne prévoit pas la procédure pour prononcer le retrait des contenus.

Sur le fond, dans la mesure où ces contenus zoophiles seraient susceptibles d'être vus par des mineurs, ils sont compris dans le champ de l'article 2 qui donne un pouvoir de mise en demeure et de sanction de l'Arcom. Pour le reste, la plateforme Pharos a mis à jour son formulaire en ligne pour pouvoir signaler des actes de cruauté envers les animaux et ces contenus manifestement illicites peuvent être signalés aux plateformes et aux hébergeurs. Ces contenus manifestement illicites sont ensuite signalés aux hébergeurs qui ont l'obligation de les retirer dans les meilleurs délais. Cet amendement est donc partiellement satisfait.

Par ailleurs, je veux faire observer que cet amendement a été déposé sans que ce sujet n'ait été abordé lors des auditions. Pourtant, nous travaillons sur ce texte depuis trois semaines ; tous les membres de la commission spéciale peuvent assister à l'ensemble des auditions et saisir les rapporteurs. Il est problématique de devoir légiférer dans ces conditions. Je suis prêt à travailler sur ce sujet, dont je ne méconnais pas la gravité, mais veillons à la méthode.

Mme Catherine Morin-Desailly, présidente. – Il est vrai que nous avons manqué de temps pour examiner de manière approfondie l'ensemble du texte.

L'amendement COM-43 rectifié bis *n'est pas adopté.*

L'amendement COM-63 rectifié est déclaré irrecevable en application de l'article 45 de la Constitution.

Avant l'article 3

M. Loïc Hervé, rapporteur. – L'amendement COM-38 entend élargir les compétences de Pharos en matière de demande administrative de retrait, pour qu'elle puisse utiliser son pouvoir de demande de retrait et de blocage dans un champ plus large que les seuls contenus terroristes et pédopornographiques. Il s'agirait d'y intégrer les représentations d'actes de torture, de barbarie et de viol.

Il ne me semble pas opportun d'élargir le champ d'action spécifique de Pharos qui s'agissant de cette mission très spécifique concentrée sur le haut du spectre des infractions, en matière de terrorisme et pédopornographie.

Je précise que le fait de réserver les procédures dérogatoires à ces deux catégories d'infractions est en cohérence avec la législation européenne : je rappelle l'existence du règlement européen relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne, dit « règlement TCO », adopté en avril 2021 et du règlement *Child Sexual Abuse Material* (CSAM) en cours de discussion.

Cela ne veut pas dire pour autant que rien n'est fait pour lutter contre les autres contenus illicites, en particulier lorsqu'ils portent sur des représentations de crimes comme ici. Ils peuvent faire l'objet de signalement auprès de Pharos pour déclencher des enquêtes et faire l'objet de demandes de retraits plus classiques auprès des éditeurs et hébergeurs.

Je souhaite avoir l'avis de Pharos et du Gouvernement en attente de la séance publique, mais à ce stade j'émets un avis défavorable.

L'amendement COM-38 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-42 de Mme Rossignol prévoit de supprimer la circonstance aggravante en matière de pédopornographie qui permet une pénalisation quand on enregistre l'image d'un rapport sexuel impliquant un mineur de moins de 15 ans, même quand ces images ne sont pas diffusées.

Je trouve dommageable de ne pas faire de différence en fonction de l'âge de la victime et de punir de la même manière les auteurs d'infractions sans tenir compte de ce critère. Je note aussi qu'il y a une différence notable entre les mineurs de moins de 15 ans et ceux qui ont plus de 15 ans : au-delà de cet âge, on a atteint la majorité sexuelle et on peut donc consentir à certains actes s'ils sont faits dans l'intimité.

L'article 227-25 du code pénal est clair sur ce sujet, et nous avons eu de longs débats sur la notion d'atteinte sexuelle et sur l'âge du consentement. Ainsi, je ne vois pas comment notre droit pourrait à la fois reconnaître qu'un mineur de 16 ou 17 ans peut consentir à des rapports sexuels, mais lui imposer les modalités de ce consentement. Il y a là un risque constitutionnel clair.

Je vous rappelle également que, quel que soit l'âge, diffuser les images d'un rapport sexuel sans le consentement de toutes les personnes concernées est une infraction lourdement réprimée ; cette protection, prévue pour les mineurs de 15 à 18 ans par l'article 227-23, s'applique déjà.

Je vous propose que nous en restions au droit actuel, qui réprime durement la diffusion d'images de mineurs, quel que soit leur âge, mais comporte un régime spécifique pour les mineurs de moins de 15 ans.

C'est pourquoi je demande le retrait de cet amendement ; à défaut, mon avis sera défavorable.

L'amendement COM-39 porte sur la pénalisation, au titre de la pédopornographie, de la diffusion d'images revêtant l'intention de représenter des mineurs.

Je comprends l'intention des auteurs de cet amendement, qui n'est pas dénué de lien avec les conclusions du rapport intitulé *L'enfer du décor* de notre délégation aux droits des femmes, dont je suis également membre. L'amendement vise à ce que tout contenu qui met en scène des images de relations entre un majeur et un mineur, même si le "mineur" ne l'est pas dans les faits, soit pénalisé au titre de la pédopornographie.

L'objectif est d'éviter que, sous couvert de fiction, on ne vienne faire l'apologie de comportements qui sont interdits et réprimés par le code pénal. Même si je comprends parfaitement l'objectif poursuivi, il faut mesurer les conséquences d'un tel amendement.

Premièrement, cette modification porterait des atteintes importantes à la liberté d'expression. Les auteurs de l'amendement visent, implicitement, les plateformes pornographiques, mais l'article 227-23 n'est pas centré sur ces sites ; il concerne tous les types de contenus audiovisuels. Or, l'atteinte à la liberté d'expression me semble en l'espèce si importante qu'elle est très probablement contraire à la Constitution. Je ne crois pas que le Conseil constitutionnel, qui sera probablement saisi du texte avant sa promulgation, accepte une telle évolution.

Deuxièmement, il faut mesurer l'impact de cet amendement sur les agents chargés de lutter contre la pédopornographie, notamment les agents de Pharos. Alors que ces derniers ont identifié des critères relativement simples pour sélectionner les contenus à bloquer, ce qui permet un blocage rapide et massif, les conditions posées par l'amendement quant au contenu, aux images et au titre vont leur demander un travail d'analyse au cas par cas qu'ils n'ont pas forcément les moyens de mener. Je crains que, bien involontairement, cet amendement ne vienne déstabiliser l'action de Pharos et nuire à l'efficacité du travail de blocage des contenus pédocriminels.

Pour ces raisons, je formule une demande de retrait ou, à défaut, un avis défavorable.

L'amendement COM-41 vise à insister sur l'intention de représenter un mineur par des images ou contenus à caractère pornographique. Même avis pour les mêmes raisons.

Mme Laurence Rossignol. – Premièrement, il n'y a pas d'atteinte à la liberté d'expression, ni de risque de sanction pour des sites non pornographiques. Tous les amendements précisent bien que seuls les sites « pornographiques » sont concernés. Le caractère pornographique de l'intention de représenter des mineurs est exigé. En cas de doute, je peux parfaitement clarifier la rédaction de mon amendement.

Je réfute également l'idée selon laquelle ces amendements augmenteraient la charge de travail des enquêteurs. Aujourd'hui, ces derniers sont contraints de vérifier image par image si la personne à l'écran est réellement mineure ou en a juste l'apparence. Les agents de Pharos et d'Europol ont reconnu distinguer les mineurs de moins de 15 ans et ceux de plus de 15 ans. Nous considérons, en revanche, qu'un mineur est un individu de moins de 18 ans. La majorité sexuelle n'est pas un concept juridique. Il y a deux ans, nous avons légiféré sur l'âge à partir duquel une relation sexuelle entre une personne majeure et une personne mineure est, par nature, un viol. Nous avons en effet retenu l'âge de 15 ans, ce qui signifie que toute relation avec une personne de moins de 15 ans est, par définition, un viol. Les relations sexuelles entre mineurs ne sont, quant à elles, pas interdites. Pour autant, je ne conçois pas que l'on puisse envisager la moindre recherche de consentement dans le cadre d'images pédopornographiques.

De plus, le droit sanctionne aujourd'hui la mise en scène d'une personne mineure dans des images pornographiques. Nos amendements vont plus loin et visent à condamner l'apologie des relations sexuelles incluant des mineurs, de la pédopornographie, de l'inceste. Peu importe que la jeune femme qui apparaît dans ces contenus ait 18 ans ou 15 ans révolus. L'important, c'est que les diffuseurs souhaitent montrer que le visionnage de relations sexuelles incluant des mineurs peut provoquer une excitation sexuelle. Nous visons donc l'intention. L'intention de diffuser de la pédopornographie est plus large que le seul critère d'avoir ou non recouru à des mineurs pour tourner des images pornographiques. Nous faisons la chasse à l'apologie de l'inceste et de la pédocriminalité par l'intermédiaire de la pornographie.

L'amendement COM-42 n'est pas adopté. (Mme Laurence Rossignol s'exclame.)

Mme Marie Mercier. – Madame la présidente, j'aimerais savoir ce qu'a dit Mme Rossignol à mon endroit !

Mme Laurence Rossignol. – Madame Mercier, vous êtes l'auteur de l'amendement à la loi de 2020 visant à protéger les jeunes mineurs des crimes sexuels et constatez avec moi que l'application de cette loi se heurte à

la résistance forte des sites pornographiques. Je pensais que nous pourrions au moins compter sur votre soutien.

Mme Marie Mercier. – Les mineurs pourront toujours compter sur moi.

Mme Catherine Morin-Desailly, présidente. – Nous aurons donc ce débat en séance.

Les amendements COM-39 et COM-41 ne sont pas adoptés.

M. Loïc Hervé, rapporteur. – L'amendement COM-40 vise à insister sur le caractère incestueux que peuvent revêtir certaines images pornographiques diffusées.

J'ai des réserves analogues à celles que j'ai formulées sur l'amendement COM-39.

De plus, en vertu du code pénal, les relations dites « incestueuses » concernent forcément un mineur, comme le rappelle l'article 227-27-2-1 : on est donc déjà dans le cadre de la pédopornographie si on diffuse de telles images. L'amendement est, par conséquent, satisfait. Retrait ou, à défaut, un avis défavorable.

Mme Laurence Rossignol. – Si le droit actuel est si efficace, pourquoi tous les sites pornographiques proposent actuellement des rubriques dédiées aux relations sexuelles entre membres d'une même famille ? L'interdiction est peut être inscrite dans notre droit, elle n'est pour autant pas appliquée.

Mme Marie Mercier. – On fait du droit !

M. Loïc Hervé, rapporteur. – Oui, je le confirme : ici, nous faisons du droit.

Mme Marie-Noëlle Lienemann. – Quand le droit n'est visiblement pas appliqué, soutenir plus clairement le refus de telles pratiques est de nature à faire en sorte que le texte juridique soit plus contraignant, ou à inciter le Gouvernement à agir de manière plus opérationnelle. Pourquoi y a-t-il un tel écart entre le droit et les faits ? Voter cet amendement nous permettrait de montrer notre détermination à vouloir que les faits s'alignent sur le droit. Il s'agit d'un acte politique qui permettrait de renforcer les textes juridiques existants.

M. Loïc Hervé, rapporteur. – La proposition de rédaction est la suivante : « ces dispositions du présent article sont applicables dès lors qu'elles ont pour intention de représenter des relations sexuelles de caractère incestueux. » Dès lors qu'un mineur est impliqué, le droit qualifie l'inceste. Va-t-on aujourd'hui redéfinir la notion de l'inceste contenue dans le code pénal ?

Mme Annick Billon. – Pour avoir mené un travail sur ce sujet avec Alexandra Borchio Fontimp et Laurence Rossignol, je puis préciser que notre

collègue veut montrer notre opposition à l'apologie, à l'incitation, à ce type d'images que nous souhaitons interdire. Je comprends la difficulté de les faire interdire.

Lors de nos travaux sur l'industrie de la pornographie, nous avons découvert une volonté réelle de faire l'apologie du racisme, de l'inceste, du viol. L'objectif de Mme Rossignol est de réaffirmer qu'un site qui ferait une telle apologie pourrait être interdit. J'ai conscience cependant que l'application de cette mesure est délicate, tout comme le contrôle de l'âge, mais je comprends la démarche, dont l'objectif est de protéger et d'éviter les apologies de l'inceste, du viol, du racisme, et non pas de la pornographie en général.

Mme Marie-Noëlle Lienemann. – Cet amendement porte principalement sur le concept d' « intention ». Ce dernier existe en droit dans d'autres cas. Notre commission pourrait voter cet amendement pour demander au Gouvernement si le champ de l'intention est déjà couvert par la loi – je ne pense pas que ce soit le cas – et, si la formulation n'est pas la bonne, lui demander de nous en proposer une autre.

M. Loïc Hervé, rapporteur. – Le sujet pourra être débattu en séance. Je vous propose d'en rester sur ma position initiale, par cohérence avec ma position sur les trois autres amendements.

Mme Alexandra Borchio Fontimp. – Les rapporteurs ne peuvent-ils pas nous proposer une nouvelle rédaction ? Si l'« intention » n'est pas un concept recevable, peut-être faudrait-il privilégier celui d'« apologie » ou d'« incitation ». Mme Rossignol, Mme Billon et moi-même avons passé huit mois à travailler sur ce sujet. Nos interventions ont donc pour seul objectif de vous prouver que nos amendements s'appuient sur des bases solides. La question des titres de vidéos ou de certains sites faisant l'apologie de l'inceste, du viol, n'est pas couverte par le droit. Cela ne relève peut-être pas du droit, mais cela permet de faire passer un message.

Mme Elsa Schalck. – Je comprends les intentions sous-tendues par cet amendement, mais nous faisons face à une difficulté juridique : notre droit pénal ne sanctionne pas l'intention. Il s'agirait donc de trouver une autre qualification pénale qui nous permettrait de sanctionner ce type de comportement. Si l'on élargissait à d'autres domaines la notion d' « intention », on ouvrirait une brèche puisque sanctionner l'intention de tout un chacun deviendrait impossible.

Mme Laurence Rossignol. – Je pense que vous vous posez des problèmes juridiques qui n'ont pas lieu d'être. À l'heure actuelle, seule la pédocriminalité est sanctionnée. Le directeur d'Europol nous a clairement expliqué que la pédopornographie n'est pas une notion utilisée par ses services. Leurs enquêtes et poursuites ne portent que sur la pédocriminalité, autrement dit sur l'abus sexuel sur mineurs prépubères.

Par cet amendement, nous souhaitons élargir le champ de l'illicite. L'inceste est illicite dans le code pénal, mais l'inceste dans la pédopornographie n'est pas considéré comme une infraction. Nous proposons donc que l'intention de montrer des scènes incestueuses soit une infraction. L'intention est une condition de la faute pénale ; c'est pourquoi j'ai choisi spécifiquement ce terme.

Avec notre amendement, l'intention d'utiliser l'inceste dans des images pornographiques devient une faute, puisque l'inceste est une infraction pénale. Je vous entends invoquer le droit, mais les sites pornographiques regorgent de ce type d'images. Le débat est le même concernant l'amendement sur la pédopornographie, qui prévoit de condamner la volonté de mettre en scène des relations sexuelles avec les enfants ou incestueuses.

Nous poursuivrons ce débat en séance.

L'amendement COM-40 n'est pas adopté.

Article 3

L'amendement de précision rédactionnelle COM-93 e*st adopté.*

M. Loïc Hervé, rapporteur. – L'amendement COM-94 permet de maintenir les conclusions du rapporteur public. Ces dernières nous semblent importantes dans tout contentieux.

L'amendement COM-94 est adopté.

L'article 3 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 3

M. Loïc Hervé, rapporteur. – L'amendement COM-158 prévoit d'aggraver la peine encourue pour un viol lorsque ce dernier est diffusé en temps réel.

Les auteurs de l'amendement entendent mieux lutter contre les viols d'enfants qui sont diffusés en temps réel sur internet ; ils visent les cas où un commanditaire prend contact par internet avec les familles pour la commission d'un tel crime. On ne peut que les rejoindre sur le fond et je ne néglige aucunement la gravité de tels actes. Toutefois, il me semble que l'amendement est satisfait par le droit en vigueur. En effet, le code pénal prévoit déjà deux circonstances aggravantes qui permettent de couvrir ce cas d'espèce et la peine de 20 ans est déjà encourue lorsque la victime est un mineur de moins de 15 ans et lorsque la mise en relation entre l'auteur et la victime a été faite par l'utilisation d'un réseau de communications électroniques. Un magistrat peut donc déjà prononcer de telles peines en s'appuyant sur le droit actuel. En conséquence, je demande le retrait de cet amendement.

L'amendement COM-158 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-159 est une demande de rapport au Parlement sur les viols commandités et diffusés en ligne. Vous connaissez la position du Sénat sur les demandes de rapports. Je demande le retrait de cet amendement.

L'amendement COM-159 n'est pas adopté.

Article 4

M. Loïc Hervé, rapporteur. – L'amendement COM-95 a vocation à donner à l'Arcom une compétence sur les services de télévision et les services de médias audiovisuels à la demande extracommunautaire diffusés en France ne relevant pas de la compétence d'un autre État membre de l'Union européenne (UE).

L'amendement COM-95 est adopté.

M. Loïc Hervé, rapporteur. – Au sujet de l'amendement COM-3, j'émets un avis défavorable par coordination avec l'avis défavorable donné à l'amendement COM-1.

L'amendement COM-3 n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'inscription dans la loi d'un délai de deux jours ouvrés laissé aux fournisseurs d'accès à internet pour bloquer l'accès aux sites incriminés, portée par l'amendement COM-4, n'apparaît pas pertinente puisque cela reviendrait à permettre à des officines de mener des actions d'ingérence librement pendant cinq jours en cas d'un week-end suivi d'un jour férié.

On peut rappeler que le dispositif de l'article 3 de la loi relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique qui organise la lutte contre le piratage des droits sportifs fait obligation aux FAI de couper l'accès aux sites de diffusion pirate en temps réel, avec d'excellents résultats au cours des premières minutes des matchs de Ligue 1.

Dans ces conditions, il n'apparaît pas judicieux d'accorder un délai trop long pour mettre un terme à des ingérences qui pourraient menacer l'ordre public et la sécurité nationale. Mon amendement prévoit de laisser à l'Arcom le soin de définir elle-même la durée de ce délai. J'émets par conséquent un avis défavorable.

L'amendement COM-96 vise à confier à l'Arcom le soin de déterminer le délai au terme duquel les FAI devront avoir nécessairement coupé l'accès aux sites considérés.

L'amendement COM-4 n'est pas adopté.

L'amendement COM-96 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-97 prévoit de renvoyer à un décret en Conseil d'État les modalités d'application du présent article, comme prévu par ailleurs par les articles 2 et 6 du projet de loi.

L'amendement COM-97 est adopté.

L'article 4 est adopté dans la rédaction issue des travaux de la commission.

Article 5

M. Loïc Hervé, rapporteur. – L'amendement COM-98 vise à inclure dans le champ de la future peine complémentaire de bannissement l'ensemble des services susceptibles de servir à une infraction : la notion de plateforme en ligne suppose un stockage de contenus et exclut, en tant que telle, les services ne procédant pas à un tel stockage.

Par l'amendement COM-60 rectifié, M. Fialaire propose que le juge puisse bloquer, à titre de peine complémentaire, non seulement le ou les comptes qui ont permis la commission de l'infraction, mais aussi les autres comptes de la personne condamnée. Cette piste a été explorée par le Gouvernement et par moi-même, mais elle semble contraire à la Constitution : il ne me paraît pas judicieux de prendre ce risque. Au demeurant, il est plausible que les infractions donnant lieu au prononcé de cette peine complémentaire seront commises en utilisant plusieurs comptes sur plusieurs plateformes. La rédaction que je propose permettrait de bloquer l'ensemble des comptes. Demande de retrait ou, à défaut, avis défavorable.

Avis défavorable sur l'amendement COM-86 rectifié. En cas d'adoption de l'amendement COM-98, il deviendrait sans objet.

L'amendement COM-98 est adopté. En conséquence, les amendements COM-60 rectifié et COM-86 rectifié deviennent sans objet.

M. Loïc Hervé, rapporteur. – Le champ matériel d'application de la nouvelle peine complémentaire de bannissement ne paraît pas couvrir l'ensemble des infractions susceptibles d'être commises par le biais d'un service en ligne. L'amendement COM-99 rectifié vise à compléter cette liste de manière la plus exhaustive possible, en prenant en compte les faits analogues au harcèlement, le proxénétisme, les atteintes à la vie privée, la violation d'une interdiction de contact posée par une ordonnance de protection du juge aux affaires familiales, les infractions qui consistent à rendre publiques des allégations infondées ou des informations secrètes ou confidentielles, le chantage, la provocation, les délits voisins à la pédocriminalité – favorisation de la corruption de mineurs et corruption elle-même – ou encore le nouveau délit d'outrage en ligne. Enfin, face à la montée en fréquence et en intensité des violences contre les élus locaux, je propose que ceux qui harcèlent, menacent ou intimident les représentants des collectivités territoriales ou entendent porter atteinte au fonctionnement normal de la démocratie soient, eux aussi, passibles de la nouvelle peine complémentaire de bannissement.

L'adoption de cet amendement rendrait sans objet les amendements COM-85 rectifié et COM-44 rectifié *bis*.

L'amendement COM-99 rectifié est adopté. En conséquence, les amendements COM-85 rectifié et COM-44 rectifié bis deviennent sans objet.

M. Loïc Hervé, rapporteur. – Le projet de loi limite la nature du bannissement à une peine complémentaire. Ainsi conçue et compte tenu également de sa durée, cette sanction sera vraisemblablement réservée, en pratique, aux condamnations les plus légères. L'amendement COM-100 apporte le complément que j'évoquais lors de mon exposé introductif.

L'amendement COM-100 est adopté.

L'article 5 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 5

Les amendements COM-17 et COM-18 *sont déclarés irrecevables en application de l'article 45 de la Constitution.*

M. Loïc Hervé, rapporteur. – L'amendement COM-27 prévoit la possibilité de prononcer le blocage du compte d'accès à une plateforme en ligne en cas de contrôle judiciaire. Là encore, je partage l'état d'esprit des auteurs : dans le même objectif, j'ai déposé un amendement appliquant le bannissement aux cas d'alternatives aux poursuites ou de sursis probatoire. Une harmonisation des rédactions reste cependant nécessaire afin de tenir compte des avancées effectuées à l'article 5.

Par ailleurs, au regard des principes applicables en matière de données personnelles, il me semble problématique de demander au fournisseur de plateformes de procéder au blocage en cas de contrôle judiciaire : nous allons finir par donner aux plateformes les moyens de disposer d'un fichier global de toutes les personnes condamnées pour des infractions commises en ligne…

Je propose donc aux auteurs de retirer cet amendement. Nous pourrons y retravailler ensemble afin qu'il soit déposé sous une forme améliorée en vue de la séance publique.

L'amendement COM-27 est retiré.

M. Loïc Hervé, rapporteur. – L'amendement COM-28 intègre au délit d'outrage sexiste ou sexuel les infractions commises en ligne. Il a pour objet de garantir une répression rapide des comportements dégradants, hostiles ou discriminatoires en les soumettant à une amende forfaitaire délictuelle. Je partage l'état d'esprit des auteurs et travaille activement pour dégager une solution à ce problème en vue de la séance publique.

La solution proposée pose en effet deux difficultés juridiques. Premièrement, elle s'insère dans un dispositif qui touche la vie réelle et vise donc les comportements, alors qu'il faudrait viser la diffusion de contenus.

Deuxièmement, notre code de procédure pénale ne permet pas de faire une réquisition pour identifier l'auteur d'une infraction commise en ligne si celle-ci n'est pas punie d'au moins un an d'emprisonnement. Or l'outrage sexiste et sexuel n'est pas sanctionné par une peine de prison. En pratique, les policiers et gendarmes ne pourront pas identifier l'auteur de l'outrage avec certitude, et ne pourront pas, *a fortiori*, lui infliger une amende. Demande de retrait.

L'amendement COM-28 est retiré.

M. Loïc Hervé, rapporteur. – L'amendement COM-33 vise à prendre en compte, dans la liste des infractions contre lesquelles les plateformes en ligne doivent lutter, la diffusion d'images présentant la commission d'un crime ou d'un délit. Il est satisfait sur le fond, par anticipation, par l'amendement que je présenterai à l'article 22. Demande de retrait.

L'amendement COM-33 est retiré.

Article 6

M. Patrick Chaize, rapporteur. – L'amendement COM-101 tend à faciliter la constatation des infractions déclenchant le dispositif de filtre anti-arnaques.

Dans la version actuelle du projet de loi, ce filtre ne peut être déclenché que si le site internet a été manifestement conçu pour réaliser des infractions comme l'usurpation d'identité, la collecte frauduleuse de données à caractère personnel ou encore l'usage frauduleux de moyens de paiement.

L'intention manifeste d'un éditeur de site internet d'arnaquer les internautes est assez difficile à prouver, d'autant qu'il n'est pas toujours évident de contacter ces éditeurs. Il est plus aisé de constater que les opérations que les internautes peuvent réaliser sur le site internet sont frauduleuses et constituent des infractions. Le dispositif empêcherait l'accès à davantage de sites frauduleux et protégerait davantage de citoyens-internautes.

L'amendement COM-101 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-59 rectifié tend à déclencher le filtre anti-arnaques lorsqu'un internaute obtient des données à caractère personnel sur un site diffusant des données obtenues par piratage.

Ce filtre anti-arnaques peut déjà être déclenché en cas d'obtention de données à caractère personnel par un moyen frauduleux, déloyal ou illicite. L'obtention de données à caractère personnel sur un site internet publiant des données obtenues par piratage est couverte par les infractions visées à l'article L. 226-18 du code pénal. Le texte satisfait déjà cette préoccupation légitime. Demande de retrait ; à défaut, l'avis sera défavorable.

L'amendement COM-59 rectifié est retiré.

M. Patrick Chaize, rapporteur. – L'amendement COM-102 permettrait la mise en demeure des éditeurs de sites internet frauduleux après constatation de l'infraction par l'autorité administrative. L'objectif est double : rendre le dispositif de filtre anti-arnaques plus opérationnel et responsabiliser davantage les éditeurs. À partir du moment où l'autorité administrative constate une infraction, elle ne doit pas se contenter d'informer l'éditeur, mais le mettre en demeure de cesser ses agissements illicites, sauf si cet éditeur apporte la preuve, sous cinq jours, que son site n'est pas frauduleux. C'est une première étape indispensable avant que l'autorité administrative n'ordonne des mesures plus contraignantes destinées à empêcher l'accès aux sites frauduleux.

L'amendement COM-102 est adopté.

L'amendement de précision rédactionnelle COM-103 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-104 tend à uniformiser l'information présentée aux internautes sur le message d'avertissement qui s'affichera sur leurs écrans en cas de tentative d'accès à un site soupçonné d'être frauduleux.

Dans ce cas de figure et dans le cadre du dispositif de filtre anti-arnaques, un message d'avertissement – le projet de loi n'en prévoit pas la nature – s'afficherait, dans l'attente de l'expiration de la période durant laquelle l'éditeur du site visé peut apporter la preuve que son site est légal.

Il convient *a minima* de s'assurer que ce message est clair, lisible, unique et compréhensible. Il y a là un double enjeu de sensibilisation des internautes et d'harmonisation de l'information qui leur est présentée. Je suis également favorable à ce que ce message d'avertissement renvoie systématiquement vers la plateforme gouvernementale *cybermalveillance.gouv.fr*. Les modalités précises d'affichage seront précisées ultérieurement par voie réglementaire.

L'amendement COM-104 est adopté.

M. Patrick Chaize, rapporteur. – Les amendements COM-105, COM-5, COM-6, COM-7 et COM-29 visent à modifier l'alinéa 7 de l'article 6.

À ce stade du déploiement du filtre anti-arnaques, si l'éditeur du site frauduleux n'a pas répondu, n'a pu être contacté ou n'a pas cessé d'agir de façon illégale, il peut être demandé le blocage de l'accès à ce site à plusieurs catégories d'intermédiaires techniques : les fournisseurs de navigateurs internet, les fournisseurs d'accès à internet ou les fournisseurs de systèmes de résolution des noms de domaine.

Par souci d'efficacité, mon amendement COM-105 précise que l'autorité administrative désigne, dans sa décision, la catégorie de fournisseurs concernée par la mesure envisagée : ce ne sont pas les mêmes acteurs qui sont mobilisés pour un déréférencement, un blocage, ou toute

autre mesure. L'implication des trois catégories d'intermédiaires techniques est donc justifiée, en particulier celle des FAI.

En conséquence, je suis défavorable à l'amendement COM-5, qui vise à supprimer les FAI du dispositif, et défavorable à l'amendement COM-29, qui exclut du dispositif les FAI et les fournisseurs de systèmes de résolution de noms de domaine.

Mon amendement COM-105 prévoit également que les intermédiaires techniques visés par l'injonction de blocage procèdent sans délai au blocage demandé. C'est déjà ce qui leur est demandé pour le retrait de certains contenus illicites. Au regard des risques financiers et de violation de données personnelles que représente l'accès à ces sites frauduleux, nous devons voter en faveur d'un dispositif réactif. C'est pourquoi je suis défavorable à l'amendement COM-7, qui introduit un délai d'au moins deux jours ouvrés, ce qui pourrait par exemple conduire à laisser un site déclaré comme frauduleux accessible pendant tout un week-end.

Enfin, mon amendement COM-105 prévoit, en cas de tentative d'accès à un site bloqué, que les internautes soient redirigés vers une page d'information de l'autorité administrative compétente les informant du motif du blocage. C'est déjà ce qui est prévu par d'autres dispositifs de blocage. L'amendement COM-6 est donc satisfait par mon amendement, d'où une demande de retrait. À défaut, l'avis y sera défavorable.

L'amendement COM-105 est adopté. Les amendements COM-5 COM-6, COM-7 et COM-29 sont rejetés.

M. Patrick Chaize, rapporteur. – L'amendement COM-106 porte sur l'obligation de vérifier, à l'approche de l'expiration de la période de blocage, la liste des adresses électroniques des sites dont l'accès a été bloqué.

L'accès à un site internet ne pouvant être bloqué indéfiniment, je tiens à m'assurer que, à l'issue de la période de blocage décidée par l'autorité administrative compétente, les adresses des services de communication au public en ligne en cause et dont l'accès a été temporairement empêché ne sont plus actives ou, si elles le sont, que le constat de l'infraction est toujours valable.

Si les sites frauduleux réalisant des opérations de cybermalveillance ont souvent une existence éphémère sur internet, il est indispensable de responsabiliser davantage les autorités administratives compétentes et de s'assurer, dans un souci de protection renforcée des citoyens en ligne, d'un suivi effectif des mesures de blocage qu'elles ordonnent.

L'amendement COM-106 est adopté.

L'amendement de précision rédactionnelle COM-107 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-8 tend à intégrer les moteurs de recherche en ligne et les annuaires dans le déploiement du dispositif anti-arnaques. À la différence du navigateur

internet, par exemple Google Chrome, qui permet d'accéder aux sites web sur internet, le moteur de recherche, par exemple Google Search, permet de trouver des informations spécifiques en ligne. Or un site bloqué peut rester référencé, même temporairement, par les moteurs de recherche. Tous les intermédiaires techniques doivent être responsabilisés. Avis favorable.

L'amendement COM-8 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-108 tend à renforcer l'information de la personnalité qualifiée de la Cnil chargée de veiller à l'application proportionnée du filtre anti-arnaques. Dans la mesure où cette personnalité peut enjoindre à tout moment à l'autorité administrative de mettre fin aux mesures conservatoires de blocage ou de déréférencement qu'elle a ordonnées, il apparaît important qu'elle soit également informée des décisions prises de façon autonome par l'autorité administrative.

L'amendement COM-108 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-109 a pour objet de clarifier les exigences du rapport d'activité annuel qui devra être élaboré par la personnalité qualifiée au sein de la Cnil, dans une perspective d'amélioration de l'efficacité de son action et de l'ensemble du dispositif prévu à cet article.

Parmi les informations devant figurer dans ce rapport, sont notamment ajoutées les informations relatives au nombre de recours éventuels dont la Cnil a été saisie, ainsi que celles qui sont relatives à l'évolution des moyens nécessaires à la Cnil pour mener à bien cette nouvelle mission.

L'amendement COM-109 est adopté.

M. Patrick Chaize, rapporteur. – En l'état actuel du projet de loi, seuls les fournisseurs de navigateurs internet étaient concernés par les sanctions en cas de manquement aux mesures conservatoires ordonnées par l'autorité administrative. L'amendement COM-110 a pour objet d'appliquer les sanctions prévues, de façon homogène, à l'ensemble des intermédiaires techniques en cas de manquement aux mesures de blocage ordonnées par l'autorité administrative. C'est un oubli majeur du Gouvernement.

L'amendement COM-110 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-9 vise à mettre en place une compensation des surcoûts des opérateurs. À la différence de la procédure de blocage des contenus terroristes et pédopornographiques prévue à l'article 6-1 de la loi pour la confiance dans l'économie numérique, plusieurs catégories d'opérateurs, au-delà des seuls fournisseurs d'accès à internet, sont concernées par le déploiement du filtre anti-arnaques.

La compensation de l'un des opérateurs n'est pas possible, au risque de créer une rupture d'égalité. La compensation de l'ensemble des opérateurs n'est pas envisageable non plus. Le dispositif inclut les fournisseurs de navigateurs sur internet aux deux stades de la procédure, ce qui reviendrait, par exemple, à autoriser l'État à compenser Google pour lutter contre les sites frauduleux ! Avis défavorable.

L'amendement COM-9 n'est pas adopté.

L'article 6 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 6

L'amendement COM-12 est déclaré irrecevable en application de l'article 45 de la Constitution.

M. Loïc Hervé, rapporteur. – Par cet amendement COM-58 rectifié, M. Fialaire propose que la sanction prenne la forme d'une amende en cas de consultation de données informatiques obtenues par fraude.

Cet amendement répond à un motif parfaitement légitime : mieux protéger les entités, notamment publiques, qui ont fait l'objet de cyberattaques et dont les données se trouvent diffusées sur internet par des hackers. Toutefois, je m'interroge sur la portée pratique d'une telle sanction : comment la police et la gendarmerie trouveront-elles l'identité de celles et ceux qui ont consulté ces données ? Comment prouver que la personne savait que les données avaient été obtenues par des hackers ? Surtout, la consultation qu'il est prévu de sanctionner n'est-elle pas déjà couverte par le code pénal, dans la mesure où sa seule vocation est de permettre dans un second temps un usage illégal des données afin d'usurper une identité ou exercer un chantage par exemple, et donc commettre des infractions déjà réprimées ? Si je comprends la logique de l'auteur de l'amendement, je ne vois pas ce que ce nouveau délit apporterait à notre arsenal répressif. Avis défavorable.

M. Bernard Fialaire. – Je suis surpris par la position du rapporteur. La personne qui consulte un contenu piraté le fait en connaissance de cause et doit être sanctionnée.

M. Loïc Hervé, rapporteur. – Certes, mais il faut en apporter la preuve matérielle.

M. Bernard Fialaire. – La preuve serait apportée de la même façon qu'on apporte la preuve matérielle de la consultation de contenus illicites.

M. Loïc Hervé, rapporteur. – Dans le cas d'espèce, ce n'est pas le piratage qui rend le contenu illicite, mais ce que vous en faites.

M. Bernard Fialaire. – Nous assistons constamment au piratage de données médicales, par exemple. Certaines assurances consultent ces données tout en sachant pertinemment qu'elles ont été piratées. Il faut faire

passer le message que la consultation et l'exploitation de ces données constituent un délit.

M. Loïc Hervé, rapporteur. – Je reste dubitatif. Nous devons respecter les principes du droit pénal et le problème de la preuve est un obstacle dirimant à cet amendement.

L'amendement COM-58 rectifié n'est pas adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-66 rectifié prévoit que les décisions prises par le juge en application de l'article L. 336-2 du code de la propriété intellectuelle pourront être actualisées par des « signaleurs de confiance », au sens du règlement sur les services numériques, et que les ayants droit disposant d'agents assermentés pourront devenir de tels signaleurs de confiance. Il s'agit donc de permettre aux ayants droit de demander directement aux FAI de bloquer les sites qui continueraient de porter atteinte à leurs droits.

Le projet de loi ne porte pas sur la lutte contre le piratage et l'amendement prévoit par ailleurs un dispositif inédit d'injonctions privées ouvrant aux titulaires de droit la possibilité d'obtenir, sans contrôle, le blocage de services de communication au public en ligne. Un tel dispositif, qui n'existe pas dans le droit français, poserait en outre des questions de proportionnalité et donc de constitutionnalité. Je vous propose de déclarer cet amendement irrecevable au titre de l'article 45.

L'amendement COM-66 rectifié est déclaré irrecevable en application de l'article 45 de la Constitution.

M. Loïc Hervé, rapporteur. – Les amendements COM-70 rectifié, COM-71 rectifié, COM-73 rectifié et COM-78 rectifié tendent à protéger les « hackers éthiques ». Ils sont irrecevables sur le fondement de l'article 45 de la Constitution.

Les amendements COM-70 rectifié, COM-71 rectifié, COM-73 rectifié et COM-78 rectifié sont déclarés irrecevables en application de l'article 45 de la Constitution.

Mme Catherine Morin-Desailly, présidente. – Un texte européen est en cours de discussion sur cette question.

Article 7

M. Patrick Chaize, rapporteur. – L'amendement COM-111 tend à aligner la définition d'un service d'informatique en nuage avec celle retenue par la directive européenne du 14 décembre 2022, dite « NIS 2 ».

L'amendement COM-111 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-112 a pour objet de clarifier la définition d'un avoir d'informatique en nuage. Nous

parlons bien d'un avantage temporaire octroyé à une entreprise, ce dernier pouvant prendre la forme notamment d'un montant de crédits offert.

Mme Catherine Morin-Desailly, présidente. – Cet amendement très important permettra de mieux structurer les possibilités offertes aux usagers et de rétablir l'équilibre concurrentiel.

L'amendement COM-112 est adopté.

M. Patrick Chaize, rapporteur. – Les amendements COM-113, COM-89 rectifié, COM-47 et COM-62 rectifié tendent à encadrer l'octroi des avoirs d'informatique en nuage.

Mon amendement COM-113 vise à limiter cet octroi à un an, y compris en cas de renouvellement. Au regard des auditions menées sur ce sujet, un tel plafonnement semble être un bon compromis : c'est la durée d'octroi que sont en mesure de proposer nos acteurs français, et cela conduira les acteurs américains à réduire la durée d'octroi des crédits *cloud* qu'ils offrent. Ainsi, la concurrence sera plus juste et nous éviterons de mettre sous perfusion des start-up et de jeunes entreprises. Cet amendement laisse également la liberté au pouvoir réglementaire de détailler les situations dans lesquelles cette durée devrait être inférieure à un an, en fonction des pratiques et des demandes du marché.

Je suis défavorable à l'amendement COM-47, plus rigide, qui fixe la durée d'octroi à neuf mois et la durée de renouvellement à trois mois.

À défaut de consensus, il semble tout de même que l'idée d'un plafonnement monétaire soit écartée par la grande majorité des acteurs concernés. Par ailleurs, en l'absence d'étude sur le taux de consommation des crédits *cloud*, il serait difficile de fixer un montant approprié. Je suis donc défavorable aux amendements COM-89 rectifié et COM-62 rectifié.

Mme Florence Blatrix Contat. – Je m'interroge sur la notion de montant. Certains *providers* proposent des offres *always free*, certaines applications étant gratuites à vie. Le texte porte-t-il uniquement sur les avoirs en montant ?

M. Patrick Chaize, rapporteur. – Le texte vise exclusivement les offres temporaires.

Mme Florence Blatrix Contat. – Les applications gratuites à vie peuvent inciter les clients à rester chez certains *providers*.

M. Patrick Chaize, rapporteur. – Le texte se limite aux crédits et ne porte pas sur les avantages d'un autre type, comme la gratuité d'accès.

Mme Florence Blatrix Contat. – Les étudiants et les universités, qui bénéficient de ces crédits, perdront un avantage. En contrepartie, augmenter les dotations n'est pas possible en raison de l'article 40 de la Constitution. Peut-être débattrons-nous en séance de l'opportunité de les exclure de la disposition ?

M. Patrick Chaize, rapporteur. – Nous aurons ce débat. Nous touchons là à la limite de l'exercice : nous savions qu'il y aurait des effets de bord.

Mme Catherine Morin-Desailly, présidente. – La question de ces offres qui paraissent avantageuses, mais qui en réalité enferment les usagers, mériterait en effet un débat en séance. Il faut être efficace pour rétablir la concurrence et stimuler le marché.

M. Bernard Fialaire. – Je comprends les arguments du rapporteur sur la question de la durée. Les montants, cependant, sont connus. Il est donc tout à fait possible de fixer une limite afin d'éviter que seules les grandes plateformes américaines ne puissent intervenir.

M. Patrick Chaize, rapporteur. – Il y a tout de même une corrélation entre le montant et la durée. La première année, les grandes plateformes proposent des avoirs limités, de l'ordre de 25 000 euros pour un an, car elles veulent s'assurer de la pérennité des acteurs. Au-delà d'une année, les montants sont plus importants et peuvent aller jusqu'à 150 000 euros.

Plutôt que le montant, nous avons choisi d'actionner le levier de la durée, qui avait été souvent cité lors des auditions et qui nous paraît plus efficace.

Mme Catherine Morin-Desailly, présidente. – La notion de montant soulève la question du *dumping*. Elle mérite d'être débattue en séance.

M. Patrick Chaize, rapporteur. – Le débat est ouvert.

L'amendement COM-113 est adopté. En conséquence, les amendements COM-89 rectifié, COM-47 et COM-62 rectifié deviennent sans objet.

M. Patrick Chaize, rapporteur. – L'amendement COM-114 réécrit l'ensemble des dispositions applicables aux frais liés aux transferts de données, afin d'en clarifier l'articulation, y compris avec le *Data Act*, qui est toujours en discussion à l'échelle européenne.

Sur cette question, il faut raisonner en deux temps.

Premièrement, dès l'entrée en vigueur de ce projet de loi, les frais liés aux transferts de données d'un client vers ses propres infrastructures, ainsi que les frais liés aux transferts de données vers les infrastructures d'un autre fournisseur dans le cadre d'une architecture *multi-cloud*, seront supprimés. En effet, ces frais ne sont pas justifiés : ils sont considérés comme abusifs, de nombreuses études et prises de position d'autorités nationales de la concurrence en Europe ayant mis en évidence les effets anticoncurrentiels de leur facturation. Ces frais sont d'ailleurs souvent facturés pour compenser l'octroi gratuit de crédits *cloud*. Autrement dit, l'entrée sur le marché est gratuite, mais la sortie est payante. Ce péage est injustifié pour nos jeunes entreprises.

Deuxièmement, trois ans après l'application du *Data Act*, soit à une date estimée au 16 février 2027, les frais liés à un changement complet de fournisseur seront supprimés. Pendant cette période de transition, il est prévu que les frais qui peuvent être facturés ne peuvent l'être qu'aux coûts réels, sous le contrôle de l'Arcep. C'est indispensable pour éviter les abus et pour sécuriser les entreprises pendant cette période de transition. Il ne faudrait pas que la suppression de la première catégorie de frais soit compensée par une hausse injustifiée des frais autorisés provisoirement.

De ce point de vue, il me semble que l'amendement COM-81 rectifié est satisfait sur le fond. J'en demande donc le retrait et à défaut, l'avis sera défavorable. Je suis également défavorable à l'amendement COM-48 : les clarifications apportées ne justifient pas une intervention du pouvoir réglementaire, laquelle n'est d'ailleurs pas prévue par le projet de loi.

L'amendement COM-114 est adopté. En conséquence, les amendements COM-81 rectifié et COM-48 deviennent sans objet.

M. Patrick Chaize, rapporteur. – Les amendements identiques COM-50 et COM-87 rectifié ont un objectif louable – lutter contre les pratiques anticoncurrentielles des acteurs dominants du marché de l'informatique en nuage –, mais ils reviennent à garantir l'interopérabilité de l'ensemble des services d'informatique en nuage, que ce soit au niveau des infrastructures, des plateformes ou des logiciels.

Les articles 8 et 9 du projet de loi prévoient justement cette interopérabilité, mais selon les modalités définies par l'Arcep, qui est chargée d'édicter des spécifications techniques en fonction de la nature du service. De très nombreux acteurs nous ont signalé que l'interopérabilité ne pouvait pas s'appréhender de la même façon selon le service concerné, notamment pour les logiciels : cela pourrait porter atteinte aux spécificités des produits qu'ils développent et donc à la propriété intellectuelle qui protège ces logiciels. Avis défavorable.

Les amendements identiques COM-50 et COM-87 rectifié ne sont pas adoptés.

M. Patrick Chaize, rapporteur. – Les amendements identiques COM-51 rectifié et COM-88 rectifié tendent à interdire la vente liée sur le marché de l'informatique en nuage, sous réserve que cela constitue une pratique commerciale déloyale. Avis favorable.

Les amendements identiques COM-51 rectifié et COM-88 rectifié sont adoptés.

M. Patrick Chaize, rapporteur. – Les amendements COM-49 et COM-83 rectifié visent à modifier le régime de sanction applicable en cas de violation des dispositions relatives à l'encadrement des avoirs d'informatique en nuage et des frais de transfert. Le régime de sanction prévu par le projet de loi me paraît adapté et proportionné, notamment car il

s'aligne sur le régime de sanction applicable aux violations des relations contractuelles entre les entreprises, tel que prévu par le code de commerce. Modifier ce régime serait disproportionné, notamment si les amendements sont fixés en pourcentage du chiffre d'affaires des entreprises. Avis défavorable.

L'amendement COM-49 n'est pas adopté, non plus que l'amendement COM-83 rectifié.

L'article 7 est adopté dans la rédaction issue des travaux de la commission.

Article 8

M. Patrick Chaize, rapporteur. – L'amendement COM-115 tend à modifier la définition de l'équivalence fonctionnelle.

L'amendement COM-115 est adopté.

L'article 8 est adopté dans la rédaction issue des travaux de la commission.

Article 9

M. Patrick Chaize, rapporteur. – L'amendement COM-116 a pour objet de rendre le processus d'élaboration des obligations d'interopérabilité et de portabilité des services d'informatique en nuage plus opérationnel, premièrement en demandant à l'Arcep de tenir compte des différences existantes entre les infrastructures, les plateformes et les logiciels de services d'informatique en nuage – c'est une absence majeure de ce projet de loi ; deuxièmement, en précisant que ces différences doivent être prises en compte lors de l'édiction des spécifications techniques plutôt que dans la définition des exigences d'interopérabilité et de portabilité, afin de laisser davantage de souplesse à l'Arcep et aux opérateurs économiques concernés ; enfin, troisièmement, en prévoyant un délai d'édiction de ces spécifications techniques et, par conséquent, un délai de mise en conformité des opérateurs économiques concernés. Ce délai devra être fixé par voie réglementaire, après consultation de l'Arcep, qui mènera des consultations auprès des opérateurs concernés.

Je suis défavorable à l'amendement COM-90 rectifié, qui fixe un délai de six mois, alors que nous ne connaissons pas les besoins des opérateurs concernés.

L'amendement COM-116 est adopté. L'amendement COM-90 rectifié est rejeté.

L'article 9 est adopté dans la rédaction issue des travaux de la commission.

Article 10

L'amendement de précision rédactionnelle et de coordination juridique COM-117 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-118 tend à introduire une procédure de saisine de l'Autorité de la concurrence par l'Arcep en cas de problème concurrentiel majeur sur le marché de l'informatique en nuage.

L'amendement COM-118 est adopté.

L'article 10 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 10

L'amendement COM-56 est déclaré irrecevable en application de l'article 45 de la Constitution.

M. Patrick Chaize, rapporteur. – Les amendements identiques COM-52 et COM-157 rectifié obligeraient les fournisseurs de services d'informatique en nuage et leurs intermédiaires à faire preuve de davantage de transparence sur leur site internet quant à l'utilisation des données de leurs utilisateurs. Avis favorable.

Les amendements identiques COM-52 et COM-157 rectifié sont adoptés et deviennent article additionnel.

Article 11

L'article 11 est adopté sans modification.

Article 12

M. Patrick Chaize, rapporteur. – L'amendement COM-84 rectifié tend à fixer à cinq ans la période pendant laquelle une majoration des sanctions contre les services d'intermédiation de données (SID) est possible en cas de réitération d'un même manquement. Ce délai de cinq ans se justifie pour des prestataires non encore professionnalisés, pour ne pas pénaliser un secteur encore balbutiant, mais n'aurait pas lieu d'être pour des SID ayant déjà un chiffre d'affaires. Avis défavorable.

L'amendement COM-84 rectifié n'est pas adopté.

L'article 12 est adopté sans modification.

Article 13

M. Patrick Chaize, rapporteur. – L'amendement COM-119 tend à clarifier l'articulation des compétences de l'Arcep et de la Cnil en matière de régulation des SID.

L'amendement COM-119 est adopté.

L'amendement de précision rédactionnelle COM-120 est adopté.

L'article 13 est adopté dans la rédaction issue des travaux de la commission.

Article 14

L'amendement de précision juridique COM-121 est adopté.

L'article 14 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 14

L'amendement COM-19 est déclaré irrecevable en application de l'article 45 de la Constitution.

Les amendements identiques COM-20 et COM-163 rectifié sont déclarés irrecevables en application de l'article 45 de la Constitution, de même que l'amendement COM-74 rectifié.

Article 15

M. Patrick Chaize, rapporteur. – Les amendements identiques COM-30 et COM-46 tendent à supprimer l'article 15. Notre commission a été tentée de faire ce choix, mais elle a préféré proposer une définition des Jonum qui lui paraissait plus pertinente. Avis défavorable.

Les amendements identiques COM-30 et COM-46 ne sont pas adoptés.

M. Patrick Chaize, rapporteur. – Alors que le sujet des Jonum mérite un véritable débat parlementaire, l'article 15, qui prévoit une habilitation à légiférer par ordonnance, est une coquille vide. Cette méthode n'est pas acceptable.

L'amendement COM-122 supprime cette habilitation et réécrit intégralement l'article. Il propose une première définition de ces jeux, qui sont à la croisée des jeux d'argent et des jeux vidéo, ainsi qu'un cadre expérimental d'autorisation. Aux termes de l'amendement, les jeux à objets numériques monétisables seraient définis comme des éléments de jeu qui confèrent aux seuls joueurs un ou plusieurs droits associés au jeu, et qui sont susceptibles d'être cédés, directement ou indirectement, à titre onéreux à des tiers. Par nature, les Jonum ne peuvent pas être des cryptomonnaies. Mon amendement interdit la cession des Jonum aux entreprises de jeux : c'est indispensable pour éviter tout contournement des interdictions des jeux de casino en ligne sous forme de Jonum.

Les entreprises de jeux qui émettent des Jonum devront s'assurer de la fiabilité et la transparence des opérations de jeu, protéger les mineurs et les joueurs contre les risques de jeu excessif et pathologique, et assurer la prévention des fraudes, du blanchiment d'argent et du financement du terrorisme. Une liste des Jonum autorisés à titre expérimental sera fixée par

décret, après un avis de l'ANJ, qui s'assurera de l'absence de tout contournement de l'interdiction des jeux de casinos en ligne.

Cet amendement important a fait l'objet de nombreuses concertations et d'un travail rédactionnel approfondi. Nous posons ici une première pierre indispensable à l'édification éventuelle d'une nouvelle et tierce législation spécifique aux Jonum. D'un côté, nous accompagnons et soutenons l'innovation et la numérisation de notre économie ; de l'autre, nous limitons les risques inhérents à l'économie numérique.

L'amendement COM-122 est adopté.

L'article 15 est ainsi rédigé.

Article 16

L'amendement de précision rédactionnelle COM-123 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-68 rectifié porte sur l'élaboration conjointe des objectifs et moyens des recherches publiques menées par le PEReN avec le coordinateur pour les services numériques. Avis défavorable.

L'amendement COM-68 rectifié n'est pas adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-124 vise à sécuriser l'accès du PEReN aux données des grandes plateformes et des grands moteurs de recherche, et prévoit l'extension de la durée de leur conservation.

L'amendement COM-124 est adopté.

L'amendement de précision légistique et rédactionnelle COM-125 est adopté.

L'article 16 est adopté dans la rédaction issue des travaux de la commission.

Article 17

M. Patrick Chaize, rapporteur. – L'amendement COM-126 tend à renforcer le caractère opérationnel du dispositif de centralisation des données relatives aux meublés de tourisme pour les communes.

L'amendement COM-126 est adopté.

L'article 17 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 17

L'amendement COM-162 rectifié est déclaré irrecevable en application de l'article 45 de la Constitution.

Article 18

L'article 18 est adopté sans modification.

Article 19

L'amendement rédactionnel COM-127 est adopté.

L'amendement de coordination légistique COM-128 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-53 rectifié vise à offrir la possibilité à l'autorité de contrôle d'adresser des recommandations et rend obligatoire la présentation d'un rapport public annuel. Avis favorable.

L'amendement COM-53 rectifié est adopté.

L'article 19 est adopté dans la rédaction issue des travaux de la commission.

Article 20

M. Loïc Hervé, rapporteur. – L'amendement COM-129 tend à ajouter le ministère public au sein de l'intitulé du nouveau chapitre du code de l'organisation judiciaire relatif au contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions judiciaires dans l'exercice de leur fonction juridictionnelle.

L'amendement COM-129 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-82 rectifié tend à corriger une coquille orthographique. Je remercie notre collègue Vanina Paoli-Gagin pour sa vigilance. Avis favorable.

L'amendement COM-82 rectifié est adopté.

M. Loïc Hervé, rapporteur. – Par l'amendement COM-130, il est proposé que le conseiller de la Cour de cassation composant l'autorité de contrôle ne soit plus désigné par le premier Président, mais soit élu.

L'amendement COM-130 est adopté.

L'amendement de coordination légistique et de clarification rédactionnelle COM-131 est adopté.

M. Loïc Hervé, rapporteur. – Pour les mêmes raisons que pour l'amendement COM-53 rectifié adopté à l'article 19, j'émets un avis favorable sur l'amendement COM-54 rectifié.

L'amendement COM-54 rectifié est adopté.

L'article 20 est adopté dans la rédaction issue des travaux de la commission.

Article 21

L'amendement de coordination légistique et de clarification rédactionnelle COM-132 est adopté.

M. Loïc Hervé, rapporteur. – Pour les mêmes raisons que pour l'amendement COM-53 rectifié adopté à l'article 19, avis favorable sur l'amendement COM-55 rectifié.

L'amendement COM-55 rectifié est adopté.

L'article 21 est adopté dans la rédaction issue des travaux de la commission.

Article 22

M. Patrick Chaize, rapporteur. – Les amendements COM-133 et COM-80 rectifié apportent des précisions juridiques et rédactionnelles. En cas d'adoption de l'amendement COM-133, la correction rédactionnelle proposée par l'amendement COM-80 rectifié serait satisfaite. Demande de retrait, sinon avis défavorable.

L'amendement COM-133 est adopté. En conséquence, l'amendement COM-80 rectifié devient sans objet.

L'amendement COM-161 rectifié est déclaré irrecevable en application de l'article 45 de la Constitution.

M. Patrick Chaize, rapporteur. – Les amendements COM-45 rectifié *bis* et COM-134 visent une coordination juridique. Avis défavorable à l'amendement COM-45 rectifié *bis* et favorable à l'amendement COM-134 de Loïc Hervé.

L'amendement COM-45 rectifié bis *devient sans objet. L'amendement COM-134 est adopté.*

L'article 22 est adopté dans la rédaction issue des travaux de la commission.

Article 23

M. Loïc Hervé, rapporteur. – L'amendement COM-135 procède à des clarifications rédactionnelles et propose de conserver le caractère facultatif de la dispense de conclusions du rapporteur public.

L'amendement COM-135 est adopté.

L'article 23 est adopté dans la rédaction issue des travaux de la commission.

Article 24

L'article 24 est adopté sans modification.

Après l'article 24

L'amendement COM-15 est déclaré irrecevable en application de l'article 45 de la Constitution.

Article 25

M. Patrick Chaize, rapporteur. – Les amendements COM-34, COM-77 rectifié, COM-75 rectifié et COM-76 rectifié visent à préciser que les autorités administratives chargées de la mise en œuvre du RSN sont tenues de veiller à l'application cohérente de ce règlement et de motiver leurs décisions si elles ne suivent pas les avis de la Commission européenne ou du Comité européen sur les services numériques. Ces quatre amendements ne correspondent pas au projet de règlement. Demande de retrait, sinon avis défavorable.

Les amendements COM-34, COM-77 rectifié, COM-75 rectifié et COM-76 rectifié ne sont pas adoptés.

M. Patrick Chaize, rapporteur. – L'amendement COM-136 porte sur l'articulation entre le coordinateur pour les services numériques et les autres autorités administratives.

L'amendement COM-136 est adopté.

L'amendement de précision juridique et rédactionnelle COM-137 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-138 vise à harmoniser la procédure de saisine et d'enquêtes domiciliaires de l'Arcom avec celle de la Cnil.

L'amendement COM-138 est adopté.

L'article 25 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 25

M. Loïc Hervé, rapporteur. – L'amendement COM-57 rectifié *ter* vise à clarifier la loi Informatique et libertés en matière d'anonymisation à bref délai des données à caractère personnel. Il me semble contraire à la directive ePrivacy, dont l'article 82 de la loi Informatique et libertés est la transposition. Je doute que l'anonymisation à bref délai facilite la communication par voie électronique et puisse à ce titre permettre une exception au recueil du consentement. C'est non pas une finalité en soi, mais une technique permettant de supprimer le lien entre les données et les personnes concernées. La Cnil accepte déjà que ne soient pas soumises à consentement les opérations de lecture et d'écriture qui ont pour unique finalité de mesurer l'audience d'un site internet ou d'une application par des statistiques anonymes.

En outre, sur la forme, il y aurait lieu d'inscrire la disposition à l'article 82 de cette loi. Avis défavorable.

L'amendement COM-57 rectifié ter n'est pas adopté.

Article 26

L'amendement de précision juridique COM-139 est adopté.

M. Patrick Chaize, rapporteur. – L'amendement COM-65 porte sur l'application des obligations des fournisseurs de places de marché en ligne aux seuls fournisseurs de plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels. Avis défavorable.

L'amendement COM-65 n'est pas adopté.

Les amendements identiques COM-35 et COM-72 rectifié ne sont pas adoptés.

L'amendement de précision juridique COM-140 est adopté.

L'article 26 est adopté dans la rédaction issue des travaux de la commission.

Article 27

L'article 27 est adopté sans modification.

Article 28

M. Loïc Hervé, rapporteur. – L'amendement COM-141 étend aux plateformes de partage de vidéo les recommandations que l'Arcom peut adresser aux services de plateforme et aux moteurs de recherche.

L'amendement COM-141 est adopté.

L'amendement de clarification rédactionnelle COM-142 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-143 tend à consacrer la compétence de l'Arcom dans la régulation des plateformes de partage de vidéo.

L'amendement COM-143 est adopté.

L'article 28 est adopté dans la rédaction issue des travaux de la commission.

Article 29

L'amendement de suppression COM-160 rectifié *n'est pas adopté.*

M. Loïc Hervé, rapporteur. – L'amendement COM-144 vise à rétablir l'obligation pour les plateformes en ligne de mettre en place un dispositif de signalement des fausses informations.

L'amendement COM-144 est adopté.

L'article 29 est ainsi rédigé.

Article 30

L'article 30 est adopté sans modification.

Article 31

M. Loïc Hervé, rapporteur. – L'amendement COM-145 rectifié tend à réécrire l'article 31. Il s'agit de reformuler et d'étendre les pouvoirs confiés à la Cnil par le règlement DGA.

L'amendement COM-145 rectifié est adopté.

L'article 31 est ainsi rédigé.

Article 32

L'amendement rédactionnel COM-146 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-147 rectifié tend à encadrer et à étendre le nouveau pouvoir de saisie de la Cnil.

L'amendement COM-147 rectifié est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-148 vise à étendre la possibilité donnée à la Cnil d'interroger les personnels des entités contrôlées.

L'amendement COM-148 est adopté.

L'amendement de clarification rédactionnelle COM-149 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-150 tend à supprimer une notion imprécise.

L'amendement COM-150 est adopté.

L'amendement de précision COM-151 est adopté.

L'amendement de coordination COM-152 est adopté.

L'amendement de précision COM-153 est adopté.

M. Loïc Hervé, rapporteur. – L'amendement COM-154 rectifié vise à encadrer les modalités de prononcé de la nouvelle injonction à caractère provisoire par la Cnil.

L'amendement COM-154 rectifié est adopté.

L'article 32 est adopté dans la rédaction issue des travaux de la commission.

Article 33

L'article 33 est adopté sans modification.

Article 34

M. Loïc Hervé, rapporteur. – L'amendement COM-79 vise à tirer les conséquences de dispositions européennes concernant le droit d'auteur et les droits voisins dans le marché unique européen. Il réaffirme la nécessité d'une juste rémunération des créateurs, notamment de la part des plateformes. Avis favorable.

L'amendement COM-79 est adopté.

L'article 34 est adopté dans la rédaction issue des travaux de la commission.

Après l'article 34

Les amendements COM-13 et COM-14 sont déclarés irrecevables en application de l'article 45 de la Constitution.

Article 35

M. Loïc Hervé, rapporteur. – L'amendement COM-155 tend à réduire de douze à six mois le délai de l'habilitation à légiférer par ordonnance.

L'amendement COM-155 est adopté.

L'article 35 est adopté dans la rédaction issue des travaux de la commission.

Article 36

L'amendement de précision juridique COM-156 est adopté.

M. Patrick Chaize, rapporteur. – Le sous-amendement COM-164 est de coordination juridique. L'amendement COM-69 rectifié tend à aligner la date d'entrée en vigueur du régime de responsabilité des services d'hébergement avec la date d'application du règlement européen sur les services numériques. Avis favorable sous réserve de l'adoption du sous-amendement COM-164.

Le sous-amendement COM-164 est adopté. L'amendement COM-69 rectifié, ainsi sous-amendé, est adopté.

L'article 36 est adopté dans la rédaction issue des travaux de la commission.

Le projet de loi est adopté dans la rédaction issue des travaux de la commission.

Le sort des amendements examinés par la commission spéciale est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Article 1er			
M. DOSSUS	26	Renvoi aux mécanismes d'évaluation et d'atténuation des risques relatifs aux mineurs prévus par le RSN pour remplacer le référentiel	**Rejeté**
M. Loïc HERVÉ, rapporteur	91	Obligation de vérifier l'âge des utilisateurs par les éditeurs de sites pornographiques et réorganisation de l'article 1er avec l'article 2	**Adopté**
Mme ROSSIGNOL	36	Suppression du référentiel d'exigences techniques établi par l'ARCOM	**Satisfait ou sans objet**
Mme ROSSIGNOL	37	Délai de publication du référentiel	**Adopté**
M. FIALAIRE	64 rect.	Avis conforme de la CNIL	**Rejeté**
M. DOSSUS	21	Prise en compte de l'empreinte environnementale du numérique par le référentiel élaboré par l'ARCOM	**Rejeté**
M. DOSSUS	23	Ajout de la garantie de la protection des données personnelles des utilisateurs	**Retiré**
M. DOSSUS	22	Exclusion de l'utilisation de technologies de reconnaissance biométriques	**Rejeté**
M. DOSSUS	24	Ajout du respect de l'anonymat	**Rejeté**
M. DOSSUS	25	Accessibilité des systèmes de vérification de l'âge sous un format ouvert et librement réutilisable	**Rejeté**
Article 2			
M. Loïc HERVÉ, rapporteur	92	Coordination des procédures initialement prévues dans les articles 1er et 2 et intégration dans la LCEN	**Adopté**
M. DOSSUS	31	Instauration d'une consultation obligatoire de la CNIL avant toute procédure de mise en demeure ou de blocage	**Retiré**
M. DOSSUS	32	Maintien de l'intervention du juge judiciaire pour contraindre l'éditeur	**Satisfait ou sans objet**
Mme NOËL	1	Restriction du champ des demandes de blocages aux seuls fournisseurs de système de résolution de nom de domaine	**Rejeté**
Mme NOËL	2	Renvoi à l'ARCOM pour fixer le délai d'exécution du blocage ou du déréférencement	**Rejeté**
M. FIALAIRE	61 rect.	Amendement rédactionnel	**Adopté**
M. FIALAIRE	67 rect.	Suppression des planchers de sanction pécuniaire exprimés en euros.	**Rejeté**

Auteur	N°	Objet	Sort de l'amendement
Article(s) additionnel(s) après Article 2			
M. BAZIN	43 rect. *bis*	Retrait des contenus zoophiles par l'ARCOM	**Rejeté**
M. FIALAIRE	63 rect.	Augmentation du nombre de séances d'information et d'éducation à la sexualité	**Irrecevable art. 45, al. 1 C (cavalier)**
Article(s) additionnel(s) avant Article 3			
Mme ROSSIGNOL	38	Élargissement des compétences de PHAROS en matière de demandes administratives de retrait	**Rejeté**
Mme ROSSIGNOL	42	Suppression du traitement différencié selon l'âge de la victime en matière de pédopornographie.	**Rejeté**
Mme ROSSIGNOL	39	Pénalisation, au titre de la pédopornographie, de la diffusion d'images revêtant l'intention de représenter des mineurs.	**Rejeté**
Mme ROSSIGNOL	41	Application des dispositions relatives à la pédopornographie à la diffusion d'images d'une personne dont l'aspect est celui d'un mineur.	**Rejeté**
Mme ROSSIGNOL	40	Pénalisation, au titre de la répression de la pédopornographie, des images représentant des relations incestueuses.	**Rejeté**
Article 3			
M. Loïc HERVÉ, rapporteur	93	Précision rédactionnelle	**Adopté**
M. Loïc HERVÉ, rapporteur	94	Maintien des conclusions du rapporteur public	**Adopté**
Article(s) additionnel(s) après Article 3			
Mme Mélanie VOGEL	158	Aggravation de la peine encourue pour un viol lorsque ce dernier est diffusé en temps réel.	**Rejeté**
Mme Mélanie VOGEL	159	Rapport au Parlement sur les viols commandités et diffusés en ligne.	**Rejeté**
Article 4			
M. Loïc HERVÉ, rapporteur	95 rect.	Compétence de l'Arcom sur les services de télévision et les SMAD extra-communautaires diffusés en France	**Adopté**
Mme NOËL	3	Définition des acteurs pouvant contribuer à la lutte contre les sites pornographiques	**Rejeté**
Mme NOËL	4	Délai de deux jours ouvrés minimum pour bloquer les sites	**Rejeté**

Auteur	N°	Objet	Sort de l'amendement
M. Loïc HERVÉ, rapporteur	96	Compétence de l'Arcom pour fixer le délai pour bloquer les sites	**Adopté**
M. Loïc HERVÉ, rapporteur	97	Décret en Conseil d'État pour définir les modalités d'application de l'article	**Adopté**
Article 5			
M. Loïc HERVÉ, rapporteur	98	Prise en compte de l'ensemble des comptes d'accès aux services de plateforme et de types complémentaires de services par la nouvelle peine complémentaire de « bannissement » ; meilleur encadrement des données collectées par les plateformes.	**Adopté**
M. FIALAIRE	60 rect.	Extension du « bannissement » à tous les comptes d'accès détenus par la personne condamnée.	**Satisfait ou sans objet**
Mme PAOLI-GAGIN	86 rect. *bis*	Amende envers les fournisseurs de plateforme en cas d'absence de mesures permettant de bloquer les comptes « tiers » d'une personne condamnée.	**Satisfait ou sans objet**
M. Loïc HERVÉ, rapporteur	99 rect.	Extension de la liste des infractions pour lesquels la peine complémentaire de "bannissement" sera encourue.	**Adopté**
Mme PAOLI-GAGIN	85 rect. *bis*	Correction d'une erreur matérielle	**Satisfait ou sans objet**
M. BAZIN	44 rect. *bis*	Possibilité de prononcer la peine complémentaire de « bannissement » en cas de condamnation pour zoo-pornographie.	**Satisfait ou sans objet**
M. Loïc HERVÉ, rapporteur	100	Extension du « bannissement » aux alternatives aux poursuites et à l'application des peines.	**Adopté**
Article(s) additionnel(s) après Article 5			
M. VERZELEN	17	Rapport au Parlement sur les flux découlant des sites illégaux proposant une offre de casino en ligne.	**Irrecevable art. 45, al. 1 C (cavalier)**
M. VERZELEN	18	Légalisation et régulation des jeux de casino en ligne.	**Irrecevable art. 45, al. 1 C (cavalier)**
M. DOSSUS	27	Possibilité de prononcer le blocage du compte d'accès à une plateforme en ligne en cas de contrôle judiciaire	**Retiré**
M. DOSSUS	28	Pénalisation des outrages sexistes ou sexuels commis en ligne	**Retiré**
M. DOSSUS	33	Prise en compte par la loi pour la confiance en l'économie numérique de l'infraction prévue à l'article 222-3-3 du code pénal	**Retiré**
Article 6			
M. CHAIZE, rapporteur	101	Facilitation de la constatation des infractions déclenchant le dispositif de filtre anti-arnaques.	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
M. FIALAIRE	59 rect.	Déclenchement du filtre anti-arnaques lorsqu'un internaute obtient des données à caractère personnel sur un site diffusant des données obtenues par piratage.	**Retiré**
M. CHAIZE, rapporteur	102	Mise en demeure des éditeurs de site internet frauduleux après constatation de l'infraction par l'autorité administrative.	**Adopté**
M. CHAIZE, rapporteur	103	Précision rédactionnelle.	**Adopté**
M. CHAIZE, rapporteur	104	Uniformisation de l'information présentée aux internautes sur le message d'avertissement qui s'affichera sur leurs écrans en cas de tentative d'accès à un site soupçonné d'être frauduleux.	**Adopté**
M. CHAIZE, rapporteur	105	Clarification de la nature des mesures que l'autorité administrative peut enjoindre aux intermédiaires techniques de prendre afin d'empêcher l'accès aux sites frauduleux.	**Adopté**
Mme NOËL	5	Suppression de l'implication des fournisseurs d'accès à internet dans le déploiement du filtre anti-arnaques.	**Rejeté**
Mme NOËL	6	Redirection des internautes vers une page d'information de l'autorité administrative justifiant le blocage d'accès au site.	**Rejeté**
Mme NOËL	7	Introduction d'un délai d'au moins deux jours ouvrés pour bloquer l'accès aux sites internet frauduleux.	**Rejeté**
M. DOSSUS	29	Suppression de l'implication des fournisseurs d'accès à internet et des fournisseurs de systèmes de résolution des noms de domaine dans le déploiement du filtre anti-arnaques.	**Rejeté**
M. CHAIZE, rapporteur	106	Obligation de vérifier, à l'approche de l'expiration de la période de blocage, la liste des adresses électroniques des sites dont l'accès a été bloqué.	**Adopté**
M. CHAIZE, rapporteur	107	Précision rédactionnelle.	**Adopté**
Mme NOËL	8	Intégration des moteurs de recherche en ligne et des annuaires dans le déploiement du dispositif anti-arnaques.	**Adopté**
M. CHAIZE, rapporteur	108	Renforcement de l'information de la personnalité qualifiée de la Cnil chargée de veiller à l'application proportionnée du filtre anti-arnaques.	**Adopté**
M. CHAIZE, rapporteur	109	Clarification des exigences du rapport d'activité annuel de la personnalité qualifiée de la Cnil chargée du suivi du déploiement du filtre anti-arnaques.	**Adopté**
M. CHAIZE, rapporteur	110	Application des sanctions à l'ensemble des intermédiaires techniques chargés du déploiement du filtre anti-arnaques.	**Adopté**
Mme NOËL	9	Compensation des surcoûts des opérateurs.	**Rejeté**

Auteur	N°	Objet	Sort de l'amendement
Article(s) additionnel(s) après Article 6			
M. HAYE	12	Demande de rapport à l'Agence nationale de cohésion des territoires sur l'exclusion numérique en France.	**Irrecevable art. 45, al. 1 C (cavalier)**
M. FIALAIRE	58 rect.	Sanction prenant la forme d'une amende en cas de consultation de données informatiques obtenues par fraude	**Rejeté**
M. FIALAIRE	66 rect.	Injonction dynamique au bénéfice des ayants droit en matière de droits d'auteur et de droits voisins	**Irrecevable art. 45, al. 1 C (cavalier)**
Mme Nathalie DELATTRE	70 rect.	Création d'un régime des « hackers éthiques ».	**Irrecevable art. 45, al. 1 C (cavalier)**
Mme Nathalie DELATTRE	71 rect.	Création d'un régime pour les « hackers éthiques ».	**Irrecevable art. 45, al. 1 C (cavalier)**
Mme Nathalie DELATTRE	73 rect.	Création d'un régime des « hackers éthiques ».	**Irrecevable art. 45, al. 1 C (cavalier)**
Mme Nathalie DELATTRE	78 rect.	Création d'un régime des « hackers éthiques ».	**Irrecevable art. 45, al. 1 C (cavalier)**
Article 7			
M. CHAIZE, rapporteur	111	Modification de la définition d'un service d'informatique en nuage.	**Adopté**
M. CHAIZE, rapporteur	112	Modification de la définition d'un avoir d'informatique en nuage.	**Adopté**
M. CHAIZE, rapporteur	113	Encadrement de l'octroi d'avoirs d'informatique en nuage afin de limiter les phénomènes de verrouillage ou de dépendance.	**Adopté**
Mme PAOLI-GAGIN	89 rect. *bis*	Fixation d'un plafond monétaire pour l'octroi d'avoirs d'informatique en nuage.	**Satisfait ou sans objet**
Mme BLATRIX CONTAT	47	Fixation d'un plafond temporel pour l'octroi d'avoirs d'informatique en nuage.	**Satisfait ou sans objet**
M. FIALAIRE	62 rect.	Fixation d'un double plafond monétaire et temporel pour l'octroi d'avoirs d'informatique en nuage.	**Satisfait ou sans objet**
M. CHAIZE, rapporteur	114	Rédaction globale sur l'encadrement des frais liés aux transferts de données.	**Adopté**
Mme PAOLI-GAGIN	81 rect. *bis*	Facturation des frais de migration aux coûts réels sous le contrôle de l'Arcep.	**Satisfait ou sans objet**

Auteur	N°	Objet	Sort de l'amendement
Mme BLATRIX CONTAT	48	Encadrement des frais de migration par voie réglementaire.	**Satisfait ou sans objet**
Mme BLATRIX CONTAT	50	Interdiction de conditionner l'accès à un environnement numérique à des conditions tarifaires ou fonctionnelles dégradées.	**Rejeté**
Mme PAOLI-GAGIN	87 rect. *bis*	Interdiction de conditionner l'accès à un environnement numérique à des conditions tarifaires ou fonctionnelles dégradées.	**Rejeté**
Mme BLATRIX CONTAT	51 rect.	Interdiction de la vente liée sur le marché de l'informatique en nuage sous réserve que cela constitue une pratique commerciale déloyale.	**Adopté**
Mme PAOLI-GAGIN	88 rect. *bis*	Interdiction de la vente liée sur le marché de l'informatique en nuage sous réserve que cela constitue une pratique commerciale déloyale.	**Adopté**
Mme BLATRIX CONTAT	49	Modification du régime de sanction applicable en cas de violation des dispositions relatives à l'encadrement des avoirs d'informatique en nuage et des frais de transfert.	**Rejeté**
Mme PAOLI-GAGIN	83 rect. *bis*	Modification du régime de sanction applicable en cas de violation des dispositions relatives à l'encadrement des avoirs d'informatique en nuage et des frais de transfert.	**Rejeté**
Article 8			
M. CHAIZE, rapporteur	115	Modification de la définition d'équivalence fonctionnelle.	**Adopté**
Article 9			
M. CHAIZE, rapporteur	116	Précisions des conditions relatives à l'édiction par l'Arcep des spécifications techniques d'interopérabilité et de portabilité.	**Adopté**
Mme PAOLI-GAGIN	90 rect. *bis*	Fixation d'un délai de 6 mois aux fournisseurs de services d'informatique en nuage pour se mettre en conformité des règles d'interopérabilité et de portabilité édictées par l'Arcep.	**Rejeté**
Article 10			
M. CHAIZE, rapporteur	117	Précisions rédactionnelle et de coordination juridique.	**Adopté**
M. CHAIZE, rapporteur	118	Introduction d'une procédure de saisine de l'Autorité de la concurrence par l'Arcep en cas de problème concurrentiel majeur sur le marché de l'informatique en nuage.	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article(s) additionnel(s) après Article 10			
Mme BLATRIX CONTAT	56	Encadrement de la publicité en ligne.	**Irrecevable au titre de l'art. 45 de la Constitution**
Mme BLATRIX CONTAT	52	Obligation pour les fournisseurs de services d'informatique en nuage et leurs intermédiaires de faire preuve de davantage de transparence sur leur site internet quant à l'utilisation des données de leurs utilisateurs.	**Adopté**
Mme PAOLI-GAGIN	157 rect. *bis*	Obligation pour les fournisseurs de services d'informatique en nuage et leurs intermédiaires de faire preuve de davantage de transparence sur leur site internet quant à l'utilisation des données de leurs utilisateurs.	**Adopté**
Article 12			
Mme PAOLI-GAGIN	84 rect. *bis*	Restriction à une période de cinq ans de la possibilité de majoration des sanctions contre les services d'intermédiation de données (SID) en cas de réitération d'un même manquement	**Rejeté**
Article 13			
M. CHAIZE, rapporteur	119	Clarification de l'articulation des compétences de l'Arcep et de la Cnil en matière de régulation des services d'intermédiation de données (SID)	**Adopté**
M. CHAIZE, rapporteur	120	Précision rédactionnelle.	**Adopté**
Article 14			
M. CHAIZE, rapporteur	121	Précision juridique.	**Adopté**
Article(s) additionnel(s) après Article 14			
M. VERZELEN	19	Légalisation et régulation des jeux de casino en ligne	**Irrecevable au titre de l'art. 45 de la Constitution**
M. VERZELEN	20	Instauration d'un mécanisme de financement associé à la régulation des jeux de casino en ligne.	**Irrecevable au titre de l'art. 45 de la Constitution)**
Mme Marie MERCIER	163 rect. *bis*	Instauration d'un mécanisme de financement associé à la régulation des jeux de casino en ligne.	**Irrecevable au titre de l'art. 45 de la Constitution**

Auteur	N°	Objet	Sort de l'amendement
Mme Marie MERCIER	74 rect. *bis*	Régulation des jeux d'argent et de hasard en ligne.	**Irrecevable au titre de l'art. 45 de la Constitution**
Article 15			
M. DOSSUS	30	Suppression de l'article 15.	**Rejeté**
M. DURAIN	46	Suppression de l'article 15.	**Rejeté**
M. CHAIZE, rapporteur	122	Définition d'un cadre expérimental d'autorisation des jeux à objets numériques monétisables.	**Adopté**
Article 16			
M. CHAIZE, rapporteur	123	Précision rédactionnelle.	**Adopté**
M. FIALAIRE	68 rect.	Élaboration conjointe des objectifs et moyens des recherches publiques menées par le PEReN avec le coordinateur pour les services numériques.	**Rejeté**
M. CHAIZE, rapporteur	124	Sécurisation de l'accès du PEReN aux données des grandes plateformes et des grands moteurs de recherche en ligne et extension de la durée de leur conservation.	**Adopté**
M. CHAIZE, rapporteur	125	Précisions légistiques et rédactionnelles.	**Adopté**
Article 17			
M. CHAIZE, rapporteur	126	Renforcement du caractère opérationnel du dispositif de centralisation des données relatives aux meublés de tourisme pour les communes.	**Adopté**
Article(s) additionnel(s) après Article 17			
Mme de MARCO	162 rect.	Interdiction de la publicité en ligne relative aux espaces naturels fragiles afin de lutter contre le surtourisme.	**Irrecevable au titre de l'art. 45 de la Constitution**
Article 19			
M. Loïc HERVÉ, rapporteur	127	Rédactionnel.	**Adopté**
M. Loïc HERVÉ, rapporteur	128	Amendement de coordination légistique et de clarification rédactionnelle, afin de préciser que l'autorité de contrôle disposera des pouvoirs dévolus aussi bien au Président de la CNIL qu'à sa formation restreinte.	**Adopté**
M. DURAIN	53 rect.	Possibilité, pour l'autorité de contrôle, d'adresser des recommandations et obligation de présenter un rapport public annuel.	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article 20			
M. Loïc HERVÉ, rapporteur	129	Ajout du ministère public au sein de l'intitulé du nouveau chapitre du code de l'organisation judiciaire relatif au contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions judiciaires dans l'exercice de leur fonction juridictionnelle	**Adopté**
Mme PAOLI-GAGIN	82 rect. *bis*	Correction d'une coquille orthographique.	**Adopté**
M. Loïc HERVÉ, rapporteur	130	Élection, au lieu d'une désignation par le premier Président, du conseiller de la Cour de cassation composant l'autorité de contrôle.	**Adopté**
M. Loïc HERVÉ, rapporteur	131	Amendement de coordination légistique et de clarification rédactionnelle, afin de préciser que l'autorité de contrôle disposera des pouvoirs dévolus aussi bien au Président de la CNIL qu'à sa formation restreinte.	**Adopté**
M. DURAIN	54 rect.	Possibilité, pour l'autorité de contrôle, d'adresser des recommandations et obligation de présenter un rapport public annuel.	**Adopté**
Article 21			
M. Loïc HERVÉ, rapporteur	132	Amendement de coordination légistique et de clarification rédactionnelle, afin de préciser que l'autorité de contrôle disposera des pouvoirs dévolus aussi bien au Président de la CNIL qu'à sa formation restreinte.	**Adopté**
M. DURAIN	55 rect.	Possibilité, pour l'autorité de contrôle, d'adresser des recommandations et obligation de présenter un rapport public annuel.	**Adopté**
Article 22			
M. CHAIZE, rapporteur	133	Précisions juridiques et rédactionnelles.	**Adopté**
Mme PAOLI-GAGIN	80 rect. *bis*	Correction rédactionnelle.	**Satisfait ou sans objet**
Mme de MARCO	161 rect.	Transmission des recommandations de sobriété numérique de l'Ademe.	**Irrecevable au titre de l'art. 45 de la Constitution**
M. BAZIN	45 rect. *bis*	Ajout des infractions liées à la zoopornographie.	**Satisfait ou sans objet**
M. Loïc HERVÉ, rapporteur	134	Coordination juridique.	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article 23			
M. Loïc HERVÉ, rapporteur	135	Amendement rédactionnel et maintien des conclusions du rapporteur public	**Adopté**
Article(s) additionnel(s) après Article 24			
M. KERN	15	Modification de la loi visant à encadrer l'influence commerciale.	**Irrecevable au titre de l'art. 45 de la Constitution**
Article 25			
M. VERZELEN	34	Reprise des dispositions du règlement européen sur les services numériques.	**Rejeté**
Mme Nathalie DELATTRE	77 rect.	Reprise des dispositions du règlement européen sur les services numériques.	**Rejeté**
Mme Nathalie DELATTRE	75 rect.	Reprise des dispositions du règlement européen sur les services numériques.	**Rejeté**
Mme Nathalie DELATTRE	76 rect.	Reprise des dispositions du règlement européen sur les services numériques.	**Rejeté**
M. CHAIZE, rapporteur	136	Articulation entre le coordinateur pour les services numériques et les autres autorités administratives.	**Adopté**
M. CHAIZE, rapporteur	137	Précisions juridiques et rédactionnelles.	**Adopté**
M. CHAIZE, rapporteur	138	Harmonisation de la procédure de saisine et d'enquêtes domiciliaires de l'Arcom avec celle de la Cnil.	**Adopté**
Article(s) additionnel(s) après Article 25			
M. VERZELEN	57 rect. *ter*	Clarification de la loi Informatique et libertés s'agissant de l'anonymisation à bref délai des données à caractère personnel	**Rejeté**
Article 26			
M. CHAIZE, rapporteur	139	Précision juridique.	**Adopté**
M. VERZELEN	65	Application des obligations des fournisseurs de places de marché en ligne aux seuls fournisseurs de plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels.	**Rejeté**
M. VERZELEN	35	Retrait de la mention de la possibilité de fixer une astreinte en proportion du chiffre d'affaires figurant dans les comptes consolidés ou combinés de l'entreprise consolidante ou combinante.	**Rejeté**

Auteur	N°	Objet	Sort de l'amendement
Mme Nathalie DELATTRE	72 rect.	Retrait de la mention de la possibilité de fixer une astreinte en proportion du chiffre d'affaires figurant dans les comptes consolidés ou combinés de l'entreprise consolidante ou combinante.	**Rejeté**
M. CHAIZE, rapporteur	140	Amendement de précision juridique.	**Adopté**
Article 28			
M. Loïc HERVÉ, rapporteur	141	Prise en compte des plateformes de partage de vidéo.	**Adopté**
M. Loïc HERVÉ, rapporteur	142	Clarification rédactionnelle.	**Adopté**
M. Loïc HERVÉ, rapporteur	143	Prise en compte des plateformes de partage de vidéo.	**Adopté**
Article 29			
Mme de MARCO	160 rect.	Suppression de l'article 29.	**Rejeté**
M. Loïc HERVÉ, rapporteur	144	Rétablissement de l'obligation, pour les plateformes en ligne, de mettre en place un dispositif de signalement des fausses informations.	**Adopté**
Article 31			
M. Loïc HERVÉ, rapporteur	145 rect.	Reformulation et extension des pouvoirs confiés à la Cnil par le règlement « DGA ».	**Adopté**
Article 32			
M. Loïc HERVÉ, rapporteur	146	Mise en cohérence rédactionnelle.	**Adopté**
M. Loïc HERVÉ, rapporteur	147 rect.	Encadrement et extension du nouveau pouvoir de saisie de la Cnil.	**Adopté**
M. Loïc HERVÉ, rapporteur	148	Extension de la possibilité donnée à la Cnil d'interroger les personnels des entités contrôlées.	**Adopté**
M. Loïc HERVÉ, rapporteur	149	Clarification rédactionnelle.	**Adopté**
M. Loïc HERVÉ, rapporteur	150	Suppression d'une notion imprécise.	**Adopté**
M. Loïc HERVÉ, rapporteur	151	Précision.	**Adopté**
M. Loïc HERVÉ, rapporteur	152	Coordination.	**Adopté**
M. Loïc HERVÉ, rapporteur	153	Précision.	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
M. Loïc HERVÉ, rapporteur	154 rect.	Encadrement des modalités de prononcé de la nouvelle injonction à caractère provisoire par la Cnil.	**Adopté**
Article 34			
M. BARGETON	79	Précision que la rémunération des auteurs cédant leurs droits exclusifs pour l'exploitation de leurs œuvres doit être « appropriée »	**Adopté**
Article(s) additionnel(s) après Article 34			
M. KERN	13	Attribution aux sociétés commerciales créées par les ligues professionnelles de la qualité à agir pour défendre leurs droits d'exploitation audiovisuelle	**Irrecevable au titre de l'art. 45 de la Constitution**
M. KERN	14	Création d'une infraction spécifique sanctionnant la diffusion et la commercialisation de programmes sportifs piratés	**Irrecevable au titre de l'art. 45 de la Constitution**
Article 35			
M. Loïc HERVÉ, rapporteur	155	Réduction du délai de l'habilitation à légiférer par ordonnance	**Adopté**
Article 36			
M. CHAIZE, rapporteur	156	Précision juridique.	**Adopté**
Mme Nathalie DELATTRE	69 rect.	Alignement de la date d'entrée en vigueur du régime de responsabilité des services d'hébergement avec la date d'application du règlement européen sur les services numériques.	**Adopté**
M. CHAIZE, rapporteur	164	Coordination juridique.	**Adopté**

.

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 44 *BIS* DU RÈGLEMENT DU SÉNAT (« CAVALIERS »)

Si le premier alinéa de l'article 45 de la Constitution, depuis la révision du 23 juillet 2008, dispose que « tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis », le Conseil constitutionnel estime que cette mention a eu pour effet de consolider, dans la Constitution, sa jurisprudence antérieure, reposant en particulier sur « la nécessité pour un amendement de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie » [100(*)].

De jurisprudence constante et en dépit de la mention du texte « transmis » dans la Constitution, le Conseil constitutionnel apprécie ainsi l'existence du lien par rapport au contenu précis des dispositions du texte initial, déposé sur le bureau de la première assemblée saisie[101(*)].

Pour les lois ordinaires, le seul critère d'analyse est le lien matériel entre le texte initial et l'amendement, la modification de l'intitulé au cours de la navette restant sans effet sur la présence de « cavaliers » dans le texte[102(*)]. Pour les lois organiques, le Conseil constitutionnel ajoute un second critère : il considère comme un « cavalier » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial[103(*)].

En application des articles 17 *bis* et 44 *bis* du Règlement du Sénat, il revient à la commission saisie au fond de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

En application du vademecum sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des Présidents, la commission spéciale **a arrêté**, lors de sa réunion du mardi 24 juin 2023, **le périmètre indicatif du projet de loi n° 593 (2022-2023) visant à sécuriser et réguler l'espace numérique**.

Elle a considéré que sont susceptibles de présenter un lien, même indirect, avec le texte déposé, les dispositions relatives :

- à l'actualisation du droit interne au règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), au règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés

numériques), au règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ainsi qu'à la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) ;

- aux mesures de contrôle et de blocage mis en œuvre pour prévenir l'accès des mineurs à des services de communication en ligne qui mettent à disposition du public des contenus pornographiques;

- à la pénalisation du défaut d'exécution par un hébergeur d'une demande de retrait de contenus pédopornographiques émanant de l'autorité administrative compétente ;

- au respect des interdictions de diffusion de contenus produits par des médias visés par des sanctions européennes ;

- à la prévention et à la répression du cyberharcèlement et des infractions pénales graves susceptibles d'être commises en ligne ;

- à la mise en place d'un dispositif national de filtrage des contenus constituant des actes de cybermalveillance ;

- à la régulation du marché dit de « l'informatique en nuage » et aux conditions économiques et techniques applicables aux opérateurs de ce marché ;

- à la régulation du marché des services d'intermédiation de données et aux conditions économiques et techniques applicables aux opérateurs de ce marché ;

- à la définition et à la régulation des jeux à objets numériques monétisables (Jonum) ;

- aux missions du pôle d'expertise pour la régulation de l'économie numérique (PEReN) ;

- à la mise à disposition des données permettant de contrôler le respect des obligations des loueurs de meublés de tourisme ;

- au contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle ;

- à la bonne articulation des autorités indépendantes, juridiques et administratives pour la mise en œuvre des règlements européens précités et pour la prise en compte dans le droit français des prérogatives qu'ils tirent de ces règlements;

- aux délais et aux modalités d'entrée en vigueur des dispositions de ce projet de loi.

Sans que l'énumération ci-dessous soit exhaustive, elle a considéré que ne sont pas susceptibles de présenter un lien, même indirect, avec le texte déposé, les dispositions relatives :

- à la lutte contre les violences pornographiques et l'éducation à la vie sexuelle et affective ;

- à la régulation du marché de la publicité en ligne ;

- à la lutte contre le piratage des programmes sportifs et des œuvres cinématographiques, musicales et audiovisuelles ;

- à la sécurité des systèmes d'information et au hacking éthique ;

- à la régulation de l'activité d'influence commerciale et d'agent d'influenceur ;

- à la réduction de l'empreinte environnementale du numérique et à la sobriété numérique ;

- aux considérations d'ordre général sur la régulation des jeux d'argent et de hasard ainsi qu'à la modification de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;

- à la couverture numérique des territoires ;

- aux mesures prises pour lutter contre l'exclusion numérique et favoriser l'inclusion numérique ;

- à la modification des obligations applicables aux loueurs de meublés de tourisme et à la lutte contre le sur-tourisme.

COMPTES RENDUS DES AUDITIONS PLÉNIÈRES

Réunion constitutive

Mardi 6 juin 2023

- Présidence de Mme Marie-Noëlle Lienemann, présidente d'âge -

Mme Marie-Noëlle Lienemann, présidente. – En ma qualité de présidente d'âge, il me revient d'ouvrir la première réunion de la commission spéciale sur la proposition de loi visant à sécuriser et réguler l'espace numérique dont la composition a été confirmée en séance publique le jeudi 1er juin dernier.

Conformément au Règlement du Sénat, nous allons tout d'abord désigner le président de la commission.

J'ai reçu la candidature de Catherine Morin-Desailly, qui a déjà travaillé avec la commission des affaires européennes sur les deux règlements qui sont au cœur du projet de loi – le règlement européen sur les services numériques (RSN) ou *Digital Services Act (DSA)* et le règlement européen sur les marchés numériques (RMN) ou *Digital Markets Act (DMA)* –, et qui arpente depuis de longues années le monde de l'Internet.

Mme Catherine Morin-Desailly est désignée présidente de la commission spéciale.

- Présidence de Mme Catherine Morin-Desailly, présidente -

Mme Catherine Morin-Desailly, présidente. – Je vous remercie pour votre confiance. Le temps qui nous est imparti est très limité, mais nous veillerons à travailler efficacement pour créer un cadre permettant de lutter contre les contenus illicites etles contrefaçons et réguler le marché numérique.

Je commencerai par présenter quelques éléments de contexte.

Pour le Sénat, ce projet de loi est une source de satisfaction, dix ans après l'affaire Snowden qui avait déclenché la création au sein de notre assemblée d'une mission commune d'information sur la gouvernance mondiale de l'Internet. L'Europe a pris du retard pour légiférer, même si nous nous félicitons de l'adoption, sous présidence française de l'Union européenne, du *DSA* et du *DMA*.

Les enjeux sont les suivants : rouvrir la directive dite « e-commerce » et mettre en place un régime de responsabilité et de redevabilité pour les plateformes. Ces dernières ont abusé de leur position dominante en verrouillant les marchés, et ont permis la prolifération de contenus illicites et contestables, préjudiciables aux utilisateurs. La pandémie, qui a accru la digitalisation de notre économie, a accéléré la prise de conscience de la nécessité d'agir.

Une nouvelle doctrine a vu le jour au niveau européen, au travers de différents textes. Trois règlements ont été adoptés en 2022 : le *DSA*, le *DMA* et le *Data Governance Act*, lequel sera complété par un texte encore en négociation, le *Data Act*.

Sur ces sujets, notre assemblée a été active, notamment grâce à la commission des affaires européennes et à son président.

Ainsi, sur le *DMA*, à la suite de notre rapport avec Florence Blatrix Contat, que je suis heureuse de retrouver dans notre commission spéciale, le Sénat a adopté une résolution européenne le 12 novembre 2021, assortie d'un avis politique au Conseil. En particulier, nous avons été suivies sur l'ajout des services essentiels et sur les interdictions, ainsi que sur la coopération entre la Commission européenne et les autorités nationales.

Sur le *DSA*, et toujours sur notre initiative, le Sénat a adopté une résolution européenne le 14 janvier 2022. Là encore, notre position a été portée au niveau européen : je pense en particulier à l'inclusion des très grands moteurs de recherche dans le périmètre des obligations définies par le règlement et à la prise en compte des critères d'audience.

Enfin, sur un sujet encore en discussion au niveau européen mais très présent dans le projet de loi, nous avons, avec Ludovic Haye et André Reichardt, que je me félicite également de retrouver dans notre commission, émis une nouvelle résolution européenne le 13 février dernier sur le projet de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants.

Notre préoccupation est d'ailleurs en parfait accord avec les travaux de la délégation aux droits de femmes, dont je salue l'engagement – en particulier au travers de son rapport sur l'industrie pornographique. Je me félicite de la présence de nombreux membres de cette délégation parmi nous, dont sa présidente Annick Billon, qui a été rapporteure sur ce sujet avec Alexandra Borchio Fontimp et Laurence Rossignol.

Je salue également Marie Mercier, qui est très impliquée sur ces sujets.

Nous pouvons nous féliciter des avancées que nous avons obtenues, mais nous n'avons pas eu satisfaction sur tout. Il faudra mesurer la marge de manœuvre dont nous disposons pour améliorer le texte, même si celle-ci

risque d'être étroite. En effet, il s'agit non pas de transposer une directive, mais des règlements. Or les règlements sont d'application directe afin d'éviter une « fragmentation » des législations et d'aller vite. Cette limite sera pour beaucoup une frustration, en nous imposant de ne pas « déborder » sur le champ des règlements, sous peine de les fragiliser et de voir certains en Europe s'y engouffrer pour en réduire la portée. Nos débats seront suivis dans l'Union européenne et serviront largement de modèle, car nous sommes les premiers à nous adapter à ces règlements.

Le projet de loi ne se limite néanmoins pas à adapter notre droit et notre régulation à ce cadre européen. Il procède également à plusieurs améliorations destinées à protéger les utilisateurs. Je pense notamment aux dispositions sur « l'informatique en nuage » – le sujet de l'hébergement et du traitement des données est au cœur de la souveraineté numérique –, sur la gestion des locations touristiques de courte durée ou encore sur les jeux à objets numériques monétisables, qui font l'objet d'une demande d'habilitation à légiférer par voie d'ordonnance.

Un énorme travail doit être fait, mais je sais que nous pourrons compter sur nos rapporteurs qui sont très aguerris sur ces sujets !

Sur la forme, si je me félicite bien entendu de voir ce texte arriver en premier au Sénat, je déplore cependant le temps très réduit dont nous disposons. Je regrette également la profusion de textes sur le numérique qui nous sont arrivés ces derniers temps sous forme de propositions de loi – en réalité d'origine gouvernementale –, ce qui nuit à la vision stratégique et globale que nous devons adopter.

Cette vision stratégique, je souhaite précisément que nous puissions tous ensemble la porter, et, au travers de ce texte, faire valoir les positions déjà exprimées par le Sénat afin de marquer notre cohérence.

En tout état de cause, ce projet de loi n'est qu'une étape, même si elle est essentielle. Ainsi, demain, il nous faudra nous pencher sur la question de l'intelligence artificielle, à propos de laquelle nous avons déjà eu un débat en séance. Il faut également mentionner la proposition de règlement européen sur les données *(Data Act)*, encore en cours de négociation, qui fixe des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données, et sur lequel, avec Florence Blatrix Contat et André Gattolin, nous venons de déposer une nouvelle proposition de résolution européenne le 11 mai dernier.

Les données sont en effet « l'or noir » du numérique, et nous devons nous organiser pour éviter leur confiscation par quelques grandes plateformes qui verrouillent techniquement, financièrement et juridiquement le marché. Le projet de loi transpose d'ailleurs par anticipation certaines dispositions de cette proposition de règlement aux articles pour l'informatique « en nuage », notamment sur l'interopérabilité et la portabilité

des données, de manière à permettre le développement d'une véritable industrie européenne.

J'espère que nous tirerons, en France comme en Europe, les conclusions de nos retards successifs en matière de numérique.

Par ailleurs, et toujours dans le cadre européen, la Commission a présenté en mars 2021 son programme d'actions pour la décennie numérique, dit boussole numérique, qui trace la voie vers une réelle souveraineté européenne. Patrick Chaize a d'ailleurs rapporté pour la commission des affaires économiques la proposition de résolution européenne que nous avions déposée avec Florence Blatrix Contat sur le sujet.

Enfin, en tant que présidente de notre commission spéciale, je serai très attentive à maintenir les règles constitutionnelles de respect des irrecevabilités, s'agissant notamment de l'article 45 de la Constitution. Il nous faudra rester vigilants et parfois réfréner nos ardeurs pour éviter la censure par le Conseil constitutionnel de dispositions qui n'auraient pas de lien avec le texte.

Mes chers collègues, je vous propose maintenant de procéder à la désignation du bureau de notre commission spéciale.

Nous procédons, dans un premier temps, à la désignation des vice-présidents et des secrétaires.

Conformément à l'article 13 de notre Règlement, selon le principe de la représentation proportionnelle et en tenant compte de la représentation déjà acquise au groupe Union Centriste (UC) pour le poste de président, nous devons désigner : quatre vice-présidents du groupe Les Républicains (LR) ; deux du groupe Socialiste, Écologiste et Républicain (SER) ; un du groupe Rassemblement des démocrates, progressistes et indépendants (RDPI) ; un du groupe communiste républicain citoyen et écologiste (CRCE) ; un du groupe du Rassemblement Démocratique et Social Européen (RDSE) ; un du groupe Les Indépendants – République et Territoires (INDEP) ; et un du groupe Écologiste – Solidarité et Territoires (GEST).

Compte tenu des candidatures qui sont parvenues au secrétariat de la commission spéciale, je vous propose de désigner comme vice-présidents : pour le groupe Les Républicains, Alexandra Borchio Fontimp, Toine Bourrat, Micheline Jacques et Marie Mercier ; pour le groupe Socialiste, Écologiste et Républicain, Sylvie Robert et Florence Blatrix Contat ; pour le groupe Rassemblement des démocrates, progressistes et indépendants, Xavier Iacovelli ; pour le groupe communiste républicain citoyen et écologiste, Pierre Ouzoulias ; pour le groupe du Rassemblement Démocratique et Social Européen, Bernard Fialaire ; pour le groupe Les Indépendants – République et Territoires, celle de Pierre-Jean Verzelen ; pour le groupe Écologiste – Solidarité et Territoires, Thomas Dossus.

Conformément aux propositions formulées par les groupes, je vous propose de désigner comme secrétaires : pour le groupe Les Républicains, MNadine Bellurot ; pour le groupe Union Centriste, Anne-Catherine Loisier ; pour le groupe Socialiste, Écologiste et Républicain, Jérôme Durain.

Les vice-présidents et secrétaires sont désignés.

Mme Catherine Morin-Desailly, présidente. – Nous procédons, dans un second temps, à la désignation des rapporteurs de notre commission spéciale, dont je précise qu'ils seront membres de droit du Bureau.

J'ai reçu les candidatures suivantes : pour le groupe Les Républicains, Patrick Chaize, et pour le groupe Union Centriste, Loïc Hervé.

M. Patrick Chaize et M. Loïc Hervé sont désignés rapporteurs de la commission spéciale.

Mme Catherine Morin-Desailly, présidente. – Nous sommes en train d'organiser le programme des auditions en plénière, que nous vous diffuserons dès que possible. Nous entendrons la cheffe de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), la commissaire divisionnaire Cécile Augeraud, responsable de la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) demain, mercredi 7 juin, et le ministre Jean-Noël Barrot le jeudi 8 juin.

Le calendrier pourrait ensuite être le suivant : pour l'examen des amendements de commission et l'adoption du rapport, le délai limite pour les amendements serait fixé au vendredi 23 juin, à 12 heures, et la réunion de commission se déroulera le mardi 27 juin, à partir de 13 h 30.

Pour l'examen des amendements de séance publique, le délai limite pourrait être fixé au lundi 3 juillet, 12 heures. Nous examinerions les amendements le mardi 4 juillet, à partir de 13 h 30. La séance publique pourrait commencer, sous réserve des contraintes d'ordre du jour, ce même mardi 4 juillet en fin d'après-midi. L'examen du texte nous occuperait mercredi 5, jeudi 6, et peut-être jusqu'au vendredi 7 juillet.

D'ici à l'examen du texte en commission, nous mènerons avec les rapporteurs des auditions pour entendre les parties prenantes sur le texte. Nous proposons d'ouvrir ces auditions à l'ensemble des membres de la commission spéciale qui voudront y participer.

J'indique enfin que M. Loïc Hervé sera chargé des articles 1er à 5, 19 à 21, 23, 24, 28 à 32, 34 et 35 ; et M. Patrick Chaize, des articles 6 à 18, 22, 25 à 27, 33 et 36.

M. Loïc Hervé, rapporteur. – Mme la présidente nous a expliqué l'importance et l'étendue du projet de loi qu'il nous revient d'examiner. Pensé, dès ses origines, comme une zone de liberté, l'espace numérique ne peut pas pour autant être une zone de non-droit. Sa régulation est une

nécessité absolue au regard de la place d'Internet dans nos vies quotidiennes, au cœur de nos modes de communication, de consommation et d'information. Tel est là tout l'enjeu des règlements dont ce projet de loi tire les conséquences : faire du numérique un espace où chacun peut s'exprimer librement, mais dans le respect des règles qui s'appliquent dans la « vraie vie » et avec le même droit d'entretenir une confiance légitime vis-à-vis de ses interlocuteurs.

Je me réjouis que, sur un sujet complexe, qui touche aux compétences de nombreuses commissions permanentes, le choix ait été fait de constituer une commission spéciale ; cette formule sera le gage de débats nourris par la pluralité de nos points de vue, de nos analyses et de nos sensibilités politiques.

Je regrette en revanche, comme notre présidente, que nous ayons si peu de temps pour conduire nos travaux. Le Conseil d'État a déploré dans son avis n'avoir eu que six jours pour se prononcer. Nous en aurons un peu plus, mais vu la complexité des dispositions et de la construction du texte qui retouche à plusieurs reprises les mêmes articles, ainsi que de sa rédaction *a minima* perfectible, j'espère que nous arriverons à produire un texte de qualité !

J'en viens aux articles dont j'aurai la charge en tant que rapporteur.

Les articles 1er à 5 portent sur la protection des citoyens dans l'espace numérique, au bénéfice notamment des mineurs.

Les articles 1er et 2 tendent à revoir le dispositif mis en place par l'article 23 de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales qui avait été adopté par la commission des lois sur l'initiative de notre collègue Marie Mercier. La procédure de blocage judiciaire peut actuellement être engagée par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) pour bloquer l'accès et déréférencer les sites pornographiques qui ne mettraient pas en place le contrôle de majorité. Il s'agirait de transformer cette procédure judiciaire en procédure administrative, conformément à une recommandation de la délégation aux droits des femmes dans son rapport sur l'industrie de la pornographie, et à permettre aux agents de l'Arcom de dresser eux-mêmes des constats.

L'article 3 vise à créer une infraction pour pénaliser les hébergeurs qui n'agiraient pas dans les vingt-quatre heures pour supprimer des contenus pédopornographiques à la demande de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

L'article 4 étend les pouvoirs de l'Arcom pour faire respecter les interdictions de diffusion des contenus produits par des médias visés par des sanctions européennes : elle pourra désormais imposer le respect de telles interdictions à de nouveaux acteurs qui ne sont aujourd'hui pas couverts par

la loi, comme les services de communication au public en ligne ou les opérateurs de réseaux satellitaires.

Quant à l'article 5, il crée une nouvelle peine complémentaire de suspension du compte d'accès à une plateforme en ligne, applicable aux personnes condamnées pour certains délits commis en utilisant ladite plateforme.

Le titre VII comporte trois articles à la rédaction similaire qui visent à confier respectivement au Conseil d'État, à la Cour de cassation et à la Cour des comptes une nouvelle mission de contrôle des opérations de traitement des données à caractère personnel effectuées par les juridictions et leur ministère public, dans l'exercice de leur fonction juridictionnelle.

Le titre VIII est un titre « Diverses dispositions d'adaptation au droit de l'Union européenne » (Ddadue) ; il vise à tirer les conséquences des règlements européens dans des textes nationaux sectoriels, s'agissant notamment des prérogatives de l'Arcom, de la Commission nationale de l'informatique et des libertés (Cnil), de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et de l'autorité judiciaire. Je m'intéresserai plus particulièrement aux articles 23, 24 et 28 à 32.

Sans entrer dans le détail des évolutions prévues par ces articles, ceux-ci me semblent cependant soulever des difficultés de fond comme de forme. Je relève tout d'abord qu'un travail de mise en cohérence et de clarification sera probablement nécessaire : en effet, la portée de certaines règles reste floue, faute pour le projet de loi d'être parvenu à en préciser le périmètre, à en définir l'articulation avec d'autres dispositifs ou à en décrire les modalités concrètes d'application. Je pense notamment aux nouvelles compétences données à la Cnil sur l'altruisme en matière de données, dont la rédaction m'apparaît imprécise.

Par ailleurs, il semblerait que, sous couvert de mise en conformité avec le règlement européen sur les services numériques, des pans entiers de notre droit national se trouvent soit abrogés, soit alignés sur le règlement sans mesures complémentaires, alors que ce dernier n'a pas les mêmes seuils, notamment en termes de taille des plateformes soumises aux diverses obligations qu'il prévoit. Il nous conviendra lors de nos travaux d'être particulièrement vigilants pour nous assurer que l'application du règlement n'aura pas pour conséquence de dédouaner certaines plateformes opérant sur notre territoire de leurs responsabilités, par exemple en matière de lutte contre la désinformation.

M. Patrick Chaize, rapporteur. – Mes chers collègues, je vous remercie pour la confiance que vous m'accordez en me nommant corapporteur aux côtés de Loïc Hervé.

Je suis chargé des dix-neuf articles de ce projet de loi qui relèvent des compétences de la commission des affaires économiques, essentiellement

en matière de régulation de l'économie numérique et des données, de concurrence, de droit de la consommation et de tourisme.

Ce projet de loi est en très grande partie un projet de loi d'adaptation de notre droit national au droit de l'Union européenne. Autrement dit, c'est un Ddadue qui ne dit pas son nom ! Il s'agit en effet d'adapter la quasi-totalité de nos lois nationales traitant des questions numériques, en particulier la loi de 1986 relative à la liberté de communication (loi Léotard) et la loi de 2004 pour la confiance dans l'économie numérique, à plusieurs règlements européens. Parmi les règlements déjà adoptés, il y a le RSN ou *DSA*, le règlement RMN ou *DMA*, et le règlement sur la gouvernance des données (RGA) ou *Data Governance Act (DGA)*. Parmi les règlements toujours en cours de négociation à l'échelle européenne, il y a le règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données *(Data Act)*, dont plusieurs articles anticipent l'adoption.

L'ensemble de ces règlements étant d'application directe, nous devons être prudents : il s'agit non seulement de rester fidèle à leur lettre comme à leur esprit, car ces textes sont issus de négociations et de compromis difficiles entre les différents États membres et les opérateurs économiques, mais également de ne pas adopter des dispositions qui seraient trop contraignantes, spécifiques à la France, et qui risqueraient de pénaliser injustement nos opérateurs économiques. Mais il faut aussi faire preuve de vigilance lorsque nos lois françaises se sont montrées particulièrement ambitieuses, protectrices et avant-gardistes, afin d'éviter que l'adoption de ce projet de loi ne se traduise par des dispositions moins-disantes par rapport aux règles existantes.

Je serai ainsi particulièrement vigilant lors de l'examen des articles 7 à 10 relatifs à la régulation du marché de l'informatique en nuage ou *cloud*. Comme le précisent l'exposé des motifs du projet de loi et l'étude d'impact du Conseil d'État, ces articles s'inscrivent dans la continuité directe des travaux de la commission des affaires économiques sur la souveraineté économique et numérique, dont le rapport a été adopté l'an dernier à l'unanimité et dont certaines recommandations ont été traduites dans le *Data Act*.

Il s'agit d'encadrer les crédits *cloud* accordés gratuitement par les grandes plateformes américaines à nos entreprises afin de les inciter à utiliser exclusivement leurs technologies plutôt que d'autres, et de supprimer progressivement les frais de transfert facturés à nos entreprises lorsqu'elles souhaitent changer de fournisseur de services d'informatique en nuage : c'est indispensable pour soutenir le développement de sociétés françaises et européennes d'informatique en nuage, pour garantir une concurrence plus saine et des marchés contestables et pour éviter de rendre nos entreprises « captives » des grandes plateformes américaines.

Je serai également vigilant lors de l'examen des articles 11 à 14, qui anticipent l'adoption des dispositions du *Data Act* relatives aux services d'intermédiation des données et qui désignent l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) comme autorité nationale compétente en la matière, en renforçant ses pouvoirs d'enquête et de sanction.

Sur les articles 16, 18, 22, 25, 26 et 27, il s'agit essentiellement de désigner les autorités nationales compétentes en matière d'application des grands règlements européens sur le numérique, d'adapter leurs prérogatives en conséquence et de faciliter leur coopération.

L'Arcom est ainsi désignée coordinateur national pour les services numériques et bénéficiera notamment de l'appui de la Cnil et de la DGCCRF pour la mise en œuvre de ce règlement. De façon plus ponctuelle et plus spécifique, l'Arcom pourra davantage solliciter le pôle d'expertise de la régulation de l'économie numérique (PEReN) afin de mieux comprendre les algorithmes, les traitements de données, les codes et les risques systémiques des grandes plateformes.

L'Autorité de la concurrence (ADLC) est ainsi désignée coordinateur national pour les marchés numériques et bénéficiera notamment de l'appui de la DGCCRF, de la Cnil et de l'Arcom pour la mise en œuvre de ce règlement.

Si ce projet de loi est en quelque sorte un Ddadue, il y a tout de même quelques mesures nouvelles, intéressantes, qui ne sont pas prévues par les règlements européens et qui méritent toute notre attention.

Je pense à l'article 15 sur les jeux à objets numériques monétisables dont une première définition a failli être adoptée lors de l'examen par la commission des affaires économiques de la loi visant à encadrer l'influence commerciale. Nous serions les premiers en Europe à définir et à encadrer ces innovations, mais, face à la complexité et à l'ampleur du travail à accomplir, le Gouvernement préfère, en l'état, recourir à une habilitation à légiférer par ordonnance.

Je pense également à l'article 17, visant à mettre en place une plateforme unique à destination des communes et des plateformes numériques permettant la location de meublés de tourisme, comme Airbnb. L'objectif de ce texte est de pallier les difficultés opérationnelles de mise en œuvre des obligations légales actuelles, qui se traduisent notamment par une charge importante pour les communes. C'est sans doute la seule disposition intéressant les collectivités territoriales dans ce texte, nous devons donc être vigilants.

Je pense enfin à l'article 6, visant à mettre en place un dispositif national de cybersécurité grand public, ou « filtre anti-arnaques », afin de mieux lutter contre les actes de cybermalveillance qui font désormais partie de notre quotidien. C'est une promesse de campagne du Président de la

République que ce projet de loi tente, à l'instar de ce qui a été fait par plusieurs autres pays européens, de mettre en forme.

Les fournisseurs de navigateurs Internet, les fournisseurs d'accès à Internet et les fournisseurs de systèmes de résolution des noms de domaine seront tous mis à contribution pour avertir les internautes lorsqu'ils seront sur le point d'accéder à des sites frauduleux, voire pour bloquer l'accès à ces sites, sous le contrôle attentif de la Cnil.

C'est, à la fois, la sécurisation de l'espace numérique et la restauration de la confiance de nos concitoyens dans l'économie numérique qui sont en jeu. Je serai très regardant sur le déploiement de ce filtre anti-arnaques : il complétera utilement l'initiative prise par notre collègue Laurent Lafon, président de la commission de la culture et auteur de la loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public – un texte qui vise à mettre en œuvre un cyberscore –, et dont notre collègue Anne-Catherine Loisier était rapporteure pour la commission des affaires économiques.

Nous pouvons être fiers, ici au Sénat, d'être à l'avant-garde de la régulation de l'économie numérique, comme nous l'avons dit à plusieurs reprises récemment lors de l'examen de diverses propositions de loi visant à réguler nos usages numériques. Nous le sommes également avec la commission d'enquête sur TikTok constituée sur l'initiative de notre collègue Claude Malhuret.

Dans le cadre de l'ensemble de ces travaux, et y compris lors de l'examen de ce projet de loi, nous devrons être prudents et veiller à la cohérence de l'ensemble des dispositions que nous voterons et recommanderons.

Mme Laurence Rossignol. – Je m'interroge sur l'application de l'article 45 de la Constitution. J'évoquerai la partie du texte qui m'intéresse tout particulièrement, celle dévolue à Loïc Hervé, en particulier les trois premiers articles. Nous sommes nombreux à considérer que ceux-ci ne répondent pas à l'objectif annoncé, et qu'il faudrait les renforcer tout en restant dans le cadre de l'intitulé du titre Ier relatif à la protection des mineurs. Le texte témoigne d'une approche étroite de ce sujet. Comment l'améliorer si l'on nous oppose l'article 45 dès qu'un amendement n'est pas parfaitement « dans les clous » ? Par exemple, s'agissant de l'établissement du référentiel, nous pouvons certes donner toute latitude à la Cnil, mais il serait préférable de prévoir un encadrement.

Mme Annick Billon. – Je vous félicite, madame la présidente, pour votre désignation à la tête de cette commission spéciale, car vous êtes engagée de longue date sur ces sujets. Je félicite également les rapporteurs qui sont des spécialistes, Loïc Hervé étant membre de la Cnil et Patrick Chaize président du groupe Numérique.

En tant que présidente de la délégation aux droits des femmes, et avec les rapporteures Alexandra Borchio Fontimp et Laurence Rossignol, nous serons attentives à la transcription des recommandations que nous avions faites dans le rapport *Porno : l'enfer du décor*.

Les objectifs sont là, mais les moyens seront-ils suffisants ? Nous approuvons diverses mesures – je pense notamment à l'assermentation des agents de l'Arcom –, mais d'autres sujets ne sont pas évoqués, comme le droit à l'oubli et le dispositif de vérification d'âge.

Il faut aller plus loin et plus rapidement, car des textes ont été votés mais ne sont toujours pas appliqués.

Mme Catherine Morin-Desailly, présidente. – La protection de l'enfance est un de nos sujets prioritaires, et nous allons organiser une table ronde sur cette question.

Madame Rossignol, je ne suis pas habituée à l'exercice de la mise en application d'un règlement européen. Des améliorations ont été apportées par le Gouvernement, nous pouvons donc apporter les nôtres. Il faut néanmoins rester dans l'esprit des règlements, pour ne pas être censurés par le Conseil constitutionnel. Un travail très fin devra être fait avec les rapporteurs. Nous ne partons pas de loin, puisque nous disposons des propositions de la délégation aux droits des femmes et de la commission des affaires européennes.

J'aurais aimé aller plus loin sur la régulation des plateformes, jusqu'à créer un statut spécifique au même titre que les éditeurs de programmes. Mais le Sénat est à la pointe sur ces sujets et sait faire preuve de créativité !

Je m'assurerai que nous puissions améliorer au mieux le texte, mais, je le redis, il s'agit d'appliquer un règlement, ce qui n'est pas la même chose qu'une directive.

Enfin, je précise que l'article 3 n'est pas issu du *DSA*.

Mme Laurence Rossignol. – Le Gouvernement surtranspose puisqu'il a amélioré le texte.

Mme Catherine Morin-Desailly, présidente. – Nous pourrons évoquer ces questions jeudi avec le ministre Jean-Noël Barrot.

Audition de Cécile Augeraud, commissaire divisionnaire, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), Pierre-Yves Lebeau, chef de l'état-major de la sous-direction de lutte contre la cybercriminalité (SDLC) et Clara Timsit, conseillère juridique rattachée à l'état-major de la SDLC

Mercredi 7 juin 2023

Mme Catherine Morin-Desailly, présidente. – Nous sommes aujourd'hui réunis pour recevoir Mme Cécile Augeraud, cheffe de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Madame Augeraud, je vous remercie d'avoir accepté notre invitation.

Créée en 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) est une branche de la direction centrale de la police judiciaire. Elle constitue la pièce centrale du dispositif de signalement des propos illicites ou offensants tenus en ligne – autant dire que votre mission est vaste.

Nous sommes très sensibles à votre travail et également très préoccupés par la situation des mineurs, victimes d'un grand nombre d'actes délictueux. Nous souhaiterions connaître le fonctionnement de Pharos et nous aimerions que vous puissiez nous présenter un bilan des dispositifs existants.

Le projet de loi reconduit des mécanismes existants, par exemple s'agissant du rôle du juge en matière de blocage des contenus illicites ; c'est pour le Parlement l'occasion de dresser avec vous le bilan de ces procédures. Il crée des outils nouveaux pour lesquels votre expertise sera précieuse : je pense, entre autres, à la peine complémentaire de suspension des comptes d'accès aux plateformes qui serait encourue en cas de condamnation pour certains délits commis en ligne.

Le projet de loi instaure en son article 3une sanction pénale pour défaut d'exécution d'une demande de retrait d'un contenu pédopornographique par un hébergeur. Je rappelle que les contenus à caractère terroriste sont dorénavant régis par la loi du 16 août 2022, qui contraint au retrait dans un délai d'une heure.

Nous sommes donc impatients de vous entendre afin que vous puissiez nous présenter le travail exigeant que vous menez au quotidien, nous donner votre point de vue sur ce nouveau texte et nous donner quelques perspectives d'amélioration des procédures en vigueur.

Mme Cécile Augeraud, cheffe de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. – Merci pour votre présentation très exhaustive.

Pharos est l'une des composantes de l'Office que je dirige. La plateforme fait partie d'un ensemble luttant contre la cybercriminalité : c'est l'action de toutes ces composantes qui rend nos dispositifs efficaces.

L'Office compte 150 agents et assure quatre missions principales. Premièrement, nous enquêtons sur les cyberattaques et sur les cyberservices criminels. Deuxièmement, nous fournissons un appui technique aux services territoriaux de police et de gendarmerie et nous dispensons des formations d'investigateurs en cybercriminalité sur l'ensemble du territoire. Troisièmement, nous effectuons des analyses du renseignement criminel : nous travaillons en étroite collaboration avec les plateformes et nous sommes le point d'entrée pour la France de nos partenaires internationaux. Quatrièmement, nous assurons une mission de détection par le biais de nos deux plateformes : Pharos, la vieille dame du service, née en 2009, mais aussi le dispositif de traitement harmonisé des enquêtes et signalements pour les e-escroqueries (Thésée), créé le 15 mars 2022, qui permet de recueillir les signalements pour huit champs infractionnels. En outre, Thésée offre aux particuliers la possibilité de déposer plainte entièrement en ligne – les victimes ne doivent, à aucun moment, se déplacer.

Pharos est une plateforme qui a connu beaucoup d'évolutions, en raison d'un accroissement des dangers, des menaces, des risques et des infractions. Elle est destinée à recevoir des signalements pour tous les contenus illicites présents sur Internet, à condition qu'ils soient publics – Pharos n'intervient pas dans la sphère privée. La plateforme a évolué au gré des événements : l'assassinat à caractère terroriste de Samuel Paty a conduit au doublement de ses effectifs, avec, à ce jour, 43 agents qui se relaient désormais vingt-quatre heures sur vingt-quatre et sept jours sur sept. Elle est en mesure de réagir en permanence à tous les signalements. Les missions sont désormais plus diversifiées, grâce à l'ouverture d'enquêtes sur le fondement des signalements de contenus illicites et à la création d'un pôle judiciaire de dix enquêteurs. Les effectifs consacrés à la lutte contre la haine en ligne ont augmenté, car c'est un sujet de préoccupation majeure.

Une cellule recueille les signalements, puis une équipe d'enquêteurs est chargée de veiller à l'application de mesures administratives prévues par la loi pour la confiance dans l'économie numérique (LCEN). Son article 6-1 nous permet de demander le retrait de contenus illicites à caractère terroriste ou pédopornographique et d'enjoindre au blocage ou au déréférencement lorsque le retrait n'a pas été effectué.

En 2022, Pharos a reçu près de 176 000 signalements, qui se sont traduits par 89 000 demandes de retrait, dont 83 % visaient des contenus pédopornographiques au titre de l'article 6-1 de la LCEN. Quelque 4 024 injonctions de déréférencement et 354 injonctions de blocage ont été décidées : cela montre que nos demandes de retrait sont suivies. En outre, 78 790 contenus illicites ont été détectés grâce à des actions

de veille : nous ne nous contentons plus de recevoir des signalements, par exemple, en matière de lutte contre les discriminations.

J'insiste sur le nombre de signalements : 176 000 en 2022, contre 246 000 en 2021 et 290 000 en 2020. Cette diminution s'explique par la baisse du nombre d'actes terroristes et par la création de la plateforme Thésée. Pharos se concentre désormais sur des faits de pédopornographie et de haine en ligne, tandis que les escroqueries ont été déportées sur la plateforme Thésée. Le traitement des signalements est très différent. Sur Thésée, les particuliers peuvent faire des signalements ou déposer des plaintes en ligne pour chantage, fausse location, faux site de vente, entre autres. Celles-ci feront l'objet d'un recoupement par l'intermédiaire d'un outil d'analyse afin d'en optimiser le traitement. Thésée peut recevoir le signalement de personnes physiques majeures, mais aussi mineures – en revanche, les dépôts de plainte sont inaccessibles aux mineurs. Les personnes ne souhaitant pas se déplacer dans un commissariat ou une gendarmerie peuvent ainsi s'affranchir du regard des forces de l'ordre : ce dispositif est parfois très pertinent pour les parents déposant plainte pour des mineurs victimes de chantage en ligne.

Ces deux plateformes fonctionnent avec des partenaires référencés et des signaleurs de confiance ; le projet de loi participe de la même philosophie. Nous travaillons à la signature de conventions avec les grandes plateformes, qui reçoivent des signalements ou détectent elles-mêmes des contenus très sensibles. Nous voulons prioriser leur traitement afin d'agir rapidement.

Si les faits d'escroquerie ont fait l'objet d'un déport partiel vers Thésée, les attaques de *phishing*, ou d'hameçonnage, restent prises en charge par Pharos, qui a reçu plus de 11 000 signalements de ce type en 2022.

M. Loïc Hervé, rapporteur. – Merci pour votre présentation.

Quel bilan qualitatif et quantitatif tirez-vous du droit en vigueur en matière de lutte contre les contenus illicites et contre la criminalité en ligne ? Y a-t-il des mécanismes plus efficaces que d'autres ? Certains gagneraient-ils à être étendus ? À l'inverse, d'autres doivent-ils être abandonnés aujourd'hui, parce qu'ils vous semblent obsolètes ou inadaptés ? Comment s'organise la coopération avec vos partenaires à l'échelle européenne ?

Comment analysez-vous les nouvelles obligations imposées aux plateformes et aux hébergeurs par le *Digital Services Act (DSA)*, ou, en français, le règlement sur les services numériques (RSN) en matière de détection et de mise hors d'accès des contenus illicites ?

Quel sera l'impact, pour l'Office et ses services partenaires, des nouveaux pouvoirs qui seraient conférés à l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), à la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et à la Commission nationale de l'informatique et des

libertés (Cnil) ? Des échanges ont-ils été engagés avec ces autorités pour définir des modes d'action partagés en matière de lutte contre les contenus illicites ?

Quelle est votre analyse du nouveau mécanisme d'évaluation des risques par les plateformes et les moteurs de recherche ? Ces évaluations sont-elles de nature, à terme, à avoir une influence sur les méthodes des services chargés de la lutte contre la criminalité en ligne ?

Comment l'action de l'OCLCTIC, notamment celle des plateformes Pharos et Thésée, s'articulera-t-elle avec les nouvelles « injonctions d'agir contre des contenus illicites » créées par l'article 9 du RSN, avec la « notification des soupçons d'infraction pénale » créée par l'article 18 de ce règlement, ou encore avec le statut nouvellement institué de « signaleur de confiance », prévu à l'article 22 ?

Comment évaluez-vous l'efficacité des nouvelles mesures coercitives créées par le projet de loi, comme l'interdiction d'accès aux sites pornographiques aux mineurs, la peine complémentaire de blocage des comptes d'accès aux plateformes, le renforcement de la lutte contre la pédopornographie, entre autres ? En particulier, comment analysez-vous la nouvelle peine complémentaire de blocage des comptes d'accès aux plateformes ? Je rappelle que l'application de cette peine serait limitée à quelques délits et qu'elle ne toucherait que le compte utilisé pour commettre l'infraction.

Y a-t-il, selon vous, des difficultés ou des lacunes, techniques ou juridiques, qui portent atteinte à l'effectivité de la lutte contre les contenus illicites et qui n'auraient pas été couvertes par le RSN et par le projet de loi ? Cette question est sans doute la plus importante : nous pourrions, le cas échéant, améliorer la qualité juridique du texte et combler ses éventuels manques.

Mme Cécile Augeraud. – Votre première question est très vaste. Les dispositifs existants sont nombreux : nous ne connaissons pas tout le spectre et je ne serai pas en mesure de vous dresser un bilan exhaustif. Les textes en vigueur nous permettent de respecter l'indispensable équilibre entre la sécurisation d'Internet et des pratiques proches de la censure – ce qui pourrait, à juste titre, nous être reproché. Nous ne travaillons pas uniquement avec des partenaires français ; certains ont des visions très éloignées des nôtres. Il existe une forte disparité parmi les législations européennes, malgré les avancées du RSN et du règlement *Terrorist Content Online* (TCO) du 29 avril 2021 ou règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

Le seul bilan quantitatif que nous sommes en mesure de dresser consiste en la recension des signalements reçus sur Pharos et Thésée. Toutefois, leur contenu est très disparate.

La loi pour la confiance dans l'économie numérique est un outil majeur de notre action quotidienne. De plus, le texte n'a cessé d'évoluer depuis 2004, le plus récemment grâce au règlement TCO et à la lutte contre

les sites « miroirs » prévue à l'article 6-3 de la LECN. Ces outils nous permettent de formuler des demandes de retrait sur les contenus faisant l'apologie du terrorisme ou pédopornographiques.

L'article 6-1 de la LCEN nous confère des pouvoirs administratifs importants : nous pouvons ainsi traiter un grand volume d'affaires. Grâce à Pharos, la France est très en avance sur les procédures de retrait par rapport à d'autres pays européens. Cela dit, certains textes en cours d'examen risquent d'alourdir les dispositifs que nous avons l'habitude d'utiliser. Lorsque nous devrons fournir des justifications plus détaillées à chaque demande de retrait, nous ne serons plus en mesure de traiter autant de signalements.

M. Loïc Hervé, rapporteur. – C'est là un point très important. Cette diminution de votre capacité d'intervention – que vous redoutez – est-elle imputable à l'application directe du règlement ou à certaines dispositions du projet de loi ? Quelle aide pourrions-nous vous apporter sur ce point ? Bien sûr, nous devons assurer le respect de certaines garanties, mais nous devons aussi ne pas entamer votre productivité.

Mme Cécile Augeraud. – Le projet de loi n'est en rien responsable de cette situation, bien au contraire. Jusqu'à présent, l'article 6-1 nous conférait une autorité limitée : nous ne pouvions que solliciter le retrait des contenus auprès des hébergeurs. Depuis l'entrée en vigueur du règlement TCO, nous bénéficions désormais d'une injonction de retrait. Il en ira de même pour les affaires pédopornographiques. Ce sont des progrès essentiels : le RSN et le projet de loi nous permettront de gagner en efficacité.

M. Pierre-Yves Lebeau, chef de l'état-major de la sous-direction de lutte contre la cybercriminalité. – Nous devons encore nous approprier les outils découlant du règlement TCO qui seront utilisés au sein d'Europol. Dans quelques années, nous pourrons dresser une première comparaison entre les outils fournis par les agences européennes et les instruments que nous offre le droit français depuis 2015.

Mme Cécile Augeraud. – Il nous est impossible de dresser un bilan aujourd'hui. Nous en sommes encore au stade des discussions pour la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, dit règlement ASM. Nous craignons qu'un formalisme excessif ne constitue un frein à notre action.

Mme Laurence Rossignol. – Pourriez-vous être plus précise ?

Mme Catherine Morin-Desailly, présidente. – Je reprends la question : pouvez-vous nous préciser votre mode opératoire ? Quels pourraient être les freins à votre action ? Le futur règlement ASM vous apportera-t-il des moyens complémentaires ?

Mme Cécile Augeraud. – Sur Pharos, des compétences en matière de retrait nous sont octroyées par l'article 6-1 de la loi pour la confiance dans l'économie numérique. Lorsque des contenus pédopornographiques ou à caractère terroriste nous sont signalés, nous pouvons demander le retrait de ces contenus auprès de l'éditeur et de l'hébergeur. Si cette première demande n'est pas exécutée, nous pouvons exiger soit un déréférencement des adresses des sites concernés soit un blocage du site.

Aujourd'hui, le règlement TCO et le nouvel article 6-1-1 nous octroient des pouvoirs plus stricts d'injonction : nous pourrons exiger le retrait dans l'heure d'un contenu à caractère terroriste. Le règlement ASM est lui en cours de discussion, mais les contours de ce texte ne sont pas encore clairement établis ; les discussions, auxquelles nous participons, sont en cours. Nous aimerions que les règles définies par le règlement ASM en matière de pédopornographie soient semblables à celles du règlement TCO en matière de contenus terroristes.

Cela dit, l'article 9 du RSN, relatif à l'injonction d'agir sur les contenus illicites, nous impose de fournir des éléments précis pour motiver nos demandes, ce qui n'est pas le cas actuellement. Aujourd'hui, nous sollicitons le retrait d'un contenu au titre des pouvoirs administratifs dont nous disposons – un pouvoir assez exceptionnel pour des policiers. Bien sûr, nous sommes contrôlés par l'Arcom, *via* la personnalité qualifiée qui formule des recommandations sur nos actions. Le dispositif actuel, grâce auquel nous pouvons formuler des demandes de retrait en masse, est relativement fluide : en 2022, 89 057 demandes de retrait ont été formulées. C'est un chiffre très important : si chaque demande devait faire l'objet d'une justification précise, nous estimons à ce stade que notre travail serait ralenti.

Mme Catherine Morin-Desailly, présidente. – Vous avez mentionné votre mission de veille. À cet égard, quel est le rôle de la personnalité qualifiée de l'Arcom, Mme Laurence Pécaut-Rivolier ?

Mme Cécile Augeraud. – L'Arcom ne nous adresse pas de signalements : elle contrôle notre action sur les retraits, les blocages et les déréférencements que nous prononçons. Elle formule des recommandations quand elle estime que nos demandes ne sont pas légitimes. Elle a récemment rendu son rapport : le nombre de recommandations est peu élevé. De plus, elle a souligné qu'elle pouvait mener à bien aisément son travail de contrôle *a posteriori*. Mais peut-être votre question portait-elle sur l'évolution du rôle de l'Arcom dans le projet de loi ?

Mme Catherine Morin-Desailly, présidente. – Ma question portait sur le mode opératoire, notamment pour répondre aux préoccupations de Mme Rossignol. La personnalité qualifiée de l'Arcom participe aussi aux travaux de la cellule de veille ; elle indique identifier chaque année 150 000 contenus pédopornographiques et terroristes. Comment sa

surveillance constante se traduit-elle très concrètement dans le suivi des signalements ?

Mme Cécile Augeraud. – Toutes nos demandes de retrait relatives aux contenus pédopornographiques et terroristes font l'objet d'un contrôle *a posteriori* de l'Arcom qui ne mène pas d'actions de détection.

M. Patrick Chaize, rapporteur. **–** Que pensez-vous de la création, prévue à l'article 6 du projet de loi, d'un filtre national de cybersécurité à destination du grand public ? Les dispositifs déjà existants de filtrage et de retrait sont-ils suffisamment efficaces ?

Comment l'OCLCTIC et la plateforme Pharos sont-ils associés au déploiement du filtre national de cybersécurité grand public ?

Le champ des infractions visées par la base commune de recensement des sites frauduleux vous semble-t-il adapté et suffisant, notamment en matière d'usurpation d'identité ou de collecte de données ? Des infractions supplémentaires correspondant à d'autres actes de cybermalveillance devraient-elles être ajoutées ?

Vous avez évoqué un risque de ralentissement de votre action en raison des futures règles européennes. En avez-vous déjà mesuré les conséquences sur vos missions ?

Les plateformes Pharos et Thésée font-elles l'objet d'opérations de communication à destination du grand public ? Il me semble que ce point devrait faire l'objet d'améliorations.

Mme Cécile Augeraud. – Le filtre anti-arnaques concernera les deux plateformes, surtout Thésée. La création d'un tel filtre est indispensable, tant les usages numériques et la consommation en ligne ont augmenté depuis la crise sanitaire.

Des filtres existent déjà, notamment Signal Spam, la plateforme 33 700, qui lutte contre les appels et les SMS indésirables ou encore le site cybermalveillance.gouv.fr. Je ne suis pas en mesure d'évaluer ces dispositifs. Cela dit, nous constatons que Pharos a recueilli en 2022 plus de 11 160 signalements de *phishing*. Pour sa part, Thésée a reçu plus de 120 000 déclarations depuis son ouverture. Il faut donc adapter nos moyens de lutte à l'ampleur du phénomène et au nombre de victimes. Le Gouvernement a déterminé une politique ambitieuse afin de mieux lutter contre la cybercriminalité.

Tel qu'il est prévu aujourd'hui, le dispositif du projet de loi ne prend pas en compte un élément central, à savoir les faux sites de vente qui ne sont pas le « miroir » d'un site existant. Or, grâce à Thésée, nous avons recensé plus de 1 500 faux sites, avec plus de 32 000 plaintes, soit autant de victimes : c'est considérable. Certes, les préjudices sont souvent faibles, mais les conséquences peuvent être dramatiques. En raison de la hausse des prix des matières premières, de nombreux internautes se sont reporté l'hiver dernier

sur les sites d'achat de bois, pensant ainsi diminuer leur facture, mais les faux sites avaient fleuri. Or ces victimes connaissaient déjà des difficultés financières.

Nous avons été associés à tous les travaux du filtre anti-arnaques depuis le mois d'octobre, notamment sur la détermination du périmètre. Nous déplorons que le périmètre évoqué initialement n'ait pas été retenu, notamment pour ce qui concerne les faux sites de vente. On ne pourrait en effet traiter que les faux sites de vente usurpant l'identité de vrais sites. Ces affaires ne représentent qu'une part très limitée des infractions constatées sur Thésée, puisque nous n'avons enregistré que quarante cas de faux sites depuis sa création en mars 2022.

M. Loïc Hervé, rapporteur. – Pourquoi ?

Mme Cécile Augeraud. – Sans doute s'agit-il d'une volonté de tester le filtre anti-arnaques avant d'envisager, dans un second temps, un élargissement de son périmètre.

Dans la mesure où le règlement TCO vient juste d'entrer en vigueur et que la proposition de règlement ASM n'en est qu'au stade des discussions, je ne suis pas capable d'évaluer les dispositifs qu'ils contiennent ni d'apprécier l'impact qu'ils auront sur Thésée.

Nous cherchons à développer la communication à l'égard du grand public. Vu le nombre de signalements reçus sur Pharos, il n'est pas possible de faire un retour à chaque personne, et ce ne sera pas possible demain non plus. En revanche, une communication plus globale, par thèmes, sur le nombre de retraits de contenus que nous avons obtenus ne peut qu'accroître la notoriété de la plateforme.

Mme Annick Billon. – La délégation aux droits des femmes a travaillé sur l'industrie de la pornographie. Avec Laurence Rossignol, Alexandra Borchio Fontimp et Laurence Cohen, nous avons publié un rapport sur le sujet. Il existe une porosité entre pornographie, prostitution et proxénétisme. Certaines vidéos comportent des actes d'inceste, de barbarie, de racisme, de viol, *etc*. Il n'est pas nécessaire de visionner les vidéos, la seule lecture des titres et des rubriques des sites pornographiques suffit. La lutte contre les violences pornographiques est insuffisante. Pensez-vous que la création d'une troisième branche au sein de Pharos consacrée aux tortures, aux actes de barbarie et aux violences sexuelles serait utile pour augmenter le nombre de signalements et mieux agir contre ces images illicites ?

Notre arsenal législatif doit-il être complété pour qualifier ces vidéos pornographiques qui mettent en scène, conformément d'ailleurs souvent à la réalité du tournage, des actes de torture, de barbarie ou de viol ? Nous avions proposé d'assermenter les agents de l'Arcom afin de leur permettre de constater eux-mêmes les infractions commises par les sites pornographiques accessibles aux mineurs. Est-ce suffisant pour accélérer les

procédures de retrait ou de blocage de ces sites ? Les moyens de l'Arcom sont-ils suffisants selon vous pour répondre à toutes vos demandes dans un temps limité ?

Deux affaires sont en cours devant la justice grâce à l'action des associations : les affaires « French Bukkake » et « Jacquie et Michel ». Disposez-vous des moyens d'enquête suffisants pour avancer sur ces sujets ?

Mme Laurence Rossignol. – Comment définissez-vous la pédocriminalité ? Quels critères retenez-vous ? Faites-vous une distinction entre pédocriminalité et pédopornographie ? Enfin, existe-t-il une convergence au niveau européen sur ces sujets, sur la définition de la pédocriminalité et sur la volonté de purger le net, autant que possible, de ces vidéos ?

M. Laurent Somon. – Comment travaillez-vous avec la gendarmerie, qui a mis en place une application Gend'Élus, laquelle renvoie vers d'autres sites comme *cybermalveillance.gouv.fr* ou *stop-djihadisme.gouv.fr*, ou avec la DGCCRF, qui anime le site info-conso.fr ?

M. Pierre-Antoine Levi. – Le projet de loi prévoit d'alourdir les sanctions contre le cyberharcèlement, avec notamment une peine complémentaire de bannissement des réseaux. Pourriez-vous nous donner plus de détails sur la manière dont l'Office compte faire appliquer ces bannissements ? Quels mécanismes seront mis en place pour garantir le respect de ces interdictions ? Enfin, comment envisagez-vous de travailler avec les plateformes de médias sociaux et les autres acteurs pour assurer l'efficacité de ces mesures ?

Mme Cécile Augeraud. – La sémantique est importante. En France, nous avons toujours parlé de pédopornographie et de contenus à caractère pédopornographique. Nous constatons un glissement de langage vers la pédocriminalité. Quoi qu'il en soit, il s'agit toujours d'actes délictuels. Tous les contenus visibles en ligne présentant des actes à caractère sexuel impliquant des mineurs ont un caractère illicite.

Vous avez dit qu'il n'était pas nécessaire de regarder certaines vidéos pour se convaincre de leur caractère illicite, dans la mesure où leur titre serait suffisamment explicite. Certes, mais, en tant que policiers, nous devons les visionner pour pouvoir caractériser les faits.

Nos moyens d'enquête sont importants : ils nous permettent de mener aussi bien des enquêtes sur le fondement des signalements qui nous sont adressés en matière de pédopornographie ou de pédocriminalité, que des enquêtes sous pseudonyme, puisqu'un certain nombre de nos agents sont habilités à procéder à ce type d'investigation visant à détecter des comportements illicites impliquant des mineurs sur les réseaux sociaux. Nous avons ainsi réussi, dans certaines affaires, à faire condamner des individus jusque-là inconnus des services d'enquête.

Les affaires que vous avez citées ne sont pas du ressort de Pharos. L'une d'entre elles a été traitée par la section de recherches de Paris. Pharos n'est pas un service d'enquête de dernier niveau. Notre rôle est d'amorcer les enquêtes afin d'identifier les individus qui se cachent derrière tel ou tel pseudonyme sur Internet, afin de pouvoir transmettre ensuite le dossier au service de police ou de gendarmerie territorialement compétent.

Certains de nos voisins européens, notamment les Pays-Bas, ont une définition plus limitée de la pédocriminalité et de la pédopornographie, ce qui aboutit parfois à des divergences de points de vue sur les contenus susceptibles d'être retirés. On l'a constaté dans une affaire concernant des hébergeurs de contenus manifestement pédopornographiques installés aux Pays-Bas : l'appréciation des autorités néerlandaises était très différente de la nôtre. Il n'y a donc pas d'homogénéité au niveau européen, même s'il existe un consensus global sur le caractère intolérable de la diffusion de contenus pédopornographiques en ligne. On obtient ainsi des retraits de contenus dans 95 % des cas.

Notre action est essentiellement concentrée sur la pédopornographie : en 2022, sur les 89 000 demandes de retrait, 83 % d'entre elles concernaient la pédopornographie.

Sur les moyens de l'Arcom, je ne me permettrai pas de répondre pas en lieu et place de Laurence Pécaut-Rivolier. L'Arcom est la seule apte à juger des moyens qui sont mis à sa disposition.

Mme Catherine Morin-Desailly, présidente. – Mme Pécaut-Rivolier est bien seule !

Mme Cécile Augeraud. – Effectivement, mais elle est entourée de personnes auxquelles nous apportons notre concours et que nous rencontrons régulièrement. Ses équipes sont, comme les miennes, soumises à la difficulté de visionner en permanence des contenus très difficiles. J'y insiste, pour les policiers c'est tout aussi difficile que pour les membres de l'Arcom. Je rappelle que les personnels de Pharos font l'objet d'un suivi psychologique obligatoire.

La plus grande difficulté de l'Arcom, c'est de visionner l'ensemble des contenus. Cette autorité joue pleinement son rôle de contrôle et vérifie chaque contenu pour lesquels nous sollicitons un retrait – et le volume est très important. Pour que les équipes puissent déconnecter de temps en temps, il faut qu'elles soient en effectifs suffisants.

Mme Catherine Morin-Desailly, présidente. – Nous avons auditionné longuement Mme Pécaut-Rivolier, nous connaissons bien le sujet.

Mme Annick Billon. – En lien avec la question de Patrick Chaize sur l'information de Pharos à destination du public, les rubriques de la plateforme sont-elles suffisamment explicites ? D'autres rubriques devraient-elles être créées pour de meilleurs signalements ?

Mme Cécile Augeraud. – Nous avons modifié en avril 2022 l'interface de Pharos pour la rendre plus ergonomique. Nous avons également simplifié, à la demande d'un certain nombre d'internautes, de parlementaires et de partenaires, certaines rubriques. Nous créons une nouvelle rubrique lorsqu'émerge un besoin particulier non couvert par les rubriques existantes. Je pense notamment à la dernière que nous venons d'ajouter, celle liée à la maltraitance animale. L'ensemble des rubriques semble pouvoir répondre aux demandes d'une grande majorité d'internautes. Le nombre de signalements sur la plateforme en est la preuve.

Mme Laurence Rossignol. – Je vous ai demandé quels étaient les critères pour établir la pédocriminalité ou la pédopornographie – je constate comme vous, le glissement de vocabulaire qui crée une certaine confusion. Est-ce la présence d'un mineur de moins de 18 ans ? Pour être très claire, lorsque vous avez été auditionnée devant le Haut Conseil à l'égalité, vous avez indiqué que l'identification de la minorité se faisait sur des critères d'apparence, liés à des signes de puberté. Est-ce bien cela ? Votre réponse a suscité bon nombre d'interrogations chez les personnes engagées dans la lutte contre la pédopornographie. Mais peut-être y a-t-il eu un malentendu dans la manière dont les choses ont été perçues et retranscrites ?

Mme Cécile Augeraud. – Lors de cette audition, j'ai dit que nous appliquions les critères définis par Interpol, qui héberge la plateforme recensant la majorité des images à caractère pédopornographique. Lorsque nous avons de nouveaux contenus à caractère pédopornographique, nous les transmettons pour alimenter la plateforme d'Interpol.

Nous nous fondons donc sur ces critères, dont celui que vous venez d'évoquer, mais nous ne nous contentons pas de ça. Comme je l'ai expliqué, Pharos fait un travail proactif, complété par de la recherche en sources ouvertes. Les policiers ou gendarmes de la plateforme essayent de retrouver en source « ouverte » des images des jeunes filles ou jeunes garçons mis en scène dans les vidéos dont nous disposons afin d'obtenir des éléments permettant de déterminer leur âge. Quand nous avons un doute extrêmement sérieux, nous contactons Europol, Interpol, et nous travaillons en concertation avec l'Office central pour la répression des violences aux personnes qui traite de tout ce qui relève de la pédocriminalité – un office « mineurs » est en cours de création.

Sur les arnaques commerciales, Gend'Élus est un outil parmi tant d'autres. Nous avons une démarche collective et guidée. Nous considérons qu'une victime ne doit pas avoir à chercher l'endroit où elle pourra faire son signalement ou son dépôt de plainte. Nous travaillons avec de très nombreux partenaires – avec la gendarmerie nationale bien sûr, puisqu'elle est partie prenante à la plateforme Pharos, mais également avec le site cybermalveillance.gouv.fr, la DGCCRF, *etc*. Le site cybermalveillance.gouv.fr renvoie vers Thésée et Pharos, tout comme le site *masecurite.interieur.gouv.fr*,

commun à la police et à la gendarmerie. La démarche de la victime est guidée pour qu'elle n'ait pas à tout recommencer si elle s'est trompée de site.

Le travail en collaboration avec la DGCCRF est très profitable pour nous. Elle est, avec cybermalveillance.gouv.fr, l'un des premiers partenaires pour Thésée, puisque ses personnels font un travail de recensement et de détection et qu'ils initient une sorte de travail d'enquête, même si leurs moyens restent limités. Ils nous ont aidés à aboutir sur des enquêtes, et nous les aidons également dans leurs démarches.

Sur le bannissement des réseaux, celui-ci se fera sur le fondement d'une décision judiciaire. L'avantage de cette mesure, c'est qu'elle permet de supprimer non pas seulement le compte concerné, mais l'ensemble des comptes qui pourraient être créés sur une plateforme. L'inconvénient, c'est le non-échange entre les différents réseaux sociaux. Pour davantage d'efficience, il faudrait bannir la personne sur l'ensemble des réseaux à un instant T, car il est extrêmement facile d'aller recréer un compte ailleurs.

Il faudrait lutter de manière plus importante contre l'utilisation d'adresses mails jetables et d'adresses IP *Tor*, associée à des numéros virtuels *Onoff*. Autant de dispositifs qui visent à camoufler une identité et qui complexifient considérablement notre action. S'il semble impossible d'interdire complètement l'utilisation de ces dispositifs – certaines personnes ont besoin d'anonymat –, il faudrait peut-être soumettre cette utilisation à la justification d'un besoin d'anonymat. Certaines plateformes et certains réseaux sociaux sont plus coopératifs que d'autres.

M. Patrick Chaize, rapporteur. – Si l'on imposait une identité numérique réelle à tous les sites, réglerait-on une grande partie du problème ?

Mme Cécile Augeraud. – Je le pense, mais c'est sûrement un vœu pieux. Il me semble assez difficile d'imposer une telle régulation : elle pourrait être assimilée à une censure trop importante. Néanmoins, l'utilisation cumulée et régulière de tous les dispositifs que j'ai cités est un véritable sujet.

M. Pierre-Yves Lebeau. – Le projet de loi prévoit le bannissement des individus multirécidivistes de la diffusion de contenus illicites. Les plateformes et les réseaux sociaux voient arriver la création de certains comptes à l'aide des outils qui permettent de s'anonymiser, tels que *Tor* et les adresses e-mail jetables. Ils peuvent être proactifs, mais encore ont-ils besoin d'une sécurité juridique pour empêcher la création de nouveaux comptes utilisés pour commettre des infractions.

Mme Catherine Morin-Desailly, présidente. – Je vous remercie pour le très bon travail que vous faites. J'ai pu constater que la France est à la pointe sur ce sujet au niveau européen.

Audition de Jean-Noël Barrot,
ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications

Jeudi 8 juin 2023

Mme Catherine Morin-Desailly, présidente. – Messieurs les rapporteurs, chers Loïc Hervé et Patrick Chaize, mes chers collègues membres de la commission spéciale, nous sommes aujourd'hui réunis pour recevoir Jean-Noël Barrot, ministre délégué chargé de la transition numérique et des télécommunications.

Monsieur le ministre, je vous remercie d'avoir pu vous rendre disponible dans un délai assez court pour venir présenter devant les membres de notre commission spéciale ce projet de loi que vous allez porter devant nous dans quelques semaines.

Monsieur le ministre, le Sénat a choisi de constituer une commission spéciale sur ce texte. Elle rassemble des membres de toutes les commissions permanentes, ce qui est assez rare. C'est dire la transversalité du sujet et cela met en exergue le fait que les sujets présents dans votre texte remplissent un large espace qui mobilise toutes les compétences du Sénat.

Ces compétences, justement, je crois que vous avez pu largement les mesurer dans le domaine du numérique. Notre assemblée a été très active dans le cadre des négociations sur les projets de règlement sur les services et les marchés numériques, avec des résolutions européennes adoptées à l'unanimité. Le Sénat a également apporté des contributions décisives au débat sur la protection de l'enfance, avec le rapport sur l'industrie pornographique de la Délégation aux droits des femmes et une nouvelle résolution européenne sur les abus sexuels sur les enfants, ou encore sur la souveraineté économique, avec le rapport de juillet 2022 de la commission des affaires économiques.

Le Sénat appelle de ses vœux une réelle régulation d'Internet, non seulement pour des raisons de souveraineté nationale et européenne, mais aussi pour donner un cadre à un espace qui fait souvent figure de véritable jungle, avec de graves dysfonctionnements : harcèlement sur des enfants, cybersécurité, pornographie, manipulation d'informations, attaques contre le secteur économique…

Je crois pouvoir dire que la voix du Sénat a été entendue, et nous reconnaissons dans les règlements européens et dans le projet de loi de nombreux éléments que nous avions défendus. Nous aurions aimé aller plus loin, mais c'est déjà un motif de satisfaction.

Vous devez, mais je crois que vous y prendrez plaisir, vous attendre à un débat de fond avec de vrais experts, à commencer par les rapporteurs, un débat comme le Sénat sait les mener, et qui nous permettra de donner une nouvelle preuve de la cohérence de nos positions.

Je vous propose donc l'organisation suivante pour nos débats : je vais vous laisser une dizaine de minutes pour nous présenter les grandes lignes de votre projet de loi, puis je donnerai la parole successivement à Patrick Chaize et Loïc Hervé, nos deux rapporteurs, pour des questions. L'ensemble des membres de la commission spéciale pourra alors engager le dialogue avec vous.

Je précise que nos débats sont retransmis en direct sur le site du Sénat.

Monsieur le ministre, je vous donne la parole.

M. Jean-Noël Barrot, ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications. – Merci beaucoup madame la présidente. Messieurs les rapporteurs, mesdames et messieurs les sénateurs, c'est un grand honneur et un grand plaisir d'être parmi vous aujourd'hui. Je vous remercie pour votre invitation, notamment la présidente Catherine Morin-Desailly, ainsi que les rapporteurs Patrick Chaize et Loïc Hervé.

La commission spéciale qui s'est constituée est une assemblée d'experts dont les travaux ont fortement nourri ce projet de loi. Je pense particulièrement aux travaux sur l'industrie de la pornographie (chantier transpartisan d'ampleur), qui ont souligné le potentiel de régulation du secteur. Un grand nombre des recommandations ont été reprises dans le projet de loi. Je remercie Alexandra Borchio Fontimp, Annick Billon, Laurence Rossignol et Laurence Cohen pour leurs travaux. Je voudrais également saluer les rapports de Mme Florence Blatrix Contat et de la présidente, notamment sur les enjeux et les ambitions relatifs au règlement DSA (règlement sur les services numériques et sur les marchés numériques), ainsi que le travail de Sophie Primas sur les enjeux et propositions d'action en vue d'accroître notre souveraineté numérique, notamment sur le marché de l'hébergement en nuage.

Je pourrai citer également les travaux de :

- Rémi Cardon et Anne-Catherine Loisier sur la cybersécurité ;

- Catherine Morin-Desailly, Patrick Chaize, Loïc Hervé, Sylvie Robert et Pierre Ouzoulias sur les sujets de concurrence et de souveraineté économique ;

- Alexandra Borchio Fontimp, Marie Mercier, Xavier Iacovelli et Pierre-Jean Verzelen en matière de lutte contre la haine en ligne ;

- Sylviane Noël sur le contrôle parental ;

- André Gattolin, Catherine Morin-Desailly, Cyril Pellevat et Elsa Schalck sur l'intelligence artificielle, qui constituent un autre sujet d'actualité, même s'il n'est pas traité directement dans le texte.

L'insécurité que nos concitoyens rencontrent au quotidien sur Internet sape leur confiance dans le numérique. Tous les Français sont concernés, particulièrement les plus vulnérables. Nos concitoyens les plus modestes, les plus âgés, les plus éloignés du numérique sont les proies privilégiées des cybercriminels. Nos enfants subissent en ligne des attaques brutales contre leur innocence. Nos entreprises également – que la loi du plus fort place dans la dépendance des géants du numérique –, sont concernées, ainsi que notre démocratie dans son ensemble, soumise aux coups de boutoir incessants des professionnels de la désinformation.

Face à l'accumulation de ces désordres, qui viennent parfois questionner, aux yeux de nos concitoyens, la pertinence de la transition numérique, la France a montré la voie, ces dernières années, au plan national, à travers des textes pris pour lutter contre la désinformation ou protéger l'enfance en ligne. Au niveau européen, la France, notamment, a porté des projets de règlement. Au niveau international, notre pays a pris part à des initiatives multipartites comme l'appel de Christchurch ou le Forum de Paris sur la paix, qui ont permis, à défaut d'ériger des règles contraignantes, d'éveiller la conscience mondiale sur certaines de ces questions.

Avec ce projet de loi, que la Première ministre a souhaité inscrire à l'ordre du jour parlementaire avant l'été, et qui a vocation à être enrichi et renforcé au Parlement, l'objectif est d'apporter des réponses concrètes aux inquiétudes, aux difficultés et aux souffrances que le numérique peut parfois causer dans la vie quotidienne de nos concitoyens.

Ce projet de loi s'est formé à partir des trois affluents que vous avez rappelés, madame la présidente.

Il s'agit d'abord des règlements européens que la France a portés l'an dernier, lorsqu'elle présidait l'Union européenne, pour mettre fin aux abus du numérique, qui nécessitent que nous prenions des mesures d'adaptation afin qu'ils puissent correctement s'appliquer dans notre pays. Le règlement sur les services numériques *(DSA)* fait entrer les grandes plateformes dans l'ère de la responsabilité :

- en leur imposant des obligations de modération des contenus qui leur sont signalés ;

- en leur enjoignant à analyser et corriger le risque systémique qu'elles font peser sur le bien-être et la santé de leurs utilisateurs ainsi que sur la qualité du débat public ;

- en leur interdisant de proposer de la publicité ciblée sur les mineurs, notamment ;

- en les contraignant à faire auditer leurs algorithmes et à ouvrir leurs données aux chercheurs.

Certaines des dispositions prévues par ce règlement ont d'ores et déjà été mises en œuvre par les géants du numérique. Il s'agit d'un compromis européen qui n'est peut-être pas allé aussi loin que ce que la France aurait souhaité, mais qui a la force du compromis européen. Il prévoit un régime de sanctions extrêmement lourd en cas de manquements par les entreprises concernées par ces obligations, avec des amendes pouvant aller jusqu'à 6 % du chiffre d'affaires mondial et une exclusion de l'Union européenne en cas de manquements répétés.

Le règlement sur les marchés numériques (DMA) a pour objet de rétablir l'équité commerciale dans l'économie numérique et de favoriser ainsi l'émergence d'acteurs français et européens, en fixant 26 interdictions qui correspondent à des pratiques commerciales déloyales. C'est le cas par exemple de l'auto-préférence qui consiste, pour l'éditeur d'un moteur de recherche, par exemple, à faire remonter plus haut dans les résultats des contenus produits par une entreprise avec laquelle cet éditeur de moteur de recherche est lié. Cette pratique est déloyale. Elle sera désormais interdite.

Un autre exemple est la pratique qui consiste, pour le vendeur d'un smartphone, à y préinstaller le moteur de recherche, le navigateur et l'assistant personnel. Il y a là une pratique déloyale, puisque c'est de la vente liée. Un autre éditeur d'un moteur de recherche ne peut alors prendre pied sur le marché, tant celui-ci est verrouillé.

Citons aussi l'utilisation à des fins publicitaires, par l'éditeur d'un réseau social, de contenus ou de données collectés sur un autre service édité par la même entreprise du numérique. Il y a là aussi une forme d'accaparement du marché et donc une pratique commerciale déloyale.

Auparavant, ces pratiques déloyales étaient constatées et sanctionnées *a posteriori*, souvent des années plus tard, par les autorités de la concurrence. Désormais, les 26 interdictions sont faites par le règlement *a priori*, sans attendre un délai éventuel de plusieurs années d'instruction de la plainte.

Il faut également souligner la puissance des sanctions, qui peuvent atteindre 10 % du chiffre d'affaires mondial la première fois, puis 20 % en cas de manquements répétés.

Les travaux parlementaires (députés et sénateurs de toutes les sensibilités politiques) ont également nourri ce projet de loi. Je citais tout à l'heure le rapport d'Annick Billon, Alexandra Borchio Fontimp, Laurence Cohen et Laurence Rossignol sur l'exposition des mineurs à la pornographie. Je voudrais citer également le rapport d'Amel Gacquerre, Franck Montaugé et Sophie Primas sur la souveraineté économique. Il comporte un chapitre dédié à la souveraineté numérique et a inspiré les mesures concernant le marché du *cloud*.

Le troisième affluent réside dans les consultations menées, notamment dans le cadre du Conseil national de la Refondation. Le texte instaure des protections nouvelles pour nos concitoyens, pour nos enfants, nos entreprises et collectivités et pour la démocratie.

Au chapitre des mesures visant à protéger nos concitoyens figure notamment le filtre anti-arnaques, qui servira de rempart contre les campagnes de mails et de SMS frauduleux. Nous avons tous reçu un SMS prétendument du Compte personnel de Formation ou de la Sécurité sociale nous invitant à suivre un lien malveillant. C'est ainsi que 18 millions de Français ont été victimes de cybercriminalité l'an dernier, dont la moitié ont perdu de l'argent. Ce sont les Français les plus fragiles, les plus démunis, les plus éloignés du numérique qui se retrouvent spoliés de leurs économies ou entraînés dans la spirale infernale de l'usurpation d'identité, dont ils mettent parfois une décennie à pouvoir sortir. Il faut donc couper le mal à la racine et dévitaliser le commerce de ces mafias qui se sont professionnalisées, et qui ont fait de nos smartphones et tablettes l'instrument de leur racket.

Une peine complémentaire de bannissement des réseaux sociaux est également prévue, durant six mois, pour les personnes reconnues coupables par le juge de cyberharcèlement. Ce phénomène, comme vous le savez, se développe massivement. Il touche toutes les catégories d'âge, plus particulièrement les femmes, qui sont 27 fois plus exposées au cyberharcèlement que les hommes. C'est une violence dont nos consultations ont montré qu'elle se délocalise dans l'espace physique, puisque le cyberharcèlement peut muter en harcèlement physique alors qu'il a commencé sur les réseaux sociaux. Les responsables sont une minorité d'internautes qui se comportent en chefs de meute et propagent la haine et la violence sur les réseaux sociaux, en désignant à leur communauté des victimes vers lesquelles ils déclenchent des raids de haine et de violence. Cette mesure les frappera là où cela fait mal, en les privant de leur caisse de résonance, en confisquant leur notoriété. À l'image de l'interdiction de stade, elle préviendra la récidive. C'est donc une peine complémentaire à une condamnation pour cyberharcèlement, pour une durée de six mois portée à un an en cas de récidive.

Je citerai un troisième exemple des mesures de protection de nos concitoyens instaurées par ce texte, à travers l'encadrement des nouveaux types de jeux en ligne. L'objectif est de définir un régime pionnier et protecteur des utilisateurs pour l'encadrement des jeux numériques fondés sur une technologie émergente du web 3, c'est-à-dire des registres distribués *(blockchain)* qui offrent les garanties nécessaires de protection des mineurs, de lutte contre le blanchiment et de lutte contre le financement du terrorisme, tout en permettant le développement en France de ce type d'activité.

Au chapitre de la protection de nos enfants, deux mesures sont prévues. Il s'agit d'abord du blocage, du déréférencement et d'amendes dissuasives prononcées par l'Arcom à l'encontre des sites pornographiques qui ne vérifient pas l'âge de leurs utilisateurs. Vous avez pu prendre connaissance comme moi de la publication de l'Arcom, il y a quelques jours, confirmant que deux millions d'enfants sont exposés chaque mois, dans notre pays, à des contenus pornographiques. À douze ans, la moitié des garçons de notre pays sont exposés à ces contenus dont nous voulons les préserver, tant les conséquences de cette exposition sont majeures sur leur santé (troubles du sommeil, troubles de l'attention, troubles de l'amélioration, développement de conduites à risque, hypersexualisation précoce, pour ne citer que ces conséquences possibles).

Les sites pornographiques ne vérifient en effet pas l'âge de leurs utilisateurs, malgré l'obligation qui leur est faite par la loi du 30 juillet 2020.

Il faut donc soustraire nos enfants au déferlement d'images pornographiques en accès libre sur Internet, déversées par des mercenaires cupides et irresponsables qui considèrent que les recettes publicitaires valent mieux que la santé de nos enfants. Une procédure est en cours. Le tribunal judiciaire de Paris rendra son verdict le 7 juillet prochain dans le cas de cinq sites pornographiques. Pour l'avenir, les mesures prévues par le projet de loi permettront d'agir plus vite et plus fort.

Une peine d'un an d'emprisonnement est également prévue, complétée par 250 000 euros d'amende, pour les hébergeurs qui ne retireront pas les contenus pédopornographiques qui leur sont signalés par la police ou la gendarmerie en moins de vingt-quatre heures, sur le modèle de la sanction qui s'applique en cas de non-retrait des contenus terroristes. Il existe aujourd'hui une obligation inscrite dans le droit, mais elle n'est pas sanctionnée par des peines, alors même qu'il s'agit d'un phénomène assez massif. Vos auditions passées et à venir vous confirmeront que l'an dernier, 72 000 demandes de retrait de contenus pédopornographiques ont été adressées aux hébergeurs, ce qui est considérable.

Pour les entreprises, le texte prévoit l'interdiction des frais de transfert, l'encadrement des avoirs commerciaux et l'interopérabilité sur le marché de l'informatique en nuage et de l'hébergement en nuage, c'est-à-dire le marché du *cloud*. Celui-ci est très concentré entre les mains d'une poignée d'entreprises qui abusent de leur position dominante, se livrent à des pratiques commerciales déloyales et placent nos entreprises dans une position d'assujettissement. Il faut en finir avec la loi du plus fort et libérer nos entreprises de ce joug. C'est un enjeu de souveraineté, ce qui constitue une priorité de l'action que nous menons avec Bruno Le Maire et l'une du Sénat également, je crois, à la lueur des rapports rendus sur ce sujet. J'ai fait référence à un certain nombre d'entre eux dans mon introduction. Inspirée par les travaux parlementaires, cette mesure permettra aux

entreprises françaises de changer beaucoup plus facilement de fournisseur de *cloud* et de retrouver une forme de liberté en faisant jouer la concurrence.

Pour nos collectivités, il est prévu la création d'une base de données unique pour recenser l'activité des meublés de tourisme. Cette mesure pérennise une expérimentation initiée par la loi Elan, qui a associé cinq collectivités et cinq plateformes de location. Elle a vocation à permettre aux collectivités de mesurer de façon beaucoup plus simple la durée de location des meublés de tourisme sur leur territoire, de façon à faire respecter la limite des 120 nuitées par an.

Sur le plan de la protection de la démocratie, la capacité sera donnée à l'Arcom de mettre en demeure et d'ordonner le blocage des sites Internet diffusant des médias frappés par les sanctions internationales, comme celles que l'Union européenne a prises contre RT France et Sputnik. La désinformation sur Internet est une des menaces les plus lourdes qui pèsent sur la démocratie. Nous l'avons vu avec l'assaut sur le Capitole aux États-Unis et avec la montée des mouvements « antivax » qui aurait pu aggraver la situation sanitaire. Cette mesure complétera notre arsenal pour lutter efficacement et rapidement contre la propagande des ennemis de la démocratie, même si, en matière de lutte contre la désinformation, il faut toujours agir avec la main tremblante et dans le respect de la liberté d'expression.

Ce texte emprunte à vos travaux et a vocation à être enrichi par les travaux de cette commission spéciale et les travaux en séance. Nous soutiendrons des propositions qui pourraient naître dans ce cadre, avec deux lignes rouges. La première sera le respect des compromis trouvés au niveau européen : c'est grâce à ces compromis que nous allons obtenir collectivement des concessions très significatives des géants du numérique. En contrepartie de ces compromis, lorsque, au niveau des États membres, des dispositions sont adoptées et empiètent sur le champ de ces compromis européens, elles deviennent fragiles, car elles peuvent alors être contestées devant les juridictions européennes, qui ont donné raison de façon constante aux plaignants dans de tels cas.

Par ailleurs, face aux drames parfois vécus par nos concitoyens, nous pourrions être tentés d'aller très loin dans les protections que nous souhaitons instaurer dans l'espace numérique. Il nous faut être vigilants à ne pas aller trop loin dans l'empiètement sur les libertés fondamentales, qui constituent le socle de notre démocratie. Connaissant la sagesse du Sénat et son attachement aux libertés fondamentales, je suis convaincu que vous saurez améliorer, par vos travaux, le projet de loi qui vous est soumis.

Mme Catherine Morin-Desailly, présidente. – Merci, monsieur le ministre. Soyez assurés qu'au Sénat, nous tentons toujours de trouver le juste équilibre. Nous sommes attachés à la rigueur, mais aussi aux libertés fondamentales. Nous avons également bien conscience des limites de

l'exercice, s'agissant de règlements européens d'application directe, mais souhaitons malgré tout travailler le mieux possible à l'amélioration du texte présenté ici.

Patrick Chaize va d'abord aborder le volet économique du projet de loi.

M. Patrick Chaize, rapporteur. – Vous indiquez, monsieur le ministre, que nous sommes dans un jeu d'équilibre entre la stricte adaptation du droit national aux règlements européens, alors que la communication gouvernementale se concentre sur les dispositifs nouveaux. Pouvez-vous nous préciser le périmètre que vous souhaitez donner à ce projet de loi, du fait de ces deux contraintes ?

Je vais poser une série de questions sur le filtre national de cybersécurité grand public. Le dispositif déjà existant de filtrage et de retrait des contenus illicites est-il suffisamment efficace ? Qu'est-ce qui justifie la mise en place d'un nouveau dispositif de filtrage des contenus pour les actes quotidiens de cybermalveillance ?

Pourquoi avoir choisi un dispositif de filtrage des contenus ordonné par voie administrative plutôt que par voie judiciaire ?

Le champ des infractions visées par ce dispositif vous semble-t-il adapté et suffisant ? Des infractions supplémentaires correspondant à d'autres actes quotidiens de cybermalveillance devraient-elles être ajoutées ?

Quelle sera l'autorité administrative désignée pour constater les infractions et notifier la mise en œuvre des mesures conservatoires ? Plusieurs autorités administratives seront-elles concernées et, si oui, lesquelles ?

Que pensez-vous de la désignation de la Cnil comme garante du caractère proportionné et justifié des mesures prises par l'autorité administrative ?

M. Jean-Noël Barrot, ministre. – S'agissant du périmètre du texte, des mesures d'adaptation du droit national devaient être prises, afin que les règlements sur les marchés numériques, sur les services numériques et sur la gouvernance des données puissent être appliqués. Il ne faut pas sous-estimer l'importance de ces règlements, qui ont fait l'objet de travaux dans lesquels la France a joué un rôle moteur, et qui permettent de changer la donne, à condition qu'ils soient mis en œuvre. Nous avons des échanges réguliers avec la Commission européenne, qui sera en première ligne pour les faire appliquer. Le poids du Marché unique est le seul susceptible de faire réellement évoluer les pratiques des géants du numérique. Le mérite de ces règlements est d'utiliser la force du Marché unique pour obtenir des concessions significatives de ces acteurs ou en tout cas une mise en conformité avec nos valeurs.

Si nous régulions en ordre dispersé dans l'Union européenne, les géants du numérique se joueraient des disparités nationales de nos régulations et procéderaient à des arbitrages en conséquence, ce qui pourrait favoriser par exemple des pratiques de dumping. Nous ne parviendrions pas à faire fondamentalement changer un certain nombre de pratiques, par exemple en matière de responsabilité sur les réseaux sociaux ou en matière d'équité commerciale.

Les dispositifs existants de filtrage et de retrait des contenus existants ont prouvé leur efficacité. La représentation nationale se penche régulièrement sur ces dispositifs, qu'ils opèrent par voie administrative ou judiciaire. Ils visent tous à protéger les internautes contre différentes catégories de contenus (contenus haineux, atteintes aux personnes, atteintes au droit d'auteur, apologie du terrorisme, désinformation en période électorale, *etc.*).

Cependant, aucun dispositif existant ne permet de couvrir le périmètre et l'objet de ce filtre national de cybersécurité, à savoir les sites intrinsèquement et ontologiquement cybermalveillants, créés par des cybercriminels pour leur permettre de conduire des opérations d'hameçonnage, c'est-à-dire de pillage des données personnelles ou d'injection de logiciels malveillants dans des terminaux pour détourner des moyens de paiement. Tel est l'objectif qui différencie le filtre anti-arnaques des dispositifs de filtrage existants.

Nous avons effectivement prévu un dispositif de filtrage par voie administrative plutôt que par voie judiciaire. Nous nous sommes basés sur une analyse précise et éclairée des phénomènes que nous souhaitions endiguer, ainsi que sur des comparaisons internationales. Aujourd'hui, une campagne d'hameçonnage s'orchestre en quelques clics et touche plusieurs centaines de milliers de nos concitoyens en quelques jours. Si vous avez reçu il y a quelques semaines de tels messages, je vous invite à cliquer sur les liens de ces faux SMS. Bien souvent, quelques jours après la réception du message, le site est d'ores et déjà désactivé : une fois que le cybercriminel a touché suffisamment de comptes, il fait disparaître le site. Il faut donc agir très rapidement, d'où la voie administrative, tout en entourant le dispositif de toutes les garanties et précautions requises. C'est la raison pour laquelle nous avons procédé à la rédaction de cet article.

Quant au champ des infractions visées, notre objectif a été double : nous inscrire dans les canons de la jurisprudence constitutionnelle, en prévoyant un champ d'application précis, afin de minimiser le risque d'atteinte aux libertés protégées par la Constitution. On va automatiquement rediriger des internautes vers une page sécurisée. Il s'agit aussi de nous conformer de la façon la plus stricte à l'esprit de la mesure : il s'agit d'un outil de protection cyber, qui doit donc être limité à la lutte contre la cybercriminalité. Tel est le sens des infractions que nous avons retenues, généralement mobilisées par le juge lorsqu'il est saisi dans une affaire

d'hameçonnage. Quant à savoir s'il faut en ajouter d'autres, nous sommes ouverts à la réflexion, à condition que cela ne dénature pas le dispositif, qui n'a pas vocation à filtrer de façon aveugle tous les contenus à problèmes sur Internet, mais bien ceux qui visent à piller les internautes de leurs données personnelles ou bancaires.

S'agissant de l'autorité administrative désignée pour constater les infractions, le champ d'application du dispositif porte sur des objets qui sont parfois à cheval sur les compétences de plusieurs autorités administratives. Dès lors, plusieurs de ces autorités seront sollicitées. Je pense à l'Agence nationale de sécurité des systèmes d'information (Anssi), au groupement d'intérêt public Action contre la cybermalveillance (Acyma), à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), au Commandement de la gendarmerie dans le cyberespace (COMCyberGend) ou à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) ainsi qu'à des autorités administratives indépendantes telles que l'Autorité des marchés financiers (AMF), l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité nationale des jeux (ANJ), qui chacune reçoit ponctuellement des notifications de sites identifiés comme malveillants. L'objectif est de mutualiser l'information reçue en temps réel par l'ensemble de ces structures et, au travers du filtre anti-arnaques, diffuser cette information le plus rapidement possible aux fournisseurs d'accès Internet afin qu'ils puissent mettre en œuvre le filtre et éviter ce type de cyber-arnaques.

Il nous a paru souhaitable que la Cnil soit associée à ce filtre anti-arnaques, s'agissant d'un régulateur qui est au fait des enjeux de liberté sur Internet et soucieux de la protection de la vie privée des utilisateurs, bien que le filtre n'ait pas vocation à faire intervenir des traitements de données personnelles. Nous n'avons pas décidé unilatéralement de confier cette responsabilité à une personnalité qualifiée rattachée à la Cnil. Nous l'avons fait dans le cadre d'un dialogue avec la Cnil elle-même et pris en compte ses observations sur le dispositif, ainsi que son souhait d'en contrôler l'application. Je pense que la Cnil pourra vous le confirmer lors de son audition.

Mme Catherine Morin-Desailly, présidente. – Abordons le deuxième chapitre, celui de la régulation du marché de l'informatique en nuage. Monsieur le rapporteur, vous avez la parole.

M. Patrick Chaize, rapporteur. – Un encadrement des crédits de l'informatique en nuage est-il prévu à l'échelle européenne ou s'agit-il d'une initiative française ? Autrement dit, n'y a-t-il pas un risque de pénaliser injustement les opérateurs français et leur activité sur notre territoire, si nous sommes les seuls à anticiper l'application du *Data Act* ou à adopter des dispositions plus restrictives ?

S'agissant de l'encadrement de l'informatique en nuage, pourquoi la durée maximale de validité et les conditions de renouvellement ne sont-elles pas fixées par la loi ? Quelle durée et quelles conditions de renouvellement recommanderiez-vous ?

Pourquoi maintenir des frais de migration facturés lorsqu'une entreprise change définitivement de fournisseur de *cloud*, alors que les autres frais sont supprimés ? Comment ces dispositions s'articulent-elles avec le *Data Act*, qui prévoit une période de trois ans pour la suppression de ces frais ?

Concrètement, qu'est-ce que l'interopérabilité des services du *cloud* ? Pourquoi n'est-ce pas défini et précisé dans la loi ? Qu'est-ce que la portabilité des services du *cloud* ? Pourquoi n'est-ce pas précisé et défini dans la loi ?

Enfin, que pensez-vous du rôle attribué à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), du renforcement de ses pouvoirs de sanction, d'enquête et de règlement des litiges ? Est-ce suffisant ? Nous sommes un peu sceptiques quant à sa capacité à assurer cette régulation supplémentaire.

Mme Catherine Morin-Desailly, présidente. – Nous sommes extrêmement attentifs à ces questions, ici au Sénat, monsieur le ministre, eu égard notamment au rapport de Mme Primas et de ses co-auteurs.

M. Jean-Noël Barrot, ministre. – S'agissant de l'encadrement des crédits d'informatique en nuage, la réponse est non : cette disposition n'est pas prévue à ce stade dans le règlement sur les données en cours de discussion au niveau européen, dans le cadre de trilogues (Commission européenne, Parlement, Conseil européen).

L'interdiction des frais de transfert et l'interopérabilité figurent dans le règlement sur les données. Le texte prévoit des clauses d'extinction : dès lors que le règlement sur les données s'appliquera de plein droit, les dispositions contenues dans le projet de loi s'éteindront.

Nous avons introduit les crédits d'informatique en nuage dans le texte, suivant en cela les recommandations des rapports que vous venez de citer. Cette proposition nous semblait en effet pertinente dès lors que l'objectif, ici, est de déverrouiller un marché sur lequel quelques acteurs se sont octroyé une position de monopole en offrant des avoirs commerciaux à l'entrée qui s'apparentent à une forme de dumping. Ils empêchent ou du moins compromettent l'arrivée de nouveaux acteurs sur ce marché. À la sortie, des frais de transfert parfois démesurés sont facturés. Ce sont donc, à l'entrée et à la sortie, des pratiques déloyales mises en œuvre par les acteurs dominants, qui éliminent toute forme de concurrence, plaçant les entreprises utilisatrices dans une situation de grande dépendance.

Comme je le soulignais, les compromis européens ne sont pas toujours pleinement satisfaisants, mais ils présentent le mérite de bénéficier de la puissance du Marché unique. Dans le règlement sur les données ne figurent pas les crédits d'informatique en nuage, mais une mesure nous semble pouvoir être prise au plan national sans entrer dans le champ d'application du règlement sur les données. Nous l'avons vérifiée. C'est la raison pour laquelle cette disposition figure dans le texte.

Ensuite se pose la question de la durée de validité de ces avoirs d'informatique en nuage. Deux possibilités s'offraient à nous. La première aurait consisté à supprimer ou plafonner ces crédits. Nous avons écarté cette possibilité, dans la mesure où de nombreuses entreprises utilisatrices de ces crédits commerciaux sont de jeunes entreprises innovantes pour lesquelles ils peuvent s'apparenter à une forme de financement. Nous avons retenu le principe d'un encadrement dans le temps. Plutôt que de brider les montants qu'une jeune entreprise innovante pourrait solliciter pour cofinancer son développement, cela permet de faire apparaître ces crédits commerciaux pour ce qu'ils sont, c'est-à-dire une forme d'échantillonnage.

Se pose la question de la durée de validité, que le texte renvoie aux décrets. Je crois qu'il est nécessaire d'essayer de faire en sorte que ces avoirs commerciaux demeurent une forme d'échantillon, pour tester la solution de tel ou tel et non rester avec lui durant des années, au point d'être, à un moment donné, enfermé dans la solution d'un acteur dominant. Une durée de validité relativement courte, de trois à six mois, nous paraît donc un point de départ intéressant. Cela suppose sans doute quelques discussions complémentaires. Aussi avons-nous proposé que cela passe par voie réglementaire.

Pourquoi maintenir les frais de migration alors que le texte propose la suppression des frais de transfert ? Si le manque de transparence et de prévisibilité des frais de migration contribue à la dynamique d'enfermement sur le marché, ceux-ci peuvent correspondre à des coûts légitimes et incompressibles pour les fournisseurs de services. En particulier, les frais de migration varient de manière significative en fonction de la complexité du projet de migration considéré. La migration des données RH d'une PME mobilisera moins de ressources que la migration du système d'information d'une grande entreprise bancaire. Il peut ainsi y avoir des frais qui se justifient en cas de migration. Les autorités françaises ont défendu, dans le cadre de la négociation du règlement sur les données, un encadrement basé sur les coûts réels supportés par le fournisseur de services dans le cadre du processus de migration, afin d'éviter de faire peser un poids disproportionné sur les fournisseurs de services français et européens, qui seraient davantage impactés en raison de la difficulté à amortir ces coûts du fait de la plus petite taille de leur base de clients. L'interdiction de la facturation des frais au titre du transfert de données s'inscrit en pleine cohérence avec l'esprit de ce qui a été défendu au plan européen, c'est-à-dire une approche par les coûts.

Une période transitoire est prévue, durant laquelle les fournisseurs ne pourront facturer des frais dépassant les coûts réels supportés au titre des transferts de données.

Au regard de la baisse constante du prix de la bande passante (principal coût lié au transfert de données) et des importantes divergences entre les pratiques des fournisseurs de services alternatifs et dominants, la suppression des frais de transfert de données apparaît comme la meilleure approximation du coût réel supporté par les fournisseurs de services.

Pourquoi la portabilité et l'interopérabilité ne sont-elles pas définies en tant que telles dans le texte ? L'interopérabilité repose sur la compatibilité des formats de données et sur l'accès à des interfaces permettant aux différents services de dialoguer et d'échanger des données, à l'instar des interfaces de programmation applicative (API). Ces principes d'interopérabilité et de portabilité ne peuvent trouver une définition satisfaisante qu'au travers de l'énonciation de spécifications techniques (nature des API, caractéristiques techniques, *etc.*). Les dispositions introduites dans le projet de loi, directement inspirées du projet de règlement européen sur les données, visent à définir, en lien étroit avec les utilisateurs et fournisseurs de services, les éléments techniques qui devront faire l'objet d'un travail de définition collective afin de rendre effectives l'interopérabilité et la portabilité entre les services de *cloud*. C'est donc l'Arcep qui sera le « régulateur » de cette interopérabilité et de cette portabilité.

Vous m'interrogez, monsieur le rapporteur, sur le rôle dévolu à l'Arcep. L'évolution constante du paysage numérique et de l'économie de la donnée crée un contexte dans lequel la proposition d'étendre le mandat de l'Arcep pour y inclure la régulation des services d'informatique en nuage est un choix logique et stratégique, l'Arcep ayant démontré une expertise notable dans les domaines de la régulation numérique, de la normalisation technique et de l'interopérabilité. Elle est donc bien positionnée pour assumer ces nouvelles responsabilités. Son expérience solide en gestion des sujets à enjeux économiques, dans le secteur des télécommunications, renforce cette proposition. Cette approche est alignée avec les objectifs du règlement sur les données, du règlement sur la gouvernance des données et converge avec la vision de la Commission européenne et de nos partenaires européens.

Évidemment, pour permettre à l'Arcep de répondre effectivement à ces nouvelles exigences, une augmentation de personnel est actuellement à l'étude dans le cadre du prochain projet de loi de finances.

Mme Catherine Morin-Desailly, présidente. – Y a-t-il des questions complémentaires sur la question de l'informatique en nuage ?

Mme Florence Blatrix Contat. – Cette dimension du texte me semble importante. Nous y avons longuement travaillé dans le cadre de notre

rapport sur le *DSA*. C'est un marché stratégique, qui conditionne la souveraineté numérique et la compétitivité économique. Nous nous sommes rendu compte, au cours de nos auditions, que ce marché était très largement dominé par des opérateurs extra-européens, comme vous l'avez souligné. Même si les acteurs européens ont progressé en termes de chiffre d'affaires, leur part de marché a reculé, passant de 27 % à 13 % en cinq ans. Il faut mettre un frein à cette hémorragie pour nos entreprises.

Globalement, les PME (petites et moyennes entreprises) et ETI (entreprises de taille intermédiaire) sont encore peu présentes sur ce marché. Il y a donc un enjeu à permettre aux entreprises européennes d'y prendre pied. Ne pourrions-nous pas envisager de ne pas facturer les frais de migration aux PME et TPE (très petites entreprises) compte tenu de ces enjeux ? Pourquoi avez-vous écarté cette option ?

Mme Catherine Morin-Desailly, présidente. – Je prolonge cette question. Les grandes plateformes, pour capter des marchés, font des offres gratuites. Doit-on autoriser les offres gratuites, qui représentent une forme de dumping ?

M. Jean-Noël Barrot, ministre. – Madame la sénatrice, j'entends votre remarque. Le principal objectif poursuivi par ces articles est de permettre de déverrouiller un marché qui concerne aujourd'hui les grandes entreprises plutôt que les petites et moyennes, qui n'ont pas encore fait leur migration vers le *cloud*. Je propose d'examiner l'idée que vous soulevez, notamment afin d'avoir un ordre de grandeur des frais de migration s'appliquant aux PME qui sont en cours de migration vers le *cloud*. Je reviendrai donc vers vous avec un avis plus définitif quant à l'opportunité d'une différenciation du régime qui s'appliquerait à la migration selon la taille de l'entreprise.

Les offres gratuites me semblent s'apparenter à des avoirs commerciaux, madame la présidente. Elles me semblent donc tomber sous le coup de l'interdiction prévue par le texte. Je propose de le vérifier avant de vous apporter une réponse définitive.

Mme Catherine Morin-Desailly, présidente. – Le déverrouillage de ce marché de l'informatique en nuage, appelé à connaître un fort développement, paraît nécessaire sur les plans technique, financier et juridique, car nous avons besoin de solutions souveraines pour nos données sensibles et critiques. Ne pourrait-on pas envisager d'afficher, à travers ce texte, d'une manière ou d'une autre, ce qu'est une donnée sensible, ce qu'est une donnée critique pour notre sécurité nationale et affirmer que ces données doivent relever d'un *cloud* souverain ? C'est une proposition que nous avions faite. Nous sommes très préoccupés par le devenir de nos données de santé. Nous avons maintes fois interrogé le ministre de la santé, vous-même et votre prédécesseur, quant au devenir de la plateforme de

données de santé, aussi appelée *HealthDataHub* et confiée à Microsoft. Nous aimerions que soit rapidement mise en place une solution souveraine.

M. Jean-Noël Barrot, ministre. – C'est effectivement un point très important et je vous remercie, madame la présidente, de le soulever. Le 12 septembre dernier, à l'occasion de l'inauguration du nouveau centre de données d'OVHcloud, Bruno Le Maire a indiqué que l'obligation serait faite aux administrations, en vertu de la doctrine du « *cloud* au centre », de loger leurs données sensibles dans des services d'informatique en nuage certifiés SecNumCloud, c'est-à-dire faisant partie de solutions immunisées contre l'extra-territorialité de législations extra-européennes. Bruno Le Maire a également précisé, le même jour, que la définition des données sensibles serait prochainement présentée dans le cadre de l'actualisation de la circulaire « *cloud* au centre », dans son neuvième paragraphe. Les entreprises, en particulier celles qui se trouvent dans des secteurs critiques et celles qui sont des opérateurs de services essentiels (OSE) ou des opérateurs d'importance vitale (OIV), ont aussi été encouragées à considérer très sérieusement de procéder comme les administrations, faute de quoi des mesures de coercition pourraient, à terme, être prises.

Le schéma de certification du *cloud* est en cours de discussion au niveau européen en vertu du règlement sur la cybersécurité. Celui-ci prévoit que ces schémas de certification peuvent être créés dans un certain nombre de secteurs, auquel cas les États membres peuvent s'y référer de manière volontaire. Une fois créés, ils écrasent les schémas de certification nationaux. Nous consacrons beaucoup d'énergie à convaincre certains de nos amis européens réticents à imposer l'immunité à l'extraterritorialité des législations extra-européennes (et américaine en particulier), car si ce schéma de certification intégrait, dans son niveau de sécurité le plus élevé, les mêmes critères que ceux que nous avons retenus pour notre certification nationale (ce qui est mon souhait), alors les acteurs français et européens qui auront choisi de faire certifier leur solution pourront les faire reconnaître dans le reste de l'Union européenne. En revanche, si ce schéma de certification européen ne retenait pas, dans son niveau de sécurité le plus élevé, l'immunité vis-à-vis de la législation extraterritoriale, notre certification SecNumCloud deviendrait illégale en France, sauf pour des motifs explicites de sécurité nationale. Nous avons des débats serrés avec un certain nombre d'États membres, notamment les Pays-Bas, qui emmènent derrière eux le groupe des pays les plus réticents. Nous avons bon espoir de parvenir à convaincre nos partenaires. Nous n'avions pas, jusqu'à la semaine dernière, publié cette circulaire actualisée. Elle l'a été le 31 mai et fait apparaître, dans son neuvième paragraphe, la définition des données sensibles que les administrations devront désormais, en cas de migration vers l'informatique en nuage, placer dans un *cloud* certifié SecNumCloud.

Parallèlement, nous soutenons les acteurs – notamment français – qui engagent le processus de certification de l'ANSSI afin que leurs offres

soient certifiées SecNumCloud, notamment grâce à un guichet que nous avons ouvert il y a quelques mois. Nous nous y étions engagés le 12 septembre dernier. Il donne un petit coup de pouce financier, en particulier aux petites et moyennes entreprises du *cloud*, lorsqu'elles souhaitent faire certifier une solution sans avoir la taille suffisante pour absorber les coûts fixes induits par le processus de certification.

Mme Catherine Morin-Desailly, présidente. – Il nous importe que les données sensibles des Français et des Européens soient bien protégées contre une législation extraterritoriale qui nous est, pour l'instant, défavorable. Les discussions se poursuivront sur ce point et nous y serons très attentifs.

Je redonne la parole au rapporteur, qui va aborder le chapitre des jeux à objets numériques monétisables.

M. Patrick Chaize, rapporteur. – Monsieur le ministre, si vous deviez définir simplement les jeux à objets numériques monétisables, quelle définition retiendriez-vous ? Quel encadrement de ces nouvelles pratiques de jeux en ligne préconisez-vous compte tenu des risques sociaux et sanitaires qui leur sont associés ? Comment justifiez-vous le recours, dans cet article, à une habilitation à légiférer par ordonnance ?

Mme Catherine Morin-Desailly, présidente. – Vous savez que le Sénat n'aime pas beaucoup habiliter le gouvernement à légiférer par ordonnance.

M. Jean-Noël Barrot, ministre. – Comment définir ces jeux ? Il s'agit de jeux d'un nouveau genre, à la confluence entre les jeux vidéo et les jeux d'argent et de hasard. Ils sont nés de la technologie des registres distribués (la blockchain), qui permet d'isoler la propriété d'un actif numérique. Ainsi, l'on peut désormais détenir un actif numérique en pleine propriété et en quelque sorte l'utiliser comme un support de jeu. J'en prends pour exemple le jeu *Stables*, développé par le PMU et lancé il y a quelques mois. Il repose sur une plateforme numérique permettant aux utilisateurs d'acquérir des jetons qui prennent l'apparence de chevaux de course, reliés à un cheval dans le monde physique et à ses performances dans le monde réel. Cela permet d'organiser des jeux d'un nouveau type.

C'est parce que ces jeux se trouvent à la confluence de deux types de jeux existants (les jeux vidéo et les jeux d'argent et de hasard), et alors que nous avons un écosystème florissant dans le Web 3, qu'il nous paraît important de créer un cadre permettant à l'innovation de se développer en France et en Europe, tout en instaurant un niveau de protection suffisant pour les utilisateurs, sans oublier la lutte effective contre le blanchiment d'argent et le financement du terrorisme.

L'esprit qui nous a guidés est celui qui a présidé à la conception, en 2018, d'un régime « PSAN » (prestataire de services sur actifs numériques) défini pour les cryptoactifs dans le cadre de la loi Pacte.

Ce régime soulevait au départ quelques interrogations, mais il a été conçu de façon à offrir un cadre suffisamment souple pour que l'innovation puisse se développer (de sorte que notre pays reste attractif pour l'innovation) tout en offrant un niveau de protection suffisamment élevé pour susciter un haut niveau de confiance.

Cinq ans plus tard, il apparaît que ce cadre a permis d'attirer en France les principaux leaders mondiaux dans ce domaine et de susciter dans notre pays des vocations entrepreneuriales très importantes. Hier soir encore, nous avons reçu la confirmation du fait qu'un acteur américain de ce domaine avait choisi la France pour s'implanter. Les États-Unis ne s'étaient initialement donné aucun cadre de régulation et lorsque des scandales ont éclaté à l'automne dernier (en particulier avec la société FTX), les autorités américaines ont fait machine arrière, serrant les boulons de façon probablement excessive. Cela a conduit un certain nombre d'acteurs américains à se délocaliser et à quitter les États-Unis au profit de l'Europe. Le cadre européen qui s'appliquera à partir de 2024, dit *Mica*, est directement inspiré du cadre français, qui avait donc fait ses preuves. Celui-ci nous met dans une certaine mesure à l'abri de scandales tels que ceux qui ont éclaté aux États-Unis à l'automne dernier, même si l'on n'est jamais à l'abri d'une fraude massive.

C'est la même démarche, au fond, qui nous guide pour ce type de jeux, c'est-à-dire la construction d'une réglementation protectrice et susceptible de favoriser l'innovation. Si nous définissons ses contours de façon suffisamment judicieuse, elle peut même inspirer la réglementation qui viendra au niveau européen, afin que les acteurs fassent de la France leur camp de base pour leur expansion européenne.

Le recours à une habilitation à légiférer par ordonnance est nécessaire pour pouvoir coordonner dans des délais suffisants des travaux interministériels particulièrement techniques et complexes, qui mobilisent de nombreuses administrations au sein de différentes branches de l'exécutif (ministère de l'économie, ministère de l'intérieur, ministère de l'agriculture, ministère des sports, ministère de la culture) et nécessitent le concours de plusieurs autorités de régulation (ANJ, Cnil, Tracfin, AMF, ACPR, Arcom). Il est par ailleurs nécessaire pour permettre des consultations des différents acteurs du secteur et des secteurs voisins des jeux vidéo et des jeux d'argent et de hasard. Il n'en demeure pas moins que l'objectif est d'avancer le plus rapidement possible dans la création de ces dispositions, afin de pouvoir présenter au plus vite au Parlement des dispositions stabilisées. Nous avons pris note de vos remarques et ferons en sorte que ces dispositions puissent vous être présentées au plus vite.

Mme Catherine Morin-Desailly, présidente. – Nous avons été saisis, comme vous pouvez vous en douter, par l'ensemble des acteurs du monde des jeux plus classiques, qui craignent une distorsion de concurrence à travers l'adaptation d'un texte qui leur serait défavorable et qui

comporterait moins d'exigences vis-à-vis du secteur des jeux en ligne. Nous serons attentifs à ces sujets, afin que le texte proposé, le cas échéant, ne soit pas en quelque sorte un dégonflage d'une architecture classique. Cette perspective serait terrible, car nous avons besoin d'une régulation sérieuse sur l'Internet. Ce sont des jeux d'argent, comme vous l'avez vous-même souligné.

M. Patrick Chaize, rapporteur. – J'en viens aux questions sur les meublés de tourisme. Comment le dispositif de centralisation des données relatives aux meublés de tourisme permettra-t-il aux communes de mieux contrôler la conformité des locations sur leur territoire ? Selon l'étude d'impact du projet de loi, le taux de non-conformité de l'offre de meublés de tourisme atteindrait 34 % à Paris et 46 % à Lyon. Comment expliquez-vous de tels taux?

Quel serait l'organisme unique désigné pour mettre en place la plateforme de déclaration à destination des communes et les plateformes numériques de la location touristique. La proposition de règlement européen sur les locations de courte durée est en cours de négociation. Comment situez-vous cette future régulation au niveau européen et le dispositif prévu par le présent projet de loi ?

S'agissant du droit de la consommation, comment se matérialisera la lutte contre les *dark patterns*, ces interfaces conçues de manière à tromper ou manipuler les internautes-consommateurs ? Est-il prévu de créer une équipe dédiée au sein de la DGCCRF, à l'image de la brigade chargée de l'influence commerciale ?

M. Jean-Noël Barrot, ministre. – Aujourd'hui, les communes concernées par un fort développement de l'activité de meublés touristiques sont contraintes d'aller chercher « à la main » les informations liées la limite des 120 jours applicables à la location de la résidence principale. Grâce au dispositif de centralisation des échanges, elles n'auront plus à formuler qu'une seule demande par plateforme pour obtenir ces informations. Il leur sera donc beaucoup plus facile d'identifier les manquements des loueurs au regard de leur obligation de déclaration et du respect du plafond de 120 jours de location par an applicable aux résidences principales. Cette base de données unique permettra une harmonisation et une fiabilisation des données, ainsi qu'une automatisation des processus. Ce sera donc une vraie simplification.

Le taux de non-conformité réglementaire correspond au pourcentage d'annonces publiées qui ne présentent pas de numéro d'enregistrement. Il est relativement élevé dans l'ensemble des marchés touristiques pour lesquels les données sont mises à disposition par *Inside Airbnb* et collectées par des techniques de moissonnage sur Internet. Il s'agit d'estimations effectuées à partir de données partielles. Le niveau élevé du taux de non-conformité tient à un facteur qui relève des loueurs eux-mêmes. *Ex ante*,

un certain nombre de propriétaires ne respectent pas la réglementation en vigueur, en particulier l'obtention d'un numéro d'enregistrement ou la déclaration de changement d'usage, ou encore la limitation des 120 jours de location pour la résidence principale.

S'agissant de l'organisme unique qui serait désigné pour mettre en place la plateforme de déclaration, plusieurs pistes sont encore à l'étude. Il est certain que le guichet de centralisation ne sera pas géré par une autorité administrative indépendante ni par une autorité publique indépendante, car la désignation d'une telle autorité ne pourrait se faire que par décret et nécessiterait l'intervention du législateur. La création d'une personne morale *ad hoc* n'est pas non plus prévue, afin de ne pas multiplier les personnes morales ou les organisations, étant donné la relative modicité des moyens nécessaires à la gestion de ce guichet. Il est envisagé à ce stade, sans préjuger de la décision finale, l'attribution de cette compétence à un service d'administration centrale ou à un opérateur de l'État existant.

Vous m'interrogez sur l'articulation avec le règlement européen en cours de discussion. Il s'agit effectivement d'une anticipation partielle du projet de règlement européen proposé en novembre 2022 par la Commission européenne concernant la collecte et le partage de données relatives aux services de location de logements de courte durée. La proposition de règlement vise à renforcer la transparence dans la collecte et la transmission de ces données. Les deux objectifs principaux de ce règlement sont l'harmonisation des exigences nationales en matière d'enregistrement et la facilitation de la transmission de données entre plateformes et autorités publiques compétentes. À ce stade, la proposition qui doit être débattue au Parlement européen prévoit que les États membres exigeant des opérateurs numériques qu'ils leur communiquent les données mettent en place un point d'entrée numérique unique. Nous sommes donc parfaitement alignés avec l'esprit du projet de règlement.

S'agissant des places de marché en ligne, l'article 26 du projet de loi comporte une habilitation des agents de la DGCCRF à rechercher et constater les infractions aux dispositions de l'article 25 du règlement sur les services numériques qui prohibe les *dark patterns*. Le règlement sur les services numériques traite des réseaux sociaux et des places de marché. À cet effet, les agents disposent de pouvoirs d'enquête prévus par le code de la consommation. Ils sont considérés comme des pouvoirs de police judiciaire exercés sous l'autorité du Procureur de la République puisqu'il s'agit d'infractions pénales punies à titre principal d'un emprisonnement de deux ans et d'une amende de 300 000 euros. Ce montant peut être porté de manière proportionnée aux avantages tirés du délit à 6 % du chiffre d'affaires mondial. L'ensemble des enquêteurs de la DGCCRF pourront donc être amenés, lors de leurs contrôles en ligne, à rechercher et constater ces « *dark patterns* ». L'enquête sur ce sujet sera diligentée dans le cadre du programme national d'enquête de la DGCCRF pour l'année 2024.

Mme Catherine Morin-Desailly, présidente. – Je donne la parole à Loïc Hervé, rapporteur de l'autre partie du texte.

M. Loïc Hervé, **rapporteur**. – Une très grande partie des acteurs de l'Internet sont établis hors de notre pays et nombre d'entre eux se trouvent hors de l'espace européen. Comment assurer l'effectivité des règles (notamment en matière de sanctions pénales) que ce projet de loi propose de soumettre à notre vote ?

J'en viens à la question de la pornographie et à la régulation de l'accès des mineurs à ces contenus. Dans quelle mesure la transformation de la procédure judiciaire en procédure administrative permettra-t-elle d'être plus efficace pour vérifier qu'un contrôle de la majorité sérieux est bien mis en place ? Les sites semblent déployer des moyens très importants pour s'opposer aux procédures judiciaires. J'imagine qu'ils feront de même dans le cadre d'une procédure administrative.

L'Arcom aura-t-elle suffisamment de moyens pour mettre en œuvre la nouvelle procédure, qui supposera l'établissement de constats par ses agents ?

Peut-être pouvez-vous également préciser les modalités techniques envisagées sur la question du contrôle de l'âge à proprement parler. Ce sujet a été abordé à de très nombreuses reprises dans cette maison, en particulier dans le cadre des travaux de la Délégation aux droits des femmes. Il suscite un certain nombre d'interrogations de notre part et plusieurs de nos voisins européens semblent être légèrement en avance sur nous, notamment l'Allemagne et l'Italie.

Le projet de loi répartit la compétence de mise en œuvre du *RSN* entre l'Arcom, la Cnil et la DGCCRF, l'Arcom étant consacrée en tant que coordinateur des services numériques. Le choix de recourir à plusieurs acteurs procède-t-il d'une spécialisation bienvenue ou crée-t-il le risque d'une dispersion qui rendrait le dispositif moins lisible et moins efficace ? Comment envisagez-vous la coopération entre les différents acteurs ?

Récemment, la commission des lois a adopté une proposition de loi qui sera débattue lundi 12 juin, comportant un amendement permettant d'intégrer le président de l'Arcom ainsi que la présidente de l'Arcep au sein du Collège de la Cnil. Qu'en pensez-vous ? Est-il prévu, réciproquement, qu'un membre de la Cnil siège dans les différentes autorités que je viens d'évoquer ?

Les plateformes disposent-elles, en l'état, des moyens techniques et humains pour mettre en œuvre les nouvelles règles européennes ? Ont-elles déjà adapté leurs moyens et leurs procédures à cette nouvelle réglementation ? Quel est l'état du dialogue entre le gouvernement, votre ministère et les acteurs du secteur, s'agissant non seulement de l'entrée en application du règlement, mais aussi des mesures autonomes prévues par le projet de loi en matière d'interdiction d'accès des mineurs aux sites

pornographiques et de renforcement de la lutte contre les contenus à caractère pédocriminel, voire terroriste ? Comment la France se positionne-t-elle en ces matières, par rapport à ses voisins et partenaires européens ?

Comme le reconnait implicitement l'étude d'impact de votre projet de loi, l'application du règlement ne couvrira pas entièrement certaines dispositions du droit national modifiées, voire abrogées par ce texte. Je pense aux articles 29 et 30, qui vont passer le seuil à partir duquel les plateformes sont soumises à des obligations en matière de transparence et de lutte contre la désinformation. Nous passerions de cinq millions d'utilisateurs nationaux à 45 millions d'utilisateurs européens. Est-ce un choix délibéré de votre part de ne pas prévoir de mesures complémentaires pour les plateformes qui ne seraient plus, dès lors, soumises à ces obligations ? Disposez-vous de données quant au nombre d'opérateurs n'entrant pas dans le champ des très grandes plateformes et des très grands moteurs de recherche au sens du règlement, qui seraient donc soustraits à ces obligations ?

Pensez-vous que la loi du 21 juin 2004 pour la confiance dans l'économie numérique gagnerait en lisibilité et en intelligibilité une fois que ce texte sera adopté ? Il me semble que l'on continue de juxtaposer des dispositifs sans une réécriture globale, ce qui semble, d'abord au plan juridique, mais aussi au plan intellectuel, rendre les choses plus complexes. J'imagine que vous avez des contacts nombreux avec un certain nombre d'acteurs du secteur pour les informer des évolutions envisagées. Peut-être pouvez-vous tracer d'autres perspectives à l'issue de cette discussion parlementaire.

M. Jean-Noël Barrot, ministre. – S'agissant de l'effectivité des règles que le gouvernement entend soumettre à votre analyse, alors que nous avons face à nous des acteurs qui se jouent parfois des frontières, j'avancerai deux éléments qu'il me paraît important de rappeler.

Dans les règlements européens que ce projet de loi permet de faire appliquer correctement, en France comme dans les autres États membres de l'Union européenne, en se donnant des règles communes et en confiant à la Commission européenne, épaulée par les régulateurs nationaux, le soin de faire appliquer ces règlements, on écarte une fois pour toutes le risque d'arbitrages et de dumping réglementaire permettant à des géants du numérique de se réfugier dans des pays considérés comme plus souples ou plus tolérants dans leur appréciation des règles européennes.

Même si, notamment pour le *DSA*, les régulateurs nationaux sont appelés à jouer un rôle important, c'est bien la Commission européenne qui sera en première ligne. Elle veillera à ce que l'application du droit soit uniforme dans les différents États. C'est un point très important, car nous nous sommes souvent heurtés à une forme d'hétérogénéité dans les approches par les autorités chargées de ces sujets, y compris concernant

l'application de règles européennes. Je pense notamment au Luxembourg ou à l'Irlande.

Si certaines sanctions pénales pourraient s'avérer plus difficilement applicables à des acteurs situés loin de l'Union européenne, les mesures de blocage (en particulier celles qui s'appliquent aux sites diffusant des contenus pornographiques ou diffusant des médias frappés par les interdictions telles que celles que l'Union européenne a prises à l'encontre des médias russes) reposent sur des acteurs basés en France, les fournisseurs d'accès Internet. Leur effectivité sera donc immédiate.

S'agissant de l'accès des mineurs aux sites pornographiques, la loi du 30 juillet 2020 précise que l'interdiction d'exposer des mineurs à des contenus pornographiques doit également s'appliquer lorsqu'un site Internet se contente de demander l'âge de l'utilisateur, sans le vérifier sérieusement. Le décret d'application de cette loi a été pris en octobre 2021. La loi et le décret d'application prévoient que l'Arcom mette en demeure un site qui ne vérifie pas l'âge de l'utilisateur. Si au bout de quinze jours, le site ne s'y est pas conformé, l'Arcom saisit le tribunal judiciaire de Paris, qui instruit ensuite l'affaire.

En octobre 2021, l'Arcom a mis en demeure cinq des principaux sites pornographiques de mettre en place un système de vérification de l'âge des utilisateurs. Constatant, quinze jours plus tard, que cette mise en demeure n'a pas été suivie d'effets, l'Arcom a saisi, au mois de novembre 2021, le tribunal judiciaire de Paris. En septembre 2022, le tribunal judiciaire de Paris a convoqué une audience qui rassemble les sites concernés et l'Arcom. Les sites concernés ont brandi à l'audience une question prioritaire de constitutionnalité (QPC). Le tribunal judiciaire de Paris a transmis la question prioritaire de constitutionnalité à la Cour de cassation et ordonné une médiation entre les sites pornographiques et l'Arcom. En janvier 2023, la Cour de cassation a annoncé ne pas transmettre la question prioritaire de constitutionnalité au Conseil constitutionnel. Quelques semaines plus tard, l'Arcom a indiqué sortir de la médiation avec les sites pornographiques. L'Arcom s'est alors tournée à nouveau vers le tribunal judiciaire de Paris, qui a convoqué une audience. Celle-ci a eu lieu en avril 2023 et le délibéré est attendu le 7 juillet prochain. Il aura donc fallu attendre environ un an et demi pour qu'un jugement soit éventuellement rendu. Il me paraît important que nous puissions aller plus vite, en donnant à l'Arcom la capacité, après avoir assermenté ses agents à cet effet, de constater et mettre en demeure, mais aussi d'ordonner plus directement le blocage.

L'Arcom devra d'abord disposer des moyens humains nécessaires pour exercer cette compétence nouvelle. L'Arcom compte actuellement 370 agents (en comptant les 16 antennes territoriales) et dix recrutements sont en cours pour la mise en œuvre des compétences nouvelles qui seraient confiées à l'Arcom par le *DSA*.

La question de la vérification de l'âge a fait l'objet de travaux approfondis par la mission parlementaire. Le texte prévoit que l'Arcom publie, après avis de la Cnil, un référentiel qui indiquera ce que doivent être, au minimum, des dispositions acceptables pour la vérification d'âge. Sans attendre que ce projet de loi soit adopté, il appartient aux sites Internet concernés notamment par la procédure en cours de mettre dès aujourd'hui en place des systèmes de vérification d'âge. Il en existe. Ils ne sont pas absolument parfaits, mais ils permettraient d'éviter l'exposition massive de mineurs aux contenus pornographiques, que l'Arcom a encore dénoncée dans son étude parue il y a quelques semaines.

Pour anticiper sur l'adoption de ce projet de loi, nous avons encouragé des entreprises françaises à se saisir de cette problématique de la vérification de l'âge en ligne et de développer, comme le proposent les recommandations du rapport des sénateurs, des solutions qui soient doublement anonymes, de sorte que le fournisseur de la preuve de majorité ne puisse pas connaître ce pour quoi cette preuve est utilisée. Peut-être le sera-t-elle pour consulter un site pornographique. Peut-être le sera-t-elle pour l'achat de produits alcoolisés, ou encore pour des transactions sur des sites proposant des jeux d'argent et de hasard, qui sont également soumis à des restrictions d'âge. Le site qui sollicitera la preuve de majorité pour donner l'accès à ce service ne doit pas non plus avoir à connaître l'identité de la personne concernée.

Du point de vue de la répartition des compétences entre les autorités et de la mise en œuvre du *RSN* autour du coordinateur des services numériques, le *RSN* est avant tout un règlement transversal qui modélise un régime d'obligation appliqué à un environnement de plateformes intervenant sur une multitude de secteurs économiques. Il est logique que sa mise en œuvre soit organisée de façon distribuée entre les principales autorités de régulation qui disposent, en France, des compétences statutaires dans chaque domaine traité par le *RSN*. Notre choix repose sur une double conviction : privilégier les compétences et les expertises acquises dans chaque domaine (la Cnil pour la protection des données personnelles, l'Arcom sur la problématique des contenus, la DGCCRF pour les pratiques du commerce en ligne), tout en veillant à une coordination et à une synergie efficaces de l'ensemble. Nous sommes conscients des écueils liés à cette gouvernance « distribuée » entre différentes autorités administratives. C'est la raison pour laquelle le projet de loi prévoit des dispositions particulières en matière de dialogue et de consultation parmi ces différentes entités.

Vous soulevez une question qui était évoquée dans l'avis du Conseil d'État, dès lors que le règlement sur les services numériques pourrait « écraser » certaines dispositions de la loi de lutte contre la manipulation de l'information que le Sénat avait passée au tamis de son examen. Il est vrai que le règlement sur les services numériques est un règlement

d'harmonisation maximale, qui interdit en principe le maintien, au niveau national, de législations poursuivant le même objectif, notamment en matière de lutte contre la désinformation en ligne. En conséquence, le projet de loi que nous proposons abroge, comme vous le soulignez, certaines dispositions de la loi relative à la lutte contre la manipulation de l'information, qui prévoit des mesures applicables aux opérateurs de plateformes en ligne. Ceci concerne en particulier les articles 11, 13 et 14 de la loi du 22 décembre 2018.

Néanmoins, ces dispositions abrogées sont couvertes en grande partie par le règlement sur les services numériques. Les articles 11, 13 et 14 de la loi de lutte contre la manipulation de l'information ont des équivalents directs dans le règlement sur les services numériques et les obligations prévues restent donc pleinement exécutoires. Ce règlement prévoit notamment l'obligation, pour les très grandes plateformes et les très grands moteurs de recherche, d'analyser les risques systémiques de désinformation engendrés par le fonctionnement de leurs services (algorithmes, systèmes de recommandation) et de prendre les mesures nécessaires pour les atténuer. Le projet de loi n'entraîne donc pas de recul sur ce point.

S'agissant du code électoral, vous pouvez constater que le gouvernement a suivi l'avis du Conseil d'État et n'a pas procédé à l'abrogation de l'article L. 163-1. Il a seulement procédé à de légères modifications de cohérence avec le *DSA*. Il a été décidé, eu égard à la sensibilité de l'information des personnes en période électorale, de conserver l'obligation, pour les très grandes plateformes et les très grands moteurs de recherche, de faire figurer les informations listées par ces articles. Cette obligation pourra ensuite être abrogée avec l'entrée en application du projet de règlement relatif au ciblage et à l'amplification des publicités à caractère politique – règlement en cours de discussion au niveau européen, à l'étape des trilogues. L'impact de cette modification sera donc quasiment nul dans la mesure où les dispositions abrogées ont un équivalent dans le *DSA* et où celles qui n'ont pas d'équivalent dans le *DSA* seront maintenues.

Enfin, s'agissant de la lisibilité de la loi pour la confiance dans l'économie numérique (LCEN), il est évident que ce texte y introduit des changements importants. La LCEN sert de socle à notre législation pour le numérique. Cette loi fondatrice a porté, depuis vingt ans, un cadre propice et dynamique en faveur de l'économie et de la société numériques. Après vingt ans de résultats, compte tenu de la transformation profonde liée à la numérisation de l'économie, à l'occasion de l'adoption du RSN, il est aujourd'hui indispensable de refonder cette loi. Le projet de loi s'emploie à cette réorganisation du corpus de la LCEN pour le rendre plus logique, lisible et l'articuler avec ces règlements européens nouveaux qui vont continuer à être adoptés. Après celui sur la gouvernance des données, le règlement sur les services numériques et les marchés numériques, viendront le règlement sur les données, celui sur l'intelligence artificielle et d'autres encore, en vue de construire un marché unique du numérique au

sein duquel devront être respectés un ensemble de principes auxquels nous sommes très attachés.

Mme Catherine Morin-Desailly, présidente. – Cela nous oblige à une certaine gymnastique dans l'anticipation de futures transpositions et dans la recherche de cohérence d'un texte à l'autre, du point de vue des dispositifs proposés.

Mme Annick Billon. – Merci, monsieur le ministre, d'avoir balayé un certain nombre de sujets en réponse à nos deux rapporteurs. Nous avons déjà eu l'occasion de nous rencontrer et de vous présenter les conclusions des travaux de la Délégation aux droits des femmes.

Nous avions préconisé la création d'une nouvelle rubrique sur la plateforme Pharos, car il se pose un problème de visibilité. Pensez-vous que la création d'une nouvelle rubrique qui concernerait notamment les actes de barbarie, de violence sexuelle ou de torture, serait de nature à faciliter les signalements ?

Lors de nos travaux au sein de la Délégation aux droits des femmes, nous avons entendu des témoignages extrêmement violents, difficiles à entendre, qui nous ont profondément marqués du point de vue du regard que nous portons sur l'industrie de la pornographie. Le retrait des vidéos serait-il possible selon vous, sans avoir à les visionner, dès lors que dans le titre d'une vidéo apparaît par exemple l'apologie d'un crime ? Serait-il envisageable de permettre le retrait plus rapide de tels contenus, sans nécessairement avoir à visionner ces vidéos pour vérifier ce qu'elles contiennent ?

La question du droit à l'oubli se pose aussi au regard de la demande potentielle de retrait de vidéos, sans contrepartie financière, de la part des actrices. Une actrice de pornographie gagne 400 euros pour une vidéo et il lui est actuellement demandé 4 000 à 5 000 euros pour le retrait d'une vidéo dans laquelle elle apparaît.

Mme Florence Blatrix Contat. – Monsieur le ministre, vous avez évoqué l'inégale diligence des différentes autorités de régulation nationales dans l'application des régulations numériques et indiqué que, dorénavant, la commission en aurait la charge. Lorsque nous avons travaillé sur le *DSA* est apparue la question suivante : la commission se dotera-t-elle des moyens, humains notamment, requis pour exercer cette régulation ?

Lors de nos auditions, qui ont notamment conduit à entendre des acteurs connaissant très bien les réseaux sociaux, nous nous sommes rendus compte qu'il manquait souvent des modérateurs dans chaque langue, notamment en français. C'est une carence dans la lutte contre la désinformation et la haine en ligne. En quoi ce texte permettra-t-il de répondre à cela ?

Mme Catherine Morin-Desailly, présidente. – Je me permets d'insister sur la question du droit à l'oubli, qui a été évoquée à plusieurs reprises au Sénat et qui a fait l'objet d'une de nos préconisations.

M. Jean-Noël Barrot, ministre. – Concernant la question de la nouvelle rubrique, qui était liée, si j'ai bien compris, à celle du retrait de vidéos diffusées par des sites pornographiques, lorsque ces contenus s'apparentent à des actes criminels, nous avons avec ma collègue Isabelle Rome, à l'appui de vos travaux, engagé des discussions avec le Haut Conseil à l'égalité entre les femmes et les hommes, en vue d'explorer les moyens juridiques qui permettraient de caractériser de façon suffisamment précise, y compris du point de vue juridique, des catégories de vidéos dont le retrait serait justifié. Nous devons le faire avec le souci de ne pas franchir la limite de la liberté d'expression et avec à l'esprit la réalité des violences que vous évoquez. Autrement dit, il s'agit de se demander si, de manière suffisamment précise, une vidéo peut être identifiée comme un acte de barbarie et faire l'objet d'un retrait sur injonction de la plateforme Pharos ou des forces de l'ordre, comme c'est le cas pour des contenus de nature terroriste ou de nature pédopornographique. Nous avions évoqué ce sujet. Nous continuons d'y réfléchir et nous n'avons pas encore trouvé la solution.

Le règlement général de protection des données personnelles (RGPD) prévoit le droit à l'oubli dans le cas de données ou d'images personnelles n'ayant pas fait l'objet d'un contrat. Vous proposez de venir écraser un contrat, dans le cas que vous citez, qui est celui des images pornographiques. Nous avons saisi le Garde des Sceaux, qui souhaite constituer un groupe de travail réunissant des experts de la question afin de trouver des réponses satisfaisantes. Ces travaux feront appel au droit des contrats et aux dispositions relatives à la protection de la vie privée des personnes.

Vous m'interrogez, madame Blatrix Contat, sur les moyens de la Commission européenne. C'est une question que je pose chaque fois que je rencontre le commissaire compétent, c'est-à-dire Thierry Breton. Il y a huit mois, nous avions des inquiétudes à ce sujet. Elles se sont dissipées, car 80 ETP (équivalents temps plein) ont été recrutés au sein de la DG Connect et de la DG Comp pour l'exécution de ces règlements. Il y aura des infractions à ces deux règlements et tant que les premières sanctions n'auront pas été prononcées, nous serons extrêmement vigilants et continuerons de faire connaître à la Commission européenne notre exigence forte de voir ces DG dotées de moyens. Il est à noter que, selon l'architecture prévue pour ce dispositif, nous solliciterons de la part des régulés une partie de la prise en charge des moyens nécessaires à leur régulation.

S'agissant de la modération, le *DSA* imposera désormais aux plateformes la mise en place de dispositifs qui devront être par ailleurs audités, avec à la clé des amendes particulièrement lourdes. Nous estimons que cela les conduira à améliorer leurs processus de modération. Ceux-ci ne

passent pas toujours, ou pas intégralement, par des moyens humains : l'intelligence artificielle, notamment, est utilisée et a contribué, sur certaines plateformes, à un retrait beaucoup plus rapide qu'auparavant de contenus qui étaient immédiatement identifiables comme illicites. La diversité de ces moyens de modération doit tenir compte de la variété des langues des pays dans lesquels ces services sont utilisés et le non-respect de ces règles sera sanctionné par des amendes particulièrement lourdes.

Au-delà de l'audit de ces processus de modération et de signalement, toutes les plateformes devront publier de manière transparente les retraits de contenus et le nombre de signalements traités, c'est-à-dire leur activité de modération. Tel est déjà le cas en France.

Mme Toine Bourrat. – Je voudrais aborder le chapitre du cyberharcèlement. Je suis préoccupée par la proposition (contenue dans le projet de loi) consistant à bannir des réseaux sociaux les personnes condamnées pour avoir diffusé des contenus haineux ou violents sur un réseau social. Compte tenu du décalage qui existe entre la vitesse à laquelle fonctionne la justice et la viralité des réseaux sociaux, serait-il envisageable de prévoir des dispositions enjoignant les réseaux sociaux à mieux traiter et mieux réguler les signalements ? Entre le moment où l'on est victime de cyberharcèlement et le moment où l'agresseur potentiel est condamné, je crains que les délais ne soient très longs, ce qui rendrait cette disposition inefficace.

M. Jean-Noël Barrot, ministre. – Effectivement, il y a assez peu de condamnations aujourd'hui et ces condamnations méritent d'être diffusées. Lorsqu'on examine qui étaient les agresseurs de Mila, d'Eddy de Pretto ou de Hoshi, on se rend compte que des personnes se pensant à l'abri derrière un pseudonyme ont participé à des raids de haine et de violence sans soupçonner qu'elles pouvaient être punies par des peines d'emprisonnement. Cette mesure de bannissement qui vient s'ajouter à une éventuelle condamnation ne constitue qu'un des éléments du dispositif.

On peut rappeler certaines des condamnations qui ont été prononcées dans ces cas. Dans l'affaire Mila, douze mois de prison ferme ont été prononcés à l'encontre d'un jardinier âgé de 23 ans, pour des menaces de mort et de viol diffusées sur Internet. En juillet 2021, des peines de quatre à six mois de prison ont été prononcées à l'encontre de onze personnes et deux mois plus tard, une personne ayant menacé Mila de mort a été condamnée à dix mois de prison.

Dans le cas d'Eddy de Pretto, onze cyberharceleurs ont été condamnés en décembre 2022 à des peines de trois à six mois de prison.

Vendredi dernier, une peine de huit mois de prison, dont deux mois de prison ferme, a été prononcée à l'encontre de l'un des cyberharceleurs de Hoshi. Celui-ci devra également verser à l'artiste 5 000 euros de dommages

et intérêts. Cette personne a dit qu'elle n'avait aucune conscience du fait que les actes qu'elle avait perpétrés étaient passibles de sanctions aussi lourdes.

Il nous paraît important que les peines, lorsqu'elles sont prononcées, soient particulièrement lourdes. Dans certains cas, le bannissement des réseaux sociaux ajoutera au caractère très symbolique de ces peines, qui doivent être connues afin que chacun réalise qu'il peut être poursuivi et que ce qui est illégal dans la rue l'est aussi sur Internet.

Mais ce n'est qu'un des éléments du dispositif « à 360 degrés » que nous devons mettre en place pour lutter contre le cyberharcèlement. Il commence avec la sensibilisation, notamment des plus jeunes. Nous allons généraliser à la rentrée prochaine le passeport numérique, c'est-à-dire la sensibilisation de tous les élèves, en sixième, aux risques et aux attitudes à adopter lorsqu'ils sont témoins ou victimes de cyberharcèlement.

Je souhaite aussi que, grâce à la loi d'orientation et de programmation du ministère de l'intérieur et grâce à la loi de programmation de la justice en cours de discussion au Sénat, des moyens viennent renforcer les capacités d'enquête et d'instruction de ce type d'affaires.

Dans le cadre de la loi de programmation du ministère de l'intérieur, il sera désormais possible de déposer une plainte en ligne et d'être accompagné par un avocat lors du dépôt de plainte. Ce sont autant d'éléments qui permettront d'améliorer la prise en compte des plaintes des nombreuses victimes de cyberharcèlement. Peut-être faudra-t-il aller plus loin. Nous étudierons toutes les propositions d'amendements que vous défendrez, tant ce phénomène doit être contenu, d'abord, puis éliminé.

Enfin, le règlement sur les services numériques va imposer aux plateformes un niveau de responsabilité particulièrement élevé. La loi existant en France leur impose, lorsqu'elles ont connaissance de faits de cyberharcèlement, d'y mettre fin, à la condition que ces faits leur aient été signalés. Deux nouveautés vont s'appliquer dès le 25 août au titre du règlement sur les services numériques. D'une part, les plateformes devront – parallèlement au traitement du signalement et à l'élimination du comportement de cyberharcèlement – signaler ces faits de cyberharcèlement aux autorités compétentes. D'autre part, là où les peines encourues actuellement dans le droit français, en cas de non-respect de cette obligation, sont d'un an d'emprisonnement et 250 000 euros d'amende, leur plafond passera à 6 % du chiffre d'affaires mondial. La peine encourue par la plateforme augmente donc de manière très significative.

Mme Catherine Morin-Desailly, présidente. – Vous avez souligné à juste titre, dans l'exposé des motifs, que la Présidence française de l'Union européenne avait été à la pointe de cette grande avancée en 2022. Force est de reconnaître également que le commissaire français, Thierry Breton, s'est montré très actif au niveau européen, où les choses ont

enfin bougé, avec plusieurs textes qui nous sont proposés. Le gouvernement entend continuer de porter de hautes ambitions dans ce domaine. Il faut s'en réjouir. Le Sénat y est très attentif, comme vous le savez. Nous avons néanmoins du mal à comprendre quelle cohérence et quelle visibilité existent lorsque, il y a quelques jours, le Président de la République déroulait en quelque sorte le tapis rouge à Elon Musk, lequel nous défie, quelques jours après, en se retirant du code des bonnes pratiques. Il a d'ailleurs été sévèrement rappelé à l'ordre par Thierry Breton, qui a assuré que le *RSN* s'appliquerait partout, y compris à Twitter, faute de quoi cette plateforme serait déréférencée. Nous avons du mal à comprendre cette fascination pour les représentants des *Big Tech*, dont vous avez dit à juste titre, en préambule, que pour elles, les recettes publicitaires primaient sur toute autre considération, y compris la sécurité des enfants. Nous vous soutenons sur ce sujet. En son temps, François Hollande avait également déroulé le tapis rouge à Mark Zuckerberg, en pleine affaire « Cambridge Analytica ». Le fait d'attribuer la plateforme de données de santé à Microsoft sans appel d'offres nous a aussi particulièrement heurtés. Nous aimerions recevoir des garanties, car nous portons la même ambition que vous. Nous serons regardés au niveau international. Je crois pouvoir dire que le RGPD constitue en quelque sorte un étalon-or. On en parle dans le monde entier, par exemple au sein des assemblées parlementaires de la francophonie. Nous sommes également attendus du point de vue de ce texte. Quelle cohérence et quelle lisibilité lieront ces différentes actions, qui engloberont également la politique industrielle de soutien à nos entreprises du *cloud* européen ?

M. Jean-Noël Barrot, ministre. – Vous avez tout à fait raison. Elon Musk a repris, il y a moins d'un an, un réseau social. Il était auparavant et reste par ailleurs constructeur de fusées et de voitures électriques. En tant que tels, compte tenu de sa position sur ces marchés, comme pour les investisseurs étrangers, nous évoquons avec lui et ses équipes toutes les possibilités d'implantation de sites industriels en France. Nous le faisons non seulement parce que nous voulons revitaliser des territoires qui ont subi de plein fouet la désindustrialisation depuis des décennies, mais aussi parce que lorsque les usines de fabrication de véhicules de M. Musk seront présentes en Europe, elles seront le client d'entreprises qui, en France, concevront des batteries électriques. Nous devons donc, pour le secteur automobile, entretenir avec les constructeurs les meilleures relations, de façon à faire advenir, dans la mutation assez brutale que représente le passage du thermique à l'électrique, la réussite industrielle de cette filière à laquelle nous sommes attachés. Les projets de « gigafactories » que nous avons réussi à attirer sur notre territoire doivent avoir des débouchés et les constructeurs automobiles en font partie.

M. Musk a repris l'an dernier un réseau social qui ne relève pas autant que la construction de fusées ou de voitures de logiques physiques : cette activité relève principalement de logiques humaines. Après un certain

nombre d'expérimentations qui n'ont pas été couronnées de succès, il a fait quelques pas en matière de transparence en ouvrant son algorithme de recommandation en *open source*. Il semble néanmoins rencontrer les plus grandes difficultés à se conformer à nos attentes, notamment en matière de lutte contre la désinformation. L'annonce, la semaine dernière, du retrait de la signature de Twitter du code volontaire de lutte contre la désinformation n'est pas l'aveu du fait que Twitter ne se conformera pas aux obligations existantes, puisque ce code est d'application volontaire. L'on peut d'ailleurs appliquer les mesures du code de bonnes pratiques contre la désinformation sans avoir signé ce code.

Je suis, pour ma part, relativement inquiet, car je ne vois pas de signaux très encourageants quant à la capacité de Twitter à se conformer à cette partie des obligations nouvelles qui lui sont faites par le règlement sur les services numériques, malgré les déclarations répétées qu'Elon Musk a pu faire au Président de la République, au ministre de l'économie et des finances et à moi-même quant à sa ferme intention de conformer Twitter à ses obligations, en particulier celles du *DSA*. Elon Musk ne cesse de répéter que le *DSA* est une bonne régulation. Nous verrons le 25 août si Twitter se conforme à ces obligations. S'il s'y plie, la plateforme pourra continuer d'exercer. Dans le cas contraire, la Commission européenne sera fondée à appliquer une amende très lourde. Je le souhaite vivement, dans une telle hypothèse, car il en va de la crédibilité de ces règlements européens et donc de l'Europe.

Mme Catherine Morin-Desailly, présidente. – Merci, monsieur le ministre, pour ces propos rassurants. Je vous remercie vivement de nous avoir consacré ces deux heures, qui ont été utiles. Je pense que des échanges auront encore lieu entre nous d'ici l'examen du texte. Certaines propositions du Sénat seront mises en débat au sein de notre commission pour pouvoir parfaire le sujet. Nous allons travailler à un rythme soutenu d'ici début juillet.

Table ronde des régulateurs

Mardi 13 juin 2023

Mme Catherine Morin-Desailly, présidente. – J'ai le plaisir d'accueillir Roch-Olivier Maistre, président de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), Laure de La Raudière, présidente de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), et Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (Cnil).

Mesdames les présidentes, monsieur le président, notre Commission spéciale a été constituée afin d'examiner le projet de loi visant à sécuriser et réguler l'espace numérique. La variété des missions que vous remplissez suffit à souligner l'ampleur de ce texte, et plus profondément l'orientation qui est la sienne et que je crois nous approuvons tous, qui est de mettre enfin en place une régulation efficace du monde numérique.

Monsieur Maistre, l'Arcom est, avec le temps et de multiples projets et propositions de loi, devenue le grand régulateur des contenus numériques, à tel point que votre désignation comme coordinateur pour les services numériques en application de l'article 49 du Règlement sur les services numériques (RSN) n'a souffert d'aucune contestation.

Le projet de loi redéfinit également votre mission en matière de contrôle de l'accès des sites à caractère pornographique, sujet très suivi par de nombreux membres de la commission spéciale, avec trois rapporteurs sur quatre du rapport de la Délégation aux droits des femmes sur l'industrie pornographique : Annick Billon, Alexandra Borchio Fontimp et Laurence Rossignol, sans oublier bien sûr Marie Mercier, à l'origine de l'article 23 de la loi du 30 juillet 2020 qui n'a jamais été réellement appliquée.

Je n'oublie pas l'article 4 qui étend votre compétence au numérique pour la mise en œuvre des mesures restrictives au niveau européen. Je réitère notre souhait que vos moyens soient à l'avenir au niveau de vos missions.

Madame de La Raudière, l'Arcep se voit attribuer le rôle de gendarme de l'informatique en nuage, ou « *cloud* », et ce sera au cœur du suivi de l'application des dispositions relatives à la régulation, à l'interopérabilité, à la portabilité des services d'informatique en nuage ainsi que des dispositions relatives au service d'intermédiation des données. Vos pouvoirs d'enquête, de sanction et de saisine sont ainsi renforcés, des mesures essentielles pour mieux affirmer notre souveraineté numérique dans les prochaines décennies. Cela soulève bien sûr de redoutables questions techniques et juridiques.

Enfin, madame Denis, la Cnil est également placée au cœur des enjeux numériques, et ce n'est pas un hasard si deux membres du Sénat de votre collège sont également membres de la Commission spéciale, notre rapporteur Loïc Hervé et Sylvie Robert. Car « l'or noir » du numérique, ce sont les données personnelles, mais aussi les données de nos administrations et de nos entreprises, et ces données doivent faire l'objet d'une protection toute particulière, encore plus à l'heure de l'Intelligence artificielle.

Il nous faut donc à chaque fois, je pense notamment au contrôle de l'âge, équilibrer entre les aspirations légitimes de protection des mineurs, et la collecte de données. Vous serez ainsi chargée avec l'Arcom de l'élaboration du référentiel prévu à l'article 2, mais vous aurez également à intervenir sur le déploiement du filtre « anti-arnaques » prévu à l'article 6, la Cnil étant désignée comme autorité garante du caractère justifié et proportionné des mesures prises dans le cadre de ce dispositif, ce qui ne constitue pas un petit rôle.

Je vous propose donc l'organisation suivante : je vais demander à chacun d'entre vous d'exposer les enjeux propres à son autorité dans le projet de loi, et les éventuels points de vigilance.

M. Roch-Olivier Maistre, président de l'Arcom. – Merci madame la présidente pour votre invitation. Je suis très heureux de retrouver ce matin les membres de la Commission spéciale, et je veux souligner d'emblée combien l'Autorité est sensible à la confiance que le Parlement lui manifeste. Grâce à cette confiance, cette autorité aura été très singulièrement transformée.

Le projet de loi qui nous réunit est bien évidemment important, notamment pour la mise en œuvre du Règlement européen sur les services numériques, qui va changer la donne en Europe, puisqu'il s'agit du premier texte au niveau européen qui s'attache à réguler les grands acteurs du numérique.

Au préalable, je souhaite souligner trois points.

Tout d'abord, la nécessité et l'importance de l'inter-régulation aujourd'hui, car les acteurs que nous avons en face de nos Autorités sont en grande partie les mêmes. Avec Marie-Laure Denis et Laure de La Raudière, mais également d'autres autorités, nous avons eu à cœur, depuis le début de nos mandats respectifs, de tisser des liens étroits de confiance et de collaboration quotidienne qui sont essentiels. L'Arcep comme la Cnil sont pour nous des interlocuteurs très importants dans la mise en œuvre de notre action.

Le deuxième point de vigilance réside dans la cohérence des textes nationaux et des textes européens. La régulation que nous déployons possède une dimension toujours plus européenne, et l'Arcom joue un rôle central au sein du Groupe des régulateurs européens (ERGA). Nous dialoguons avec la Commission sur beaucoup de textes, comme la directive « Services de médias audiovisuels », la mise en œuvre du RSN, la législation

européenne sur la liberté des médias, sur laquelle vous allez travailler prochainement. L'articulation des textes nationaux et européens constitue donc un élément très important.

Le troisième point sur lequel nous serons très attentifs concerne la liberté de communication. Nous devons ainsi toujours veiller à l'équilibre entre les mesures de protection des publics, en l'occurrence des plus jeunes, et la protection d'une liberté essentielle, celle de communication.

À l'égard du texte qui est soumis au Parlement aujourd'hui par le Gouvernement, l'Arcom a rendu un avis favorable. Je rappelle que ce texte comporte trois types de données. Tout d'abord, une première série de dispositions ayant trait à la protection des mineurs en ligne, à l'égard en particulier des sites pornographiques. La sénatrice Marie Mercier pourra le souligner : ce texte vise à répondre aux difficultés que nous rencontrons depuis la loi de 2020 sur les violences conjugales, en raison de manœuvres dilatoires de la part des sites de l'industrie pornographique. Depuis l'adoption de ce texte en 2020, ces sites n'ont pris aucune initiative pour s'y conformer, et ont multiplié toutes les initiatives juridiques que permet un État de droit pour faire obstacle à sa mise en œuvre.

L'Arcom a combattu pied à pied pour déployer cette mise en œuvre par les procédures de mise en demeure que permet le texte. Chacune d'entre elles ont été contestées devant les juridictions *ad-hoc*, puis par une saisine du tribunal judiciaire de Paris pour demander le blocage de ces sites. Nous attendons maintenant la décision du tribunal, prévue le 7 juillet prochain. Nous formons le vœu que notre demande de blocage soit suivie, en ayant la conviction que rien ne bougera tant que cette décision n'aura pas été rendue.

Nous accueillons donc favorablement le texte qui vous est proposé aujourd'hui, et qui doit permettre à l'Autorité de disposer elle-même d'un pouvoir de blocage, et d'une capacité de demander le déréférencement de ces sites sur les moteurs de recherche s'ils ne se conforment pas aux dispositions du code pénal en matière de protection des mineurs. Nous formons néanmoins avec la Cnil une proposition conjointe de rédaction de texte, comme nous l'avons évoqué avec le rapporteur Loïc Hervé pour une meilleure articulation entre les articles 1 et 2, qui ont des finalités un peu différentes. Nous proposons également d'instaurer avant la mise en œuvre d'une procédure coercitive engagée sur le fondement de l'atteinte à la vie privée, une procédure de consultation formelle de la Cnil par l'Arcom. Le texte présente en effet une double finalité : la protection des mineurs, mais également une dimension touchant à la protection de la vie privée.

Ce texte ne met pas à l'abri de difficultés contentieuses. Lorsqu'il sera adopté, nous n'échapperons pas à des procédures, et à une question prioritaire de constitutionnalité (QPC). Beaucoup des sites évoqués sont localisés à l'étranger, ce qui complexifie la situation.

La deuxième dimension du texte a trait aux chaînes étrangères. Cette proposition découle de ce que nous avons vécu avec les événements se déroulant en Ukraine. Nous avons été dès le début du conflit confrontés à la question de la suspension de chaînes diffusant de la propagande russe, ce qui a donné lieu à des décisions de sanctions d'application immédiate directe adoptées par la Commission européenne. Du fait de ses compétences, l'Arcom a participé à la mise en œuvre de ces sanctions, et a prononcé elle-même des mesures de blocage. Mais nous avons constaté des cas de contournements, auquel le cadre juridique actuel n'apportait pas de réponse satisfaisante. Le signal de la chaîne RT, pourtant bloqué, a ainsi été repris sur le site *Odysee*. Nous avons alors été confrontés aux lacunes pour assurer le blocage effectif de cette diffusion.

Le texte vise précisément à renforcer l'efficacité de la mise en œuvre des mesures de sanctions décidées par l'Union européenne à l'encontre de chaînes étrangères, en application de l'article 215 du Traité. Le texte renforce les pouvoirs du régulateur, en lui donnant un pouvoir d'injonction et de retrait auprès des services qui diffuseraient ou hébergeraient des contenus de médias eux-mêmes sous sanctions, avec en cas d'inaction, la possibilité sous 72 heures de demander le blocage et le déréférencement du site contrefaisant aux fournisseurs d'accès et aux moteurs de recherche.

Dans notre esprit, l'objectif est de s'attaquer aux mesures de contournement d'une décision adoptée par l'Union européenne, et non d'aller sur un contrôle contenu par contenu, site Internet par site Internet.

Comme pour les articles précédents, nous devons avoir conscience des difficultés que nous rencontrerons pour la mise en œuvre des sanctions financières à l'égard d'éditeurs ou d'hébergeurs établis partout dans le monde. Le recouvrement financier sera donc probablement très ardu.

La dernière disposition, très importante, concerne la désignation du coordinateur pour les services numériques *(DSC)*, l'un des éléments de la gouvernance du nouveau règlement européen sur les services numériques. Il s'agit d'un texte très important pour nous, car il parachève la création de l'Arcom en la désignant comme autorité de coordination nationale *(DSC)* en France pour la mise en œuvre de ce texte. Pour nous, la dimension fondamentale dans ce texte réside dans le *C* de *DSC*, à savoir cette mission de coordination que nous porterons en liaison étroite avec la Cnil. Je n'oublie pas la Direction générale de la concurrence, puisque des dispositions du texte visent des questions de contrefaçon, qui touchent au droit de la consommation. Dans notre fonction de *DSC*, nous aurons à cœur d'organiser la coordination avec les autres autorités nationales concernées par ce texte pour assurer sa bonne application.

Nous nous réjouissons également que le texte mette en lumière l'articulation entre l'Arcom et le PEReN, service national créé pour mettre à disposition de l'ensemble des administrations françaises et des autorités

administratives des compétences techniques et des expertises rares. Cette collaboration sera pour l'Arcom précieuse dans la mise en œuvre de ce Règlement européen.

Par ailleurs, la mise en œuvre de ce texte va nécessiter une étroite collaboration avec la Commission européenne, car le règlement prévoit un niveau d'obligation différent en fonction de la taille des plateformes. Les plus importantes d'entre elles (Facebook, Twitter, TikTok, Google…) seront sous un contrôle plus direct de la Commission européenne en liaison avec les autorités nationales désignées par chaque pays, dont l'Arcom pour la France. Ce Conseil organisé autour de la Commission européenne devra donc fonctionner de manière fluide. De la même façon, nous devrons avoir une articulation étroite avec nos homologues étrangers, dont l'Irlande qui héberge nombre de plateformes. J'étais en Irlande il y a très peu de temps pour précisément organiser ce flux de relations.

Enfin, madame la présidente, je suis sensible aux vœux que vous avez exprimés pour le renforcement des moyens de l'Autorité. Nous avions obtenu dans le cadre de la loi de finances pour 2023 la possibilité de créer quelques emplois supplémentaires, et nous souhaitons que la loi de finances pour 2024 permette de compléter ce mouvement pour doter des bons profils notre direction des plateformes, créée il y a deux ans et demi, et chargée du volet de la régulation des acteurs du numérique. Il s'agit en effet d'une régulation d'un nouveau type qui fait appel à des techniques nouvelles, et il est donc important qu'elle dispose des moyens pour mener à bien ses missions.

L'Arcom exprime donc un avis favorable sur le texte, avec quelques petites observations notamment sur la protection des mineurs, sur laquelle il est sans doute possible d'optimiser la rédaction.

Mme Catherine Morin-Desailly, présidente. – Je vous remercie monsieur le président, je passe maintenant la parole à la présidente de l'Arcep.

Mme Laure de La Raudière, présidente de l'Arcep. – Merci madame la présidente.

Messieurs les rapporteurs, mesdames et messieurs les sénatrices et sénateurs, madame la présidente de la Cnil, monsieur le président de l'Arcom, je suis très heureuse d'être aujourd'hui parmi vous pour vous donner l'avis de l'Arcep sur le texte de loi. Nous sommes concernés par le titre III, qui vise à renforcer la confiance et la concurrence dans l'économie de la donnée, et renforcer l'innovation dans le domaine du numérique.

L'Arcep a été créée au moment de l'ouverture du marché des télécoms en 1997 avec comme objectif le développement de la concurrence et de l'innovation. D'autres compétences nous ont été données par la suite, comme la définition des normes permettant l'interopérabilité et la portabilité dans le domaine des réseaux des télécommunications. Nous sommes

également le garant de la neutralité de l'Internet qui favorise l'innovation et la liberté d'expression. Le règlement de la neutralité d'Internet a été proposé par la Commission européenne pour garantir à l'ensemble des acteurs d'avoir accès à Internet sans discrimination, et aux utilisateurs d'accéder à l'ensemble des contenus. Nous avons également travaillé sur l'ouverture des marchés numériques, en amont du règlement européen sur les marchés numériques (RMN). L'Arcep a rendu un rapport à propos des terminaux comme maillons faibles de la neutralité d'Internet. Les smartphones étaient identifiés comme des lieux où les gens étaient prisonniers. La Commission des affaires économiques du Sénat avait à ce sujet déposé un texte en amont du RMN pour déverrouiller ce marché numérique.

L'Arcep possède donc une culture d'ouverture des écosystèmes numériques. Nous sommes une autorité pro-innovation et pro-concurrence, et un régulateur économique sur le champ des télécoms ayant élargi progressivement notre action sur le champ du numérique. Nous attendons avec beaucoup d'intérêt les nouvelles compétences qui s'inscrivent en continuité de nos réflexions, comme l'interopérabilité et la portabilité des services *cloud*, ou concernant l'autorité en charge de la régulation de ce nouveau type d'acteurs que sont les prestataires de services d'intermédiation de données.

L'objectif du texte est de déverrouiller le marché du *cloud*, aujourd'hui fortement concentré autour de quelques acteurs principalement américains, situation renforcée par des pratiques qui verrouillent les utilisateurs sur les plateformes. Le sujet est abordé dans l'article 6 pour lequel l'Arcep n'est pas compétente, et qui est délégué à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). Le texte confie à l'Arcep la définition des spécifications et des modalités permettant l'interopérabilité et la portabilité des services *cloud*. Les freins sont en effet à la fois commerciaux, contractuels, mais aussi techniques.

Le texte prévoit la mise en place d'interfaces d'application pour permettre le transfert, et permet pour les services *cloud* d'infrastructure une équivalence fonctionnelle. Ces prévisions sont cohérentes par rapport à la position du Conseil au niveau européen, dans le cadre des discussions actuellement en trilogue pour le règlement européen du *Data Act*.

Vous allez légiférer sur les articles concernant le *cloud* en amont de l'adoption définitive du règlement *Data Act*, et nous pensons qu'une vigilance particulière doit être apportée aux articles concernant l'interopérabilité et la portabilité du service de *cloud*. Il serait souhaitable de ne pas trop détailler pour laisser à la régulation la possibilité d'évoluer en fonction de ce qui sera décidé *in fine* sur le *Data Act*. L'Arcep considère que les rédactions et les définitions proposées permettent cette évolution, et sont donc bienvenues.

Nous sommes également concernés par l'application du *Data Governance Act*, adopté en 2022 au niveau européen, qui nécessite de désigner une autorité indépendante, notamment pour la régulation des prestataires de service d'intermédiation de données. Ces entités vont permettre l'échange de données sur un marché, en mettant en place une plateforme technique mais aussi contractuelle pour assurer des échanges de données en toute confiance entre les acteurs d'un secteur.

L'opérateur Hub One, filiale d'Aéroports de Paris (ADP), souhaite ainsi développer ce type de plateforme d'échange de données en situation de confiance, avec l'ensemble des clients d'ADP, pour améliorer le service rendu aux passagers et aux différentes entreprises travaillant sur les aéroports.

Cette partie du texte prévoit une coopération avec la Cnil, détaillée avec trois mécanismes. Le premier est un mécanisme général prévoyant que l'Arcep saisisse la Cnil avant toute décision des pratiques des prestataires de service d'intermédiation de données de nature à soulever des questions liées à la protection des données personnelles. Un mécanisme spécifique est lié à la labellisation et aux réclamations éventuelles concernant les prestataires de services d'intermédiation de données, et une autre concerne les procédures de sanction.

La rédaction actuelle du texte nous paraît correspondre à nos besoins d'échanges avec la Cnil, sachant que le Règlement européen du *Data Governance Act* prévoit que les dispositions concernant les prestataires de services d'intermédiation de données se font sans préjudice de celles concernant le Règlement général sur la protection des données (RGPD). Par ailleurs, le texte européen prévoit que l'ensemble des autorités concernées exerceront toujours leur rôle. Nous pourrions ainsi saisir l'Autorité de la concurrence, ou l'Agence nationale de sécurité des systèmes d'information (Anssi) pour leur demander un avis sur certaines pratiques des prestataires de services d'intermédiation de données. Nous serons ainsi amenés à poursuivre nos coopérations avec les hautes autorités indépendantes, ce qui n'est pas une pratique nouvelle, comme l'a précisé Roch-Olivier Maistre : l'Arcep et l'Autorité de la concurrence se saisissent régulièrement l'une l'autre, et nous disposons avec l'Arcom d'un pôle commun qui fonctionne bien, pour travailler sur des sujets comme les enjeux environnementaux du numérique.

Enfin, nous serons très vigilants, dans notre mise en œuvre de l'interopérabilité et de la portabilité des services *cloud*, sur les enjeux et les évolutions du texte européen. Faut-il légiférer maintenant ou attendre le règlement européen ? L'intérêt de légiférer maintenant permettrait de monter en compétences, de rencontrer les acteurs, de comprendre le système. L'interopérabilité et la portabilité des services *cloud* représentent un enjeu complexe, et l'anticipation du règlement européen peut donner à la France une avance en matière de compétences. Nous devrons recruter pour ce sujet,

et du personnel sera mobilisé en interne. Un important travail en amont, notamment auprès des acteurs, doit être mené avant de prendre des décisions de spécifications et de modalités de l'interopérabilité. La nouvelle compétence de la distribution de la presse nous a demandé un an et demi avant de prendre les premières décisions majeures. Ce sujet est sensible d'un point de vue économique, mais moins d'un point de vue technique.

Mme Catherine Morin-Desailly, présidente. – Merci madame la présidente. Il est vrai que nous avons l'impression que ce texte permet d'anticiper les sujets que vous avez évoqués, et le Data Act est toujours en cours de discussion. Vous nous avez mis en garde de ne pas trop préciser le texte, ce qui met un peu dans l'embarras le législateur français, car nous considérons que nous avons notre mot à dire. Par ailleurs, nous avons bien noté ce décalage temporel dans l'adoption des règlements européens.

Je donne maintenant la parole à Marie-Laure Denis pour la Cnil.

Mme Marie-Laure Denis, présidente de la Cnil. – Merci, madame la présidente.

Messieurs les rapporteurs, mesdames et messieurs les sénateurs, je vous remercie d'avoir sollicité la Cnil pour cette table ronde chargée d'examiner le projet de loi visant à sécuriser et à réguler l'espace numérique, et qui traduit le souci de votre Commission spéciale de veiller à la bonne articulation entre les autorités indépendantes représentées ici pour la mise en œuvre de ces dispositions.

Dans un avis adopté le 20 avril dernier, la Cnil s'est prononcée sur les dispositions de ce texte en lien avec la protection des données à caractère personnel. Je ferai en préambule trois remarques d'ordre général.

Tout d'abord, ces nouvelles dispositions de la loi s'appliqueront sans préjudice de celles fixées par le RGPD. À cet égard, en cas de conflit entre ces dispositions et le droit de l'Union en matière de protection des données à caractère personnel, ce sont les dispositions pertinentes en matière de données personnelles qui prévalent, et il reviendra à la Cnil de veiller à leur pleine effectivité.

Ensuite, nous constatons une multiplication des réglementations régissant le numérique, tant du fait des nombreux textes européens adoptés ou en cours d'adoption que de nouvelles réglementations nationales. Ces régimes prévoient l'intervention d'un nombre croissant de régulateurs dans l'espace numérique. Si la pénétration croissante des technologies numériques dans toutes les activités humaines est évidente, l'inflation normative et la multiplicité des textes comportent deux risques : la complexité juridique et donc l'insécurité juridique dans l'articulation de ces textes, et celui d'une régulation moins cohérente ou moins efficace de l'espace numérique. C'est la raison pour laquelle des mécanismes de coordination entre les régulateurs sont prévus, et je me permets d'attirer

votre attention sur ces enjeux d'articulation et de coordination qui me paraissent essentiels.

Enfin, la Cnil partage les préoccupations du Gouvernement, et son objectif de sécuriser l'espace numérique. Elle s'y emploie au quotidien, au travers de son action en matière de cybersécurité et en promouvant des actions d'éducation au numérique. Néanmoins, certaines des mesures proposées par le projet de loi soulèvent des questions importantes en matière de protection des libertés fondamentales des internautes, dont le respect de la protection de la vie privée. Nous appelons donc le Parlement à poursuivre cette réflexion sur le juste équilibre nécessaire entre sécurité et liberté.

Je souhaite maintenant aborder quelques dispositions en particulier.

Tout d'abord, s'agissant des dispositions de vérification de l'âge sur Internet, la Cnil réaffirme son soutien à l'objectif poursuivi de protection de la jeunesse. Les systèmes de contrôle de l'âge présentent des enjeux importants en matière de protection des données personnelles, et la Cnil a émis plusieurs recommandations à ce sujet. Le texte prévoit que la Cnil sera consultée par l'Arcom sur le projet de référentiel qui fixera les exigences techniques permettant d'empêcher les mineurs d'avoir accès à des contenus pornographiques. En pratique, nous travaillons déjà main dans la main sur ce sujet avec l'Arcom pour qu'on ne puisse pas opposer la protection des mineurs et la protection des données personnelles.

Dans son avis, le collège de la Cnil a appelé à préciser l'articulation entre les différentes mesures susceptibles d'être prises, évoquées par Roch-Olivier Maistre. Par ailleurs, dès lors que nous constatons au quotidien le besoin d'un dialogue continu sur ces sujets très techniques entre l'Arcom et la Cnil, il serait pertinent d'introduire un mécanisme permettant formellement à l'Arcom de saisir la Cnil pour avis dans le cadre d'une procédure de mise en demeure ou de sanction d'un opérateur de sites pornographiques, en cas d'enjeux de protection de vie privée.

Ensuite, l'article 5 du projet de loi prévoit de créer une peine de bannissement numérique infligée aux personnes condamnées pour diverses formes de harcèlement en ligne, qui leur interdirait d'accéder à leurs comptes sur la plateforme en cause, et d'en créer de nouveaux. Je vous fais part de mes interrogations sur les solutions concrètes qui pourraient être mises en œuvre, afin notamment d'empêcher la création de nouveaux comptes par la personne condamnée. En tout état de cause, les mesures pour bloquer les comptes existants et empêcher la création de nouveaux comptes, qui ne sont pas précisées dans le projet de loi, devront être proportionnées à l'objectif poursuivi. Ces dispositions ne devraient pas conduire les réseaux sociaux à collecter des données supplémentaires, ou à mettre en œuvre des traitements intrusifs pour l'ensemble de leurs utilisateurs, alors que ces mesures ne concerneront qu'un nombre limité de ces derniers.

En outre, je m'interroge sur la pertinence d'un blocage qui reposerait sur l'adresse IP, dans la mesure où il pourrait être facilement contourné, par exemple avec un VPN, et que cela porterait atteinte aux libertés de toutes les personnes vivant dans le foyer concerné.

En ce qui concerne maintenant le filtre national de cybersécurité à destination du grand public, porté par l'article 6, la Cnil approuve le souhait du Gouvernement de renforcer la protection de l'internaute contre les risques cyber *via* l'affichage d'un message dans leur navigateur lorsqu'il accède à un site comportant des risques. Là aussi, il est crucial que l'objectif légitime de cybersécurité ne conduise pas en pratique à une restriction abusive des libertés de communication et d'expression. À cet égard, je note avec satisfaction que des garanties ont été apportées et qu'un contrôle indépendant de la mise en œuvre du filtrage sera confié à un membre de la Cnil.

Nous soulignons néanmoins que le nombre potentiel de sites cybermalveillants serait de l'ordre de 300 000 par an. Le contrôle de ces sites constituera donc un défi considérable qui implique des moyens adéquats. Concrètement, la Cnil est susceptible de recevoir des notifications concernant peut-être 1 000 adresses par jour.

S'agissant des modalités techniques de déploiement de ce filtre, la Cnil, comme elle l'a indiqué dans son avis, est favorable à ce que le filtrage soit réalisé au sein du navigateur Internet, donc sous la responsabilité de l'internaute, préservant ainsi sa liberté de communication, et que l'activation du dispositif au niveau des fournisseurs d'accès à Internet (FAI) et des systèmes de résolution des noms de domaine (DNS) soit réservée aux cas les plus graves.

Par ailleurs, s'agissant de la régulation des services d'intermédiation de données (articles 11 et 12 notamment), instaurée par le règlement européen sur la gouvernance des données *(DGA)*, le projet de loi désigne l'Arcep pour superviser ces nouveaux acteurs. La Cnil souligne que, si certains de ces acteurs traitent de données industrielles et très peu de données personnelles, une partie d'entre eux ont pour activité principale de commercialiser un accès à des bases de données personnelles. Pour ces acteurs, le *DGA* et le RGPD s'appliqueront parallèlement, et le *DGA* prévoit qu'en cas de contrariété le RGPD prévaut.

En outre, les règles du *DGA* sont en partie des règles décalquées ou précisées du RGPD. Il existe donc un risque de complexité et d'insécurité juridique que l'Arcep et la Cnil devront parer en travaillant ensemble. La Cnil doit pouvoir notamment jouer pleinement son rôle dans la qualification des acteurs et des données qui traitent ces acteurs, afin qu'eux-mêmes et l'Arcep puissent déterminer les règles s'appliquant.

La Cnil a formulé certaines propositions dans son avis. Le collège de la Cnil propose que la loi soit complétée pour prévoir une transmission

systématique à la Cnil des notifications que ces prestataires feront à l'Arcep pour déclarer leur activité. Cela permettrait à la Cnil de rendre un avis pour indiquer à l'acteur et à l'Arcep si le RGPD s'applique ou non en parallèle du *DGA*, et dans quelle mesure. Cela améliorerait la sécurité juridique et nourrirait le dialogue entre les régulateurs.

Dans le même esprit, une consultation systématique et préalable de chacune des deux autorités Arcep et Cnil avant toute adoption d'un texte de droit souple par l'un ou l'autre des deux régulateurs me paraît également nécessaire. Il serait par ailleurs utile d'apporter une modification rédactionnelle à l'alinéa 2 de l'article 13, qui évoque sur des sujets précis la consultation de la Cnil par l'Arcep mais en parlant d'un « cas échéant », dont j'ai un peu du mal à comprendre ce à quoi il se rapporte. Je propose donc sa suppression.

Enfin, je conclurai sur les compétences confiées à la Cnil dans le cadre du *DGA* et du RSN. Cela concerne l'altruisme des données, la publicité en ligne et la protection des mineurs. J'approuve les choix du Gouvernement dans la mesure où l'altruisme des données reste à construire, et présentera des enjeux en matière de protection des personnes. Concernant la publicité en ligne et la protection des mineurs, le RSN précise des règles déjà présentes dans le RGPD.

Au regard de la diversité des acteurs qui devront appliquer le RSN, je ne peux pour conclure qu'insister à nouveau sur la nécessité d'une coopération étroite entre les autorités compétentes, l'Arcom, la DGCCRF et la Cnil, qui existe déjà de fait, pour assurer une régulation cohérente et garantir une sécurité juridique des acteurs concernés. Je vous remercie.

Mme Catherine Morin-Desailly, présidente. – Merci madame la présidente. Je vais passer maintenant la parole à Loïc Hervé, pour une première série de questions relatives à notre texte.

M. Loïc Hervé, rapporteur. – Tout d'abord une question d'ordre général. Le Sénat a adopté hier après-midi une proposition de loi relative à la reconnaissance biométrique, qui prévoit un panachage des collèges permettant par exemple au président d'une autorité d'être membre de droit du collège d'une autre autorité, comme ce qui existe avec la Commission d'accès aux documents administratifs (Cada) et la Cnil. Est-ce un sujet qui doit selon vous être développé ? Est-ce le gage d'une meilleure coopération entre les différentes autorités administratives indépendantes ?

Vous avez évoqué de manière très complète le texte de loi qui présente des conséquences sur la vie de vos autorités administratives indépendantes. Ce texte comporte-t-il selon vous des lacunes, des domaines non couverts qui mériteraient de l'être et qui pourraient alimenter le travail parlementaire de cette commission spéciale ?

Monsieur le président de l'Arcom, nous avons évoqué hier dans une audition la question du référentiel. Le législateur va vous confier la mission

de rédaction, ce qui peut apparaître comme une question technique, alors qu'elle ne l'est pas à bien des égards. J'aimerais que vous puissiez ainsi détailler les questions de planning et de technologies préconisées, afin que nous appréhendions au mieux les enjeux et les difficultés potentielles. Ce référentiel sera important, car il fera jurisprudence lorsqu'il s'agira d'évoquer la régulation d'autres secteurs de l'Internet, ce que craignent un certain nombre d'acteurs.

Concernant votre pouvoir d'injonction administrative créé par l'article 2, comment le concevez-vous, particulièrement sur l'accès des sites pornographiques aux mineurs ? Nous avons constaté les difficultés de mise en œuvre de textes de loi déjà votés. Par ailleurs, comment pouvez-vous lier ce nouveau travail à l'exploitation du travail accompli avec la plateforme Pharos ?

Madame la présidente de la Cnil, vous avez abordé à deux reprises la question des moyens : disposez-vous d'une évaluation de vos besoins au regard de l'ampleur des missions qui vous seraient confiées ?

Mme Catherine Morin-Desailly, présidente. – La question de l'accès aux sites pédopornographiques est essentielle, mais ne doit pas faire oublier celle du harcèlement de nos jeunes, avec des conséquences dramatiques, comme nous l'avons constaté récemment. Comment ce nouveau texte pourrait permettre de résoudre cette problématique ?

Mme Laure de La Raudière. – Concernant le panachage des collèges d'autorité, je rappelle que la coopération est bonne et que nous échangeons régulièrement. Le fait que le président d'une autorité comme l'Arcep soit membre du collège de la Cnil par droit, et vice-versa, ne me paraît pas la solution idéale, en raison d'un risque de biais dans la mesure où la décision d'une autorité emporterait l'avis de l'autre, au moins en communication à l'extérieur. Par exemple, une décision prise par l'Arcep avec un membre de la Cnil en son sein pourrait être perçue comme validée par la Cnil. Je préfère donc largement les avis croisés où chaque autorité s'exprime selon ses objectifs spécifiques de régulation. Les trois autorités possèdent en effet des objectifs de régulation différents : les contenus pour l'Arcom, la défense des libertés individuelles pour la Cnil, la défense de la concurrence pour l'Arcep.

Par ailleurs, les coopérations entre autorités existent. Nous disposons de collèges communs à l'Arcom et à l'Arcep, mis en place sans le recours à des textes de loi. Ils se réunissent une à deux fois par an. Nous bénéficions également d'un pôle de travail commun entre l'Arcom et l'Arcep. Cette coopération doit exister au niveau des collèges, mais aussi par des groupes de travail commun ou par des pôles commun au niveau des équipes, ce qui est essentiel.

M. Roch-Olivier Maistre. – Concernant le premier point, je fais volontiers mienne la réponse de Laure de La Raudière. Il existe des mécanismes de consultation prévus par les textes et que nous pratiquons

chaque fois qu'une problématique intéresse une autre autorité. Nous avons en l'occurrence suggéré d'instaurer une procédure formelle s'agissant de la protection des mineurs dans le texte qui vous est soumis. Par ailleurs, la mécanique des conventions constitue un dispositif souple mais tout à fait efficace, mis en pratique avec l'Arcep lors de ma prise de fonctions. Il existe également des procédures d'audition périodiques. Marie-Laure Denis m'a ainsi convié à une intervention devant le collège de la Cnil il y a quelques semaines, et elle a également répondu à l'invitation du collège de l'Arcom. Nous avons aussi reçu le président de l'Autorité de la concurrence, et je suis auditionné cette semaine par cette autorité. Ce type de mécanisme me paraît donc préférable.

Les membres de nos collèges sont déjà nombreux, donc je pense souhaitable de privilégier les mécanismes évoqués plutôt qu'une présence supplémentaire institutionnelle.

Concernant les lacunes, je n'en identifie pas à ce stade.

Par ailleurs, le référentiel constituera en effet un sujet important. J'ai évoqué dans mon propos introductif l'attente d'une décision de justice le 7 juillet, et je serai donc prudent dans mon expression. Nous travaillons sur ce sujet avec la Cnil et le PEReN pour préparer ce document qui devrait être prêt à l'automne. Nous serons sans doute confrontés sur ce volet à une consultation de niveau européen.

Concernant les procédures d'injonction, nous distinguons à la lecture du projet de loi deux types de dispositions entre l'article 1 et l'article 2. Le premier vise plus spécifiquement des dispositifs de vérification d'âge qui ne respecteraient pas suffisamment la vie privée au regard du référentiel élaboré par l'Arcom après avis de la Cnil et la collaboration du PEReN. Dans ce cas, le texte évoque la possibilité de mise en demeure et de sanctions financières. L'article 2 vise l'absence de mise en place d'un dispositif efficace de vérification de l'âge qui pourrait conduire l'autorité à demander le blocage du site, mais cet article ne fait pas référence au référentiel, raison pour laquelle il nous semblerait utile, en accord avec la Cnil, d'harmoniser ces deux articles en un seul, de prévoir une mesure de consultation formelle de la Cnil par l'Arcom dans l'hypothèse du constat d'un dispositif mis en œuvre par un site qui porterait atteinte de façon excessive à la vie privée en regard du référentiel. Nous disposerions alors d'un seul schéma de procédure pour éviter ces zones d'ambiguïté.

Concernant la question du harcèlement, il s'agit d'un sujet central. Je vois aujourd'hui le ministre de l'Éducation nationale pour en parler. Le règlement sur les services numériques a pour ambition de conduire les sites couverts par ce texte à lutter contre tous les contenus de nature illicite, et vise plus spécifiquement tout ce qui a trait à la haine en ligne et aux mécanismes de harcèlement. Il mentionne par ailleurs l'obligation de procéder à l'évaluation des risques de nature systémique que chacune

de leur plateforme peut comporter, d'imposer à ces sites des mécanismes annuels d'audit externe pour vérifier les dispositifs mis en place, soit d'Intelligence artificielle, soit de modération humaine. Une autre obligation contraint ces sites à mettre leurs données à disposition de la sphère académique pour qu'elle puisse mener ses travaux de recherche et contrôler la manière dont leurs algorithmes procèdent. Par ailleurs, les autorités de régulation disposeraient d'un important pouvoir de sanction, pouvant aller jusqu'à 6 % du chiffre d'affaires mondial. Il s'agit donc de réponses très importantes.

Pour les très grandes plateformes, ce règlement sera effectif à partir de la fin du mois d'août de cette année. Twitter ou TikTok répondent-ils aux dispositions du RSN ? Pour l'Union européenne, pour la Commission, pour la gouvernance de ce texte, les réponses vont arriver très vite. L'enjeu de crédibilité est essentiel.

Une autre dimension tout aussi importante réside dans le volet éducation aux médias, et à la citoyenneté numérique : comment proposer très tôt l'apprentissage d'une citoyenneté numérique ? Ouvrir un compte sur TikTok, Facebook ou Twitter ne doit pas être synonyme d'une transformation en délinquant potentiel, en harceleur de ses camarades de classe ou en diffuseur de fausses informations. Le travail éducatif en amont est donc très important.

Mme Marie-Laure Denis. – Concernant l'éventuel élargissement du collège de la Cnil et des hautes autorités, l'idée exprimée dans le rapport de Philippe Latombe et de Philippe Gosselin à l'Assemblée nationale sur l'utilisation des images de sécurité dans le domaine public pour lutter contre l'insécurité, a été reprise hier dans la proposition de loi sur la reconnaissance faciale. La recommandation 36 de ce rapport liait l'élargissement du collège de la Cnil à la proposition qui suggérait de consacrer la Cnil en tant que chef de file de la régulation des systèmes d'Intelligence artificielle, donc pour une compétence très particulière, très structurante.

Par ailleurs, nous pratiquons déjà beaucoup l'inter-régulation, de manière structurelle à la Cnil avec le président de la Cada, membre de droit de notre collège, tout comme la défenseure des droits. Notre collège comporte 18 membres, ce qui en fait probablement le plus important des autorités de régulation.

Concernant les lacunes, je n'en ai pas décelé. Parmi la mise en œuvre de dispositions du RSN, certains pouvoirs de sanctions et d'enquête de la Cnil sont précisés ou modifiés, et il faudrait par cohérence que ces règles de procédure répressive soient harmonisées dans tous les textes concernant la Cnil. Je rejoins les propos du président de l'Arcom sur l'utilité de fusionner les articles 1 et 2 de la loi par souci de cohérence.

Concernant les moyens de la Cnil, des précisions pourront être apportées lorsqu'un décret d'application sera pris sur le filtre cyber-arnaque

et le rôle de l'autorité administrative qui sera en première ligne, le rôle du membre du collège de la Cnil, et donc des services de la Cnil. L'enjeu de l'efficacité est très fort. Nous disposions de 270 agents à la fin de l'année dernière. Nous sommes vus comme le gendarme de la protection des données, nous traitons de 12 à 14 000 plaintes par an, nous prononçons des sanctions et réalisons des contrôles, notre but étant la mise en conformité plus que la sanction. Nous accompagnons beaucoup d'entreprises innovantes dans le domaine du numérique, comme le montre l'opération « bac à sable » consacrée cette année à l'Intelligence artificielle et les administrations. Nous avons également créé un accompagnement renforcé de six mois auprès d'entreprises à très fort potentiel de développement économique et numérique. Il aurait ainsi été intéressant pour la Cnil d'accompagner Doctolib au moment de sa création, plutôt qu'au moment où l'entreprise est très installée. Cette année, 47 entreprises à fort potentiel de développement économique ont souhaité être accompagnées par la Cnil en matière de protection des données.

Notre rôle ne se limite donc pas à celui de gendarme de la protection des données. Nous sommes par ailleurs la seule autorité de protection des données en Europe à disposer d'un laboratoire d'innovation numérique traitant notamment des assistants vocaux, de l'Intelligence artificielle. Nous organisons également un *Privacy Research Day* sur les enjeux entre recherche, régulation, entreprises en matière de protection des données.

Concernant le filtre anti-arnaques, la Cnil devra disposer de moyens supplémentaires, indépendamment de ceux déjà budgétés, si nous voulons garantir l'efficacité de ce dispositif.

Mme Catherine Morin-Desailly, présidente. – Je me permets une remarque, madame la présidente : il est dommage d'entendre le terme de *Privacy Research Day* quand la loi sur la défense du français fête ses 40 ans.

Mme Marie-Laure Denis. – Ma langue a fourché, et il est vrai que certains citoyens nous reprochent l'utilisation de tels termes. Par ailleurs, j'ai beaucoup de sympathie pour Jacques Toubon, initiateur de cette loi, et je reformulerai donc autrement l'intitulé de la manifestation.

Mme Catherine Morin-Desailly, présidente. – Je donne maintenant la parole à notre deuxième rapporteur, Patrick Chaize, pour l'autre volet.

M. Patrick Chaize, **rapporteur**. – Je vais évoquer l'article 6 de ce texte, et vous questionner sur la manière dont les autorités que vous représentez contribueront au déploiement du filtre anti-arnaques prévu à cet article. La mise en place d'un dispositif ordonné par voie administrative plutôt que par voie judiciaire vous semble-t-elle plus efficace ? La Cnil est désignée comme autorité garante du caractère adapté et proportionné des mesures prises dans le cadre de ce dispositif : qui sera la personnalité qualifiée ou quel sera le profil de la personne qui assurera ce rôle ?

Concernant la régulation du marché de l'informatique en nuage, l'encadrement des crédits et la suppression des frais de transfert sortant de données, le projet de loi attribue à l'Arcep un nouveau rôle de gendarme de l'informatique en nuage. Êtes-vous satisfaite, madame la présidente, de ce nouveau rôle ?

Concernant les services d'intermédiation de données, d'autres États membres ont-ils effectué ou ont-ils manifesté l'intention d'effectuer un autre choix que la désignation de leur autorité de régulation des télécommunications comme seule compétente pour l'application du *Data Act* ? Concernant l'article 11, vous avez, madame la présidente de la Cnil, des propositions à nous faire et je leur suis ouvert. Une compétence de l'Arcep et de la Cnil exercée en commun ou partagée a-t-elle été envisagée ? Quels avantages et inconvénients cette solution aurait-elle présentés ?

Concernant l'article 25 sur les procédures de saisine et de visite de l'Arcom, en quoi est-il nécessaire de préciser dans la loi que les autorités compétentes pour la mise en œuvre du règlement sur les services numériques coopèrent étroitement, se prêtent mutuellement assistance et se communiquent librement des informations ? Quel sera l'objet des conventions de coopération que vous allez signer, et pourriez-vous nous en dire davantage sur ces conventions ?

La procédure de saisine et de visite des locaux fournisseurs des services entre 6 heures et 21 heures nous interpelle par sa rédaction. Si la procédure ne peut être autorisée que par le juge des libertés et de la détention, il est prévu que toutes les conditions de réalisation de cette procédure soient fixées par voie réglementaire, ce qui nous étonne. Pourriez-vous nous détailler la procédure prévue qui s'apparente à une perquisition ?

Mme Marie-Laure Denis. – Concernant l'article 6 et la création d'un filtre national de cybersécurité qui permet d'alerter les internautes par le biais d'un message d'alerte dans leur navigateur lorsqu'ils souhaitent accéder à un site malveillant, tout le sujet consiste à avoir des garanties sur l'efficacité de ce filtre, et en matière de liberté, de communication et d'expression. Pour cela, le texte prévoit, en reprenant largement l'avis du Conseil d'État, un certain nombre de procédures et de délais.

Je comprends du texte qu'il reviendrait à un membre indépendant du collège de la Cnil de s'assurer du caractère justifié des mesures, des conditions d'établissement, de mise à jour et de communication de l'utilisation de la liste des adresses électroniques concernées. Mais nous ne pourrons désigner cette personnalité qualifiée que lorsque le décret d'application prévu dans le texte sera pris.

Nous considérons que le blocage peut être envisagé, mais seulement pour les cas les plus graves, et la question des modalités et des moyens doit être précisée.

S'agissant des services d'intermédiaire de données, il nous semble important que la Cnil soit saisie pour avis systématiquement et au préalable de toute déclaration d'un intermédiaire de données auprès de l'Arcep, pour que ce soit la Cnil qui précise si ces données comportent des données personnelles, et quelles sont les règles qui s'appliquent à ces acteurs. Par sécurité juridique et par lisibilité de ces textes complexes, il nous semblerait utile que si l'Arcep ou la Cnil édictent des règles de droit souple sur le sujet des intermédiaires de données, il y ait une consultation préalable là aussi systématique de l'autre autorité concernée.

Par ailleurs, l'article 13 comporte l'expression « le cas échéant » que je propose de supprimer du fait de son ambiguïté. Il s'agit du paragraphe à propos de la consultation de la Cnil par l'Arcep, qui précise que « dans les conditions fixées par décret, cette autorité recueille le cas échéant les observations éventuelles de la commission par rapport à des demandes qui peuvent concerner un règlement sur la gouvernance européenne des données ».

M. Roch-Olivier Maistre. – Sur le principe de la coopération, l'équilibre proposé par le texte nous semble adapté en fixant les grands principes dans la loi, mais en renvoyant les modalités de ces coopérations entre les uns et les autres à des outils plus souples, du type convention. La nature des informations que nous allons échanger peut être sensible, et il est important de disposer d'une référence législative. Chaque autorité possède des champs de compétences propres. Concernant la mise en œuvre du RSN, nous aurons chacun des attributions respectives à faire valoir, et cela doit être couvert par la convention.

Le pouvoir de visite est inspiré de celui dont peut disposer l'Autorité de de la concurrence. Nous avons face à nous des acteurs puissants, avec lesquels nous devons dialoguer dans une position de force.

Mme Laure de La Raudière. – Merci pour votre question sur la manière dont l'Arcep accueille ces nouvelles compétences, notamment en matière d'informatique en nuage. Notre accueil est très favorable, car ce marché doit être déverrouillé. Il existe des freins contractuels mais aussi techniques liés à la migration des clients vers d'autres fournisseurs, le marché étant concentré à 70 % autour de trois ou quatre fournisseurs, tous américains. Pour faire émerger des entreprises européennes puissantes dans ce secteur, nous devons déverrouiller ce marché. L'enjeu est économique, car le marché est en croissance, mais il touche aussi à la souveraineté de l'Europe sur l'hébergement des différents services informatiques.

L'Arcep est d'autant plus favorable qu'elle possède un rôle de régulateur technico-économique du numérique, que son expertise technique

et sa culture d'ouverture des écosystèmes numériques la motivent beaucoup à prendre en compte cette nouvelle compétence, et ce nouveau marché à déverrouiller.

Par ailleurs, l'Arcep aura également besoin de moyens supplémentaires pour assurer ces nouvelles compétences sur l'informatique en nuage ou sur le *Data Governance Act*. Les personnels de l'Arcep, comme ceux de l'Arcom et de la Cnil, sont très, très occupés. Certains d'entre vous, ou d'autres acteurs, nous reprochent notre manque de réactivité, mais le problème réside souvent dans une question de moyens. Nous espérons donc que cette demande sera prise en compte lors de la loi de finances de 2024.

Concernant la question de l'exercice en commun de la compétence sur les précepteurs de services d'intermédiation de données, il serait complexe, à la fois pour les acteurs et pour les autorités, d'exercer ensemble une compétence au sein de deux autorités qui n'ont pas été créées pour les mêmes objectifs, les mêmes enjeux, avec des cultures de régulation différentes. Modifier l'architecture actuelle du texte sur le *DGA* ne constituerait donc pas une bonne idée à mon sens.

Le *DGA* prévoit une notification systématique par l'Arcep de l'ensemble des prestataires de services d'intermédiation de données déclarés auprès de l'Arcep. La Commission européenne a prévu de rendre publiques ces déclarations, raison pour laquelle le texte ne prévoit pas que l'Arcep notifie à la Cnil.

Mme Marie-Laure Denis. – Je précise que l'enjeu n'est pas que cela soit public ou non, mais réside dans la possibilité que les données soient à la fois personnelles et non personnelles. Notifier à la Cnil permet d'informer ces acteurs, qui font face à la fois au *DGA* et au RGPD, et qui sont potentiellement soumis à deux législations. Je pense que la notification à la Commission européenne n'a pas le même objectif que la notification à la Cnil. Ces acteurs ne sont pas si nombreux, puisque l'analyse d'impact de la Commission européenne sur les services d'intermédiation de données identifiait une cinquantaine d'acteurs en « *B to B* », et un nombre proche en « *B to C* ». À très court terme, seule une demi-douzaine d'acteurs est concernée. Je ne vois pas où serait l'impossibilité et l'inconvénient de notifier à la Cnil, à qui il appartient de déterminer s'il existe des données personnelles ou non.

Mme Laure de La Raudière. – Par rapport à l'expression « le cas échéant » précisée dans le texte et par rapport à l'obligation de saisine uniquement en cas d'impact sur les données personnelles, la logique est identique : des prestataires de services d'intermédiation de données vont offrir des services avec uniquement des données industrielles. Il s'agit d'un nouveau champ d'activité censé se développer avec ce texte, qui touche beaucoup plus les données industrielles et les données économiques des acteurs et le partage au sein d'un secteur de données économiques et

industrielles, et pas nécessairement des données personnelles. Le texte, comme le *DGA*, prévoit une articulation de ce type.

Mme Marie-Laure Denis. – Je suis d'accord que les acteurs présentant des données industrielles relèvent totalement du *DGA* et de la compétence de l'Arcep. Je précise simplement que des données industrielles peuvent comprendre des données personnelles, de clients, de salariés, *etc.* Il est donc important que les acteurs comprennent qu'il existe potentiellement deux séries de textes sur des données différentes, sachant que lorsque les données sont inextricablement liées, elles basculent du côté du RGPD.

Mme Laure de La Raudière. – C'est la raison pour laquelle il est dommage que ce texte anticipe le Data Act, car ce dernier venait équilibrer le *Data Governance Act*. Dans tous les cas, le RGPD prévaudra toujours. Vous avez raison de dire que les données industrielles doivent être brutes pour ne pas porter préjudice aux entreprises.

Mme Marie-Laure Denis. – Comme vous l'avez précisé, cela intervient sans préjudice du RGPD.

Mme Catherine Morin-Desailly, présidente. – Merci. Nous avons six demandes de prise de parole, dont trois concernent la lutte contre la pédopornographie.

Mme Annick Billon. – Merci madame la présidente, monsieur le président et mesdames les présidentes, pour les nombreuses réponses déjà fournies.

J'évoquerai l'industrie des sites pornographiques, ayant été auteure avec mes collègues du rapport *Porno, l'enfer du décor*.

Nous constatons que de nouveaux pouvoirs de sanction et de blocage sont donnés à l'Arcom. Pensez-vous, dans l'état actuel de ces nouveaux pouvoirs, réussir à agir ? Nous avons en effet démontré dans notre rapport que les sites pornographiques sont souvent dirigés depuis des paradis fiscaux.

Je soulèverai ensuite une autre question importante liée au retrait des contenus pédopornographiques : *quid* de la définition des contenus illicites ? *Quid* de la définition d'un contenu pédopornographique ? Il a été question de pilosité, de la grosseur des seins. Pensez-vous que la définition doit être complétée pour une meilleure efficacité ?

Ma dernière question porte sur le dispositif Cnil-PEReN, actuellement en test avec le groupe Dorcel : disposez-vous de retours ?

Mme Marie Mercier. – Ma remarque concerne la loi du 30 juillet 2020, qui n'est pas appliquée. Pensez-vous qu'un nouveau texte changera quelque chose ? En effet, le tribunal a placé l'Arcom en position de faiblesse avec une médiation surréaliste. La Cour de cassation a rendu un

avis formel, et il n'y a pas de discussion juridique sur ces textes. Nos enfants doivent se protéger seuls, et nous sommes face à des mastodontes. Le nouveau texte va immédiatement engendrer une QPC, et nous allons à nouveau perdre du temps.

Par ailleurs, il n'est pas liberticide de contrôler l'âge pour jouer de l'argent. Pourquoi cela deviendrait liberticide pour le visionnage de sites pornographiques ?

Mme Laurence Rossignol. – Ma question sur le même thème s'adresse à la présidente de la Cnil. Vous avez précisé qu'il fallait toujours veiller à la fois à la protection des mineurs et à la protection des données personnelles. Or, j'ai le sentiment que lorsqu'il s'agit des données personnelles des consommateurs de sites pornographiques, les mêmes règles ne sont pas appliquées que pour les utilisateurs d'autres sites. J'ai cru comprendre qu'il fallait que les données personnelles ne circulent pas, notre objectif étant la protection.

Marie Mercier a rappelé que pour la fréquentation par les mineurs de sites de jeux d'argent en ligne, la règle est claire avec les cartes de crédit et la preuve de l'âge. Nous ne nous posons donc pas dans ce cas la question d'une particulière protection des données. Pourquoi se poser la question pour les personnes fréquentant les sites pornographiques ? Je ne comprends pas cette distinction.

M. Roch-Olivier Maistre. – Il faut souligner l'ampleur du phénomène. Nous avons publié une étude très complète sur l'accès à ces sites de la part des mineurs, conduite notamment avec Médiamétrie, avec des mesures très concrètes. L'âge de consultation de ces sites est de plus en plus bas, et cette consultation se fait très largement par l'intermédiaire de téléphones qui ne disposent pas de contrôle parental. Nous bénéficions par ailleurs d'une documentation très riche sur les effets de cette consultation, sur les comportements et la sexualité des jeunes gens.

Je crois que l'opinion publique a largement évolué sur ces sujets-là, et les effets de tolérance sont bien moindres. La justice pénale elle-même s'est mise en mouvement, avec des actions judiciaires en cours contre l'industrie pornographique. Les lignes sont donc en train de bouger.

Mais vos remarques sont justes. Je suis frappé qu'avec un texte de cette nature qui date de trois ans, aucune initiative n'a été menée pour essayer de se conformer à la réglementation. Par ailleurs, la réglementation ne date pas de 2020, puisque l'interdiction d'exposer des mineurs à des contenus pédopornographiques est inscrite dans le Code pénal depuis de très nombreuses années.

Nous avons beaucoup travaillé pour la mise en œuvre de ce texte. Chaque notification engendre des procédures très lourdes. Chaque acte pris a été contesté, avec une procédure de médiation surprenante, puisqu'il

n'était question que de respect de la loi. Nous sommes maintenant suspendus à la décision du juge judiciaire.

Le texte soumis aujourd'hui va-t-il tout résoudre ? Nous suivons un schéma plus classique de régulation par le biais d'une autorité administrative, qui pourra prononcer une mesure de blocage et de déréférencement. Cette action sera menée sous le contrôle du juge, et le texte fera très tôt l'objet d'une QPC. Le référentiel pourra aussi être contesté, et devra faire l'objet de mesures de notification à Bruxelles.

Nous avons face à nous une industrie organisée. La Grande-Bretagne a été mise en échec sur des dispositifs équivalents il y a quatre ou cinq ans. L'Arcom aura comme seule feuille de route la loi, mais la guérilla contentieuse enrichira sans aucun doute quelques cabinets d'avocats.

Mme Catherine Morin-Desailly, présidente. – Nous avons travaillé avec Ludovic Haye sur le projet de règlement visant à combattre et prévenir les abus sexuels sur les enfants. Ce texte, encore en cours de discussion, amènera-t-il quelque chose de supplémentaire, sera-t-il complétement articulé au RSN et aux mesures que la France s'autorise de prendre ?

M. Roch-Olivier Maistre. – Votre question est pertinente. J'évoquerai aussi le sujet du règlement sur les services numériques. La Commission européenne n'a pas été insensible à notre démarche, car certains de ces sites entreront dans la mise en œuvre de ce règlement, qui peut constituer un biais d'action. Mais je rappelle qu'il existe des centaines de sites pornographiques et qu'ils représentent une consommation de la bande passante tout à fait considérable. Il est donc important de trouver la bonne articulation juridique, et nous examinons le point que vous évoquez.

Mme Marie-Laure Denis. – Concernant l'expérimentation menée aujourd'hui, je n'ai pas encore de retour, mais les services de la Cnil sont en contact avec des entreprises qui cherchent à mettre en œuvre le dispositif technique préconisé, en travaillant avec le PEReN sur cette solution de double anonymat, qui doit permettre qu'un tiers de confiance certifie votre majorité sans savoir quel site vous allez consulter, et que le site consulté n'ait pas accès à votre identité. Sinon, les techniques multiples de hacking aboutiraient à la diffusion immédiate du fichier des personnes qui consultent ces sites pornographiques.

La Cnil n'avait aucune compétence particulière pour appliquer la disposition législative prise. La Cnil est dans son rôle en cherchant à protéger les données des personnes, et elle a d'elle-même décidé de travailler sur des solutions et d'expérimenter pour concilier ces enjeux de protection de vie privée et de protection de l'enfance. Nous sommes tous conscients des ravages de la consultation de la pornographie sur les mineurs.

Par ailleurs, le collège de la Cnil a autorisé l'utilisation des cartes bancaires, même si cette solution est imparfaite car un adolescent de 17 ans

peut disposer d'une telle carte. La Cnil a également autorisé des systèmes d'estimation de l'âge, qui seront sans doute imprécis entre 17 et 19 ans, mais permettront d'identifier un enfant de 13 ans.

La Cnil a donc déployé toute l'énergie nécessaire en peu de temps en assumant ses compétences et son rôle pour faciliter le travail de l'Arcom et répondre à vos préoccupations légitimes.

Mme Alexandra Borchio Fontimp. – Je trouve regrettable que tout le monde autour de cette table partage les constats et les conséquences de l'exposition des mineurs aux contenus pornographiques, mais que personne ne puisse affirmer qu'une solution existe.

Ma question s'adresse à monsieur le président de l'Arcom et à madame la présidente de la Cnil sur l'articulation entre les référentiels prévus par la récente proposition de loi qui instaure une majorité numérique sur les réseaux sociaux, et le projet de loi sur le contrôle de l'âge sur les sites pornographiques. Comment allez-vous organiser votre coopération ?

Mme Marie-Laure Denis. – Le référentiel relève de la compétence de l'Arcom, qui va l'élaborer, et qui consultera la Cnil avant de l'adopter définitivement, notamment concernant les caractéristiques techniques des dispositifs comme le double anonymat, car la Cnil possède les compétences sur ces sujets.

M. Roch-Olivier Maistre. – La coordination sera en effet très étroite, et je partage les propos de Marie-Laure Denis.

Les lignes bougent dans le monde : des États américains ont déjà adopté des législations proches de la nôtre. Plusieurs États européens comme l'Allemagne prennent des initiatives identiques à l'égard des sites pornographiques, et se heurtent aux mêmes difficultés que nous en termes de procédures. L'état de droit donne à un justiciable le droit de faire valoir et de contester des décisions prises par une autorité administrative. Nous attendons le 7 juillet, et je fais confiance à notre justice. L'opinion est aujourd'hui très réceptive à la nécessité de protéger les mineurs, comme le montrent les nombreux articles publiés récemment, et l'écho médiatique rencontré par notre étude sur les statistiques.

Ce chantier est de longue haleine, et nous devons tous maintenir nos efforts.

Mme Catherine Morin-Desailly, présidente. – C'est la raison pour laquelle l'Europe jugeant le phénomène suffisamment grave, s'en empare au plus haut niveau.

Mme Florence Blatrix Contat. – Avant de vous interroger sur la question de la publicité ciblée, je souhaitais exprimer avec d'autres collègues nos craintes pas encore levées, malgré vos réponses, à propos de la coordination. Cette coordination constitue une condition essentielle de l'efficacité de ce dispositif législatif.

Avec ma collègue Catherine Morin-Desailly, nous avons constaté dans nos rapports sur le RSN et le RMN que le modèle économique des plateformes se révèle un enjeu essentiel. La publicité vous paraît-elle suffisamment traitée dans ce texte qui a vocation à mieux protéger les consommateurs ? Par ailleurs, la part des opérateurs européens sur le marché du *cloud* a pratiquement été divisée par deux en cinq ans. Pensez-vous que les mesures figurant dans ce texte, comme l'interdiction des frais de transferts pour l'interopérabilité, seront suffisantes pour permettre aux opérateurs européens de se réinscrire dans ce marché et de se développer ?

M. Roch-Olivier Maistre. – Concernant votre première observation, je souhaite être tout à fait catégorique sur l'état d'esprit des présidentes et présidents des autorités indépendantes. La coopération fait partie de notre culture personnelle, et notre quotidien est la loi. Il n'existe pas de patriotisme ou de susceptibilités d'autorité l'une vis-à-vis de l'autre. Nous avons pleinement conscience de l'attente du législateur, et nous construisons ensemble de la manière la plus efficace possible l'action nécessaire pour mettre en œuvre ce texte. Nos autorités ne montrent pas la moindre hésitation, la moindre réticence, la moindre différence à ce sujet.

Concernant la publicité, je pense qu'avec les textes de niveau européen et d'autres comme celui récemment adopté sur les influenceurs, la protection du consommateur est mieux assurée, mais il faudra s'assurer de l'application de ces textes.

Mme Laure de La Raudière. – Sur la question de l'informatique en nuage, les mesures du texte sont absolument nécessaires, à la fois pour la partie purement contractuelle avec l'abandon des frais de transfert et la limitation et l'encadrement des crédits des services d'informatique en nuage, mais aussi les mesures techniques de l'interopérabilité et de la portabilité.

Les grands utilisateurs font de plus en plus appel à plusieurs fournisseurs *cloud* pour un enjeu de résilience, mais aussi pour protéger certaines données sensibles dans des espaces de *cloud* souverains et hermétiques aux lois extraterritoriales de transfert des données.

Le marché est encore en très forte croissance, et les mesures sont certainement nécessaires, mais seront-elles suffisantes ? De nombreuses entreprises, notamment les PME, ne sont pas encore pleinement équipées, ce qui laisse la place pour de nouveaux acteurs répondant à des enjeux de souveraineté, de proximité, ou à la volonté de certains clients de privilégier l'Europe.

Les acteurs du *cloud* sont soumis pour certains d'entre eux au RMN, qui offre des dispositions visant à favoriser plus de concurrence sur l'ensemble du marché numérique.

Mme Catherine Morin-Desailly, présidente. – Ne croyez-vous, pas madame la présidente de l'Arcep, qu'au-delà des mesures, une forte volonté

est nécessaire de la part des autorités de ce pays pour confier de manière stratégique à nos entreprises le marché des données d'un certain nombre d'entreprises et d'administrations, pour gagner en souveraineté et pour soutenir le développement et l'innovation dans notre pays ? Les Américains, les Russes et les Chinois agissent ainsi en faveur de leurs entreprises, la plupart du marché du *cloud* étant confié aujourd'hui aux GAFAM. Dans ce cadre, l'Arcep ne doit-elle pas jouer un rôle de stimulation auprès des décideurs ? Par ailleurs, lorsque la plateforme des données de santé a été confiée en 2020 à Microsoft sans appel d'offres, pourquoi l'Arcep, chargée de la régulation de ce marché, n'a-t-elle pas alarmé sur cette absence d'appel d'offres ? La Cnil s'est prononcée sur ce sujet, car il s'agissait de données ultra-sensibles.

Enfin, ne croyez-vous pas qu'il serait urgent d'inscrire au cœur de ce texte la définition des données sensibles et stratégiques pour la Nation, pour bénéficier d'une vision globale et d'un plan d'action stratégique ?

Mme Laure de La Raudière. – Vous évoquez un sujet de grande importance, madame la présidente. L'Arcep possède une culture pro-concurrence et pro-innovation. Nous allons chercher par tous les moyens à déverrouiller le marché pour permettre plus de migrations, plus de fluidité, mais l'exercice de nos compétences se fait dans le cadre de la loi. Si la loi ne prévoit pas l'obligation pour les services administratifs de se tourner vers un service d'informatique en nuage souverain, nous ne pourrons pas l'imposer aux administrations. En revanche, nous exercerons nos compétences pour mettre en place des spécificités équilibrées, qui permettent à de nouveaux acteurs d'émerger. Nous consultons pour cela tous les acteurs du marché, nous montons en compétences par des échanges bilatéraux avec les acteurs, les organismes de normalisation, et nous présenterons en consultation publique nos propositions, ce qui permettra à chacun des acteurs concernés de s'exprimer. L'Arcep procède toujours ainsi avant de prendre une décision.

Mme Catherine Morin-Desailly, présidente. – Il ne s'agit pas ici d'appliquer ou non une loi qui n'existerait pas sur la souveraineté, mais de s'émouvoir de l'absence d'appel d'offres et d'une procédure non respectée.

Mme Laure de La Raudière. – Je n'en connais pas la raison car je n'étais pas présente en 2020.

Mme Marie-Laure Denis. – Sur ce sujet, le collège de la Cnil a obtenu du Gouvernement des garanties s'agissant du non-transfert du Système national des données de santé (SNDS) sur la plateforme des données de santé, précisément parce qu'elle est hébergée par Microsoft, tant que cet hébergement de données n'est pas immunisé contre des accès d'autorités étrangères.

Par ailleurs, la Cnil a beaucoup travaillé avec l'Agence nationale de la sécurité des systèmes d'information (Anssi) sur la certification

SecNumCloud qui permet de sécuriser l'hébergement des données les plus sensibles, dont la liste vient d'être précisée par une circulaire du 31 mai de la Première ministre. Les entreprises conformes à ce référentiel SecNumCloud le seront aussi aux exigences en matière de transfert de données, de non-transfert des données, ou de localisation des données des Français de façon sécurisée.

Mme Catherine Morin-Desailly, présidente. – Vous n'avez pas répondu à ma question sur l'inscription dans le texte de la notion de données sensibles ou stratégiques pour la Nation.

Mme Marie-Laure Denis. – Des données sensibles sont présentes dans le RGPD. Les données biométriques, de santé, des mineurs, sont qualifiées de données sensibles méritant une protection particulière. Dans la circulaire du 31 mai, la Première ministre détaille avec la rubrique R9 les catégories de données devant être hébergées par des systèmes d'informatique en nuage parfaitement sécurisés. Les services de la Cnil auront à cœur de clarifier les règles applicables, *a fortiori* dans l'hypothèse d'une décision d'adéquation prochaine prise par la Commission européenne sur la question des transferts de données entre l'Union européenne et les États-Unis.

Mme Catherine Morin-Desailly, présidente. – Le Gouvernement a en effet répondu aux sollicitations constantes du Parlement sur cette question très stratégique des données sensibles.

Mme Laure de La Raudière. – Il faut distinguer les données sensibles et les données stratégiques. Les premières couvrent la santé et la sécurité, quand les secondes peuvent avoir un lien avec les données économiques.

Mme Catherine Morin-Desailly, présidente. – Je parlais des données stratégiques pour notre sécurité nationale.

Je vous remercie pour votre participation éclairante.

Audition de Lucas Verney,
directeur adjoint du Pôle d'expertise de la régulation numérique (PEReN)

Mardi 13 juin 2023

Mme Catherine Morin-Desailly, présidente. – Nous accueillons aujourd'hui M. Lucas Verney, directeur adjoint du Pôle d'expertise de la régulation numérique, le PEReN.

Le PEReN est un service à compétence nationale, créé en 2020, placé sous l'autorité conjointe des ministres chargés de l'économie, de la culture et du numérique. Il répond à un enjeu crucial, que nous avons tous identifié depuis bien longtemps : le déséquilibre majeur dans l'expertise technique entre les États et les grands opérateurs du numérique, qui disposent de budgets de plusieurs milliards d'euros et de compétences parmi les meilleures du monde.

Dans ce contexte, trop souvent, les entreprises nous renvoient à notre manque de compétences techniques et à notre incapacité à simplement comprendre les logiques algorithmiques, le traitement massif des données, *etc.*

Le PEReN est déjà intervenu comme expert, notamment aux côtés de la Cnil pour la détermination d'une solution technique de contrôle de l'âge (le « double anonymat »). Je tiens d'ailleurs à citer votre rapport de mai 2022 sur le sujet.

Le PEReN doit donc apporter une expertise et une crédibilité à la France. L'article 16 permet de renforcer vos capacités de collecte de données publiques et d'analyse à des fins de recherche publique, tandis que l'article 18 vise à faciliter votre coopération avec l'Arcom : vous allez pouvoir nous en dire un mot.

Au-delà, nous serons heureux de bénéficier de votre regard d'expert sur l'évolution des technologies, et les moyens pour nous de les encadrer pour les cantonner au service de leurs utilisateurs, en limitant le plus possible les effets toxiques qui, malheureusement, obscurcissent Internet.

Je vais vous laisser une dizaine de minutes pour présenter le PEReN (que quelques-uns d'entre nous ont visité il y a quelques semaines) et surtout la place qui lui est faite dans le projet de loi. Je passerai ensuite la parole aux rapporteurs, puis à l'ensemble des membres de la commission spéciale.

M. Lucas Verney, directeur adjoint du Pôle d'expertise de la régulation numérique (PEReN). – Comme vous l'avez indiqué, le PEReN est un service à compétence nationale, sous la triple tutelle du ministère de la culture, du ministère de l'économie et des finances et du ministère chargé du numérique. Son objectif est de mutualiser une expertise technique et de capitaliser cette expertise au sein de l'État, à destination des services de l'État

et des autorités indépendantes, pour toutes les missions qui ont trait à la régulation des plateformes numériques. Ce service compte aujourd'hui 25 personnes, exclusivement des ingénieurs, docteurs et experts en sciences des données. Cet effectif constitue le plafond d'emploi fixé pour notre service.

Le PEReN peut intervenir dans deux principaux types de missions. D'une part, il peut apporter des éclairages, notes, études à destination des services de l'État, des administrations, des autorités et du grand public. Les travaux du PEReN sur les systèmes de vérification de l'âge et la protection des mineurs viennent d'être évoqués. Nous sommes intervenus par exemple en appui des négociations sur le règlement européen *Child sexual abuse material (CSAM)*. Ces éléments ont conduit le PEReN à être auditionné par le Sénat il y a un an sur ce sujet et un certain nombre de publications sont en ligne sur notre site web, notamment des éléments sur la protection des mineurs et la vérification de l'âge.

Plus récemment, nous sommes intervenus sur des questions d'actualité, en particulier autour de l'émergence de l'Intelligence artificielle (IA) dite générative (dont ChatGPT est un exemple). Nous serons prochainement auditionnés à l'Assemblée nationale sur ces questions. Nous animons aussi un certain nombre de groupes de travail entre les différentes administrations sur des questions techniques afin de partager entre administrations une compréhension commune des enjeux techniques de telle ou telle technologie. Il existe par exemple un groupe de travail créé sur l'initiative *Privacy Sandbox* de Google, qui vise à supprimer les cookies tiers dans le navigateur et plus récemment la création d'un groupe de travail sur les *dark patterns*.

Le second type de missions a trait au développement d'outils et d'analyses pour le compte des différentes administrations. Nous pouvons le faire directement, en mobilisant les pouvoirs de nos partenaires administratifs pour les services de l'État, à travers le décret de création du PEReN qui lui confie ces missions. Pour les autorités indépendantes, nous le faisons en vertu de l'alinéa 1 de l'article 36 de la loi du 25 octobre 2021, qui permet à huit autorités indépendantes énumérées dans un décret pris en Conseil d'État de faire appel au PEReN pour la conduite de ces projets. Ces sept autorités sont :

- l'Autorité de la concurrence (ADC) ;
- l'Autorité des marchés financiers (AMF) ;
- l'Autorité nationale des jeux (ANJ) ;
- l'Autorité de régulation des communications électroniques (Arcep) ;
- l'Autorité de régulation des transports (ART) ;

– la Commission nationale de l'informatique et des libertés (Cnil) ;

– le Défenseur des droits.

Ces outils peuvent être développés dans le cadre de conventions passées avec des partenaires administratifs. Ils peuvent aussi être développés en propre par le PEReN, à travers deux modalités prévues par l'article 36 de la loi du 25 octobre 2021. L'alinéa 6 de cet article prévoit ainsi, dans sa formulation actuelle, la possibilité, pour le PEReN, de conduire des travaux de recherche publique, ce qui permet au PEReN de se maintenir à niveau et de contribuer à l'état de l'art scientifique sur des questions liées à l'intelligence artificielle ou à la régulation des plateformes. À ce titre, nous travaillons notamment sur des questions d'articulation et des aspects techniques d'analyse multimodale, pour des contenus qui allient du texte et de l'image – alors que jusqu'à présent, les modèles sont plutôt définis pour du texte ou pour des images. Tous ces travaux font l'objet de publications lors de conférences, avec une revue par les pairs. Nous avons notamment participé à des conférences de groupes de travail du CNRS. Ces outils sont placés en *open source* dès lors que ceci ne nuit pas aux finalités pour lesquelles ils ont été conçus.

Enfin, l'alinéa 5 de l'article 36 confère au PEReN un pouvoir d'expérimentation. Le PEReN peut, à ce titre, bénéficier de facilités pour collecter des données publiquement disponibles sur les plateformes et développer des outils sur la base de ces données. Ce pouvoir a été conçu de manière à pouvoir développer l'outil tout en préservant une collecte des données équitable. Toutes les données doivent ainsi être supprimées au plus tard neuf mois après leur collecte. Seul l'outil construit peut être conservé. Il peut ensuite être reversé à une administration ou à une autorité qui le mettrait en œuvre dans le cadre de ses missions.

Ces modalités (alinéas 5 et 6 de l'article 36) font l'objet d'un rapport au Parlement et à la Cnil. La première édition de ce rapport a été transmise en mai 2023.

Ces éléments ne sont pas nécessairement publics. Nous avons réalisé en particulier un certain nombre de travaux sur la plateforme TikTok, ce qui a conduit à l'audition du PEReN par la commission d'enquête du Sénat sur TikTok. Nous avons également conduit des travaux sur Amazon, afin de comprendre comment s'articulaient les différentes places de marché au niveau européen et saisir les spécificités d'Amazon France par rapport à Amazon Allemagne ou Amazon Espagne, par exemple, en termes de nationalité des vendeurs et de prédominance de ceux-ci dans ce qui s'appelle l'*apply box*, c'est-à-dire le carré d'achat en un clic.

Ce cadre actuel souffre de certaines limites. S'agissant des modalités d'expérimentation, certaines de ces limites ont été détaillées dans le rapport au Parlement. Les plateformes coopèrent plus ou moins. Certaines coopèrent activement et nous fournissent des données en levant les quotas ou

restrictions, dans la collecte, à la hauteur de ce que nous demandons. D'autres argumentent, voire invoquent des difficultés techniques, à des degrés divers, pour freiner, voire empêcher notre accès aux données. Ces modalités permettent, par exemple, d'entraîner un réseau de neurones sur la base des données fournies. Au bout de neuf mois, nous supprimons toutes les données et nous ne conservons que le modèle d'IA. Cela ne permet donc pas de tirer des enseignements sur les pratiques observées à partir des données collectées.

Enfin, quant au cadre de l'alinéa 6 (compétence de recherche publique), nous nous heurtons à une dimension discrétionnaire de l'accès aux interfaces de programmation, parfois restreintes aux chercheurs, suite à une interprétation parfois anglo-saxonne de la définition du système éducatif. Certaines plateformes distinguent ainsi ce qui relève des établissements universitaires qui délivrent des diplômes et ce qui relève des instituts de recherche. Le PEReN relève de cette seconde catégorie. Or, pour l'accès à certaines applications de programmation académiques, les plateformes exigent que la demande émane d'une institution qui délivre des diplômes.

Un dernier axe est émergent et concerne la collecte de données sur mobile. Tout ce que j'ai évoqué jusqu'à présent se rapportait à des interfaces de programmation ou à la collecte de données sur des sites web. Cependant, de plus en plus de plateformes sont accessibles uniquement sur des applications mobiles. C'est le cas par exemple de Snapchat. D'autres sont accessibles au travers d'interfaces web ou au travers d'applications mobiles mais il s'agit généralement de deux produits distincts, conçus comme tels en silo au sein de la plateforme. Pour obtenir une réelle compréhension de la plateforme, il faut approcher celle-ci à travers l'interface que les utilisateurs utilisent. Or l'analyse de ces applications mobiles se heurte à deux problématiques. D'une part, une tierce partie entre en ligne de compte dans le fonctionnement de ces applications, à savoir le téléphone et son système d'exploitation, qui donne accès à l'application. Il en découle une spécificité notamment pour les appareils utilisant le système d'exploitation iOS, car Apple a défini des conditions contractuelles très restrictives qui empêchent le PEReN de conduire un certain nombre d'analyses, sauf à ne pas respecter ces clauses contractuelles. C'est un élément bloquant pour des projets portant sur les systèmes iOS, sachant que l'alinéa 5 de l'article 36 prévoit de notifier l'opérateur de la plateforme. Or, en l'espèce, ce n'est pas lui qui impose les conditions générales d'utilisation (CGU) mais une entité tierce, le fournisseur du système d'exploitation.

Par ailleurs, dès lors que nous examinons les applications mobiles, cela suppose d'instrumenter un téléphone, de simuler des comportements et d'étudier le fonctionnement de l'application, un peu comme on étudierait des bactéries dans une boîte de Petri, en contrôlant l'environnement dans lequel s'exécute l'application. Ces éléments peuvent nécessiter un cadrage

juridique plus fort afin d'affirmer la possibilité, pour le PEReN, de conduire ces analyses.

Ce sont des travaux que nous avons pu esquisser devant la commission d'enquête sénatoriale sur TikTok. Il s'agit d'examiner comment fonctionne l'application, quelles données sont collectées, à quel moment, selon quelles modalités, de quelle manière elles sont éventuellement transmises sur le réseau, etc. L'analyse de ces aspects pourrait nécessiter un renforcement des compétences confiées au PEReN.

Le présent projet de loi offre un élargissement des missions du PEReN, qui sort ainsi de son rôle d'expérimentation. Ce texte l'inscrit dans une nouvelle dynamique tout en le confortant. Il instaure également une modalité de coopération avec l'Arcom, en qualité de future coordinateur des services numériques. C'est une disposition qui est de nature à donner à l'Arcom la garantie de pouvoir faire appel au PEReN dans des conditions cohérentes avec ses nouvelles missions et ses nouvelles compétences.

Néanmoins, il faut prendre garde à la charge qui pèse sur ce jeune service. Nous sommes 25 aujourd'hui. Tel était le plafond d'emploi qui avait été défini par le décret de création du PEReN. Celui-ci travaille sur la base d'une feuille de route annuelle : chaque automne, nous nous concertons avec toutes les autorités ayant des compétences de régulation des plateformes numériques et nous construisons avec elles un catalogue de projets qui constitue la feuille de route qui sera déroulée durant l'année. Cette feuille de route représente un nombre de projets qui a été multiplié par quatre depuis la création du service jusqu'à ce jour. Cette montée en puissance s'est faite, jusqu'à présent, en cohérence et de façon synchronisée avec l'augmentation des effectifs du service (trois personnes en 2020, 25 personnes aujourd'hui). Nous devons cependant, de plus en plus, définir des priorités et des arbitrages, voire refuser certains projets par manque de ressources.

Cette situation est actuellement gérable dans la mesure où il y a très peu d'impératifs temporels : ces projets doivent être réalisés au cours de l'année tout en permettant un lissage de la charge sur l'ensemble de l'année. Si de nouvelles missions donnaient naissance à des projets assortis de délais contraints, le PEReN serait alors soumis à des exigences de réactivité et cela pourrait avoir des impacts quant au volume de projets pouvant être traités dans le cadre de notre feuille de route annuelle.

Ce projet de loi permet aussi de réaffirmer et d'étendre les modalités d'accès aux données du PEReN, en particulier en mobilisant l'article 34 du *DSA* (*Digital Services Act*, ou règlement des services numériques) et en réaffirmant son caractère d'institut de recherche publique, qui est parfois nié par les plateformes numériques. Pour autant, le projet de loi ne résout pas toutes les difficultés, en particulier celles qui sont liées aux applications mobiles.

En conclusion, le PEReN travaille depuis trois ans à des missions de plus en plus larges, toujours liées à la régulation du numérique. Nous avons développé depuis notre création une approche modulaire : nous nous efforçons de construire chaque projet en tant que brique élémentaire pouvant être ensuite interconnectée avec d'autres briques pour constituer des projets plus importants. S'agissant par exemple d'une analyse algorithmique d'une plateforme de recommandation de vidéos, une brique traitera de la collecte de données, une autre de l'analyse statistique et une autre effectuera peut-être une rétroaction entre les deux. Nous avons conçu et affiné ces trois briques depuis trois ans de sorte que chacune ait le maximum d'efficacité. Le coût d'incrément, pour un nouveau projet, consiste essentiellement à recombiner ces briques et à les étendre un peu. La feuille de route du PEReN s'apparente donc parfois à un jeu de Lego, ce qui permet d'absorber un grand volume de projets et de fournir un grand volume de résultats, tout en mutualisant le plus possible les outils développés.

Ce projet de loi nous apporte une sécurisation de certaines pratiques et offre la perspective de nombreuses nouvelles collaborations. Parallèlement à ces initiatives nationales, nous avons des échanges au niveau européen avec la Commission européenne, qui s'est inspirée du modèle du PEReN pour construire le Centre européen pour la transparence algorithmique de Séville *(ECAT)*. Le PEReN est en train de signer une convention tripartite avec la Commission européenne et le centre commun de recherche *ECAT* afin de pouvoir travailler directement sur les questions d'application du RSN et du RMN.

Enfin, l'article 18 de la loi du 25 octobre 2021 portant sur l'articulation avec le coordinateur des services numériques et les modalités d'accès aux données, le PEReN est aussi affecté, à la marge, par la disparition de l'article L. 111-7 du Code de la consommation, qui portait la définition d'une plateforme numérique. L'article 36, de mémoire, reprend cette formulation afin que continue d'apparaître une définition des plateformes numériques sur la base de laquelle le PEReN peut intervenir.

Mme Catherine Morin-Desailly, présidente. – Si je comprends bien, vous aurez un statut vous permettant d'effectuer des recherches sur les plateformes, dans le cadre permis par le *DSA*.

M. Lucas Verney. – Nous aurons le statut de chercheurs, ce qui permet d'accéder à des données publiquement disponibles. Il existe une forme d'articulation avec le coordinateur des services numériques permettant de travailler avec lui sur des données plus spécifiques, éventuellement non publiques. Il existe aussi la convention en cours de signature avec la Commission européenne, qui permettra de travailler sur des plateformes d'envergure européenne.

Mme Catherine Morin-Desailly, présidente. – C'est un aspect très important. Nous nous étions posé cette question lors de l'examen du RSN.

M. Patrick Chaize, rapporteur. – Quel sera l'impact des dispositions du projet de loi sur votre service, en particulier du point de vue des moyens financiers et humains à votre disposition ?

Au titre de l'article 16, votre accès aux données est-il actuellement suffisant pour mener à bien vos travaux ? À quelles autres données auriez-vous besoin d'accéder ? Le cadre juridique actuel est-il suffisant pour vous garantir l'accès à ces données ?

S'agissant de l'article 17, quel est le retour d'expérience du PEReN sur l'expérimentation « API meublé » en 2022 ? Le dispositif prévu à l'article 17 est-il dans les faits une généralisation de cette expérimentation ?

Les dispositions de l'article 18 renforcent-elles la coopération avec l'Arcom, déjà inscrite à l'article 36 de la loi sur la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique ? En quoi est-il nécessaire, selon vous, d'inscrire cette coopération avec l'Arcom dans la loi ?

M. Lucas Verney. – En ce qui concerne l'article 17, le PEReN a travaillé dès sa création avec la direction générale des entreprises afin de réaliser les développements techniques nécessaires pour l'expérimentation « API meublé », c'est-à-dire pour réaliser le socle logiciel qui l'a rendue possible et héberger cette solution de logiciels sur des serveurs de PEReN, ainsi que pour réaliser l'interface avec les équipes techniques auprès des plateformes et permettre une certaine fluidité dans les échanges.

Cinq plateformes et cinq communes se sont inscrites pour participer à cette expérimentation. Son bilan est très positif : elle a donné lieu à une simplification des échanges et globalement à une montée en qualité des données transmises. Les dispositions de l'article 17 reprennent essentiellement les enseignements de cette expérimentation, en n'allant peut-être pas aussi loin dans la démarche volontaire de montée en qualité des données. Au titre de l'expérimentation, il existait notamment la volonté de consolider des données et de fournir aux communes qui le souhaitaient des données déjà consolidées entre les différentes plateformes, avec des heuristiques visant par exemple à supprimer des ambiguïtés afin de distinguer des logements similaires. Les modalités définies par l'article 17 ne portent que sur la transmission des données.

Comme je l'ai indiqué, le PEReN compte 25 personnes, ce qui correspond au plafond d'emploi qui a été défini sur la base de ses missions, définies par le décret de création du PEReN. Le service connaît un rythme de croissance soutenu. Réussir à recruter 25 personnes, avec des profils d'ingénieurs et de docteurs en sciences des données, pour construire un service capable, au sein de l'État, de dialoguer avec nos homologues au sein des plateformes, n'était pas chose acquise d'avance mais cet objectif a été atteint. Les profils qui composent notre équipe sont accessibles en ligne. Ce sont majoritairement des personnes qui auraient pu faire le choix de rejoindre les GAFAM mais qui ont préféré rejoindre le PEReN. C'est un très

beau succès qu'il faut inscrire dans la durée, ce qui peut faire naître des questions sur le plan des ressources humaines, avec le souci de conserver et capitaliser ces ressources au sein de l'État.

Sur le plan budgétaire, le PEReN fonctionne de façon assez légère et économe en ressources. L'objectif du PEReN est de conduire l'intégralité des projets de A à Z en propre, de sorte que la compétence technique et numérique soit capitalisée au sein de l'État. Le PEReN opère en particulier ses propres infrastructures SI, c'est-à-dire ses propres serveurs. Lorsqu'il faut entraîner des modèles, nous les entraînons sur nos propres machines de calcul. Lorsqu'il existe des besoins spécifiques, nous bénéficions d'un accès, notamment, au supercalculateur Jean Zay, afin de pouvoir manipuler des modèles tels que ChatGPT, qui sont d'envergure.

Le service a été créé à partir de fonds d'investissement, de fonds de transformation ministériels et de fonds du plan de relance à hauteur de 500 000 euros. Le PEReN fonctionne aujourd'hui, en régime continu (hors de l'élargissement prévu de ses missions) avec une ligne budgétaire de 100 000 euros, hors T2, c'est-à-dire uniquement pour couvrir les frais de mission et les coûts d'infrastructures (en incluant l'ensemble du matériel nécessaire à la conduite de nos projets).

Ce projet de loi confie de nouvelles missions au PEReN. Nous voyons affluer des demandes de plus en plus nombreuses de la part des autorités pouvant déjà solliciter le PEReN. Le nombre de projets inscrits à notre feuille de route annuelle connaît une multiplication par quatre, ce qui impose de plus en plus d'arbitrages. Jusqu'à présent, la priorisation n'a jamais dû être revue ni posé de difficultés, dans la mesure où en jouant sur les éléments de calendrier, nous parvenons assez bien à répondre à la demande. Certaines administrations nous commandent des projets qui ne se concrétisent pas dans l'année, ce qui permet finalement de satisfaire l'ensemble des demandes. Si l'on ajoute des contraintes en termes d'échéances et de livraison des projets, du fait de procédures ou de contentieux, par exemple, cela impliquerait une réactivité du service qui pourrait limiter le nombre de projets que nous pourrions traiter.

J'ai aussi une remarque générale sur la formulation de l'alinéa 5 (pouvoirs d'expérimentation du PEReN), qui prévoit actuellement une notification des plateformes. Lorsque nous exerçons ce pouvoir, qui nous permet essentiellement de collecter des données sur les interfaces publiques sans restriction, moyennant la notification de la plateforme, celle-ci dispose d'un délai de deux mois, pour formuler des observations. Passé ce délai, nous pouvons mettre en œuvre la collecte. Il existe aujourd'hui une asymétrie entre cette modalité et la modalité de recherche publique, pour laquelle aucune notification n'est à effectuer : nous sommes alignés sur le cadre d'un institut de recherche publique. Avec la formulation actuelle du projet de loi, une factorisation a été faite et nous devrions également notifier les plateformes pour des activités de recherche publique,

ce qui peut induire une charge administrative supplémentaire pour le service, au détriment de projets techniques.

L'Arcom figure déjà sur le décret pris en Conseil d'État, ce qui lui permet de solliciter le PEReN. Un certain nombre de projets sont déjà conduits pour le compte de l'Arcom au titre de ses compétences passées (en particulier les compétences issues de l'ancien Conseil supérieur de l'audiovisuel et de l'ancienne Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet), notamment sur des questions de modération d'offres illégales en ligne et de désinformation. Aujourd'hui, l'Arcom est un partenaire du PEReN comme un autre. Elle nous propose des projets inscrits à notre feuille de route, laquelle fait l'objet, *in fine*, d'arbitrages par les trois ministres de tutelle. Cette proposition, dans le projet de loi, vise à réaffirmer la possibilité, pour l'Arcom, en qualité de *DSC*, de saisir directement le PEReN pour bénéficier de son expertise technique. Elle permettrait, en cela, d'anticiper et de garantir une bonne disponibilité des équipes pour les besoins spécifiques aux *DSC*.

M. Loïc Hervé, rapporteur. – Avez-vous les moyens d'analyser le fonctionnement des algorithmes que les plateformes utilisent pour la modération de leurs contenus ? On nous a parlé de logiciels qui viennent des États-Unis. Avez-vous les moyens d'analyser la manière dont les plateformes régulent les contenus, notamment du point de vue du risque de « sur-censure », lorsqu'elles font appel à l'intelligence artificielle ? Tous ceux qui sont familiers des réseaux sociaux ont eu l'expérience de voir censurés des contenus relativement anodins en raison d'un mot ou d'une image considérés comme contrevenant aux conditions générales d'utilisation de la plateforme. Allez-vous conserver une compétence nationale en la matière et de quelle manière allez-vous articuler vos travaux avec le Centre européen pour la transparence algorithmique de Séville ?

Pouvez-vous faire le point sur les travaux du PEReN sur les dispositifs de contrôle de l'âge ? De votre point de vue, et sans prendre en compte les questions liées à la vie privée, quels sont les dispositifs qui vous semblent les plus fiables techniquement ? Y a-t-il des spécificités à prévoir selon que la consultation a lieu sur Internet ou *via* une application ?

L'article 5 crée une nouvelle peine complémentaire « de bannissement » et fixe pour les plateformes une obligation de moyens pour le blocage des autres comptes de la personne condamnée. Quels sont les moyens techniques qui pourraient être déployés pour répondre à cette obligation de moyens et existe-t-il des moyens de s'assurer que la personne bannie ne pourra pas utiliser un autre compte que celui qui lui est officiellement rattaché ?

M. Lucas Verney. – L'audit algorithmique constitue l'une des raisons d'être du PEReN. Ce sont des méthodes que le PEReN a développées

depuis sa création. Il continue de les consolider et elles font aujourd'hui l'objet d'une thèse en co-tutelle avec un laboratoire de l'INRIA à Rennes.

Le PEReN n'a pas vocation à être un régulateur. Il n'a pas accès à des données internes. Il peut travailler avec des régulateurs ayant accès à des données privilégiées, notamment au titre de l'alinéa 1. Le PEReN travaille donc sur la base de données publiques, ce qui oriente la façon dont nous concevons un audit algorithmique aujourd'hui. Nous procédons par une analyse statistique des informations accessibles publiquement sur un site, une plateforme ou un réseau social et en essayant, sur la base de ces informations, de déterminer les grands comportements de ces algorithmes. Sans entrer dans le détail, une application directe de ces principes concerne la directive *Platform to Business (PtoB)* européenne, qui impose aux plateformes de décrire les grands paramètres qui influent sur les recommandations. Si l'on parcourt par exemple une liste d'hôtels, celle-ci sera peut-être triée, par défaut, par pertinence. Quelle est cette notion de pertinence ? La plateforme doit indiquer que la pertinence se définit, si tel est le cas, par le degré d'adéquation entre la recherche et l'hôtel proposé. Il peut s'agir du prix, du niveau de la commission, etc. En simulant un certain nombre de recherches et par une analyse statistique des listes proposées, on peut reconstruire des pondérations ou des approximations de ces pondérations pour les différentes variables entrant en ligne de compte et ainsi confronter les principaux paramètres déclarés par la plateforme, quant aux paramètres utilisés, avec ce qui est constaté sur le site web.

Sur cette base, nous n'avons à ce stade qu'une heuristique de détection. Peut-être n'avons-nous pas les mêmes résultats que ce que la plateforme annonce. Il peut s'agir d'une erreur statistique, d'un véritable biais ou d'une triche. Le travail du PEReN peut permettre d'indiquer que, sur la base de données publiques, on constate que l'algorithme se comporte bizarrement pour telle ou telle recherche. Le régulateur peut alors se saisir de ce dossier et solliciter des données qui représentent des accès proportionnés, puisque justifiés par un comportement inexplicable.

Le même principe peut se décliner pour des questions de modération ou de recommandation. Le PEReN a conduit en particulier un certain nombre de travaux pour analyser des « parcours utilisateur » et la manière dont une application de contenus vidéo pourrait entraîner un utilisateur d'un ensemble de contenus à un autre. Nous pourrions chercher à comprendre la façon dont cette « bulle de filtre » se comporte et la manière dont l'utilisateur évolue dans cette bulle de filtre. Ces travaux ont été présentés lors de l'inauguration du Centre européen pour la transparence algorithmique. Je vous invite à consulter, sur notre site Internet, une vidéo explicative qui illustre, par des captures d'écran, la manière dont cet audit peut être conduit.

Le Centre européen pour la transparence algorithmique *(ECAT)* est construit en s'inspirant fortement du modèle du PEReN. Nous échangeons

régulièrement avec eux pour accompagner leur installation et leur montée en compétences du point de vue des outils, des méthodes de collecte des données ou encore dans l'approche vis-à-vis des plateformes numériques. Il s'agit aussi d'articuler nos travaux efficacement afin de collaborer dans le futur à travers la convention passée avec l'*ECAT*.

Un certain nombre de travaux sont en cours sur le contrôle de majorité. Des discussions ont lieu avec des acteurs privés qui proposent des premières solutions. Le PEReN est associé à ces discussions, tant pour l'analyse technique que, dans la mesure du possible, pour le test de la robustesse de ces systèmes au regard de différentes altérations. Pour un système basé sur un flux vidéo, nous pouvons par exemple essayer de l'attaquer en lui présentant une photo plutôt qu'une vraie personne, de façon à voir s'il résiste à ce type d'approche. On peut ainsi tester les limites effectives de ces différentes solutions. À ce jour, il existe plusieurs options disponibles. Elles impliquent des arbitrages, qui ne relèvent pas du PEReN, entre des considérations de vie privée, de fiabilité et d'efficacité. La solution la plus efficace est probablement la vérification en personne chez un buraliste ou dans un bureau de poste, sur présentation d'une carte d'identité. C'est aussi la solution la plus intrusive, qui soulève probablement des questions d'acceptabilité.

Un certain nombre de sociétés développent des outils de vérification de l'identité d'une personne à distance, sur la base d'une vérification de la carte d'identité ou sur la base d'une captation d'images vidéo. Le PEReN travaille sur ces solutions en testant là aussi différentes altérations ou attaques possibles (filtre, *deep fake*, détournement, *etc.*). La portion pour laquelle le PEReN peut intervenir ne constitue en tout cas que la portion technique du fonctionnement de ces solutions et concernant la robustesse de celles-ci. Elles s'insèrent dans un écosystème plus large d'utilisateurs, qui ont eux-mêmes des stratégies de détournement ou de contournement ne pouvant pas toujours être anticipées ou appréciées avec les outils dont dispose le PEReN.

Les conséquences ne sont pas tout à fait les mêmes selon que la consultation d'un site Internet a lieu sur une application mobile ou sur un ordinateur. Dans le cas d'une consultation à partir d'un ordinateur, le navigateur met en relation l'internaute et le site mais peu de briques techniques ont la capacité de connaître l'âge de l'utilisateur et de couper éventuellement la connexion en fonction de cette information.

Les applications mobiles dédiées sont principalement diffusées par deux magasins, le Google Play Store et l'Apple App Store. Ces deux magasins d'applications sont très fortement intégrés au système, couplés au contrôle parental. Ils ont connaissance en particulier du système PEGI qui permet d'appliquer des restrictions d'âge aux applications diffusées. Ils ont connaissance du fait que l'utilisateur est majeur ou non, suivant la configuration de l'appareil. Restreindre l'installation d'une application

mobile est donc plus facile que de restreindre l'accès à un site Internet. Le PEReN est aussi associé à un certain nombre d'échanges autour de solutions techniques qui pourraient faciliter au moins la déclaration volontaire du caractère restreint aux mineurs, le cas échéant, de telle ou telle ressource en ligne.

Enfin, le sujet du bannissement peut se rapprocher, à certains égards, de la question de la vérification d'âge. Il faut, pour mettre en place un bannissement, disposer d'une liste d'identifiants ou de comptes à bloquer et confronter les identifiants de cette liste à ceux fournis par un utilisateur lors de son inscription sur un site. L'une des solutions les plus simples consiste à établir une liste noire d'adresses mail, car cette adresse est aujourd'hui l'identifiant utilisé de manière quasi universelle pour créer un compte. Nous pourrions, lors de l'inscription sur un réseau social, comparer l'adresse mail fournie à celles figurant sur une liste noire. Ce dispositif permet le bannissement mais ne serait pas nécessairement le plus efficace puisqu'il est très facile de recréer une adresse mail et ainsi contourner ce mécanisme. Au lieu de rechercher une preuve de majorité, nous pourrions fonder le dispositif sur une preuve de non-bannissement, sur la base d'un test à jouer, par exemple avec sa carte d'identité. C'est techniquement possible et cela ne présente pas le même degré d'intrusion dans la vie privée. Le PEReN a pour rôle d'établir le panorama des solutions techniques envisageables en indiquant leurs limites mais la question du choix de l'une ou l'autre de ces solutions dépasse ce seul cadre technique.

Mme Catherine Morin-Desailly, présidente. – Avez-vous les moyens d'expertiser et d'analyser le fonctionnement de tout type d'application ou d'un algorithme ? Cela renvoie à une proposition que nous avions faite au sein de la Commission des affaires européennes, selon laquelle on ne pourrait mettre sur le marché une application ou une plateforme que si elle a été analysée, expertisée et que si une autorité compétente a vérifié l'absence d'effets pervers ou délétères dans son utilisation. Sous réserve que vous disposiez des moyens requis, auriez-vous, dans l'absolu, la possibilité de réaliser cette analyse ?

M. Lucas Verney. – La question est différente selon que l'on cherche à démontrer l'existence ou l'absence d'un comportement problématique. Il est possible, à l'échelle du PEReN, d'identifier des comportements problématiques sur des plateformes et, dès lors que nous avons une première heuristique, de creuser celle-ci pour la transformer en une constatation effective. À l'inverse, réaliser l'audit d'une application et démontrer qu'en aucun cas son algorithme ne se comporte de manière problématique nécessite une exhaustivité qui a des implications tout autres en termes de charge et d'analyses à conduire.

Aujourd'hui, le PEReN peut disposer de trois sources de données publiques. Les premières sont les éléments volontairement mis en ligne par les plateformes. On peut penser par exemple aux rapports de transparence.

Ce sont des jeux de données (ou parfois des documents) très peu structurés, présentant une granularité informationnelle et temporelle très large, et qui fournissent peu d'enseignements en pratique, en dehors de grandes lignes. Ces éléments sont très minoritairement utilisés par le PEReN.

La deuxième source est constituée par des interfaces de programmation dites publiquement disponibles. Dès lors qu'elles sont mises à la disposition d'un tiers, le PEReN peut s'y connecter, au titre de son pouvoir d'expérimentation ou de ses compétences d'institut de recherche. Ces interfaces offrent des données très fines, parfaitement structurées et des quotas d'accès assez élevés et assez faciles à suivre. En contrepartie, nous sommes complètement observés par la plateforme, qui sait que nous accédons à cette interface et dans quelles conditions nous y accédons.

La troisième modalité relève du « *scraping* », c'est-à-dire le moissonnage de données, en se connectant directement sur les mêmes interfaces que celles utilisées par les utilisateurs, soit sur le site web soit dans l'application mobile. Cette collecte garantit d'obtenir des données aussi proches que possible du comportement de la plateforme en production mais elle est très limitée en volume car elle est très coûteuse : cela nécessite une approche plateforme par plateforme, en développant du code spécifiquement pour chaque plateforme. S'y ajoutent des restrictions imposées par les plateformes afin d'éviter ce trafic automatisé qui, en dehors du cadre du PEReN, est généralement malveillant.

Ces deux dernières modalités s'articulent l'une et l'autre et se font écho. L'une des approches du PEReN consiste à bâtir, sur la base de données publiquement disponibles, des méthodes qui permettent de collecter de nombreuses données à travers des API et d'échantillonner par du *scraping* les données ainsi recueillies afin de vérifier que la plateforme se comporte de manière loyale dans ces API, en cohérence avec ce que l'on observe sur le site en production. Il s'agit, en d'autres termes, de contrer « l'effet Volkswagen », c'est-à-dire le cas de figure dans lequel la plateforme, se sachant auditée, adapte ses réponses. Nous construisons des méthodes qui offrent certaines garanties de ce point de vue. Cette méthode peut être mise en œuvre dès lors qu'un algorithme est publiquement visible, exposé à l'utilisateur. Cela vaut par exemple pour des algorithmes de fixation du prix sur des plateformes de VTC et de livraison de repas, pour des algorithmes de recommandation de contenus ou de partage de vidéos ou encore pour des algorithmes de classement sur des plateformes de type *Marketplace* où opèrent de nombreux vendeurs différents. C'est plus compliqué pour des algorithmes de modération qui, par définition, sont internes à la plateforme : on peut alors avoir des traces de la modération appliquée en suivant les contenus que l'on voit de manière transitoire sur la plateforme, puis qui disparaissent. Cela veut dire qu'ils ont été probablement modérés (ou retirés par l'utilisateur). Nous avons certains projets bâtis sur ce volet. Un nouveau mode d'accès à des données, du fait des nouvelles compétences qu'aura le PEReN au titre

du RSN, consistera à accéder à des données internes, par le biais du coordinateur des services numériques ou par le biais des accès réservés aux chercheurs, afin d'analyser spécifiquement ces algorithmes internes à la plateforme.

Mme Alexandra Borchio Fontimp. – Selon vous, le recours à l'intelligence artificielle pourrait-il permettre une détection meilleure et plus rapide des contenus illicites sur Internet ? Si oui, quels seraient à vos yeux les garde-fous essentiels à mettre en place pour assurer un bon traitement des données personnelles ? Autrement dit, comment l'IA peut-elle contribuer à développer des solutions techniques qui rendraient efficientes les réglementations futures ?

M. Lucas Verney. – Nous utilisons l'IA en propre, au sein du PEReN, avec des objectifs assez proches. Nous entraînons et affinons certains modèles d'IA à l'état de l'art pour conduire des analyses, en particulier sur des effets de modération, dans le but de construire des modèles qui nous donnent des heuristiques permettant de savoir si tel ou tel contenu est susceptible d'être modéré ou non. Ces travaux sont un peu différents du cadre dans lequel ils seraient mis en œuvre par une plateforme, puisque notre objectif est de déployer une stratégie à grosse maille à des fins de minimisation. Nous ne souhaitons conserver que les contenus qui présentent un intérêt pour l'étude que nous allons mener. Cela reste une heuristique. Pour une plateforme, l'objectif est inverse : il faut avoir le filtre le plus parfait possible, au risque d'amener des censures ou des modérations indues.

Le sujet de l'application éventuelle de l'IA à des modèles de modération est assez vaste et dépend du type de contenu envisagé. Ce n'est pas la même chose d'avoir du texte ou des images, ni de modérer selon tel ou tel prisme. Nous voyons par exemple certains réseaux sociaux qui interdisent des contenus de nudité et « surmodèrent », de ce fait, des contenus relevant d'œuvres culturelles. Cela montre qu'il faut prendre en compte le contexte et peut-être l'IA n'est-elle pas encore suffisamment mature pour faire preuve de cette compréhension du contexte. S'agissant de textes, des questions de réappropriation des termes peuvent se faire jour, en particulier par des communautés pouvant se sentir discriminées. Il s'agit donc de trouver un bon équilibre entre ce qui peut relever d'une modération assez simple (pouvant, de ce fait, mobiliser l'IA) et ce qui doit bénéficier d'une revue humaine ou au moins d'une possibilité « d'appel » afin de permettre, le cas échéant, la restauration rapide des contenus qui auraient été modérés par erreur.

Mme Annick Billon. – Vous avez fait référence, monsieur Verney, à la question de la priorisation en indiquant que jusqu'à présent, vous parveniez à différer certaines des missions qui vous sont confiées. Avec l'élargissement de ces missions, la priorisation peut devenir un problème. L'accès à des mineurs constitue une véritable problématique. Vous avez fait

des propositions en ce sens. Elles n'ont pas été utilisées jusqu'à présent, ce qui démontre que la loi, qui devrait être une priorité, ne l'est pas. Nous devons désormais fixer des priorités, alors que les thèmes qu'embrasse ce projet de loi numérique sont nombreux (pédopornographie, industrie de la pornographie, arnaques, jeux, haine en ligne, terrorisme). Attendez-vous une feuille de route pour prioriser les sujets ?

Ce projet de loi va aussi consacrer une nouvelle gouvernance, une nouvelle organisation et un nouveau fonctionnement des instances, ce qui va induire des relations qui n'existaient pas auparavant, par exemple entre le PEReN et l'Arcom, comme vous l'avez indiqué. Cette nouvelle gouvernance et ces nouvelles manières de travailler seront-elles, selon vous, synonymes d'efficacité et de rapidité – la célérité étant tout aussi nécessaire que les ressources, notamment pour traiter les faits de pédocriminalité ou les infractions liées à la pornographie ?

M. Lucas Verney. – Aujourd'hui, nous parvenons à couvrir un large éventail de besoins. La priorisation se décide sur la base de la mutualisation maximale : le PEReN a vocation à construire en son sein des outils pouvant bénéficier à tous. Dès lors que plusieurs projets se font écho entre des administrations distinctes, ce projet sera traité en priorité, puisqu'il bénéficiera à un plus grand nombre d'administrations. Si nous avons par exemple le projet d'analyse d'un algorithme de recommandation de produit et un projet d'analyse d'un algorithme de recommandation de vidéos, cela reste un algorithme de recommandation. Les méthodes développées seront les mêmes et ces deux projets seront vus par le PEReN comme un seul développement. Conduire ce projet bénéficiera aux deux projets finaux. Actuellement, en l'absence de contraintes et d'impératifs temporels, nous sommes en mesure de lisser la charge sur l'année et de conduire un volume conséquent de projets. Nous en avons 80 inscrits à notre feuille de route cette année.

Cette feuille de route repose sur quatre grandes thématiques en 2023, traduisant les centres d'intérêt et l'expression de besoins qui nous a été adressée.

Le premier de ces piliers est la protection des individus en ligne, ce qui fait écho aux thématiques que nous venons d'évoquer. Notre intervention peut se traduire par l'apport d'éléments techniques en appui aux négociations du règlement européen CSAM sur la pédopornographie. Elle peut porter sur l'évaluation et l'appui aux questions du contrôle de l'âge pour l'accès aux sites pornographiques, ou encore sur la mise en œuvre d'autres droits, en particulier le droit à la portabilité.

Le deuxième axe a trait à la lutte contre les pratiques illégales en ligne. Il s'agit de projets qui nous sont commandés par les régulateurs.

Le troisième axe porte sur la publicité en ligne. Nous évoquions tout à l'heure l'initiative de Google *Privacy Sandbox*. Le groupe de travail animé par le PEReN s'inscrit dans cet axe.

Le quatrième axe, émergent cette année, porte sur l'impact environnemental du numérique, au vu en particulier de l'actualité de l'hiver dernier et des enjeux de charge des réseaux (électrique et Internet). Cet impact constitue aussi un enjeu du point de vue de l'adéquation de la qualité fournie par les services de VOD (vidéo à la demande) en fonction de la connexion Internet de l'utilisateur ou de l'appareil sur lequel il consulte ces contenus.

Nous menons tous ces projets de front. Chaque membre de l'équipe est porteur d'un certain nombre de projets. Nous constituons de petites équipes de deux à quatre personnes, qui sont en relation directe avec nos partenaires pour répondre à leurs besoins et leur transmettre les contenus que nous développons, jusqu'à leur mise en œuvre.

Nos relations avec l'Arcom existent et se fondent sur l'article 36 de la loi du 25 octobre 2021. Il existe déjà un certain nombre de projets avec l'Arcom. Ces dispositions législatives ont instauré la possibilité, pour l'Arcom, en qualité de coordinateur des services numériques, de nous solliciter. Nous devons prendre en compte ces demandes, les anticiper et réserver une certaine allocation de nos ressources, dans notre feuille de route, pour répondre à ces commandes sur les questions liées à l'application du RSN.

Mme Toine Bourrat. **–** Je voudrais évoquer le fléau du cyberharcèlement, qui est amplifié par l'anonymat et le pseudonymat, qui permet de démultiplier le nombre de faux comptes utilisés par une même personne. Existe-t-il ou peut-on imaginer des outils qui permettent de faire le lien entre tous ces comptes sous pseudonyme et la personne qui les aurait créés ?

M. Lucas Verney. – Ce sont bien sûr des sujets d'intérêt pour le PEReN, sur lesquels il est amené à intervenir, qu'il s'agisse de la modération ou de l'évaluation de l'amplitude de ces phénomènes. Je rappelle que l'objectif du PEReN est de construire des outils pour permettre aux administrations compétentes d'appréhender le fonctionnement de ces plateformes, sous le prisme des obligations qui incombent à celles-ci. Il ne s'agit pas d'identifier spécifiquement ces comptes ni d'engager des poursuites.

Mme Catherine Morin-Desailly, présidente. – Existe-t-il l'équivalent d'un PEReN dans chaque État membre européen ?

M. Lucas Verney. – À ma connaissance, il n'y en a qu'un, en France. Il y a quelque temps, nous avons été contactés par des équipes anglaises qui envisageaient de proposer un modèle similaire au Royaume-Uni.

Elles avaient réalisé un grand nombre d'interviews et le PEReN était le seul objet de ce type que leurs recherches avaient identifié.

Je constate que le fait d'avoir mutualisé dans un service ces compétences numériques est assez unique en Europe. Cela a inspiré la Commission pour la mise en œuvre de son ECAT à Séville. Ailleurs, la stratégie consiste plutôt à saupoudrer quelques compétences dans les différentes autorités. Généralement, les autorités régaliennes ou de renseignement sont les mieux dotées, en particulier lorsqu'il est question de contenus terroristes ou pédopornographiques. Nous faisons prévaloir une approche algorithmique et numérique de ces sujets, là où nos homologues sont plutôt issus, la plupart du temps, de la police ou de l'institution judiciaire. Ils ont une approche très « métier », complémentaire, qui n'est pas toujours aussi pointue sur les questions techniques telles que l'efficacité qu'un algorithme de modération automatique peut présenter pour tel type de contenu, ou les ressorts possibles permettant d'amplifier artificiellement ces contenus.

Mme Catherine Morin-Desailly, présidente. – Il est essentiel, au vu des « boîtes noires » que constituent les plateformes, d'avoir une telle expertise. C'est une chance et il est bon que la France joue un rôle moteur dans ce domaine. Nous vous remercions beaucoup de votre participation à cette audition.

Table ronde des sociétés d'informatique en nuage *(clouders)* européennes

Jeudi 15 juin 2023

Mme Catherine Morin-Desailly, présidente. – Notre table ronde de ce jour est consacrée à un sujet essentiel dont nous avons déjà beaucoup parlé, celui de « l'informatique en nuage », ou « *cloud* ». Nous accueillons aujourd'hui Séverine Denys, directrice des relations institutionnelles de Docaposte, et Alain Issarni, directeur général de Numspot ; Damien Lucas, directeur général de Scaleway, et Lucas Buthion, responsable des affaires publiques du groupe Iliad-Free ; Thibault de Tersant, directeur général adjoint d'Outscale, secrétaire général de Dassault Systèmes, et Grégory Abate de la société Outscale, filiale du groupe Dassault Systèmes ; Solange Viegas Dos Reis, directrice juridique et membre du Comité exécutif d'OVHcloud, Blandine Eggrickx, responsable des affaires publiques, et Jean-Paul Smets, vice-président d'Euclidia, une alliance qui réunit des acteurs prêts à fournir sous licence des technologies *cloud* à des gouvernements qui veulent dépendre le moins possible d'acteurs étrangers.

Les sociétés représentées ici incarnent l'avenir du stockage et du traitement des données au niveau européen. Notre continent doit en effet se prémunir le plus possible de la dépendance aux technologies étrangères et de la soumission à l'extra-territorialité, notamment américaine. Cet impératif de souveraineté, grandement défendu par la commission des affaires économiques dans son rapport de l'an dernier, est incarné par le titre III du projet de loi, qui va des articles 7 à 14. Il est en effet consacré au « renforcement de la confiance et de la concurrence dans l'économie de la donnée ». Je veux rappeler quelques données à ce propos : selon l'étude d'impact du projet de loi, au niveau mondial, le *cloud* représenterait 384 milliards d'euros en 2022, et 65 milliards en Europe. Il pourrait être multiplié par 10 d'ici 2030.

À ce propos, nous sommes confrontés à un double problème : d'une part, les entreprises françaises sont en retard dans l'utilisation de l'informatique en nuage, ce qui nuit à leur compétitivité ; d'autre part, là encore, le marché est très concentré et dominé par Amazon Web Services, Microsoft Azure et Google *cloud*, avec une part de marché cumulée de 71 %.

Au-delà de considérations économiques déjà essentielles, le stockage et le traitement des données posent ainsi la question de notre capacité à assurer notre souveraineté. C'est à cela que cherchent à répondre les dispositions du projet de loi, en régulant des pratiques commerciales déloyales qui altèrent la liberté de choix des entreprises ou limitent la portabilité et l'interopérabilité des services, notamment la faculté à changer de fournisseur.

Mme Séverine Denys, directrice des relations institutionnelles de Docaposte. – Vous examinez un texte que nous attendions non seulement sur le sujet du *cloud* mais également sur ses dispositions visant à protéger les enfants, les citoyens, les consommateurs, les entreprises et les collectivités dans les espaces numériques. En tant que filiale du groupe La Poste et partie prenante d'un grand pôle financier public, Docaposte soutient cette initiative qui complète les textes européens sur le numérique, clarifie la situation et propose un cadre cohérent. Au niveau national, ce texte s'inscrit dans une démarche de l'État visant à soutenir l'autonomie industrielle de la France et Docaposte a une position clairement assumée de leadership de la confiance ainsi que de la souveraineté numérique dans les activités comme la banque, la finance, l'assurance, le secteur public et la santé, ce qui nécessite autonomie et régulation. Le texte répond à ces attentes en proposant des dispositions visant à garantir un cadre concurrentiel loyal et un soutien aux acteurs français ou européens dont la part de marché dans le *cloud* n'est pas à la hauteur de nos ambitions.

Une feuille de route a été structurée, pour chacun des secteurs que j'ai mentionnés, sur le développement des services de Docaposte en matière de données et d'intelligence artificielle. La souveraineté des données concernant les consommateurs, les citoyens ou les entreprises mérite une attention particulière. En effet, lorsqu'elles sont réunies, ces données – de faible intérêt si on les considère isolement - peuvent prendre une grande importance. C'est dans cet esprit que nous avons travaillé avec d'autres secteurs et que nous avons annoncé la création de Numspot qui est l'entité spécifiquement dédiée à l'informatique en nuage et que je laisse son directeur général vous présenter.

M. Alain Issarni, directeur général de Numspot. – Numspot est une entreprise toute récente créée en février dernier, avec un actionnariat comprenant la Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Telecom. Ces acteurs se sont associés pour remédier à l'insuffisance quantitative et qualitative de l'offre dans le domaine de l'informatique en nuage. En particulier, il leur est apparu nécessaire de renforcer la sécurité technique et juridique des données surtout vis-à-vis des lois extraterritoriales. Sans entrer dans les détails techniques, les offres existantes sont un peu trop basiques et ne correspondent pas tout à fait aux standards attendus par les entreprises qui souhaitent utiliser le *cloud*.

L'objectif de Numspot est d'adosser à l'offre existante d'Outscale – c'est-à-dire la marque *cloud* de Dassault Systèmes - des couches supplémentaires de prestations dites managées qui permettront aux utilisateurs et aux clients de bénéficier de services *cloud* plus avancés. Notre but est de répondre aux exigences de confiance, de sécurité et de souveraineté en proposant de nouvelles offres conformes au référentiel SecNumCloud pour enrichir l'existant.

M. Damien Lucas, directeur général de Scaleway. – Scaleway, filiale du groupe Iliad, existe depuis plus de 20 ans et je souligne qu'elle dispose de

l'ensemble de la maîtrise d'ouvrage sans être soumise à un lien de dépendance unique, ce qui est une singularité en Europe. Tout d'abord, aucune dépendance ne s'exerce sur Scaleway dans l'ensemble de sa chaîne de valeur de l'informatique en nuage : elle est en effet rattachée à un groupe de télécommunications propriétaire de ses réseaux et qui a privilégié des partenariats industriels ou technologiques avec des équipementiers européens. De plus, Scaleway est à la fois propriétaire de ses quatre datacenters en région parisienne et du hardware qu'elle utilise. Notre entreprise maitrise également la couche logicielle qui est entièrement développée en interne. Je souligne l'importance de cette architecture d'ensemble puisque pour fournir les services du *cloud*, il faut disposer de l'immobilier, des ressources en serveurs ainsi que de la maîtrise de la couche logicielle qui occupe une part de plus en plus importante dans ce secteur.

Scaleway développe donc un écosystème de *cloud* que nous qualifions techniquement de « public », basé sur les standards du marché et sur des éléments *open source*. Nous plaçons ainsi la liberté de choix et la réversibilité au cœur de nos valeurs. Aujourd'hui, Scaleway compte environ 600 collaborateurs : nous avons recruté massivement ces dernières années et doublé de taille en trois ans grâce à des investissements considérables, rendus possibles grâce au soutien du groupe Iliad, et principalement consacrés au développement d'une couche logicielle performante.

Sans revenir sur les chiffres représentatifs du marché du *cloud* que vous avez très clairement présentés, je fais observer que le segment du *cloud* public est celui qui connaît la plus forte croissance : cet écosystème n'a jamais été aussi dynamique et mature sur le plan technologique. Cependant, comme vous le soulignez, nous perdons du terrain en Europe face aux trois principaux acteurs qui renforcent de plus en plus leur position. Cette amplification des dynamiques oligopolistiques sur le marché de l'informatique en nuage s'explique en grande partie par l'existence d'un certain nombre de barrières à l'entrée qui entravent les acteurs alternatifs. J'attire tout particulièrement l'attention sur les pratiques commerciales qui verrouillent fortement les clients et limitent leur résilience numérique en les rendant dépendants de leur fournisseur de *cloud*.

Le législateur national et européen a donc un rôle clé à jouer pour rétablir des conditions de concurrence équilibrée, étant donné le pouvoir de marché dont jouissent ces acteurs dominants. J'insiste sur l'importance d'agir à l'échelle européenne pour réguler ce marché : cela est nécessaire pour atteindre une masse critique et garantir une harmonisation entre les États membres afin de limiter toute possibilité de dumping. Le fait que la France prenne le leadership en légiférant la première de manière ambitieuse est un signal intéressant adressé à l'extérieur de nos frontières. Nous saluons donc les objectifs fixés par le projet de loi, que ce soit en matière d'encadrement ou d'octroi des services informatiques en nuage, d'interdiction des frais de transfert et de simplification de l'interopérabilité. Nous soutenons

véritablement l'ambition mise en avant par le Gouvernement et espérons que ce volontarisme se diffusera à l'échelle européenne, voire au-delà.

Les occasions de légiférer sur le *cloud* sont rares ; c'est pourquoi nous accordons une grande importance à l'élaboration de ce texte. Nous souhaitons nous assurer, à vos côtés, que les dispositions sont pensées et rédigées de manière à atteindre les objectifs recherchés, tout en étant proportionnées aux capacités des PME ou des ETI, et sans pour autant limiter la capacité d'innovation de notre écosystème ni ralentir son expansion vers de nouveaux marchés. En effet, au-delà des enjeux de régulation, notre positionnement sur les marchés du *cloud* en Europe à l'horizon 2030 dépendra de notre agilité ainsi que de notre capacité à investir pour proposer des services de pointe et anticiper de nouveaux besoins.

M. Lucas Buthion, responsable des affaires publiques du groupe Iliad-Free. –Mon collègue ayant exprimé nos principales idées, je me concentrerai sur les réponses à vos questions dans la suite du débat.

M. Thibault de Tersant, directeur général adjoint de Dassault Systèmes. –Dassault Systèmes est le deuxième éditeur de logiciels en Europe et occupe la place de leader mondial dans son domaine, qui consiste à aider à concevoir et à fabriquer des produits ou substances dans à peu près tous les domaines de l'économie. Par exemple, les objets affichés dans la salle où nous nous réunissons ont été conçus, à un moment ou à un autre de leur processus de fabrication, avec des logiciels de Dassault Systèmes. L'automobile, l'aéronautique, les équipements industriels, la high-tech font partie des domaines très importants pour Dassault Systèmes, mais j'ajoute que les sciences de la vie sont devenues le deuxième secteur le plus important pour nous. Cela signifie que, depuis très longtemps, notre entreprise a l'habitude de gérer un haut niveau de confidentialité pour les données – de conception et de propriété intellectuelle – très sensibles de ses clients. Une des meilleures manières d'assurer cette confidentialité est de développer de l'informatique en nuage : cela permet de faire tourner les logiciels dans des environnements extrêmement sécurisés et de s'assurer que toutes les mises à jour sont effectuées par l'informatique en nuage tout en préservant l'intégrité des données. Voici déjà dix ans que Dassault Systèmes a investi pour développer sa filiale Outscale et permettre ainsi à ses clients d'utiliser tous leurs logiciels Dassault Systèmes dans les infrastructures en nuage d'Outscale. Cela nous a également permis de leur offrir de la souveraineté : nous garantissons à nos clients dont les données sont extrêmement sensibles que celles-ci resteront sur le territoire français quand elles sont hébergées chez Outscale. Je souligne également qu'Outscale a été la première société ayant obtenu la norme SecNumCloud de la part de l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui apporte donc une garantie de grande sécurité.

Mme Catherine Morin-Desailly, présidente. – Pouvez-vous préciser en quelques mots, pour ceux qui nous écoutent et l'ensemble de nos collègues, ce qu'est la labellisation SecNumCloud ?

M. Thibault de Tersant. – Le label SecNumCloud, est le plus élevé en matière de sécurité informatique. Pour l'obtenir, le processus est extrêmement exigeant : on vérifie qu'aucun accès aux données de cette informatique en nuage n'est possible dans l'état actuel de l'art. L'audit effectué par l'ANSSI s'étend sur une durée d'environ 18 mois : ces conditions strictes permettent de valider un haut niveau de cybersécurité.

J'ajoute que notre sensibilité à la souveraineté des données et à la cybersécurité nous a conduits à participer à la création de NumSpot qui vise à permettre aux administrations, collectivités territoriales, hôpitaux et pharmacies, de préserver la sécurité et la souveraineté des données sensibles de santé, d'identité, ou de fiscalité en les logeant dans le *cloud* de NumSpot où elles seront préservées.

J'en termine avec quelques informations quantitatives : Dassault Systèmes rassemble 24 000 collaborateurs dans le monde, ses principaux centres de recherche et de développement sont localisés en France et nous réalisons un chiffre d'affaires d'environ six milliards d'euros.

Mme Solange Viegas Dos Reis, directrice juridique et membre du Comité exécutif d'OVHcloud. – Nous estimons que les dispositions de ce projet de loi sont absolument nécessaires pour rétablir une équité concurrentielle sur le marché du *cloud*. Je rappelle qu'OVHcloud a été créé il y a vingt ans dans le Nord de la France et que cet acteur d'origine française est devenu depuis quelques années le leader européen du *cloud*, au sens où nous sommes le premier fournisseur de *cloud* basé en Europe. Nous sommes également un acteur international avec 34 datacenters répartis sur quatre continents. Notre chiffre d'affaires s'est élevé à près de 800 millions d'euros l'année dernière et nous comptons près de 3 000 collaborateurs sur ces quatre continents. Nous sommes donc un acteur d'une certaine envergure avec un modèle intégré assez unique sur le marché. En effet, nous construisons nos propres serveurs dans nos usines d'assemblage en France et au Canada, nous exploitons nos propres *datacenters* et nous fournissons des services de *cloud* de différents types : du *cloud* public, avec des hébergements mutualisés, et du *cloud* privé, avec un hébergement plus dédié. Nous sommes également présents sur deux des trois couches du *cloud* que sont d'abord l'infrastructure (IaaS pour Infrastructure en tant que Service), ensuite la plateforme (PaaS – Plateforme en tant que Service) et enfin le logiciel (SaS –Software ou Logiciel en tant que Service). Présente sur les deux premières couches, OVHcloud n'est pas un éditeur de logiciels et nous ne mélangeons donc pas les intérêts entre fournisseurs de services de *cloud* et fournisseurs de services de logiciel.

Le marché du *cloud* est aujourd'hui stratégique et a un immense potentiel de croissance. En effet, toutes les entreprises, des PME aux grands

groupes, ont besoin de systèmes d'information qui migrent de plus en plus vers le *cloud*. Cependant, ce marché souffre de problèmes de concurrence et nous rejoignons les propos du représentant de Scaleway : les acteurs dominants verrouillent le marché avec des pratiques mortifères pour la concurrence, en particulier pour les acteurs plus petits, y compris les acteurs européens comme nous. Cela a des impacts toxiques, non seulement pour les utilisateurs qui – enfermés dans des contrats longs dont ils perdent le contrôle – sont privés de liberté de choix, mais aussi pour notre industrie et la protection de notre souveraineté nationale et européenne. Ces pratiques de verrouillage, d'abus de positions de marché et d'absence de transparence peuvent perdurer tant qu'il nous manquera un cadre réglementaire adapté et il faut remédier à la carence actuelle dans ce domaine, comme en témoignent les chiffres éloquents qui ont été rappelés en préambule.

Face à cette situation, plusieurs initiatives ont émergé au niveau européen avec le règlement *DMA* (pour *Digital Markets Act*) ou celui sur les données intitulé *Data Act*. De plus, des autorités régulatrices du monde entier en charge de la concurrence, en France, aux Pays-Bas, en Angleterre, au Japon, en Corée et aux États-Unis, ont déclenché des études sur le *cloud* liées aux positions dominantes qui s'y manifestent. C'est pourquoi OVHcloud soutient pleinement ce projet de loi dont nous estimons qu'il sera positif pour l'écosystème européen et répondra à l'urgence de la situation. Enfin, ce texte vise à anticiper certaines dispositions du *Data Act* et prolonge ce dernier. OVHcloud souligne tout particulièrement l'intérêt des dispositions favorisant la fin des frais de transfert de données, la fin du verrouillage des clients et les efforts en matière d'interopérabilité.

Notre ambition étant d'aborder toutes les difficultés actuelles, nous estimons qu'un certain nombre de compléments pourraient être apportés à ce texte. Il s'agirait, en particulier, de mettre un terme à certaines pratiques de ventes liées ou d'auto-préférence, ainsi que de protéger les données en imposant la transparence aux différents acteurs du *cloud*, ces derniers devant être en mesure de préciser où sont les données, quelle est leur utilisation et qui peut y accéder.

M. Jean-Paul Smets, vice-président d'Euclidia. – Euclidia que je co-préside est une alliance européenne d'industriels du *cloud* et j'ai par ailleurs deux entreprises à titre personnel.

Je souhaite au préalable vous permettre de mieux cerner la notion d'industriel du *cloud*. Dans le secteur des télécommunications, on distingue, d'une part, les équipementiers – qui comme Ericsson fabriquent des stations de base – et, d'autre part, les opérateurs, comme Orange, qui exploitent des réseaux de télécommunication avec des équipements de diverses marques. Par une distinction similaire, je précise qu'Euclidia regroupe les équipementiers du *cloud*, mais pas les opérateurs du *cloud* qui utilisent les technologies que nous fabriquons. Je signale cependant que certains opérateurs du *cloud* fabriquent également leurs propres technologies, tout comme Free a fabriqué sa Freebox à une certaine époque.

On retrouve des cas similaires en Turquie ou au Vietnam : quelques opérateurs de télécoms dans le monde sont également leur propre équipementier. En revanche, Euclidia rassemble des équipementiers du *cloud* mais pas d'opérateurs du *cloud* : nous n'avons donc pas d'observations particulières à formuler sur un assez grand nombre de dispositions du projet de loi qui ne concernent que les opérateurs et non les équipementiers.

L'alliance Euclidia compte 30 membres dans sept pays européens, avec cinq associations partenaires. Euclidia a recensé 120 fournisseurs européens de technologie *cloud*, qui proposent 308 technologies et ont réalisé 1 200 succès à l'export. Je souligne que 15 % des exportations réalisées par nos fournisseurs européens référencés ont été réalisés vers les GAFAM et pratiquement aucune chez les opérateurs européens de *cloud*. Ces informations figurent dans une étude que détient depuis six mois la direction générale des entreprises (DGE) et qu'elle publiera peut-être un jour. La moitié des technologies utilisées par un opérateur comme Amazon Web Services provient d'Europe. Contrairement à certaines affirmations totalement infondées, les technologies les plus avancées dans le *cloud*, le *Edge computing* (informatique de périphérie) ou la 5G virtualisée, sont souvent européennes. Par exemple, au salon du Bourget, vous verrez du *Edge cloud* volant pour des systèmes de combat des avions du futur 100 % européens.

Il y a un an et demi, les membres d'Euclidia ont fait dix offres aux gouvernements européens. L'idée consistait à proposer à chaque Gouvernement de disposer de son propre *cloud* en quelques mois, pour la somme symbolique d'un million d'euros. L'offre comprend toutes les technologies et l'assistance pour la mise en œuvre initiale. Si les 27 membres de l'Union européenne avaient acheté ces dix offres, il leur en aurait coûté 270 millions d'euros soit 40 fois moins que les budgets alloués aujourd'hui par l'Union européenne ou les États membres pour essayer de redévelopper ce qui existe déjà. Euclidia s'efforce ainsi de démontrer que tout existe déjà sur le plan technologique mais qu'il faut plutôt se tourner vers certaines entreprises de petite taille que vers les grands groupes traditionnels pour bénéficier de notre avance technologique, par exemple sur le *Edge* industriel ou la 5G virtualisée.

Nous regrettons que le projet de loi n'aborde les technologies numériques que sous l'angle de la sécurité du consommateur et qu'il ne propose rien de concret pour privilégier l'adoption des nombreuses technologies européennes et dynamiser notre écosystème industriel du *cloud*.

De plus, il comporte même plusieurs aspects qui favorisent les technologies américaines du *cloud* au détriment des technologies européennes. Cela suscite l'inquiétude de certains de nos membres.

Mme Catherine Morin-Desailly, présidente. – Peut-être pourriez-vous formuler dès à présent vos suggestions pour accompagner le développement de votre secteur ?

M. Jean-Paul Smets. – Par exemple, une mesure très simple est de considérer que le logiciel relève du droit d'auteur. En effet, un développeur – pour peu qu'on connaisse la réalité de ce métier – est un artiste au même titre qu'un musicien ou un cinéaste : il écrit du logiciel comme on écrit un roman. Il n'y a donc aucun obstacle pour appliquer l'exception culturelle au logiciel. Nul besoin de passer par la loi ni une directive : du jour au lendemain, un État peut, par exemple, exiger un ratio minimum de contenu logiciel créé en Europe sans en demander l'autorisation à l'Union européenne. On pourrait également s'inspirer du *Small Business Act*, envisager un *Buy European Act* ou créer des « crédits blancs » – comme dans le domaine des émissions de CO2 - avec des échanges de titres représentant un quota de contenu logiciel européen dans telle ou telle activité. Inévitablement, certain s'opposeront à cette idée en indiquant qu'il s'agit de protectionnisme mais je fais observer que c'est, au final, ce qui se pratique aujourd'hui en matière de CO_2 et il n'est pas choquant de protéger de la même façon notre culture. Une dizaine de méthodes et de propositions envisageables ont d'ores et déjà été formulées par écrit et il revient à nos élus de choisir la voie qui leur semble la plus raisonnable, éclairée par les propositions des acteurs qui font le *cloud*.

M. Patrick Chaize, rapporteur. – **Merci pour vos propos introductifs riches en informations dont il ressort que le secteur français ou européen du *cloud* est en difficulté et nous allons essayer d'y apporter remède.**

Estimez-vous que le retard pris par les entreprises françaises par rapport aux entités américaines est rattrapable et, si oui, comment peut-il l'être grâce à ce projet de loi : sur quel vecteur ou point particulier pensez-vous utile de focaliser notre attention ?

L'article 7 du projet de loi porte sur l'offre de crédits *cloud*, c'est-à-dire une sorte d'accompagnement offert de façon attractive à certaines entreprises pour les engager dans un service *cloud*. De telles offres de crédits *cloud* sont aujourd'hui proposées par vos entreprises respectives. Inversement, avez-vous recours à des crédits *cloud* proposés par des opérateurs étrangers, en particulier par les GAFAM ? Êtes-vous favorable à un encadrement de ces crédits ? Quelle durée maximale de validité de ces offres promotionnelles recommandez-vous ? Le Gouvernement nous a indiqué qu'il envisageait un plafond de trois à six mois : ce délai vous paraît-il judicieux et opérationnel ?

S'agissant des frais de transfert sortants qui sont facturés par vos entreprises respectives : quels sont, inversement, les frais qui vous ont déjà été facturés à l'occasion d'un éventuel changement de logiciel, de plateforme ou d'infrastructure de *cloud* ? Êtes-vous favorable à une suppression de ces frais de transfert sortants comme l'envisage le projet de loi ?

Certains d'entre vous ont évoqué la question de la séparation éditeur-plateforme. Avez-vous une position consensuelle sur ce sujet et, le cas échéant, comment identifier de façon précise ce partage entre fournisseurs de services de *cloud* et fournisseurs de services de logiciel ?

Pouvez-vous également nous éclairer sur la signification concrète, pour les clients du *cloud*, de trois mécanismes : l'interopérabilité prévue par l'article 8, la portabilité des actifs numériques et enfin la mise à disposition d'une interface de programmation d'applications ?

Enfin, que pensez-vous du rôle de l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) dans la régulation du marché du *cloud* ? Estimez-vous que l'Arcep dispose des moyens humains et techniques suffisants pour lui permettre d'assumer le rôle de gendarme du *cloud* ?

M. Thibault de Tersant. – Les crédits *cloud* se définissent à ma connaissance comme la mise à disposition gratuite de services d'informatique en nuage par des acteurs américains dits *hyperscalers*. Le premier réflexe, qui se manifeste d'ailleurs dans le présent projet de loi, est de les encadrer très strictement. En effet, les crédits *cloud* permettent d'attirer une clientèle de startups qui n'ont pas les moyens de payer l'informatique en nuage et qui, par la suite, ne vont pas changer de fournisseur de *cloud*. Je pense néanmoins qu'il faut tenir compte de la nécessité d'offrir une période gratuite de test à des clients, en particulier quand on souhaite les convaincre de changer d'informatique en nuage en migrant d'un acteur américain ou chinois à un acteur français. Nous ne voyons pas d'objections particulière à un encadrement de cette pratique mais il faut conserver la possibilité d'un essai gratuit et long sans quoi on va avoir un effet opposé à celui qu'on souhaite en supprimant le moyen de faire migrer des clients dans du *cloud* français.

M. Patrick Chaize, rapporteur. – **Pouvez-vous préciser la durée qui vous paraît appropriée à cet essai gratuit ?**

M. Thibault de Tersant. – Une année est généralement nécessaire pour faire le tour d'un projet de migration assez important.

S'agissant de frais de transfert sortants, je précise d'abord qu'Outscale n'en facture pas au client qui souhaite reprendre ses données. En revanche, des prestations permettant de migrer les données vers un autre environnement sont parfois nécessaires et ont un coût pour le fournisseur de *cloud*. Il faut donc bien distinguer les frais arbitraires de ceux qui correspondent à un véritable service rendu, avec des personnes et de la puissance informatique. La formulation juridique de « frais directs et indirects » prête à confusion car les frais indirects peuvent s'appliquer au recours à un prestataire extérieur pour faciliter la migration des données : si tel est bien le cas, alors on tarira toutes les possibilités de transfert vers les opérateurs de *cloud* français. Il faut donc préserver la possibilité de

rémunérer un service rendu. En revanche, ce qui s'apparente à une « taxe » ou un « péage » de sortie est néfaste et nous sommes très favorables à sa suppression le plus vite possible.

Ensuite, vous avez évoqué la portabilité des actifs numériques. Je souligne que la notion d'actifs numériques est définie de façon confuse dans le projet de loi. Il s'agit en outre d'une notion dangereuse car elle recoupe un ensemble plus vaste que les simples données du client : les métadonnées, par exemple, font partie des actifs numériques. Faute de définition précise des éléments portables, on s'expose à un fort risque de non-conformité à la propriété intellectuelle. C'est un des domaines où les institutions européennes ont décidé d'intervenir en employant le terme de « données exportables » : je pense que le présent projet de loi devrait utiliser cette formulation car les données exportables visent précisément les données du client. L'objectif essentiel de la partie du texte consacrée à l'informatique en nuage est de permettre aux clients de récupérer leurs données qui sont incluses dans leur patrimoine. Ce n'est pas toujours facile aujourd'hui et c'est précisément ce qu'il faut permettre.

Il faut cependant prendre garde aux pressions qui sont exercées par divers acteurs pour aller beaucoup plus loin vers une interopérabilité et une portabilité d'actifs numériques plus vastes que les données du client et qui exposent la propriété intellectuelle. L'autre danger, dans une démarche un peu plus raffinée, serait de rendre au final le texte inopérant parce que son périmètre serait trop large. En effet, l'interopérabilité au niveau des logiciels est extraordinairement complexe et il en va de même quand le projet de loi parle d'*API* (*Application Programming Interface* ou interface de programmation d'application) ouverte. Nous sommes aujourd'hui dans l'économie de la donnée et pas dans l'économie des *API*. Je pense donc qu'il faut recentrer le projet de loi sur les données ainsi que les possibilités offertes aux clients de les transférer. S'aventurer dans le domaine des *API* créerait des obligations qui ne sont pas raisonnables pour les éditeurs de logiciels. J'appelle à une extrême prudence car un certain nombre de pays sont très favorables à cette récupération de propriété intellectuelle sous forme d'*API*. De la même manière, il faut se méfier du concept d'équivalence fonctionnelle qui ne signifie pas grand-chose et peut s'étendre à des logiciels dans le *cloud*. En résumé, j'appelle à renoncer au concept d'actifs numériques pour en revenir à celui de données exportables qui, je l'espère, sera inscrit dans le *Data Act* européen.

M. Patrick Chaize, rapporteur. – J'imagine que vous avez des propositions à nous faire sur le sujet.

M. Thibault de Tersant. – Nous pouvons effectivement vous fournir des propositions d'amendements très précises.

S'agissant de l'Arcep, j'indique que l'idée fondamentale est que si on veut permettre la portabilité des données, il faut que celles-ci répondent à

certains standards pour les rendre réutilisables d'un service à l'autre. Au risque de paraître brutal, j'indique que ces standards ne sont pas français. L'élaboration de standards est longue et onéreuse : je pense donc qu'il est préférable de miser sur l'élaboration de standards européens en impliquant dans ce processus les industriels qui sont les consommateurs des données et en évitant une démarche trop intellectuelle. Les organismes ayant élaboré les standards pour l'échange de données de produit (STEP) auxquels j'ai participé réunissent les industriels concernés, par exemple dans le secteur automobile ou aéronautique, avec des éditeurs de logiciels du type d'Assystem. Nous avons une haute opinion de l'Arcep mais la mission d'élaborer les standards nécessaires à la portabilité des données est tout à fait au-dessus de ses moyens.

M. Jean-Paul Smets. – Pour des raisons très différentes de celles qui viennent d'être exposées, nous arrivons chez Euclidia à des conclusions similaires sur les questions fonctionnelles, d'actifs numériques et de normalisation.

Notre principale différence d'approche avec les propos précédents porte, par exemple, sur le fait que nous souhaitons que les *API* soient publiques car nous estimons qu'il n'y a pas de propriété intellectuelle sur ces interfaces logicielles.

Nos conclusions sont cependant les mêmes. Ainsi, le fait de confier à l'Arcep une mission qui s'apparente à une standardisation du *cloud* me paraîtrait personnellement, assez catastrophique car l'Arcep est spécialisée dans les télécommunications : son personnel a marqué, à une certaine époque, sa préférence pour le minitel plutôt que le web, et l'Arcep reste marquée par une forme de pensée parfois un peu rigide. Je connais à l'Arcep des gens qui comprennent parfaitement le secteur des télécommunications mais quasiment aucun qui ait un haut niveau de compréhension des logiciels.

Par ailleurs, l'idée de normalisation des systèmes dans le monde du logiciel me laisse interrogatif. En effet, je ne connais que trois normes – la norme japonaise TRON, W3C (World Wide Web Consortium) et POSIX (Portable Operating System Interface) – qui permettent de définir les mêmes règles pour tous les développeurs de logiciels du monde. Je vous mets au défi de m'en citer d'autres.

Mme Catherine Morin-Desailly, présidente. – Nous entrons ici dans un débat extrêmement technique et je me permets de recentrer le débat sur son aspect législatif et sur les questions soulevées par notre rapporteur. Il nous importe avant tout que le texte de loi permette l'émergence d'un *cloud* souverain français et européen qui, aujourd'hui, est un peu en retrait en raison de l'hégémonie des GAFAM qui ont tendance à vampiriser ce marché en plein développement. Nous souhaitons savoir si le texte de loi vous satisfait en rééquilibrant le marché et en facilitant la migration des données

vers les solutions respectueuses des valeurs européennes que vous offrez. Devrions-nous, par exemple, inscrire dans le texte la notion de données stratégiques et sensibles ? Nous souhaitons également participer à la mise au point des politiques industrielles d'accompagnement de votre secteur en nous concentrant sur des questions stratégiques.

M. Jean-Paul Smets. – Je faisais référence aux propos de M. Thibault de Tersant qui, à juste titre, a indiqué que la notion de données exportables pourrait faire l'objet d'une normalisation ; j'ai également fait observer que le contenu du projet de loi fait référence à quelque chose qui n'existe pas.

M. Lucas Buthion, responsable des affaires publiques du groupe Iliad. – Tout d'abord, nous soulignons l'importance de ce projet de loi qui marque une certaine inflexion. En s'efforçant de réguler certaines pratiques qualifiées par une intervenante de « mortifères », ce texte pourra participer à une forme de rééquilibrage des conditions de concurrence qui vont permettre à Scaleway comme au reste de l'écosystème français européen de montrer leur valeur de façon plus juste et équitable.

S'agissant des différentes questions soulevées par le rapporteur, je commencerai par m'associer aux interrogations, voire aux craintes suscitées par la définition des actifs numériques. Pour aller plus dans le détail des propositions concrètes, nous pouvons vous inviter, en faisant référence à la notion de donnée exportable, à examiner la dernière définition – plus cadrée, plus précise et plus concrète – qui figure dans le trilogue européen sur le *Data Act*.

Par ailleurs, à notre connaissance, la notion de portabilité en matière de *cloud* n'est pas définie dans le Data Act.

Mme Catherine Morin-Desailly, présidente. – Je précise que le Data Act n'est pas encore adopté et nous sommes donc dans une phase d'anticipation des dispositions qui pourraient figurer dans sa version définitive.

M. Lucas Buthion. – Tout à fait, mais, à l'échelle européenne, il faudra bien choisir la définition à laquelle on se réfère dans la phase ultérieure de normalisation. Il nous paraît donc pertinent d'essayer d'anticiper au niveau français cette évolution et de permettre à l'Arcep d'agir de façon proactive en prévision de la mise en œuvre future du *Data Act*.

Par ailleurs, il me semble qu'un consensus se dégage sur les frais de transfert. Notre groupe n'en facture pas non plus, hormis de façon très marginale, tandis qu'un certain nombre d'acteurs dominants peuvent avoir des marges sur ces frais de transfert de l'ordre de 800 % – selon nos estimations qu'il convient sans doute d'approfondir – par rapport à leur coût réel. L'encadrement ou l'interdiction de ces frais de transfert est donc, pour nous, une excellente chose pour lever un vrai verrouillage des clients. Ceci dit, nous estimons à notre tour nécessaire de mieux définir ces frais de transfert pour bien les distinguer des frais et éviter les contournements.

Je précise que le projet de *Data Act* prévoit une période de transition au niveau européen pour ces frais de transfert tandis que le présent projet de loi envisage une interdiction immédiate : cela ne nous ne poserait aucun problème, si ces frais ne sont pas justifiés par des impératifs techniques et permettrait de renforcer sans délai la liberté de choix des utilisateurs.

Enfin, s'agissant des offres de crédit *cloud*, je précise en toute transparence que ces pratiques ne sont pas l'apanage exclusif des *hyperscalers* américains. Scaleway, par exemple, propose des offres de crédit *cloud* à des écosystèmes de développeurs et de start-up mais pas du tout dans les mêmes proportions ou montants et à la même échelle que les acteurs dominants, ce qui crée une dissymétrie. Je fais observer qu'en raison d'une certaine accoutumance à des prix négatifs, nous sommes contraints de proposer de telles offres.

La réflexion sur l'encadrement de ces pratiques est probablement justifiée mais je signale que la limitation des crédits *cloud* ne figure pas, comme vous le savez, dans le projet de *Data Act* européen. On risque donc d'aboutir à un encadrement spécifique à notre territoire assez facile à contourner par les filiales non françaises des acteurs dominants qui pourraient continuer à distribuer ces crédits à des entités françaises. La situation ainsi créée serait un peu paradoxale, voire inverse à l'effet recherché : l'encadrement de l'octroi de crédit *cloud* s'imposerait uniquement aux acteurs français situés sur le territoire national qui n'auraient pas les moyens de contourner cet encadrement. Il faut donc, à mon sens, être attentif aux effets de bord d'un tel dispositif pour ne pas détourner les clients potentiels de nos offres.

M. Patrick Chaize, rapporteur. – **J'entends parfaitement vos objections et, comme vous l'avez bien compris, nous comptons sur vous** pour nous aider à bien définir les frais de transfert ainsi qu'à trouver le bon équilibre dans la rédaction du texte.

S'agissant des crédits *cloud*, il s'agit d'éviter l'effet pervers qui aboutirait à priver certaines startups d'un accompagnement utile à leur développement par des entités françaises. Là aussi, il faut trouver le bon équilibre, mais pour l'instant, je ne pense pas qu'il faille s'interdire d'être plus vertueux que le *Data Act* en s'efforçant d'éviter que certaines entreprises américaines préemptent le marché sans pénaliser les acteurs nationaux.

Mme Solange Viegas Dos Reis. – Tout d'abord, sur le crédit *cloud*, je partage la plupart des propos tenus par les intervenants. La difficulté est que le système des crédits *cloud* a une dimension vertueuse pour accompagner l'écosystème des startups ou des PME françaises et européennes qui ont besoin de migrer vers le *cloud* et hésitent à passer le cap. D'un autre côté, on constate que les crédits *cloud* sont détournés de leur finalité d'outils d'accompagnement pour tester le *cloud* : cela devient un produit d'appel pour attirer ces startups, même très précoces dans leur

développement, et les verrouiller en tant que clients. Une interdiction totale des crédits *cloud* serait donc excessive.

Pour être à notre tour transparent, OVHcloud, met également en œuvre une politique de crédit *cloud*, mais de façon modérée. Il est impossible, pour les petits acteurs, de répliquer les propositions de crédit *cloud* d'un montant très élevé faites par les entreprises extrêmement puissantes. C'est ce décalage qui pose aujourd'hui un énorme problème et non pas le crédit *cloud* en soi.

L'approche que nous défendons est celle d'un encadrement précis des crédits *cloud* avec une limitation de leur montant et de leur durée à un niveau accessible à des acteurs. Par-dessus tout, ce mécanisme doit rester un véritable test, en permettant à une startup ou une entreprise quelconque bénéficiant d'un crédit *cloud* de sortir à tout moment de sa période d'essai sans pénalisation financière. Il s'agit de s'aligner sur les offres d'essai gratuit de grands quotidiens de presse qui n'engagent pas le souscripteur.

Nous estimons qu'une durée de gratuité comprise entre six mois et un an assortie d'un plafond annuel de 50 000 euros pourrait être envisageable dans un certain nombre de cas. Il est cependant difficile de fixer des paramètres précis adaptés à l'ensemble des acteurs.

Quoi qu'il en soit, la logique du crédit *cloud* est saine : il a été détourné en rendant le client captif et il faut aujourd'hui lui rendre sa fonction première de test.

M. Patrick Chaize, rapporteur. – Si je vous entends bien, vous êtes favorable à un cumul de limitations à la fois dans le temps et en montant, le Gouvernement ayant, pour sa part, envisagé de ne fixer qu'une durée maximale.

Mme Solange Viegas Dos Reis. – Je pense qu'à défaut de limitation du montant des crédits *cloud*, les distorsions de concurrence entre les acteurs vont perdurer mais je reconnais qu'il n'est pas facile de fixer une somme précise et il ne m'appartient pas de le faire.

Ensuite, sur les frais de transfert, je précise tout d'abord qu'OVHcloud n'applique pas de frais de sortie de contrat. Dans le sillage des précédents intervenants, j'estime nécessaire de bien distinguer les frais de transfert et les frais de migration. Je précise que la circulation des données entre différents serveurs pendant le contrat – en particulier quand le client dispose en même temps de plusieurs opérateurs de *cloud* – ne doit pas non plus donner lieu à facturation de frais de transfert. En revanche, lorsque tout ou partie du contrat s'arrête, c'est-à-dire lorsque le client décide de retirer une partie de ses services hébergés chez un prestataire de *cloud* – pour les transférer vers ses propres serveurs, chez un autre opérateur, ou même pour arrêter complétement – il s'expose alors à des frais de migration. Ces frais peuvent jouer un rôle de barrières à la sortie pour les clients : il est essentiel de rester extrêmement vigilants à leur égard et de vérifier qu'ils se limitent à

répercuter le coût spécifiquement engagé pour la migration. Il peut légitimement s'agir de prestations de services – qui méritent salaire – pour accompagner le client dans sa migration mais d'éventuels « frais de bande passante » ou autres n'ont aucun sens, sans quoi on peut parler de « péage » pour reprendre la formule pertinente du rapporteur. Toute la difficulté, au plan juridique, est de bien définir les composantes des frais de transfert et de migration. OVHcloud facture des prestations humaines d'accompagnement à la migration mais nous n'appliquons pas de frais sur le reste et ne comprenons pas ce qui pourrait être facturé.

Sur les questions plus techniques d'interopérabilité et d'actifs numériques, nous estimons que le projet de loi va dans le bon sens. OVHcloud est confronté à cette difficulté : l'interopérabilité est une barrière à la migration entre fournisseurs de *cloud*, tout comme l'absence de portabilité des données. En revanche, une définition approximative de ces notions pourrait entraîner des effets pervers que M. de Tersant a évoqués. L'interopérabilité, se définit concrètement par la faculté pour des systèmes, applications, ou composants différents de pouvoir se connecter, partager, fonctionner ensemble et communiquer entre eux. Cette interopérabilité n'est pas naturelle et il faut parfois la forcer. Nous pensons que le texte doit fortement la stimuler car si on ne fixe pas *ex ante* des conditions nécessaires à une bonne interopérabilité, les acteurs dominants vont encore accroître leur pouvoir de marché. En effet, les trois acteurs qui représentent 71 % du marché en France et 72 % en Europe vont imposer leur propre format. On constate dès à présent que quand certains *hyperscalers* américains modifient leurs formats ou leurs services, tout le reste de l'industrie s'empresse de se mettre à niveau. L'entreprise dominante risque ainsi d'imposer son modèle à l'ensemble du marché et c'est précisément ce phénomène qui doit être anticipé par le projet de loi : celui-ci doit donc favoriser l'interopérabilité et la portabilité.

J'ai bien noté que les définitions retenues pourraient entraîner des effets de bord et il faut faire en sorte de les éviter. Je précise ici que la notion d'actifs numériques inclut les données exportables mais il faut également que les données soit transmises dans un format structuré, couramment utilisé et lisible – de la même façon qu'un déménageur doit vous livrer vos affaires sans se contenter de les déposer en vrac dans le salon. Le principe de portabilité doit donc inclure la possibilité pour le client de réutiliser ses données de façon rapidement opérationnelle.

M. Alain Issarni. – En réponse à la première interrogation du rapporteur sur le retard pris par les entreprises françaises ou européennes du *cloud*, j'indique que NumSpot n'existerait pas si nous pensions que ce décalage n'est pas rattrapable et le projet de loi va effectivement dans le bon sens pour nous faciliter la tâche.

Je souhaite mentionner des éléments de nature à renforcer les acteurs du *cloud* dont nous parlons. Vous avez évoqué, madame la

présidente, la récente mise à jour de la « doctrine *cloud* au centre » destinée à accélérer la transformation numérique de l'État. Celle-ci va également dans le bon sens en précisant le contour exact des données à sensibilité particulière qui sont de nature à justifier le référentiel SecNumCloud. Cette doctrine s'adresse au secteur public et nous souhaitons que celui-ci puisse contribuer à faire émerger des petits acteurs du *cloud* à travers la commande publique.

Le troisième levier de nature à rééquilibrer l'offre de marché réside dans la sensibilisation de l'utilisateur final. Nous souhaitons que des efforts soient amplifiés dans ce domaine. Peut-être faudrait-il s'inspirer, dans le *cloud*, du cyberscore, qui est un système de notation des sites web, à l'image du Nutri-score : le cyberscore s'est installé dans le paysage numérique, quoique de façon assez timide puisqu'il ne concerne, pour 2024, que les très gros acteurs. En revanche, lorsqu'on se connecte aujourd'hui à un site localisé dans le *cloud*, il est extrêmement difficile de savoir où sont vos données, qui en est l'hébergeur et si elles sont ou pas soumises à un quelconque risque. Pour autant, je pense que l'éducation des utilisateurs est importante et peut influencer les fournisseurs de services sur l'utilisation des données. Il me paraît donc souhaitable d'encourager la création d'un équivalent du cyberscore ou du Nutri-score appliqué à la sécurité des données pour favoriser l'émergence d'acteurs plus vertueux en termes de sécurité et de confidentialité des données.

Mme Catherine Morin-Desailly, présidente. – Vous avez mentionné la labellisation SecNumCloud mise en place par le Gouvernement. Je signale que certains acteurs, et en particulier les petites entreprises, ont fait valoir que le processus de labellisation est, comme vous l'avez vous-même rappelé, très long – environ dix-huit mois – et coûte cher, avec des sommes voisines de 50 000 euros. Pouvez-vous confirmer ces données ?

M. Jean-Paul Smets. – Je précise à ce sujet qu'Euclidia rassemble deux catégories de membres. Certains, très minoritaires, ont subi une sorte de chantage en recevant des subventions d'État conditionnées à la labellisation SecNumCloud. Ils ont pu communiquer sur cette qualification et ne sont pas enclins à la critiquer. En revanche, pour la majorité de nos membres, SecNumCloud a pour effet de favoriser les technologies américaines du *cloud*. Aujourd'hui, les quatre offres d'hébergement labellisées SecNumCloud, fonctionnent – sans parler du système de vente qui les entoure – avec un cœur technologique américain, ce qui ne garantit pas leur immunité contre une prise de contrôle à distance par un État tiers, par exemple concernant les équipements Cisco ou, comme on peut le lire, dans les logiciels propriétaires d'origine américaine. SecNumCloud favorise en réalité l'absence d'offres basées sur des technologies européennes. Il favorise également les offres propriétaires par rapport aux logiciels libres, ce qui pourrait enfreindre la loi de 2016 sur la République numérique

d'Axelle Lemaire, car quand on utilise un logiciel libre, la qualification SecNumCloud impose de procéder à de nombreuses vérifications. On peut même, sur la base de la dernière mise à jour de la circulaire SecNumCloud qui exige d'utiliser des équipements immunisés contre un accès à distance par un État tiers, considérer que la quasi-totalité des offres ne sont pas conformes car elles utilisent le plus souvent des processeurs Intel ou AMD, contenant un dispositif d'accès à distance contrôlable par les États-Unis. Tout ceci illustre, selon la majorité de nos membres, l'aspect absurde de cette signalétique qui défavorise l'industrie européenne.

M. Thibault de Tersant. – Très franchement, nous avons besoin d'une norme exigeante pour garantir la sécurité des données et le contrôle de leur souveraineté. C'est le rôle de SecNumCloud et il y a aujourd'hui beaucoup de pression pour minorer le niveau d'exigence de cette norme.

Mme Catherine Morin-Desailly, présidente. – Qui exerce ces pressions ? Pouvez-vous citer des noms ?

M. Thibault de Tersant. – Un certain nombre de *joint ventures* créées ou en voie de création avec des *hyperscalers* américains, comme par exemple Bleu auquel participe Microsoft et Cap Gemini, sont assez intéressés par un abaissement de la norme SecNumCloud. Notre entreprise a obtenu cette norme à juste titre extrêmement exigeante, de façon à garantir la sécurité des données et j'ajoute que les délais de vérification requis sont en train d'être réduits.

Par ailleurs, j'estime qu'on peut encadrer la durée des crédits *cloud* mais leur fixer un montant maximum nuira à notre capacité de migrer vers des environnements français des grands clients qui travaillent actuellement avec des fournisseurs américains ou chinois. Il en va de notre capacité à livrer bataille aux grands opérateurs.

Le dernier point que je souhaite signaler porte sur l'insécurité contractuelle : je signale qu'une disposition du *Data Act* prévoit que tout client peut interrompre son contrat *cloud* avec un délai de préavis de 60 jours, ce qui, en apparence apparaît comme un gage de liberté. J'estime cependant qu'il serait inopportun d'introduire une disposition similaire dans le projet de loi en discussion car si on veut développer le *cloud* en France et obtenir des grands comptes, cela nécessite un engagement pluriannuel. Une sécurité contractuelle d'une durée approximative de trois ans est en effet le seul moyen de financer des investissements très importants. L'engagement pluriannuel d'un client s'accompagne d'ailleurs souvent d'un rabais important. Au final, cette disposition du *Data Act* est très pernicieuse et favorise en réalité nos grands concurrents américains.

M. Jean-Paul Smets. – J'ajoute qu'un certain nombre de projets de textes européens vont dans une direction similaire. Par exemple, le *Cyber Resilience Act (CRA)* fait planer un risque d'amende de 15 millions d'euros sur les créateurs de logiciel libre en cas d'erreurs commises par un utilisateur

de ces logiciels qui ne leur a rien payé pour l'utiliser : cela donne envie d'arrêter de faire des logiciels libres. On trouve le même genre de disposition dans la directive *Product Liability* qui institue une responsabilité supplémentaire à la charge des développeurs de logiciels libres, notamment pour le *cloud*, et qui le partagent. Pour sa part, la directive sur l'intelligence artificielle impose de s'inscrire dans une base de données pour vérifier qu'ils respectent la démocratie et qu'ils ont mis en place un système de traçabilité de leur code dont la conformité à toutes les lois européennes doit être vérifiée ligne par ligne avant tout partage avec les autres développeurs de logiciels libres.

On constate donc une accumulation de textes qui renforcent la charge mise sur les personnes qui développent les technologies *open source*. Cela va encore plus loin puisque, dans le système des noms de domaine, en cas de plainte, le défendeur devra acquitter les frais de procédure même s'il est mis hors de cause, ce qui est dérogatoire du cours normal de la Justice. Ce genre de texte donne aux producteurs de technologie une envie furieuse d'aller s'établir ailleurs.

Mme Solange Viegas Dos Reis. – En ce qui concerne SecNumCloud, OVHcloud a obtenu cette certification et je tiens à préciser qu'il s'agit effectivement d'un long processus mais que le Gouvernement a mis en place un accompagnement adapté. À son tour, OVHcloud s'est engagée auprès des éditeurs de logiciels sur cet accompagnement pour les aider à comprendre l'écosystème de la certification. Au final, SecNumCloud procure un avantage concurrentiel aujourd'hui déterminant et incorpore des critères d'immunité aux lois extraterritoriales pour prévenir un certain nombre de risques. Quoi que fassent les hyperscalers américains, les acteurs européens dotés d'une certification de ce niveau auront un avantage concurrentiel qu'il est important de préserver.

Mme Catherine Morin-Desailly, présidente. – Vous êtes plusieurs à participer au projet de plateforme de données de santé qui pourrait être une alternative à Microsoft, d'après ce que nous aurions pu comprendre. Pourriez-vous nous en dire plus à ce sujet ?

Nous ne connaissons pas l'état d'avancement du projet d'offre alternative à Bleu et sommes très préoccupés à ce sujet sur lequel nous avons interpellé à plusieurs reprises les différents ministres en charge de la Santé et du Numérique, ainsi que la Première ministre. Celle-ci nous a promis qu'un appel d'offres serait lancé, ce qui n'avait pas été le cas en 2020. Par la suite, Bernard Charlès, président de Dassault Systèmes, a interpellé le Président de la République en indiquant que sa société n'avait pu candidater à un appel d'offres en bonne et due forme. Où en est ce projet ? Vous paraît-il stratégiquement pertinent et suffisamment accompagné par les administrations compétentes ?

M. Jean-Paul Smets. – Pedro Lucas, qui dirige une des grandes entités françaises de l'hébergement de santé et une de mes entreprises, et moi-même avons, il y a un ou deux ans, fait une offre au *Health Data Hub* portant sur un système complet hébergé avec toute la conformité HDS (Hébergeur de Données de Santé). Le *Health Data Hub* a donc, depuis le début, connaissance d'offres conformes et européennes et Achille Lerpinière, qui y travaillait, connaît depuis le premier jour les produits européens disponibles pour construire un système 100 % européen.

Toutefois, la récente circulaire de la Première ministre sur le *cloud* de confiance indique qu'une dérogation peut être accordée sans qu'elle ne puisse aller au-delà de douze mois après la date à laquelle une offre de *cloud* acceptable sera disponible en France. Ce terme d'« acceptable », particulièrement vague, permet en fait de continuer d'avoir le *Health Data Hub* chez Microsoft *ad vitam aeternam* malgré l'existence d'une pléthore d'offres 100 % européennes.

Mme Catherine Morin-Desailly, présidente. – Vous contredisez l'idée selon laquelle nous n'aurions pas de solutions alternatives : elle avait été émise par la secrétaire d'État en charge du numérique, et on constate une forme d'autodénigrement permanent à l'égard de nos propres compétences numériques dans les sphères académique, politique et administrative. En tant que représentants de ce secteur, pouvez-vous au contraire affirmer qu'on peut progressivement récupérer une forme d'autonomie stratégique et de souveraineté en établissant des choix préférentiels, à commencer par nos données de santé. Peut-on construire progressivement cet écosystème ?

M. Thibault de Tersant. – Nous en sommes convaincus et c'est la raison pour laquelle nous avons réalisé le projet Numspot, qui a vocation à traiter les données de santé des Français : nous avons bien l'intention de faire valoir nos arguments dont je confirme la pertinence.

M. Alain Issarni. – Je confirme ces propos : Numspot a l'ambition de bâtir un *cloud* souverain et de confiance, avec des services évolués qui nous rapprochent de ce qui se pratique par ailleurs. Nous serons donc ravis de pouvoir participer à une compétition sur un appel d'offres pour le *Health Data Hub*.

Mme Catherine Morin-Desailly, présidente. – Nous sommes preneurs des propositions que vous n'auriez pas pu nous faire oralement compte tenu de nos contraintes de temps. C'est important, parce qu'au-delà du cadre juridique, nous restons attentifs à la stratégie industrielle qui va accompagner très concrètement et financièrement ces projets de *cloud* souverain.

Table ronde des opérateurs du numérique

Jeudi 15 juin 2023

Mme Catherine Morin-Desailly, présidente. – Sans plus attendre j'ouvre cette table ronde qui s'inscrit dans le cadre des travaux de notre commission spéciale, une commission transversale au Sénat qui rassemble l'ensemble de nos commissions. Elle a été mise en place afin d'étudier le projet de loi « Sécuriser et réguler l'espace numérique ». Le texte a déjà fait l'objet de travaux au sein de la commission des affaires européennes dans la mesure où il s'agit d'un texte d'application de règlements européens, dont le règlement sur les marchés numériques (RMN), le règlement sur les services numériques (RSN), le règlement sur la gouvernance des données *(DGA)* et le règlement sur les données *(DA)*. Ce dernier, encore en cours de discussion, est pourtant quelque peu anticipé dans le projet de loi.

Je souhaite accueillir Arnaud David, directeur des affaires publiques européennes d'Amazon Web Services, Yohann Bénard, directeur des affaires publiques d'Amazon, Benoît Tabaka, secrétaire général de Google France, Frédéric Géraud, directeur des affaires publiques de Google Cloud France, Anton'Maria Battesti, directeur des affaires publiques de Meta France, et Béatrice Oeuvrard, responsable des affaires publiques de Meta France.

Les entreprises que vous représentez sont très importantes. Qualifiées le plus souvent de *big tech*, elles reposent sur le modèle économique de « capitalisme de surveillance » tel que défini par Shoshana Zuboff, une professeure de Harvard. Ce modèle n'est pas sans poser problème aux Européens. D'un régime de non-redevabilité et de non-responsabilité établi par la directive sur le commerce électronique (LCEN), nous allons passer à un autre type de régime qui vise à réguler les grandes plateformes, tant sur le volet des marchés numériques, qui concerne l'ensemble des acteurs économiques, que sur celui des services numériques, qui concerne plutôt les usagers.

La question des données est au centre de la problématique qui nous réunit et les textes apportent des solutions pour mieux protéger la vie privée, également au vu des intérêts stratégiques que cela représente pour l'Europe. Mais les textes visent aussi à rééquilibrer un système qui est très fortement anti-concurrentiel et verrouillé d'un point de vue juridique, financier et technique, et ce à votre bénéfice. Les textes, et notamment le RSN, sont également conçus pour répondre aux effets toxiques et finalement pervers du modèle économique des plateformes. Des faiblesses permettent des mésusages tels que la désinformation, la manipulation de l'information, la surexposition des contenus pédopornographiques, et les phénomènes de harcèlement et de haine en ligne. Sans régulation, tout cela est devenu une jungle. Il faut pouvoir travailler à retrouver de la confiance et de meilleurs

usages dans le cadre d'un modèle qui est redoutablement addictif et, il faut aussi l'admettre, efficace.

Ce sont des constats que vous connaissez. Le Sénat est très attaché à ces questions et nos nombreux travaux l'ont montré. Nous souhaitons comprendre comment et dans quels délais vous appliquerez le RSN et le RMN, et dans quelle mesure vous pouvez, à travers les propositions qui sont faites, contribuer à une meilleure régulation de l'espace numérique.

Mme Béatrice Oeuvrard, responsable des affaires publiques de Meta France. – Je précise que, Meta n'étant pas un service *cloud*, nous nous cantonnerons à la discussion sur les plateformes.

En premier lieu, nous nous interrogeons sur la pré-transposition en droit français de certains éléments qui sont encore en cours de discussion au niveau européen. Certains articles n'ont pas été notifiés à la Commission, notamment l'article 16 relatif au Pôle d'expertise de la régulation du numérique (PEReN), alors qu'il fait référence aux articles 34 et 40 du RSN.

Nous souhaitons également réagir sur la partie relative au cyberharcèlement. Nous développons depuis de nombreuses années des outils pour diminuer les effets du harcèlement qui peut exister sur les plateformes. Pour les personnes condamnées, le projet de loi prévoit la possibilité pour le juge de prononcer la suspension pour six mois (et douze mois en cas de récidive) du compte d'accès au service en ligne, ce qui nous paraît intéressant. Le fournisseur de service est également tenu de mettre en œuvre des mesures permettant de procéder au blocage des autres comptes d'accès à son service éventuellement détenus par la personne condamnée et d'empêcher la création de nouveaux comptes. Or, comment identifier ces comptes ? Nous seront-ils notifiés et si oui, sous quelle forme ? Il s'agit de données sensibles dans la mesure où il y a inscription sur le casier judiciaire. Nous suggérons d'utiliser la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) et ses agents assermentés pour mettre en place un système intermédiaire de contraventions. Plus de 25 000 réquisitions sont émises tous les ans. Ce système intermédiaire permettrait d'éviter que tout passe par la voie judiciaire, où les délais de traitement sont plus longs, et ainsi de répondre aux attentes des utilisateurs.

M. Anton'Maria Battesti, directeur des affaires publiques de Meta France. – Je souhaite d'abord pointer un risque de fractionnement de la législation. Dans le projet de loi, les questions d'âge sont traitées dans la partie sur l'accès aux sites pornographiques. Or, en parallèle une proposition de loi portée par le député Laurent Marcangeli concernant la majorité numérique a été déposée. Il serait peut-être utile d'essayer de réconcilier ces questions par le projet de loi. Au niveau européen, les questions d'âge sont traitées dans le *DSA*, mais la commission s'est également saisie de ces sujets *via* son code de conduite *Child Safety*.

La France pourrait être moteur sur ces sujets, mais l'adoption d'une loi nationale sans solution technique évidente interroge aujourd'hui les parties prenantes. Il conviendrait de se mettre tous autour de la table : opérateurs de télécom, fournisseurs de services d'exploitation, magasins d'applications, mais aussi bien sûr les plateformes, pour essayer de traiter ces points. Il me semble que le gouvernement y travaille et qu'il y a eu des propositions. Nous espérons que ce sujet très important pourra avancer dans le cadre de ce projet de loi.

M. Benoît Tabaka, secrétaire général de Google France. – Le projet de loi et l'adoption des deux textes européens viennent parachever le travail de refonte engagé depuis 20 ans et l'ordonnancement juridique en sera modifié. Nous avons suivi l'adoption des textes sur la lutte contre la désinformation et la lutte contre la haine. Pour la première fois, nous avions avec l'Arcom un interlocuteur et un régulateur avec qui échanger, ce qui nous a paru intéressant. Nous espérons que ce travail avec l'Arcom pourra se poursuivre après l'entrée en vigueur du RSN.

Sur le projet de loi en tant que tel et l'application du RSN et du RMN, notre analyse est toujours en cours. Le seul élément identifié à ce jour concerne les dates d'entrée en vigueur. Le nouveau cadre juridique français entrerait en vigueur après le nouveau cadre européen. Pour les grandes plateformes, il y aurait un moment où les deux cadres juridiques européens et français se superposeraient.

Sur le volet *cloud*, je laisse Frédéric Géraud vous apporter des éléments.

Comme évoqué lors des deux dernières auditions, nous travaillons spécifiquement sur la question de la lutte contre les arnaques et cherchons à encore améliorer ce dispositif qui nous semble intéressant. Le texte comporte de nombreuses briques : filtre anti-arnaques, protection de l'enfance. Les premiers dispositifs concernant la vérification d'âge et le contrôle par l'Arcom pourraient sans doute être améliorés en termes d'efficacité.

Concernant le filtre anti-arnaques, il serait utile de créer un canal de communication unique plutôt que d'avoir de multiples autorités qui viennent signaler tel ou tel site comme étant potentiellement une arnaque. Le système de sanctions pourrait être aligné sur le système de sanctions du RSN, avec la reprise du concept de « défaillance systémique ». Aujourd'hui les opérateurs ne participent pas à la mise en œuvre du filtre anti-arnaques, alors qu'il s'agit du premier canal de survenance de l'arnaque. Les opérateurs pourraient eux aussi, avec les systèmes d'affichage de page, participer au blocage et *a minima* à l'information préalable du consommateur.

Sur la lutte contre le cyberharcèlement, plusieurs dispositifs existent aujourd'hui et le dispositif prévu par la loi va dans le bon sens. Cinquante-quatre personnes sont condamnées chaque année en France, souvent plusieurs années après les faits. Les mesures de blocage de compte

interviennent donc plusieurs années après l'infraction, et la personne condamnée peut continuer ses agissements pendant cette période. Nous suggérons de prendre exemple sur le système d'amendes mis en place pour lutter contre le harcèlement de rue. Aujourd'hui, il est possible de mettre une amende pour harcèlement de rue dans les heures qui suivent les faits, mais nous n'en sommes pas capables en cas de cyberharcèlement.

Mme Catherine Morin-Desailly, présidente. – Je précise que certaines entreprises représentées ce jour comptent parmi leurs activités, l'informatique en nuage, soit le stockage et le traitement de la donnée. Vous n'êtes pas que des réseaux sociaux.

M. Frédéric Géraud, directeur des affaires publiques de Google Cloud France. – Je pense utile et important de préciser que Google Cloud est l'un des derniers entrants sur le marché de l'informatique en nuage. Google Cloud est souvent cité dans la presse comme cinquième acteur du marché de l'informatique en nuage en France, avec moins de 10 % de parts de marché, loin derrière Amazon et Microsoft et moins loin d'OVHcloud et d'Orange. Compte tenu de cette position de challenger, nous sommes favorables à toute action qui fluidifie un marché qui est toujours en expansion, notamment en France où l'adoption des technologies en nuage se fait plus lentement que dans le reste de l'Union européenne. Nous sommes donc toujours surpris d'être associés aux deux *leaders* du marché. Chez Google Cloud, nous croyons en un nuage qui tient sa promesse initiale. Ouverture et sécurité, élasticité et simplicité et surtout une grande liberté de choix pour le client, notamment pour tester de nouvelles fonctionnalités et des innovations.

Google *cloud* souhaite se différencier des autres acteurs, notamment grâce à ses services basés sur des technologies *open source*. Ces technologies sont la pierre angulaire de l'interopérabilité, de la portabilité, d'une meilleure utilisation des ressources énergétiques et de l'indépendance de ses fournisseurs. Google *cloud* est d'ailleurs l'un des premiers fournisseurs à s'être mis volontairement en conformité avec le code européen *Switching cloud Providers and Porting Data (SWIPO)* pour promouvoir la portabilité et la liberté de changer de fournisseur, ce qui n'est pas le cas de tous les acteurs du marché. Google Cloud est reconnu comme un acteur majeur du monde de l'*open source*. Nous remettons régulièrement des technologies à fort impact entre les mains de la communauté *open source* mondiale, notamment des logiciels comme Kubernetes ou TensorFlow qui sont aujourd'hui utilisés par d'autres, y compris nos concurrents directs. Chez Google Cloud, nous avons toujours eu comme mantra que nous ne sommes ni les meilleurs ni les plus parfaits, mais que nous sommes sérieux, fiables, pragmatiques et surtout que nous avons toujours quelque chose à apprendre de nos partenaires et interlocuteurs, notamment ici aujourd'hui. Comme nous apprenons tous les jours de notre principal partenaire en France, le groupe Thalès, avec qui nous travaillons une offre portée par S3NS, la filiale *cloud* de Thalès et qui a pour vocation de décrocher la qualification SecNumCloud.

Notre vision d'un *cloud* de confiance passe donc par des technologies *open source*, garantes de sécurité, de maintenance à long terme et donc d'une plus grande robustesse pour les utilisateurs finaux. Ce propos introductif portera donc sur le titre 3 du projet de loi et notamment ses deux premiers chapitres consacrés à l'informatique en nuage. Quel ne fut pas notre plaisir de lire dans le titre de ce chapitre 1er « Pratiques commerciales déloyales entre entreprises sur le marché de l'informatique en nuage ». Car de notre point de vue, et nous l'avons exprimé déjà auprès de l'Autorité de la concurrence française, il existe des pratiques commerciales que nous souhaitons voir qualifiées de déloyales. Google Cloud souhaite souligner ici la grande qualité des travaux portés par le Cigref en France et par le *Cloud Infrastructure Services Providers in Europe (CISPE)* au niveau européen et leurs dix principes pour l'octroi de licences logicielles équitables pour les clients utilisant l'informatique en nuage. Je précise que Google n'est membre d'aucune de ces deux organisations. Nous attendons aussi le travail de l'Autorité de la concurrence qui devrait utilement nourrir ce débat. Quelle ne fut donc pas notre surprise de ne pas trouver dans ce chapitre 1er le résultat des travaux du Cigref et du *CISPE*, mais d'y trouver le sujet des avoirs ou crédits *cloud* alors même que nombre d'autorités de la concurrence, notamment française, britannique, néerlandaise ou japonaise, les voient comme un véhicule de fluidification et d'ouverture du marché et que l'ensemble des acteurs, petits, moyens et gros, les propose.

Il est à noter que le règlement européen sur les données dit *Data Act* n'aborde pas ce sujet. En revanche, le *Data Act* aborde bien le sujet des coûts de transfert. Sur ce sujet, nous souhaitons souligner, comme nombre d'autorités et d'acteurs du marché l'ont déjà fait, que l'anticipation de ce texte européen est dommageable car, en fonction du résultat des travaux du législateur français, cela créera peut-être de la confusion et des différences notables au sein même du marché unique européen. Notre lecture du texte français est d'ailleurs assez orthogonale avec celle des travaux européens toujours en cours sur ces questions de coûts de sortie comparativement aux coûts de transfert. Nous appelons donc de nos vœux le législateur à clarifier avec pragmatisme et avec beaucoup de précision ce sujet et surtout à ne pas être distant des travaux européens en cours. Il y a aussi la définition, ô combien cruciale !, de l'équivalence fonctionnelle qui nous paraît aujourd'hui différente des travaux européens, un sujet fort complexe qui nécessite à nos yeux beaucoup de pragmatisme. Concernant les nouveaux pouvoirs confiés à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) en matière d'interopérabilité, nous sommes reconnus dans ce domaine et serons ravis de travailler avec l'autorité. Nous croyons dans le pragmatisme de l'autorité et sommes plutôt dubitatifs sur l'opportunité de créer une norme française en la matière. En effet, les normes internationales ont fait leur preuve sur le marché des télécommunications et de l'Internet depuis quelques années déjà. En conclusion, nous souhaitons apporter avec joie notre contribution à vos

travaux, notamment, vous l'aurez compris, sur les licences logicielles équitables et un marché de l'informatique en nuage toujours plus ouvert.

M. Yohann Bénard, directeur des affaires publiques d'Amazon. – Je souhaite profiter de l'occasion qui m'est donnée pour inscrire le texte que vous allez examiner dans un contexte plus large, qui est celui de l'ambition auquel il répond. Cette ambition, inscrite dans la stratégie numérique européenne en 2015, consiste à construire le marché unique du numérique afin de garantir aux consommateurs et aux entreprises un meilleur accès aux biens et aux services en ligne, d'une part, et d'autre part, de créer un environnement favorable à la croissance des réseaux et des services numériques, pour faire du numérique un moteur de croissance en Europe. Amazon est pleinement en phase avec cette ambition que nous faisons nôtre.

Mme Catherine Morin-Desailly, présidente. – Il s'agissait d'une ambition exclusivement au service du consommateur et pas forcément en faveur d'une industrie européenne. Certains événements sont survenus depuis et l'Europe a pris conscience de la nécessité d'une politique industrielle et de souveraineté. Nous ne sommes plus dans la même configuration qu'en 2015 avec la Boussole numérique pour 2030.

M. Yohann Bénard. – Amazon a une obsession qui est celle des consommateurs et je souhaite rappeler l'importance de ces textes et du marché unique européen pour les consommateurs, qu'il s'agisse de particuliers ou d'entreprises. Nous contribuons depuis près d'un quart de siècle à la construction de ce marché unique et de sa composante numérique, puisque lorsque nous nous sommes installés en France en 2000, le marché unique venait alors d'être proclamé. Ses quatre libertés constitutives avaient été énoncées, mais leur mise en œuvre était encore limitée : la libre circulation des biens notamment, avec des réseaux logistiques qui n'étaient pas adaptés à l'échelle de l'Union européenne ; la libre prestation de services, avec peu de services en ligne fiables, sûrs et faciles d'accès pour tous les Européens. Les consommateurs et les entreprises européens avaient donc un accès au marché unique en droit, mais pas dans les faits. Aujourd'hui, ces libertés sont devenues des réalités.

Lorsque les consommateurs se rendent sur Amazon.fr ou sur des sites équivalents dans d'autres pays européens, ils ont accès à des millions de produits disponibles au sein de l'Union européenne et aux offres de 225 000 entreprises européennes, pour la plupart des TPE et des PME, dont 13 000 françaises qui utilisent Amazon pour accéder à la clientèle européenne et qui recourent à notre réseau logistique pour livrer leurs produits à des consommateurs parfois localisés dans un autre pays et ne parlant pas la même langue. Cette réalité est le fruit du marché unique et de sa composante numérique.

La construction du marché unique s'est exprimée dans d'autres domaines comme les services d'informatique en nuage, qui permettent à des

entreprises européennes de stocker et de traiter leurs données de manière efficace et sécurisée. Amazon est également présent dans les industries créatives avec le financement depuis deux ans de 130 créations européennes originales, dont *Salade grecque* de Cédric Klapisch. Cette suite de *L'Auberge espagnole* est diffusée partout en Europe et aide à la constitution d'un espace culturel commun.

Amazon a ainsi investi 142 milliards d'euros en Europe depuis 2010, dont 16 milliards en France. Amazon est l'entreprise en France qui a créé le plus d'emplois depuis 2010 avec près de 100 000 emplois directs et indirects tous secteurs confondus. Les PME et les TPE françaises qui utilisent Amazon pour accéder à leurs clients ont exporté pour 600 millions d'euros *via* Amazon en 2021.

Le marché unique et sa composante numérique sont aujourd'hui devenus des réalités, au bénéfice des consommateurs, mais aussi des salariés et des entreprises européennes. Nous en sommes très fiers.

Amazon adhère pleinement à l'idée que ce marché doit être régulé et que les règles qui s'appliquent dans le monde physique doivent également s'appliquer en ligne.

C'est déjà le cas en droit, même si des difficultés demeurent en pratique. Amazon fait plus qu'adhérer à l'idée et se mobilise en offrant à ses clients européens des services sûrs et en les préservant des fraudes en ligne, de la contrefaçon, de la cybercriminalité et de contenus et comportements illégaux. Plus de 800 000 tentatives de création de comptes frauduleux ont été bloquées en 2022. En coopération avec les marques et les autorités, plus de 1 300 contrefacteurs ont été signalés ou poursuivis et six millions de produits contrefaits ont été repérés et saisis, empêchant toute revente. Amazon a la confiance des Français, comme le confirment les enquêtes année après année. Durement acquise, cette confiance nous engage à poursuivre dans cette voie. En 2022, plus d'un milliard d'euros a été investi dans l'ensemble des actions citées.

En réponse à la question posée en introduction, Amazon se conformera aux règlements européens en cours d'adaptation en droit français, même si certaines dispositions ne semblent pas de nature à renforcer la protection des Européens dans le monde numérique.

En conclusion, je souhaite attirer votre attention sur un premier risque associé à l'examen du texte, celui de la fragmentation géographique. Le marché numérique européen n'est unique que parce que les mêmes règles s'appliquent d'un bout à l'autre de l'Europe. Les effets positifs en termes d'innovation, d'investissement, de création d'emplois ou de protection des citoyens et des consommateurs disparaîtraient si la transposition des textes ou leur application aboutissait à désolidariser la France de ses voisins européens. Les consommateurs français seraient alors soumis à des règles et à des niveaux de protection différents selon qu'ils choisissent d'acheter en

ligne sur un site, par exemple, français ou belge, ce qui n'est évidemment pas souhaitable. La création d'un espace numérique à deux vitesses dans lequel certaines règles ne s'appliqueraient qu'aux acteurs les plus importants serait problématique. Dans le monde physique, la loi protège de la même façon tous les consommateurs qu'ils se rendent dans un hypermarché ou dans un petit commerce de centre-ville. À notre sens, ils devraient en être de même dans le monde numérique.

Nous espérons que vos débats permettront, si ce n'est d'éviter, au moins d'aplanir ces deux écueils et contribueront à donner les mêmes droits et les mêmes protections dans le monde numérique et à garantir un environnement numérique à la fois sûr et propice à l'innovation, au bénéfice des citoyens et des acteurs économiques européens.

Mme Catherine Morin-Desailly, présidente. – Nous avons conscience du risque de fragmentation de la législation, mais je rappelle que le RSN et le RMN sont des règlements et non des directives. Il y a une harmonisation par le haut qui s'impose.

M. Arnaud David, directeur des affaires publiques européennes d'Amazon Web Services (AWS). – AWS est une entreprise d'informatique en nuage. Les premiers centres de données en France ont été ouverts en 2017, dans le cadre d'un plan d'investissement sur 15 ans d'un montant de six milliards d'euros. Aujourd'hui, AWS compte 1 000 salariés en France et génère, d'après l'institut Public First, 1,6 milliard d'euros de valeur économique qui soutient 130 000 entreprises et 22 000 emplois. AWS investit également dans la formation pour aider les citoyens français à acquérir des compétences numériques dans la sécurité ou dans l'intelligence artificielle. Il est prévu de former 29 000 personnes d'ici 2025. Notre métier est de fournir des ressources informatiques à la demande avec une tarification à l'usage. AWS fournit aujourd'hui aux clients français plus de 200 services en lien avec le stockage et la gestion de bases de données, la sécurité ou encore l'intelligence artificielle.

Le modèle d'affaires repose sur la confiance de nos clients et AWS investit continuellement pour permettre à ses clients de décider où ils stockent leurs données, comment elles sont utilisées, qui y a accès et comment elles sont sécurisées. AWS soutient le développement d'un écosystème numérique ouvert et compétitif pour les industries, les gouvernements et les citoyens européens. En France en particulier, AWS soutient les initiatives qui consistent à accélérer la transition numérique des organisations publiques et privées, tout en garantissant que les utilisateurs disposent d'une entière liberté dans le choix de la technologie qui corresponde le mieux à leurs besoins. Cette liberté de choix est fondamentale.

Selon une étude du cabinet IDC, le nombre de fournisseurs d'informatique en nuage a considérablement augmenté entre 2017 et 2021 : de 17 à 40 pour les fournisseurs de taille moyenne dont le chiffre d'affaires

excède les 20 millions d'euros ; de 47 à 132 pour les fournisseurs qui font moins de 5 millions d'euros de chiffre d'affaires.

Ce projet de loi nécessite la main attentive du législateur sur trois points en particulier.

L'encadrement des avoirs en premier lieu, proposé à l'article 7, est une pratique courante dans de nombreux secteurs. L'octroi d'avoirs aux clients d'AWS a un objectif double : d'une part permettre d'accélérer la transition numérique des entreprises en les encourageant à utiliser ces nouveaux services, et d'autre part donner notamment aux PME et aux jeunes pousses l'occasion de tester ces nouvelles technologies. Comme souligné par l'Autorité de la concurrence dans son avis, l'avoir n'est pas une pratique anti-concurrentielle et le supprimer ou en réduire la portée pourrait entraver la *French Tech* en la privant de crédits alors que ses avoirs seraient disponibles dans d'autres pays européens. Il convient de se demander si une *lex specialis* est nécessaire en la matière, là où des sanctions en cas de pratique anti-concurrentielle existent, que ce soit au titre du déséquilibre significatif ou de l'avantage sans contrepartie.

Concernant en second lieu les frais au titre des transferts de données vers un nouveau fournisseur, il est à noter que la grande majorité des prestataires de services informatiques ne facturent pas de frais supplémentaires ni de pénalités lorsqu'un client passe d'un fournisseur à un autre. AWS ne facture pas de frais supplémentaires lorsqu'un client change d'environnement numérique. Par contre AWS facture l'utilisation du réseau, quel que soit le motif défini par l'entreprise utilisatrice. Lorsqu'une entreprise de services de radiodiffusion ou de vidéos à la demande diffuse du contenu à ses consommateurs finaux, son utilisation du réseau lui sera facturée en fonction de la quantité de données transférées et de la distance que cette donnée doit parcourir. Chez AWS, ces frais d'utilisation ont diminué de 50 % entre 2018 et 2022. La mesure d'encadrement des frais aux titres de transfert doit être mise en cohérence avec l'article 25 du règlement sur les données actuellement en discussion à Bruxelles. En effet, le règlement sur les données prévoit à ce jour une suppression progressive des frais de transfert sur trois ans, alors que la mesure inscrite au projet de loi pourrait s'appliquer dans quelques mois. À défaut et comme souligné par l'Autorité de la concurrence, cela pourrait entraîner un problème d'attractivité pour les fournisseurs.

En dernier lieu, l'approche proposée aux articles 8 et 9 sur la portabilité des actifs numériques ne reflète pas la variété et la complexité des services d'informatique en nuage et l'utilisation qu'en font nos clients. Ces services ne peuvent être comparés à des services téléphoniques, et regroupent des services aussi variés que la gestion d'une messagerie électronique comme laposte.net, des outils de traitement de photos, une base de données de gestion de contrats commerciaux ou les services proposés par la société française Hugging Face en matière d'intelligence artificielle.

Les clients d'AWS utilisent des briques technologiques, des codes et des formats pour développer leurs propres applications et leurs propres services. Ils jouent un rôle actif en cas de transfert vers un nouveau fournisseur puisqu'ils ont défini l'architecture de leurs solutions. En pratique, ces clients vont consulter leurs équipes en interne, avoir recours à des prestataires externes et/ou s'appuyer sur les compétences du nouveau fournisseur pour mener à bien le transfert. La notion d'équivalence fonctionnelle est problématique dans la mesure où, comme souligné par l'autorité de la concurrence, elle pourrait étouffer l'innovation en standardisant les services vers le plus petit des dénominateurs communs.

Mme Catherine Morin-Desailly, présidente. – Le caractère stratégique et privé de nos données est au centre de notre préoccupation. En tant qu'entreprises extra-européennes américaines, vous êtes soumis aux lois extraterritoriales. Avec la loi *Foreign Intelligence Surveillance Act (FISA)*, vous êtes tenus de transmettre les données des Européens sur requête de la NSA, oui ou non ?

M. Arnaud David. – À mon sens, non. Le régime s'applique, mais nous avons la possibilité de contester son application en justice. Toute entreprise opérant dans un pays hors Union européenne ou même hors de France est soumise à des réglementations différentes.

M. Frédéric Géraud. – Nous contestons un certain nombre de requêtes formulées par le gouvernement américain. Le nombre de requêtes par typologie de services est publié dans notre rapport de transparence. Cela étant, le juge peut nous contraindre à soumettre ces données ; en tant qu'acteur local, nous sommes contraints par la loi et nous respectons les législations locales partout où nous opérons.

Mme Catherine Morin-Desailly, présidente. – En l'absence d'accord de transfert des données entre les Européens et les États-Unis, il me semble que vous êtes contraints de soumettre les données.

M. Loïc Hervé, rapporteur. – Quel est l'état de vos relations avec les autorités administratives indépendantes dont la Cnil, l'Arcom, l'Arcep, le PEReN ? Quelles sont éventuellement les difficultés rencontrées ?

Pharos nous a indiqué travailler en partenariat avec les opérateurs, qui eux-mêmes traitent des signalements relatifs à des contenus illicites ou en assurent la détection. Quelles actions menez-vous de votre côté et comment communiquez-vous avec les autorités nationales, y compris les juridictions ?

Comment analysez-vous les nouvelles règles créées par le *DSA*, celles qui créent de nouveaux types d'injonctions comme celles qui instituent un exposé des motifs en cas de contenu illicite ou une notification de soupçon d'infraction pénale, ou encore celles qui renforcent vos obligations en matière de transparence, d'audit et d'évaluation des risques ?

Le *DSA* vous impose de mettre en place des mesures spécifiques pour protéger les mineurs. Qu'avez-vous prévu en la matière ?

Pensez-vous qu'il soit possible, voire opportun, de développer des dispositifs d'identité numérique allant au-delà du simple contrôle de la majorité lorsqu'il s'agit de contrôler l'accès aux sites pornographiques ?

Je souhaite également avoir votre position sur les articles 1er à 5.

Le référentiel de vérification de majorité mis en place à l'article 1er du projet de loi semble concerner uniquement les éditeurs de services permettant l'accès à un contenu pornographique. Ne serait-il pas également utile en dehors de ce secteur spécifique ? Comment vérifiez-vous aujourd'hui que vos utilisateurs sont majeurs et dans quels cas procédez-vous à ce type de contrôles ?

Les services que vous fournissez peuvent conduire au visionnage d'images pornographiques par des mineurs. Que mettez-vous en place pour l'éviter ou le limiter, notamment dans le contrôle de vos publicités ?

Concernant l'article 3, que pensez-vous du cadre français de lutte contre les contenus terroristes et pédocriminels ? Quelle est votre analyse sur la nouvelle sanction pénale créée par l'article 3 en cas de défaut du retrait par un hébergeur d'un contenu pédopornographique dans un délai de vingt-quatre heures ?

Comment analysez-vous l'extension des pouvoirs de l'Arcom dans la lutte contre la diffusion des contenus produits par les médias visés par les sanctions européennes ? Quelles mesures avez-vous mises en place depuis 2022 pour éviter la diffusion des programmes produits par Russia Today et par Sputnik.

L'article 5 crée une peine supplémentaire dite de bannissement et fixe deux obligations pour les plateformes : obligation de blocage du compte qui a servi à commettre l'infraction avec sanction associée et obligation de moyens sans sanction associée pour le blocage des autres comptes de la personne condamnée. Avez-vous les moyens techniques de faire respecter une telle obligation ? Comment procédez-vous lorsqu'une personne est bannie de votre service pour ne pas avoir respecté les conditions générales d'utilisation pour éviter qu'elle n'y revienne en dissimulant son identité ?

Mme Béatrice Oeuvrard. – Concernant les relations avec les autorités, nous n'avons pas attendu la loi contre la manipulation de l'information pour échanger avec l'Arcom notamment. Lancée il y a cinq ans, la mission dite « Facebook » visait à expliquer notre manière de travailler aux régulateurs et a abouti au rapport *Loutrel*, sur lequel s'est appuyé le RSN. Les échanges avec le régulateur sont très importants et utiles pour nous aider à prendre des décisions ou *a minima* échanger sur les décisions à prendre. Ces relations fonctionnent de manière satisfaisante depuis plusieurs années. Au sein de Meta France, une personne est dédiée à la relation avec

l'OCLCTIC. Environ 25 000 réquisitions par an sont traitées avec un taux de conformité approchant 90 %, comme indiqué dans notre rapport de transparence. Cela étant, nous manquons de visibilité sur la part des réquisitions qui sont judiciarisées. C'est dans ce contexte que s'inscrit notre proposition d'avoir recours à des agents assermentés qui disposeraient d'un pouvoir efficace. Nous pouvons retirer des millions de contenus, il faut aussi que le pouvoir étatique joue son rôle. Le chiffre de 54 condamnations pour cyberharcèlement montre que la justice a des difficultés à suivre. Un système intermédiaire permettrait de désengorger les tribunaux et de répondre à cette attente des utilisateurs.

Nous sommes également en relation avec le PEReN. Selon notre compréhension, le PEReN doit être mandaté par un régulateur comme l'Arcep, la Cnil ou l'Arcom afin de pouvoir initier des études et capter des données, ce qui n'est pas en ligne avec l'article 16 du projet de loi. Ils sont assimilés non pas à une institution gouvernementale mais à des chercheurs, ce qui nous interroge. Nous nous questionnons sur la nature des données, les moyens mis en place et les raisons pour lesquelles ce dispositif n'a pas été notifié à la commission européenne, alors même qu'il touche aux articles 34 et 40 du RSN.

Concernant les types d'injonction inscrits à l'article 5, nous souscrivons aux dispositions de lutte contre le cyberharcèlement, mais comme indiqué nous nous interrogeons sur les modalités pratiques de blocage des comptes à venir de personnes condamnées. L'identification de ces personnes supposerait un échange de fichiers contenant des informations sensibles, ce qui devrait en premier lieu être discuté avec la Cnil. De plus, au regard de la LCEN et du RSN, le principe de spécialité implique la communication d'informations très spécifiques comme une URL. Agir uniquement sur la base d'un nom et d'un prénom poserait problème en cas d'homonymie. Les dispositions du projet de loi ne sont d'ailleurs pas alignées avec celles du RSN.

Dans les articles 1er et 2, il est tour à tour fait référence aux éditeurs et aux services de communication en ligne, ce qui peut porter à confusion. Selon nous, ces articles visent les éditeurs et non la partie hébergeur telle qu'on l'entend côté plateforme.

L'une des dispositions relatives aux contenus pédopornographiques nous oblige à notifier au potentiel pédocriminel les contenus qui ont été signalés, mettant potentiellement à risque les personnes ayant effectué le signalement.

Concernant Russia Today et Sputnik, nous avons répercuté les décisions telles qu'elles nous ont été notifiées au niveau européen et par l'Arcom. Ces mesures avaient déjà été identifiées, car il y avait des violations de contenu. Lors des discussions sur le RSN, nous avions indiqué que la labellisation et le *sourcing* de ce type de contenus posaient problème.

Aujourd'hui, la source du contenu apparaît sur Facebook et Instagram et les contenus d'un média étatique sont identifiés comme tels, lorsque nous disposons de l'information. Cette labellisation s'appuie sur l'article 215 du traité sur le fonctionnement de l'Union européenne, ce qui garantit un cadrage et une définition précise et donc une identification facilitée.

M. Anton'Maria Battesti. – La question des jeunes publics et de l'identité numérique est traitée de différentes manières.

Le contenu doit d'abord être adapté à ces personnes. Sur Instagram, par exemple, quand vous êtes un mineur, certaines fonctionnalités sont activées par défaut. La pornographie étant interdite sur ces plateformes, le point n'est pas traité ici.

Un partenariat a été mis en place avec la société Yoti qui a développé une solution de vérification de l'âge par analyse morphologique. Dans 95 % des cas, si le jeune veut mentir il ne passe pas le test de Yoti ; la barrière est donc assez efficace. Si nous progressons en matière de contrôle de la majorité, les difficultés demeurent pour les utilisateurs plus jeunes et notamment les 13-14 ans. Les jeunes utilisent les réseaux sociaux comme un système d'entraide et y exercent leurs droits fondamentaux comme la liberté d'association et la liberté d'expression. Il faut donc accepter l'idée que c'est compliqué de trouver le bon équilibre.

Le RSN prévoit la réalisation d'analyses d'impact spécifiques pour les jeunes et contient des dispositions en matière de publicité pour ces publics. Sur la question de l'âge, il est important de mettre tous les acteurs autour de la table et d'en parler de manière régulière.

Mme Béatrice Oeuvrard. – Le délai de vingt-quatre heures donné aux plateformes pour retirer les contenus pédopornographiques s'assimile au dispositif mis en place par le règlement relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne (TCO). Cela suppose une coordination au niveau européen avec les autorités et avec les autres plateformes, pour éviter, grâce à l'apposition de *tags*, que ces contenus apparaissent sur d'autres plateformes. Une coordination au niveau mondial *via* NCMEC, avec qui toutes les plateformes travaillent, est aussi souhaitable pour garantir la rapidité et l'efficacité de l'action. Il paraît difficile de tenir le délai de vingt-quatre heures sans cette coordination. Or, on ne retrouve pas la coopération entre autorités dans le projet de loi.

M. Benoît Tabaka. – Le régulateur naturel d'Internet a longtemps été le juge et il y a eu longtemps une vraie difficulté à rentrer dans une logique de régulation, mais nous avons assisté au cours des dix dernières années à une montée en compétences des divers régulateurs, autorités administratives et administrations comme le PEReN.

De véritables canaux de communication sont en place et des discussions, y compris sur le plan technique, sont menées avec les différents régulateurs comme l'Arcep, la Cnil, l'Arcom ou le PEReN.

De nombreuses questions font aujourd'hui intervenir plusieurs régulateurs, pour couvrir les différents prismes : concurrence, protection des données, régulation des contenus ou encore la liberté d'expression. Comme piste d'amélioration il nous semble qu'il faudrait mieux structurer cet échange et permettre à une entreprise en prise avec une question complexe d'obtenir une réponse tenant compte de l'ensemble des équilibres à trouver entre les différents droits et libertés.

Nos équipes sont entièrement engagées dans la préparation de la mise en œuvre du RSN, maintenant que les différentes grandes plateformes ont été désignées. Les services que nous avions identifiés comme entrant dans le périmètre du RSN ont sans surprise effectivement été désignés comme tels. Parmi les dispositifs mis en œuvre pour cet été, dès qu'il y aura un retrait de contenu, la personne sera informée des raisons et disposera de capacités d'appel.

Concernant les articles 1er et 2 et la vérification de l'âge pour l'accès aux sites pornographiques, il conviendrait d'ajouter la possibilité de faire reposer ces dispositifs de vérification sur les opérateurs de télécommunication comme c'est le cas dans d'autres pays. Le contrôle de l'âge ne se ferait plus au niveau du service, mais au niveau de l'opérateur, par l'intermédiaire d'un code d'accès, l'opérateur disposant d'informations sur l'identité du détenteur de compte. Une réflexion est à mener, mais il faut peut-être l'anticiper dans le texte.

L'article 227-24 du code pénal, auquel fait référence l'article 2, ne se limite pas aux contenus pornographiques. Il porte entre autres sur les contenus qui mettent les mineurs en danger, comme les jeux dangereux. Ces contenus non pornographiques ne sont pas dans le périmètre de la loi et nous nous demandons comment ils seront traités en termes de blocage d'accès.

L'article 2 revoit la mécanique existante, qui était quasiment finalisée malgré tous les recours déposés par certains sites. Nous entrons sans doute dans une phase émaillée de débats judiciaires, de questions prioritaires de constitutionnalité et de recours au niveau européen. Le texte ne pourrait-il pas être stabilisé en s'inspirant de ce qui existe en matière de lutte contre le piratage ? Le juge donne une première orientation, et le régulateur s'appuie sur cette orientation pour être plus large en termes de mesures de blocage.

Concernant les contenus pédopornographiques, il s'agit là d'un vrai problème qui concerne notamment la France. Près de sept millions de contenus pédopornographiques sont retirés chaque trimestre et notifiés aux autorités américaines, qui ensuite informent les différents pays et pour la France, l'Office central pour la répression des violences aux personnes.

Cela représente 1,1 million de personnes dans le monde, et la France est le deuxième ou le troisième pays hébergeur de ces contenus selon les années. Il faut donc que cette mesure soit mise en œuvre. Pour être encore plus efficace, il faudrait prévoir un rapport de transparence indiquant où sont stockés les contenus dont les autorités ont demandé la suppression. Si on a un problème en France, il est important de le savoir.

Concernant l'article 4, nous avons bloqué 800 chaînes YouTube et plus de quatre millions de vidéos sur décision de la commission européenne. La volumétrie est importante et ne concerne pas uniquement Russia Today et Sputnik. Le ministre du numérique de l'époque nous avait notifiés lorsque Russia Today avait refait une apparition *via* la plateforme Odysee, et nous l'avions fait déréférencer par le moteur de recherche. Cela étant, nous sommes favorables à des pouvoirs accrus du régulateur en la matière.

La désinformation et les pratiques d'influence étrangère prennent de plus en plus l'apparence et la qualification juridique de média. Le choix de l'Arcom, le régulateur des médias, est donc pertinent.

Sur l'article 5, les 54 condamnations par an pour des faits de cyberharcèlement sont à rapprocher des 130 000 à 150 000 contenus YouTube qui sont supprimés tous les ans. Que peut-ont faire ? Il existe un mécanisme en France qui permet d'envoyer un message d'avertissement à une personne qui a téléchargé ou piraté un film. Et nous ne serions pas capables de faire de même lorsqu'une personne tient en ligne des propos antisémites ou autres propos haineux, ou lorsqu'elle s'adonne à du cyberharcèlement ? La mécanique et les outils juridiques existent pourtant et ce dispositif aurait un réel impact en termes d'efficacité.

Nous avons la possibilité de bloquer les comptes, même si c'est compliqué techniquement. Des informations beaucoup plus détaillées seront nécessaires si nous voulons aller au-delà de l'obligation de moyens et assurer un vrai blocage de nouveaux comptes, et cela soulèvera des questions en termes de protection des données. Il faudrait avoir un échange avec la Cnil pour déterminer où mettre les moyens et assurer la collecte des données et les interconnexions. Ce sera fait pour les 54 personnes condamnées chaque année, à condition encore que le juge, pour chacune d'entre elles, prononce la peine complémentaire d'interdiction de réseaux sociaux. Ce sera donc fait sans doute pour 25 personnes chaque année.

La mesure est utile, mais ne peut-on pas mettre en place d'autres mesures beaucoup plus efficaces ?

Concernant les dispositifs de protection de la jeunesse et de vérification d'âge, nos systèmes permettent d'identifier des incertitudes et/ou des incohérences qui déclencheront une vérification *via* la carte bancaire ou par la fourniture d'une pièce d'identité. Ce sera le cas, par exemple, pour une personne qui visionne beaucoup de contenus pour enfants sur YouTube, mais qui, dans nos systèmes, n'est pas présentée

comme une personne mineure. En cas de doute, la personne sera poussée dans un univers jeunesse. Si le doute est levé, la personne pourra continuer à évoluer dans un univers tout public.

On peut se poser la question du blocage par l'Arcom de sites qui ne proposent pas la vérification d'âge, comme les sites pornographiques, et de l'extension du rôle de l'Arcom à tous les types de vérification d'âge.

Une même logique de régulation commence à émerger notamment en matière de contrôle des contenus sur Internet, avec la capacité pour une autorité administrative de retirer du contenu pour différentes raisons et derrière, une autorité référente. Notre recommandation serait de concentrer au sein d'une même autorité les personnalités qualifiées, qui ont une connaissance, une culture et des procédures. Pourquoi ne pas faire converger les moyens vers une autorité unique lorsqu'il s'agit de contenus sur Internet ?

M. Arnaud David. – La protection de l'enfant est un engagement très fort d'Amazon. Si les dispositifs de vérification d'âge devaient être étendus à d'autres domaines, l'Arcom et la Cnil auraient un rôle à jouer et il en résulterait une procédure intéressante, car procédant d'une consultation de standard technique et d'un référentiel technique.

Il nous semble essentiel de travailler avec les associations. Sur les questions de cyberharcèlement et de protection de l'enfance, nous nous appuyons sur l'expertise d'associations françaises (Respect Zone par exemple) et internationales.

Il est par ailleurs important d'initier une harmonisation des standards internationaux. La France a un rôle moteur à jouer, avec par exemple l'Appel de Christchurch lancé avec la Première ministre de Nouvelle-Zélande sur la question du terrorisme en ligne. Une initiative lancée au Forum de Paris sur la Paix a débouché récemment sur la création d'un laboratoire sur la protection de l'enfance en ligne piloté par Henri Verdier, l'Ambassadeur pour le numérique. Amazon est membre fondateur de ces deux initiatives et s'associe en tant qu'entreprise à ces projets particulièrement pertinents.

M. Patrick Chaize, rapporteur. – Comment vos entreprises vont-elles contribuer au déploiement du filtre anti-arnaques ? Pour les fournisseurs de navigateurs Internet, de quelle façon allez-vous répondre aux demandes des autorités administratives pour prendre les mesures qui sont prévues par le texte ?

Vos entreprises ont aujourd'hui un poids certain sur l'informatique en nuage et il semble tout de même y avoir une forme de verrouillage du marché au détriment des entreprises françaises. Je partage votre analyse sur l'utilité des crédits *cloud* pour les jeunes pousses, mais quel est votre avis sur les orientations prises et notamment sur le fait de limiter dans le temps ces crédits *cloud* ? Sur le sujet des frais de transfert, est-ce votre position

commune d'affirmer que vous n'en facturez pas ? Auquel cas l'intégrer dans la loi n'aurait aucune conséquence et ne poserait de problème à personne.

Sur l'intermédiation de données, pouvez-vous donner des exemples concrets de données qui pourraient être partagées volontairement par des entreprises sur ces nouvelles plateformes numériques ?

Concernant les jeux numériques monétisables abordés à l'article 15, vos entreprises en développent ou en proposent-elles ? Un encadrement spécifique est-il nécessaire selon vous ?

Mme Béatrice Oeuvrard. – Meta France n'est pas concerné par ces mesures.

M. Benoît Tabaka. – Google n'est pas concerné par les jeux numériques monétisables.

Concernant le filtre anti-arnaques inscrit à l'article 6, notre solution mondiale *Google Safe Browsing* permet de détecter des suspicions de *phishing*, de téléchargements de logiciels malveillants et autres grâce à l'intelligence artificielle et sur la base d'analyses menées par nos équipes. Cette interface de programmation d'application (API) affiche les informations dans les navigateurs comme Safari, Firefox ou Google Chrome, mais aussi dans les navigateurs internes de certaines applications. Nos équipes travaillent aujourd'hui sur l'articulation entre l'outil et le nouveau cadre juridique français, en sachant qu'un blocage *via Safe Browsing* serait par nature mondial.

Il serait par ailleurs intéressant de mettre en place une sorte de guichet unique qui centralise l'ensemble de ces contenus. Il faudrait aussi définir une personnalité qualifiée pour recevoir ces signalements, et l'Arcom pourrait jouer ce rôle. La Cnil est à écarter selon nous, car elle ne peut être à la fois autorité notifiante et personnalité qualifiée. Il serait aussi utile d'instaurer un mécanisme de dialogue entre les opérateurs du numérique et les autorités, pour éviter ce qui s'est passé récemment avec le blocage de Telegram.

Sur le volet des sanctions, il est important d'aligner les dispositions du projet de loi avec la logique RSN. C'est la mauvaise volonté dans la mise en œuvre de la loi qui devrait être sanctionnée, plutôt que d'appliquer une sanction dès le premier cas.

Il serait également intéressant que le gouvernement lance une opération de communication et publie un rapport annuel pour informer le public de ces nouvelles mesures.

Enfin, si l'obligation pèsera principalement sur les navigateurs, les faire participer est une piste à explorer au nom de l'efficacité.

M. Frédéric Géraud. – Concernant les crédits *cloud*, leur validité est limitée à deux ans et nous ne sommes pas favorables à une durée de vie plus

courte. Sur l'année 2021 en France, Google Cloud a soutenu au travers de ces crédits 4 414 jeunes pousses, qui ont consommé en moyenne 1 300 euros de crédits. Il ne s'agit pas de dizaines ou de centaines de milliers d'euros, et un certain nombre d'acteurs du marché sont capables d'offrir le même type de conditions. Ces crédits aident les entreprises françaises à adopter des technologies numériques et d'informatique en nuage.

Sur la question des coûts de transfert, le texte nous semble prendre le contre-pied des discussions au niveau européen. Il y a d'une part les coûts de sortie lorsqu'un client met fin à sa relation contractuelle, et d'autre part les coûts de transfert quand les données sont envoyées chez un autre fournisseur, dans des cas de *multi cloud* notamment, pour ensuite revenir chez le fournisseur d'origine. Dans ce deuxième cas de figure, il y a des coûts de réseau et de transport qu'il faut bien répercuter au client final. Google Cloud n'applique pas de pénalités en cas de transfert et facture strictement le coût d'utilisation des réseaux lors du transport de ces données. Nous sommes cependant disponibles pour approfondir la discussion sur ces coûts de transfert.

Concernant l'intermédiation de données, Google Cloud est membre de Gaia-X, une initiative du secteur privé qui réunit des acteurs industriels par activité et non par branche. Le groupe de travail Gaia-X sur les services financiers, les banques et les assurances a ainsi beaucoup avancé sur la question du partage de données selon le niveau de sécurité, selon l'usage et selon le type de fournisseur (de rang 1, de rang 2 et de rang 3). Le groupe de travail sur l'automobile a lui aussi produit des travaux intéressants. Et on sait aussi que le groupe de travail qui suit les questions autour de l'automobile au sein de Gaia-X aussi, a déjà beaucoup avancé sur ces questions. Nous partons du principe que l'ensemble de l'industrie, lorsqu'elle arrive à se mettre autour d'une table et à discuter pour définir des standards, des processus de communication et d'interopérabilité entre les acteurs, est toujours une excellente solution. Et donc, on continuera de participer activement au travail de Gaia-X.

M. Arnaud David. – La question du filtre anti-arnaques ne relève pas *a priori* de l'activité d'AWS, qui n'est pas producteur de contenus. Nos clients utilisent nos briques technologiques pour construire des sites qui peuvent avoir des contenus particuliers. Ça fait le lien avec les discussions de tout à l'heure sur les contenus pédopornographiques.

AWS applique une politique d'utilisation du service stricte qui oblige le client à respecter les réglementations applicables d'une part (européennes notamment), et nos termes de service qui interdisent tout type de contenu illégal d'autre part. En cas de signalement, nous travaillons avec le client pour que le contenu soit retiré. Si le client n'obtempère pas, la seule solution technique à notre disposition est la fermeture de l'accès à la plateforme.

Concernant les crédits *cloud*, nous y sommes favorables et nos clients, PME et entreprises de taille plus importante, les considèrent comme un moyen d'expérimenter des services et de la technologie. Nos programmes ont une durée d'un ou deux ans en fonction de la complexité du projet informatique, et nous sommes disponibles pour échanger avec la commission sur les durées appropriées.

En matière de frais de transfert, il y a une distinction à faire entre les pratiques délibérées qui visent à bloquer un changement de prestataire et un modèle économique qui consiste à facturer l'utilisation d'un réseau. L'entreprise a sa part de responsabilité dans le coût du transfert, en fonction de la manière dont elle a codé son service et développé son application. Dans le texte, les frais de transfert sont définis de manière large et peuvent englober la prestation d'un prestataire externe rendue nécessaire par la complexité de la solution. Il est nécessaire selon nous d'affiner les définitions et les périmètres.

La question de l'intermédiation de données est à rapprocher de celles des espaces de données, qui n'existent pas encore en tant que tel. Neuf projets sont en cours au niveau européen, notamment dans le transport, la finance et la santé. AWS est membre fondateur de Gaia-X à la demande de nos clients et a participé au développement de standards communs. En décembre 2022, AWS a été la première entreprise américaine à se conformer lors d'une démonstration à l'ensemble des critères de Gaia-X, que ce soit en matière de portabilité des données et de transfert d'un opérateur vers un autre en fonction du code *SWIPO* ou en matière de protection des données. Plus d'une centaine de services AWS sont conformes au code de protection des données *CISPE* qui a été validé par l'ensemble des autorités de protection européennes avec la Cnil en chef de file.

Mme Florence Blatrix Contat. – Vous aviez indiqué dans vos propos introductifs Madame la présidente que l'enjeu de ce texte est de retrouver la confiance et la concurrence sur ces marchés du numérique. Et je me satisfais, monsieur Géraud, que vous ayez indiqué que vous souhaitiez un marché toujours plus ouvert. Cela dit, je souhaitais vous interpeller sur la question de la publicité en ligne. Même si ce n'est pas directement en lien avec le texte, il s'agit d'une question de concurrence essentielle. Le ministère américain de la Justice a porté plainte contre Google en janvier pour avoir utilisé des méthodes illégales et Google est visé par une enquête de la commission européenne. La commissaire à la concurrence, Margrethe Vestager, a indiqué que Google pourrait avoir abusé de sa position dominante en favorisant ses propres services. Ce qui vous est rapproché, c'est de favoriser vos propres services de technologie d'affichage publicitaire en ligne au détriment de prestataires de services de technologie publicitaire, d'annonceurs et d'éditeurs. Quelle est votre appréciation de ces griefs ? Avez-vous la volonté de mettre fin à ces pratiques qu'on peut qualifier d'anti-concurrentielles et comment ?

Par ailleurs, le *DMA* implique de ne plus utiliser les données personnelles d'un utilisateur à des fins de publicité ciblée, sans son consentement explicite. Comment cette mesure est-elle mise en œuvre ?

Enfin, vous avez indiqué que le marché du *cloud* est un marché dynamique avec de nombreux nouveaux opérateurs, dont le chiffre d'affaires augmente. Mais il faut bien constater que les opérateurs européens ont vu leurs parts de marché fondre sur le marché européen. Nous sommes bien dans une concentration du marché avec une domination des opérateurs extra européens. Vous semblez critiquer les mesures qui sont proposées. Quelles solutions nous proposez-vous pour rendre le marché du *cloud* plus contestable ?

Quand vous évoquez la possibilité de facturer l'utilisation du réseau, pensez-vous aux frais de bande passante ? À combien s'élèvent en moyenne ces facturations, en fonction de la taille des entreprises et des données hébergées ?

Mme Toine Bourrat. – Concernant le cyberharcèlement, le pseudonymat permet la multiplicité des comptes et son interdiction limiterait la publication de contenus haineux. Le RSN repose sur le principe suivant : ce qui est illégal hors ligne est illégal en ligne. Or dans la vie réelle, il est illégal d'avoir plusieurs identités.

Le texte prévoit l'obligation pour les plateformes de supprimer les contenus illicites qu'elles relaient dès leur signalement par la victime. Aujourd'hui, lorsqu'on est victime de cyberharcèlement, on subit une double peine. Non seulement on est victime de cyberharcèlement, mais en plus, on doit apporter la preuve de ce qu'on avance. Pendant ce temps, la publication continue à être diffusée à des milliers de personnes. Pour mieux modérer les réseaux, certains d'entre vous ont évoqué des ressources techniques, mais les moyens humains pour assurer la modération des différentes plateformes n'ont pas été mis en avant. Pouvez-vous nous en dire davantage sur ce point ?

Concernant le contrôle de l'âge, l'idée d'associer les opérateurs qui disposent de tous les éléments concernant l'identité des détenteurs du compte est très intéressante. Une solution de vérification de l'âge par analyse morphologique a été mentionnée. La solution repose-t-elle aussi sur la vérification d'une pièce d'identité ?

M. Anton'Maria Battesti. – Non, cette solution est utilisée en l'absence d'une pièce d'identité. Les adolescents n'ont pas nécessairement de pièce d'identité, en fonction notamment de leur localisation géographique. Des études ont permis de donner un âge en fonction de la morphologie. L'identité n'étant pas vérifiée, il ne s'agit pas de reconnaissance faciale.

Mme Toine Bourrat. – Comment peut-on s'assurer que la personne est bien celle qui va utiliser le compte ?

M. Anton'Maria Battesti. – La vérification de l'âge et la vérification de l'identité sont deux sujets importants, mais distincts. La solution Yoti apporte une réponse à la question de l'âge. Aujourd'hui, l'identité n'est pas vérifiée à l'inscription sur les réseaux sociaux.

Mme Toine Bourrat. – Selon ma compréhension, cette solution ne permet pas de s'assurer que le détenteur du téléphone est bien celui qui a été identifié comme majeur au départ.

M. Anton'Maria Battesti. – C'est aussi une question de proportion des moyens mis en œuvre et du type de documents que le législateur souhaite voir collectés. Ce sujet est important, je partage votre position.

Mme Toine Bourrat. – Je relaye une question de mon collègue Laurent Somon.

Sur le sujet du commerce en ligne, si vous vous assurez que la législation du pays du vendeur est conforme, faites-vous de même dans le pays du client ? À titre d'exemple, si je suis dans un pays où la drogue n'est pas autorisée, serais-je en mesure d'en acheter dans un pays où c'est le cas ?

M. Benoît Tabaka. – Concernant la publicité, je ne commenterai pas les procédures en cours. Le marché de la publicité, qui a longtemps été défini comme un duopole entre Google et Facebook, est aujourd'hui en pleine évolution. Microsoft a racheté Xandr et Netflix a fait une entrée remarquée sur le marché publicitaire en ligne. Amazon et Meta participent à ce dynamisme du marché, tout comme Apple qui est entré récemment et qui devrait atteindre 30 milliards de dollars de revenus publicitaires dans les trois ou quatre ans à venir. TikTok est également présent depuis peu et réalise environ 10 milliards de dollars de revenus publicitaires par an.

En parallèle, on assiste à des bouleversements technologiques comme le blocage des *cookies* qui est déjà une réalité sur le navigateur Safari par exemple. Pour Google, le blocage progressif des *cookies* sur les sites tiers débutera en 2024 pour laisser le temps à l'ensemble du secteur de trouver des solutions conformes à la réglementation en matière de protection des données.

Le *DMA* apporte de nouveaux éléments sur l'utilisation des données et le recueil du consentement. Nous sommes en attente de lignes directrices de la part de la commission européenne sur la manière dont chaque article doit être interprété. Les services publicitaires entrent par ailleurs dans le périmètre du RMN et de nouvelles obligations en résultent.

Internet se caractérise effectivement par une forte logique de pseudonymat. Cela étant, on ne connaît pas nécessairement l'identité des personnes qui prononcent des propos illégaux dans la rue. Un sentiment d'impunité se développe lorsque seules 50 personnes par an sont condamnées pour cyberharcèlement. La loi française et le RSN imposeront aux plateformes des obligations de retrait de ces contenus. Tous les

trimestres, nous supprimons près de 500 000 vidéos YouTube au niveau mondial pour des faits de cyberharcèlement.

En premier lieu, nous identifions et bloquons les contenus les plus évidents grâce à des outils technologiques. Un système en entonnoir permet ensuite d'amener les contenus pour lesquels nous avons des interrogations vers des équipes de modérateurs humains. Après l'entrée en vigueur du RSN, la personne ayant mis en ligne le contenu recevra un message d'explication et pourra faire appel. Si elle fait usage de ce droit, le dossier reviendra dans le giron de l'équipe de modération humaine.

Ce qui est interdit dans la vie hors ligne doit aussi l'être en ligne. Je reviens au parallèle avec le système d'amendes mis en place pour le harcèlement de rue et qui n'a pas d'équivalent en matière de harcèlement en ligne. Les opérateurs vont supprimer du contenu et bientôt seront aussi en mesure de supprimer des comptes, mais rien n'empêchera la personne de cyberharceler sa victime sur un autre réseau social ou un autre site Internet. Un travail à l'échelle européenne est en cours autour de la question du traitement de l'auteur et non plus seulement du contenu.

Sur le commerce en ligne, Google n'a pas d'activité dans ce secteur à proprement parler. Certains annonceurs comme les pharmacies ou les jeux en ligne pourront ou non être présents en fonction de la législation locale et des agréments, grâce à un mécanisme de territorialisation.

Mme Toine Bourrat. – Je reviens sur la question du pseudonymat en réponse à Monsieur Tabaka. On ne connaît pas nécessairement l'identité d'une personne qui prononce des propos haineux dans la rue, mais il s'agit d'anonymat et non de pseudonymat.

M. Anton'Maria Battesti. – Autour de 40 000 personnes dans le monde travaillent sur les enjeux de sécurité au sein du groupe Meta, dont environ 15 000 personnes sur la modération. Ces données sont publiques et nous rendons compte de ces ressources aux régulateurs.

Sur 10 000 contenus vus sur une plateforme comme Instagram, sept ont fait l'objet d'une action de modération pour du harcèlement. Au-delà des moyens, les régulateurs se penchent aussi sur l'efficacité des mesures. La majorité de ces contenus est aujourd'hui pré-détectée grâce à l'intelligence artificielle, qui joue un rôle de plus en plus important.

Concernant l'anonymat, on pouvait lire dans un célèbre dessin de presse des années 1990 que « sur Internet, personne ne sait que vous êtes un chien ». Aujourd'hui, du fait de la coopération avec les autorités, cet anonymat n'existe pas. Nous recevons 25 000 réquisitions par an et sommes susceptibles de communiquer l'adresse électronique, le numéro de téléphone et l'adresse IP. Il y a des débats de fond sur la question de l'anonymat et du pseudonymat. Certaines associations actives dans des domaines sensibles veulent ainsi pouvoir garder une capacité de s'exprimer en ligne sans forcément révéler l'identité. Cela étant, que l'on agisse sous son

vrai nom ou sous un pseudonyme, on doit pouvoir être identifié et le cas échéant, répondre de ses actes devant la justice. Contrairement à d'autres plateformes sur lesquelles il faudrait peut-être concentrer les moyens, Meta répond aux requêtes des autorités françaises.

Sur les questions de cyberharcèlement, Meta travaille avec des associations dont e-Enfance, qui anime la *hotline* joignable au 30 18 et peut remonter des cas particuliers aux équipes de Meta. Dans certains cas récents, ce numéro n'avait pas été suffisamment activé par les services administratifs, et parfois par les parents et les victimes eux-mêmes. Il n'est pas question de les blâmer, mais de constater que le 30 18 est insuffisamment connu et doit faire l'objet de campagnes d'information. Un récent rapport du Sénat sur le sujet du harcèlement scolaire montre l'ampleur du problème, qui a souvent une double composante physique et en ligne. La situation est comparable à celle de la sécurité routière il y a vingt ans, lorsque des dizaines de milliers de personnes perdaient la vie sur les routes tous les ans. Le président Jacques Chirac avait alors réuni l'ensemble des parties prenantes autour d'une table et avait ainsi réussi à inverser la tendance. Il faut provoquer un choc de société et faire de la lutte contre le harcèlement une grande cause nationale. Il me semble que le ministre de l'éducation nationale et d'autres acteurs sont réceptifs, c'est le moment.

Mme Toine Bourrat. – L'efficacité du 30 18 me semble limitée, mais ce n'est pas le sujet aujourd'hui. Le projet de loi comporte un volet sur la protection des citoyens, et l'essentiel est de comprendre comment est protégé celui qui a fait le signalement.

Mme Béatrice Oeuvrard. – Les plateformes ont un rôle à jouer, mais il s'agit d'une chaîne de responsabilités. Les auteurs sont les grands absents du *DSA* et d'autres textes comme la loi *Avia*. Comment sont-ils sanctionnés ? Je reviens sur notre proposition d'avoir recours à des agents assermentés pour faire usage des données mentionnées. Le retrait de milliards de contenus n'endiguera pas le phénomène en l'absence d'un pouvoir étatique et de sanctions sur les auteurs. Les parents et les associations ont aussi leur rôle à jouer, c'est véritablement l'ensemble de la chaîne qu'il faut impliquer.

Mme Catherine Morin-Desailly, présidente. – Nous en avons bien conscience. Cela étant, le modèle économique de vos plateformes est fondé sur la gratuité, une publicité ciblée et un algorithme qui travaille à surexposer les contenus les plus sensationnels et les plus contestables. Comment travaillez-vous à la transparence des algorithmes et comment intégrez-vous la notion de « *safety by design* », selon laquelle il faut étudier les effets potentiellement pervers d'un algorithme avant de le mettre sur le marché ? Il est très important que vous ayez conscience que le modèle économique des plateformes pour lesquelles vous travaillez génère ce phénomène.

Au lendemain de l'affaire « Cambridge Analytica », Damian Collins, président de la commission Culture digitale de la Chambre des communes, a fait un rapport extrêmement sévère sur les failles de Facebook et leur rôle dans la manipulation des opinions et des votes lors de l'élection présidentielle américaine. Tout cela a été démontré.

Le sujet des ingérences étrangères est traité dans le projet de loi. Pouvez-vous nous garantir qu'il n'y a plus de failles permettant des ingérences étrangères, la manipulation des opinions et la déstabilisation de nos sociétés occidentales dans leur modèle démocratique ? Avec l'application du RSN, avez-vous réellement pris « le taureau par les cornes » de sorte que l'on puisse contredire Frances Haugen dans les propos qu'elle a tenus à Bruxelles devant des parlementaires venus du monde entier ? Monsieur Mark Zuckerberg n'avait d'ailleurs pas daigné se déplacer. Qu'avez-vous fait pour mettre un terme à ces dérives qui sont tout simplement inadmissibles ? Si Internet doit rester une source d'échanges, de progrès et de connaissances, il faut agir.

M. Anton'Maria Battesti. – Concernant le modèle économique, notre chiffre d'affaires provient des annonceurs. Lorsque les manquement et imperfections que vous décrivez sont repris par la presse, les annonceurs nous demandent des comptes et menacent d'arrêter les campagnes. Nous n'avons donc aucun intérêt à voir le réseau se transformer en poubelle. Si des améliorations sont nécessaires, je ne peux pas laisser dire que le modèle économique est basé sur la recommandation de contenus malicieux ou illégaux.

Sur « Cambridge Analytica », Mark Zuckerberg s'est exprimé devant le Parlement européen.

Mme Catherine Morin-Desailly, présidente. – Il a également témoigné devant le congrès américain. C'était assez édifiant.

M. Anton'Maria Battesti. – Chacun a son opinion, mais il est à noter que Mark Zuckerberg a rendu des comptes devant le parlement européen et devant le Congrès américain. Une amende de plusieurs milliards de dollars a été acquittée auprès de la *Federal Trade Commission (FTC)* et des engagements personnels ont été pris par Mark Zuckerberg et d'autres responsables de Facebook pour mettre en place des procédures dont nous rendons compte de manière régulière. Le régulateur américain régule, on ne peut pas parler d'ultra libéralisme et de laisser-faire.

L'affaire « Cambridge Analytica » pose la question du degré d'ouverture des plateformes, notamment dans les échanges avec les chercheurs, dans la mesure où un chercheur a détourné des données et les a revendues. Des mesures très documentées ont été prises pour mettre un terme à certains partages de données dans nos applications.

Sur les ingérences étrangères, nous avons été les premiers à mettre en place une bibliothèque publicitaire qui identifie la cible, le budget,

l'émetteur et le destinataire de chaque publicité publiée sur le réseau. L'Arcom a publié des rapports sur la mise en œuvre de la loi *Fake news* qui donnent plutôt crédit de nos efforts ces dernières années. Je salue aussi l'effort de nos équipes, pilotées par Béatrice Oeuvrard. Le *DSA* nous fait entrer dans une phase de mise en œuvre et aucune entreprise ne peut s'y dérober.

Mme Béatrice Oeuvrard. – Concernant les ingérences étrangères, nous publions des rapports de transparence sur les actions coordonnées inauthentiques à destination des chercheurs.

Concernant la bulle algorithmique, nous avons développé de nombreux outils permettant aux utilisateurs de choisir leur fil d'actualités : le fil proposé par Facebook, celui de votre famille, de vos amis, ou encore de manière purement chronologique. Dans chaque contenu qui apparaît sur le fil, l'utilisateur a la possibilité d'accéder au schéma expliquant pourquoi ce *post* ou cette publicité a été sélectionné.

Mme Catherine Morin-Desailly, présidente. – Merci pour vos réponses. Croyez bien que nous sommes aussi exigeants et sévères avec les autres plateformes que Facebook. Nous avons une commission d'enquête TikTok au sein de cette maison.

M. Arnaud David. – Concernant l'informatique en nuage et les parts de marché des entreprises européennes, vos chiffres semblent être en contradiction avec les miens. En tant que pionner de ce marché en Europe et dans le monde, AWS compte un nombre de clients important qui nous l'espérons sont satisfaits de nos services. Lorsqu'ils ne le sont plus, ils changent de fournisseur avec les facilités et les outils mis à leur disposition, comme je l'ai rappelé dans mon propos liminaire. Le marché *cloud* ne représente que 15 % du marché informatique global, ce qui n'est pas très significatif, et est en constante évolution. En Europe et en France, il manque une impulsion du côté de la commande publique qui peine à aller vers ces technologies. Le contexte réglementaire avec l'adoption de plusieurs textes au niveau national et au niveau européen explique aussi l'attitude attentiste de certains clients qui attendent l'entrée en vigueur et les mesures d'application effectives avant de migrer.

Sur les questions de portabilité, nos services ont été conçus pour permettre l'interopérabilité avec les logiciels *open source*, la mise à disposition d'API et les standards au niveau européen. Nous avons ainsi contribué à l'élaboration du code SWIPO, le seul standard existant aujourd'hui, auquel nous avons déclaré un certain nombre de produits. Cela a été salué par la commission européenne. Nos clients n'ont *a priori* pas constaté de barrière au changement de prestataire.

Concernant la facturation de l'utilisation du réseau, vous mentionnez le terme de bande passante alors que par réseau j'entends notre réseau privé interne, avant même de pouvoir accéder à un réseau public.

AWS dispose de centres de données en France et dans plusieurs pays d'Europe et nos clients font faire une utilisation plus ou moins intensive de notre réseau en fonction de la quantité de données à transférer. Nous estimons que la facturation représente entre 1 % et 3 % de leurs dépenses annuelles en services informatiques. Selon une étude, le coût annuel de ce qu'on appelle le *run* en informatique serait en moyenne de 0,5 %. Il s'agit donc de sommes plutôt réduites. Les clients sont facturés par paliers avec un effet dégressif, et les tarifs sont en baisse de 50 % sur les cinq dernières années.

M. Frédéric Géraud. – Google Cloud fait partie de la maison Google, mais son modèle économique de services aux entreprises est différent du marché publicitaire. Dans le marché de l'informatique en nuage, on paye en fonction de la capacité et de la puissance souhaitées, pendant un laps de temps donné. C'est très éloigné d'un modèle économique de plateforme.

Concernant les propositions, il nous semble que pour enrichir le texte, il faut s'inspirer de la charte en dix points établie par le Cigref, qui rassemble des DSI du secteur public et du secteur privé, et le *CISPE*, qui réunit des fournisseurs d'informatique en nuage au niveau européen.

Sur la question de la bande passante, Google a fait dès le départ le choix d'investir massivement dans des réseaux de fibre optique propres qui permettent *in fine* une meilleure qualité de service et une différenciation de la concurrence. D'autres acteurs qui n'ont pas investi de la même manière vont passer des tiers qui vont pratiquer leurs prix.

Si vous êtes un acteur international, l'activité dépasse très largement le champ géographique de la France et implique des transferts de données à travers l'Europe et à travers le monde, avec à la clé des coûts différents. Si vous êtes un fournisseur de services plus petit avec des clients locaux, la donnée sera transportée moins loin pour un coût plus faible. Les fournisseurs se rejoignent sur les questions de normes et de standards internationaux, mais chacun a fait des choix technologiques différents.

Concernant l'interopérabilité et le *multi cloud*, je rappelle que Google *cloud* détient moins de 10 % de parts de marché. Nous sommes un *challenger* avec des ambitions importantes, comme en témoigne la création d'une nouvelle société avec Thalès afin d'offrir l'ensemble des services de Google Cloud Platform. En tant que dernier arrivé sur le marché, Google Cloud se doit d'être interopérable pour exister au milieu des autres solutions.

Sur la question des coûts de transfert, nous ne souhaitons pas communiquer de chiffres dans ce forum, mais nous avons partagé ce type de données avec l'autorité de la concurrence.

M. Yohann Bénard. – Pour ce qui concerne les produits vendus en France, la place de marché d'Amazon est bien soumise au droit français, sous le contrôle de la Direction générale de la consommation, de la concurrence et de la répression des fraudes (DGCCRF) et du juge français. Le droit français

est une combinaison de règles d'origine nationale et de textes issus de la transposition de textes européens. La loi pour la confiance en l'économie numérique (LCEN) de 2003 et d'autres textes plus récents visent justement à rehausser les standards pour que le droit français soit à la fois très protecteur pour les consommateurs et aligné sur les droits voisins.

Mme Catherine Morin-Desailly, présidente. – Le marché européen numérique est un marché profond et durable avec ses 500 millions de consommateurs. Nous avons changé d'ère en prenant conscience que nous dépendons tous de cet écosystème et qu'il faut à la fois assurer les conditions de juste concurrence et corriger les effets pervers sur les réseaux sociaux. Comme le disait l'un des co-fondateurs du *web*, si nous voulons un monde soutenable en matière de nouvelles technologies et qu'elles puissent être des sources de progrès, il faut que ce monde soit parfaitement régulé et sécurisé. C'est une responsabilité que tous les acteurs quels qu'ils soient, européens comme extra européens, doivent partager. C'est un sujet de très grande importance et nous sommes véritablement à la croisée des chemins. Sous l'impulsion du commissaire Thierry Breton, l'Europe développe désormais une politique beaucoup plus stratégique. Les textes qui se succèdent à l'heure actuelle, qui visent à corriger cette absence de régulation, serviront sans doute d'étalon-or pour le monde, à l'image du règlement général sur la protection des données.

Audition de Jean-Philippe Lecouffe,
directeur exécutif adjoint des opérations d'Europol

Mardi 20 juin 2023

Mme Catherine Morin-Desailly, présidente. – Nous avons le plaisir d'accueillir aujourd'hui Jean-Philippe Lecouffe, directeur exécutif adjoint des opérations d'Europol.

Europol est l'Agence européenne de police criminelle, chargée de la coordination de la lutte contre les stupéfiants, la pédocriminalité ou encore le terrorisme.

Si nous avons souhaité vous entendre dans le cadre des travaux de notre commission spéciale, monsieur le directeur, c'est pour bien marquer la dimension internationale de ces délits et l'indispensable coordination qui doit être réalisée à l'échelon européen pour les contenir.

Le texte qui nous occupera dans l'hémicycle au mois de juillet est la traduction du règlement européen sur les services numériques (RSN, ou *Digital Services Act*, *DSA*), qui établit Europol comme un signaleur de confiance, dont le statut est prévu à l'article 22 de ce règlement. Il contraint les plateformes à traiter par priorité vos signalements. Dans le cas de la prévention d'une infraction pénale, l'article 18 indique par ailleurs que, si le fournisseur d'accès auprès duquel un signalement est opéré ne peut pas identifier avec certitude le pays concerné, il en informe immédiatement Europol.

Au-delà de ces ajouts utiles, nous serons très attentifs à votre analyse de ce que l'on pourrait qualifier de « criminalité numérique ». Dans quelle mesure les plateformes, avec lesquelles vous travaillez au quotidien, vous semblent-elles coopératives ? Pensez-vous que les nouvelles obligations que le règlement leur imposera seront de nature à mieux appréhender les comportements délictueux qui peuvent commencer en ligne, avant de déborder dans la « vie réelle » ?

Je vous donne la parole pour une dizaine de minutes, puis je passerai la parole à nos rapporteurs.

M. Jean-Philippe Lecouffe, directeur exécutif adjoint des opérations d'Europol. – Je suis très honoré de pouvoir m'exprimer aujourd'hui devant vous et de vous livrer, au nom d'Europol, un point de vue sur le travail législatif en cours.

Nous savons à quel point les évolutions technologiques, dans leur majorité, sont sources d'opportunités. Nous savons aussi, cependant, combien la numérisation peut être un puissant catalyseur pour les criminels. C'est la raison pour laquelle le traitement des preuves électroniques et des contenus criminels en ligne est devenu une tâche quotidienne et essentielle

pour l'ensemble des services répressifs de l'Union européenne et pour Europol. La criminalité en ligne évolue régulièrement ; les services d'investigation se heurtent régulièrement à des défis nouveaux et le législateur peine à suivre le rythme effréné de ces changements technologiques. Le règlement sur les services numériques, ou DSA, ainsi que le travail de votre commission, sont donc bienvenus pour nous aider à faire face à ces défis.

En outre, il est important de souligner que le caractère international des services et des crimes numériques limite les approches nationales et nous impose de privilégier une approche européenne, voire internationale, pour plus de puissance et d'impact.

Je commencerai par un état des lieux des menaces numériques aujourd'hui. Au sein de l'Union européenne, la menace qui arrive en tête est celle des abus et de l'exploitation sexuelle des enfants, préoccupation majeure et priorité essentielle des services répressifs, parce que cette menace concerne des personnes vulnérables. Depuis la pandémie de covid-19, ce type d'affaires connaît une véritable explosion, en particulier sous la forme de contenus autoproduits, des personnes mineures étant amenées, par des discussions, à dévoiler une partie de leur intimité en ligne.

Sur ce point, je précise que les équipes d'Europol sont soucieuses de ne pas utiliser le terme de pédopornographie, dans la mesure où, bien qu'elle puisse être moralement condamnable, la pornographie ne constitue pas en soi une infraction. En revanche, les attentats à la pudeur et le viol sur mineur relèvent du crime. L'emploi de ce terme affaiblit le crime en créant une confusion entre, d'une part, la pornographie et, d'autre part, les abus et les exploitations sexuelles des enfants, qui sont des crimes. Vous m'entendrez donc parler non pas de pornographie mais d'abus ou d'exploitation sexuelle sur les enfants. Ce point de vocabulaire nous paraît crucial.

Il existe pour ce type de contenus un vaste marché, en pleine expansion. La gravité des infractions augmente également, puisque le développement des moyens technologiques donne naissance à des infractions nouvelles et particulièrement abjectes, comme le *live streaming* de viols d'enfants, dont les délinquants font preuve, en la matière, de connaissances techniques poussées, pour se dissimuler. À cela s'ajoute une augmentation de la monétisation de ces contenus, y compris en direct, et certaines plateformes ne parviennent pas à empêcher l'accès des mineurs, capables d'utiliser soit des *virtual private networks* (VPN), soit de fausses cartes d'identité, pour poster eux-mêmes des vidéos explicites.

Les cyberattaques constituent le deuxième type de menaces liées au monde numérique. Même si elles ne concernent pas directement votre sujet, elles augmentent elles aussi de manière prononcée : attaques d'hôpitaux, d'administrations ou d'entreprises, attaques par logiciels malveillants, rançongiciels, piratages, attaques par déni de service, etc. Pour la première

fois cette année, deux cybercriminels ont été inscrits sur la liste des personnes les plus recherchées dans l'Union Européenne, une liste que détient aussi Europol, preuve que nous sommes face à une menace qui monte.

La fraude en ligne est également massive : fraude au paiement en ligne et cyber-escroqueries figurent parmi les infractions criminelles les plus établies.

Enfin, les contenus terroristes en ligne constituent une menace particulièrement importante. La semaine dernière, Europol a publié son rapport annuel sur le terrorisme et l'extrémisme dans l'Union européenne (TE-SAT 2023), qui montre que la menace terroriste ne faiblit pas et qu'Internet reste un outil essentiel d'échange de contenus à caractère terroriste et de diffusion d'idéologies extrémistes pouvant conduire au terrorisme : radicalisation en ligne ou recrutement de jeunes vulnérables, jusque sur des plateformes de jeux, sont des exemples de formes que peut prendre cette menace.

Devant ce panorama des menaces, Europol se félicite de voir émerger des textes législatifs novateurs – le règlement sur les contenus terroristes en ligne, ou *terrorist content online regulation* (*TCO*), le règlement sur les services numériques (RSN ou *DSA*) –, qui sont les premières tentatives mises en place au niveau européen de lutte contre les contenus illicites en ligne à grande échelle. Dans la mesure où les services et les délits numériques se propagent dans le monde entier, faire peser des obligations sur les diffuseurs peut avoir un impact réel à l'échelle mondiale.

Je vais évoquer à présent le soutien qu'apporte Europol aux États membres de l'Union européenne dans la lutte contre ces menaces numériques, avec une attention particulière sur les domaines qui sont au cœur du travail de votre commission : les contenus illégaux en ligne.

Ce soutien prend d'abord la forme de signalements et de retrait des contenus terroristes en ligne. En effet, en 2015, Europol a créé une unité de signalement sur Internet, *Internet Referral Unit (EU-IRU)*, qui collabore étroitement, d'une part, avec les autorités compétentes des États membres de l'Union européenne et, d'autre part, avec les fournisseurs de services d'hébergement, afin d'entraver la diffusion de contenus terroristes. La Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) est l'un de nos grands partenaires dans ce domaine. De façon conjointe, nous signalons les contenus terroristes aux fournisseurs de services en ligne qui prendront ou non la décision de les supprimer.

Depuis sa création, l'*IRU* a détecté des comptes terroristes sur plus de 430 plateformes en ligne. Bien qu'elle ait produit des résultats satisfaisants, cette approche volontaire laisse apparaître de grandes différences dans la manière dont les entreprises répondent à nos

signalements et modèrent leurs contenus ; cela conduit les réseaux terroristes à privilégier, pour diffuser leurs contenus, les plateformes ayant des politiques internes de modération moins contraignantes. C'est la raison pour laquelle l'Union européenne a adopté le règlement sur les contenus terroristes en ligne, en 2021, à la suite de l'attentat terroriste sur la personne de Samuel Paty en France. En effet, l'assassinat de cet enseignant avait donné lieu à la diffusion de contenus particulièrement intolérables sur les réseaux sociaux. Le règlement va permettre de rendre les demandes de retraits obligatoires et non plus seulement volontaires.

Ce règlement permet aussi de coordonner les actions de demande de retrait entre les différentes autorités compétentes des États membres : si Pharos et l'unité équivalente italienne ou allemande passent par un point d'accès unique comme Europol, nous limitons le risque de duplication qui existe quand ces organismes travaillent en même temps sur les mêmes dossiers. Dans l'heure qui suit la réception d'un ordre de retrait, les fournisseurs de services d'hébergement doivent s'exécuter ; en outre, on requiert de la part des plateformes une vigilance active en matière de détection des contenus terroristes. Enfin, le règlement établit que les autorités nationales, et non les fournisseurs de services en ligne, auront le dernier mot dans la modération de ces contenus.

Toutefois, l'approche partenariale avec les plateformes doit perdurer ; l'ordre de retrait doit rester une arme de dissuasion à utiliser quand le dialogue a échoué.

Le règlement sur les contenus terroristes en ligne désigne Europol comme interface entre les autorités nationales et les plateformes. À ce titre, nous lancerons dans quelques jours la Plateforme européenne des retraits des contenus illégaux sur Internet (Persil), un système unique et collaboratif de transmission des signalements et des ordres de retrait par les autorités compétentes de tous les États membres vers l'ensemble des fournisseurs de services, qui ont l'obligation de s'immatriculer auprès de l'un des pays de l'Union européenne, l'Irlande dans un grand nombre de cas. Persil favorisera les échanges d'information avec ces fournisseurs de service d'hébergement et facilitera la coopération et la coordination des efforts entre les autorités compétentes pour lutter contre les contenus terroristes en ligne et éviter les duplications. Cette plateforme permet ainsi une application harmonisée du règlement dans les 27 États membres.

J'en profite pour souligner que les relations que nous avons établies avec Pharos sont excellentes ; la plateforme est l'un de nos plus anciens et solides partenaires et nous l'avons consultée, de même que ses homologues, dans la création et le développement de Persil.

Le règlement sur les services numériques *(DSA)*, adopté en 2022, prévoit de manière plus générale la modération de tous les contenus en ligne et pas seulement des contenus à caractère terroriste, comme le *Terrorist*

Content Online (TCO). Comme avec celui-ci, Europol pourrait aider les États à appliquer ses dispositions pour optimiser son impact sur les mesures répressives ; des discussions avec la DG Connect de la Commission, qui sera chargée de sa mise en œuvre, ont déjà eu lieu à ce sujet, afin d'offrir notre expertise et notre infrastructure. Persil, qui n'a pas été conçu uniquement pour des contenus terroristes, pourrait être là aussi très utile. Notre but principal est d'éviter les doublons au sein des Vingt-Sept.

Concernant les abus et l'exploitation sexuelle des enfants, Europol dispose depuis plus de vingt ans d'une équipe spécialisée dans la lutte contre les contenus illégaux de cette nature. Une équipe d'experts, l'*Analysis Project Twins (APT)*, soutient les forces de l'ordre des États membres de l'Union européenne vingt-quatre heures sur vingt-quatre dans la lutte contre l'exploitation et les abus sexuels des enfants. En 2022, par exemple, elle a coordonné 93 enquêtes internationales portant sur ces contenus. Au cours d'une seule opération, qui impliquait une dizaine de milliers de comptes et 13 pays sur trois continents, 146 enfants ont pu être identifiés à travers le monde et les informations transmises aux services de police. C'est la coordination internationale des activités d'enquête qui a permis d'identifier ce grand nombre de victimes et de suspects.

En ce qui concerne plus spécifiquement la modération des contenus, notre équipe APT facilite la réception puis la diffusion des signalements d'exploitation sexuelle des enfants en ligne. Aux États-Unis, les plateformes signalent tous les contenus suspects à l'organisme américain *National Center for Missing and Exploited Children (NCMEC)*. Un accord conclu avec le *NCMEC* permet à Europol d'être un point d'entrée unique pour 20 pays européens pour le partage des informations, les autres fonctionnant par transmission directe du *NCMEC*. Cela permet de déclencher des enquêtes dans les États membres. En 2022, nous avons ainsi reçu, analysé et diffusé plus de 290 000 signalements du *NCMEC*, environ 5 600 par semaine. Europol dispose aujourd'hui de la deuxième plus grande base de données au monde de ces contenus.

J'espère que cet état des lieux aura permis de rendre plus claires trois choses principales : premièrement, la criminalité numérique évolue rapidement et les criminels agissent plus vite en détournant les plateformes et services présents sur le marché ; deuxièmement, l'efficacité de la réglementation, comme les règlements *TCO* et *DSA*, repose sur des règles communes à l'échelle de l'Union et sur la coordination et la coopération des services répressifs au niveau européen, la dimension européenne étant de nature à améliorer l'impact auprès de partenaires privés de taille mondiale ; troisièmement, Europol joue un rôle central en aidant les États membres dans la lutte contre la criminalité numérique et la clef du succès se trouve dans la coopération des États membres pour éviter les duplications.

M. Loïc Hervé, **rapporteur**. – *Vous avez évoqué vos relations avec les plateformes : quelle est leur qualité ? Les plateformes sont-elles, selon vous, à la hauteur des enjeux ? Comment peut-on améliorer ces relations ?*

Concernant le DSA, y a-t-il selon vous des manques, des éléments à préciser ? Bien sûr, nous ne pouvons pas compléter le règlement européen, qui est d'application directe en droit interne, mais son application française peut nous donner l'occasion de faire passer des messages ou d'inscrire directement dans la loi des évolutions importantes. J'ajoute que le DSA prévoit des contraintes importantes pour les très grandes plateformes, qui sont au nombre de 19, dont aucune n'est française. Comment faire pour que le règlement concerne davantage les plateformes au-delà de celles qui revendiquent 49 millions de connexions ?

Lors de son audition, Mme Augereau, cheffe de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui gère Pharos, s'est inquiétée de l'alourdissement que pourraient engendrer les procédures européennes, notamment au moment de procéder à des blocages massifs. Que pensez-vous de ce risque ?

Pouvez-vous détailler les conséquences de l'adoption à brève échéance d'un nouveau règlement visant à prévenir et à lutter contre les abus sexuels sur les enfants ? Pouvez-vous revenir sur son calendrier d'adoption ?

Mme Catherine Morin-Desailly, présidente. – *Pensez-vous que le projet de loi qui nous est soumis pourrait être complété par quelques dispositions qui y seraient insérées par anticipation du projet de règlement de lutte contre les abus sexuels des enfants ?*

M. Loïc Hervé, **rapporteur**. – *Les auditions que nous avons menées ont permis de mettre en lumière un problème d'équilibre entre la protection des données personnelles, d'une part, et les nécessités de la lutte contre la criminalité en ligne, d'autre part. Comment Europol procède-t-il pour identifier les auteurs des infractions ? Dans quelle mesure les outils actuels pour mener ces investigations dépendent-ils des plateformes et non des informations collectées par les services d'enquête des États ?*

Concernant *votre réflexion sur le terme de pédopornographie, d'autres personnes auditionnées ont également souligné son caractère ambigu. Il a toutefois un seul mérite, même s'il pose un problème conceptuel : on sait de quoi on parle. On peut le contourner avec une périphrase, mais celle-ci posera d'autres difficultés.*

Enfin, le projet de loi, s'il est adopté, prévoit une sanction pénale en cas de défaut d'exécution d'une demande de retrait d'un contenu mettant en scène des enfants victimes d'abus sexuels. Que pensez-vous de cette disposition ? Pouvez-vous dresser un premier bilan d'une procédure analogue créée pour les comptes terroristes par le règlement TCO ?

M. Jean-Philippe Lecouffe. – Les relations avec les plateformes sont globalement de bonne qualité, mais cela s'explique par le fait que le retrait des contenus se fait, comme je vous le disais, de manière volontaire. Le plus souvent, nous intervenons en réaction, c'est-à-dire après qu'un contenu

illicite nous a été signalé. Jusqu'à présent, sur le fondement du *TCO*, nous n'avons adressé qu'une douzaine d'ordres de retrait, parce que Persil n'est pas encore complétement opérationnel.

Ce que les plateformes apprécient également est le fait que nous sommes pour elles un point d'entrée unique, ce qui leur évite de discuter avec plusieurs autorités nationales. Néanmoins, je le disais, nous nous heurtons aux politiques internes de chaque plateforme, auxquelles elles se réfèrent pour supprimer ou non les contenus signalés. Par conséquent, nous sommes preneurs d'un instrument coercitif pour l'exécution des ordres de retrait, afin de faire de la pédagogie.

Le RSN présente-t-il des lacunes ? L'enjeu nous semble être de faire des textes technologiquement neutres, autrement dit qui restent pertinents alors même que les technologies évoluent. Le règlement y réussit en partie, je pense, mais il restera sûrement des choses à adapter pour couvrir toutes les situations.

Ensuite, notre approche ne doit pas être exclusivement répressive ; au contraire, nous avons besoin d'entretenir nos partenariats avec les plateformes pour qu'elles continuent, de leur propre chef, à réguler leurs contenus. Elon Musk déclarait d'ailleurs ce matin dans les médias, en parlant de Twitter, vouloir se conformer à la réglementation en vigueur.

L'Union européenne concentrera son action sur les 19 plateformes les plus importantes – sur les 430 identifiées –, qui regroupent environ 45 millions d'utilisateurs, donc la législation des États membres est elle aussi pertinente, notamment pour les plateformes plus petites, surtout si elles s'inspirent du règlement sur les services numériques. Encore faut-il que les plateformes soient hébergées sur le territoire du pays concerné : le RSN vise justement à éviter ce nomadisme juridique, en partant du principe que les plateformes ne peuvent se priver du marché européen.

Je comprends l'argument sur l'alourdissement des procédures. Celles-ci ont toutefois un gros avantage : elles évitent les doublons. Pourquoi la plateforme Pharos ouvrirait-elle un dossier sur des faits déjà signalés par des collègues d'autres États membres ? La mutualisation des informations à l'échelon européen est la contrepartie de l'alourdissement des procédures. En outre, l'ordre de retrait doit être utilisé en dernier recours : il faut d'abord privilégier le dialogue avec les plateformes.

Europol ne participe évidemment pas aux discussions sur le règlement européen en cours de préparation ; cette tâche incombe au Conseil, au Parlement et à la Commission. Je ne sais pas quelle sera l'issue des discussions. Il est toutefois impossible que l'Union européenne n'adopte pas de position commune sur le sujet. La transmission de contenus par nos collègues américains repose sur une exception à la réglementation européenne. Or celle-ci s'achèvera en août 2024 : il nous faut donc un texte efficace pour continuer à disposer de signalements volontaires. Anticiper les

conséquences du futur règlement me semble difficile à l'heure actuelle, tant les discussions entre les États membres sont encore nombreuses sur ce texte nécessaire à la poursuite de notre action. Cela dit, la saisie de nombreux contenus lors de nos enquêtes nous permet aussi de récolter des informations encore inconnues des plateformes.

Mener à bien notre travail tout en respectant le règlement général sur la protection des données (RGPD) est un défi quotidien. L'action d'Europol est soumise au Contrôleur européen de la protection des données (CEPD). Nous plaidons en faveur d'un équilibre entre protection des données et sécurité de nos concitoyens. En tout état de cause, nous avons besoin de moyens pour assumer au mieux nos missions.

M. Loïc Hervé, rapporteur. – Une sanction pénale en cas de défaut d'exécution de la demande de retrait vous semble-t-elle pertinente ? Cette possibilité existe déjà pour les affaires de terrorisme, entre autres.

M. Jean-Philippe Lecouffe. – Une telle sanction serait utile, en complément des amendes déjà prévues ; un tel point de vue ne vous étonnera pas de la part d'un gendarme. En outre, les entreprises souffriraient d'un préjudice réputationnel en cas de poursuites pénales, ce qui constitue parfois un moyen d'action efficace.

M. Patrick Chaize, rapporteur. – Le projet de loi prévoit la création d'un filtre anti-arnaques. Qu'en pensez-vous ?

M. Jean-Philippe Lecouffe. – Cette initiative est bienvenue. Les fraudes en ligne se multiplient, même si les montants extorqués ne sont pas très importants. Le travail de prévention est crucial.

Le filtre protégera nos concitoyens les plus vulnérables. Cela dit, je ne connais pas encore les détails de son fonctionnement : il faut que les dispositions légales résistent aux évolutions technologiques futures.

Mme Laurence Rossignol. – Vous avez indiqué que vous préfériez retenir la notion d'abus sexuels sur les enfants plutôt que le terme de pédopornographie qui, selon vous, minore l'ampleur du crime. Je comprends le fondement de votre raisonnement, mais je m'interroge sur ses conséquences. Certes, la pornographie n'est pas en tant que telle une infraction pénale, comme vous venez de le rappeler, mais certains contenus constituent des incitations à la haine, à la violence ou à l'inceste. En ne retenant que les abus sexuels sur les enfants, je crains que cela ne limite le champ de votre intervention. Les enquêteurs examinent chaque image d'un contenu pornographique – j'en profite pour saluer leur travail. Lors de leur audition par notre commission spéciale, les représentants de Pharos ont indiqué qu'ils retenaient les critères d'Europol pour déterminer si les victimes étaient des mineurs. Par ailleurs, j'ai lu que Pharos avait reconnu à mots couverts qu'elle s'en tenait uniquement aux critères d'apparence, c'est-à-dire les signes extérieurs de puberté tels que les poils ou les seins.

Mais ces derniers apparaissent bien avant 18 ans ! Que pensez-vous du critère retenu pour les infractions commises sur les mineurs déjà pubères ?

En outre, à préférer le terme de pédocriminalité à celui de pédopornographie, vous ne cherchez pas à faire retirer les images représentant la sexualité enfantine. Finalement, que la personne filmée ait ou non 18 ans importe peu : avec de telles images, les rapports sexuels entre des enfants et des adultes sont banalisés. Ne pensez-vous pas que la distinction que vous opérez limite votre champ d'action ?

M. Jean-Philippe Lecouffe. – Nous n'établissons pas de critères formels. Dans de nombreux contenus que nous visionnons, il ne fait aucun doute que les victimes sont des enfants. Ces images sont ensuite transmises aux autorités nationales, car les poursuites sont décidées non pas par Europol, mais par des magistrats, sur le fondement du travail des enquêteurs. Il en va de même lorsque nous avons un doute sur l'âge des protagonistes : nous transmettons l'affaire aux autorités nationales, sous réserve que nous disposions de suffisamment d'éléments pour alimenter l'enquête.

Les critères utilisés par Europol sont les mêmes que ceux qui sont retenus par Interpol et, plus largement, par toute la communauté d'enquêteurs et de magistrats de l'Union européenne. Nous adoptons la même vigilance pour les faits de violence commis contre des adultes, mais ces poursuites relèvent d'un autre champ du droit.

Nous adoptons une vision multidirectionnelle en matière d'infraction. Nous ne fixons pas les limites, mais nous en référons toujours aux autorités nationales, dont les réglementations diffèrent selon chaque État membre.

Mme Catherine Morin-Desailly, présidente. – Merci pour ces informations et pour l'ensemble de vos actions. Lors de ma visite au siège d'Europol, j'ai été frappée par la très bonne coordination entre les États membres, et même avec des États ne faisant pas partie de l'Union européenne. Je me souviens ainsi du rôle essentiel joué par Europol dans le démantèlement du réseau *Boystown*. Nous vous souhaitons toute la réussite possible pour votre entreprise de longue haleine.

Table ronde sur la protection de l'enfance

Mardi 20 juin 2023

Mme Catherine Morin-Desailly, présidente. – Nous sommes réunis pour notre huitième et dernière audition en commission spéciale. Nous avons décidé avec les rapporteurs de la consacrer à un sujet au cœur des préoccupations du Sénat, sur lequel portent notamment les premiers articles du projet de loi, à savoir la protection de l'enfance face aux contenus pornographiques et au cyberharcèlement – la commission de la culture, de l'éducation et de la communication a travaillé sur ce dernier sujet.

Nous accueillons Olivier Gérard, coordonnateur du pôle « médias – usages numériques » de l'Union nationale des associations familiales (Unaf), Arthur Melon, délégué général du Conseil français des associations pour les droits de l'enfant (Cofrade), et Angélique Gozlan, membre du comité d'experts de l'Observatoire de la parentalité et de l'éducation numérique (Open).

Le sujet de la protection de l'enfance est au cœur de nos préoccupations et vous avez tous été plusieurs fois entendus sur les différents textes que nous avons portés dans cette assemblée, ainsi que sur les rapports d'information que nous avons produits. Je veux citer bien entendu le travail pionnier de la délégation aux droits des femmes sur l'industrie pornographique, qui a souligné les ravages d'un accès totalement libre à des contenus plus qu'inappropriés pour les mineurs. Selon la dernière enquête de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), 2,3 millions de mineurs visitent chaque mois des sites pornographiques. Dès 12 ans, la moitié des garçons se rendent en moyenne au moins une fois par mois sur l'un de ces sites. Ce chiffre est révélateur et notre assemblée s'honore, sur l'initiative de notre collègue Marie Mercier, d'avoir voulu y mettre un terme dès 2020. De l'autre côté du spectre, l'actualité dramatique, avec le suicide de la jeune Lindsay et plus récemment celui du jeune Thibault, nous a rappelé à tous l'urgence d'agir contre le cyberharcèlement, facilité par les réseaux sociaux, pour que le monde numérique ne se transforme pas en un monde totalement dénué de règles.

Les mineurs sont donc les premières victimes du développement des outils numériques. Récemment, nous avons adopté une proposition de loi dont notre collègue Alexandra Borchio Fontimp était rapporteure, sur la majorité numérique à 15 ans pour l'accès aux réseaux sociaux. La commission mixte paritaire a abouti aujourd'hui même.

Le 12 juin dernier, le Sénat a adopté la résolution européenne que nous avions déposée avec Ludovic Haye et André Reichardt sur la proposition de règlement européen établissant des règles en vue de prévenir

et de combattre les abus sexuels sur enfants. Ce texte est en cours de négociation à l'échelle européenne.

Nous souhaitons donc vous entendre, tout d'abord sur le constat et plus encore sur votre appréciation des dispositions qui seront prises dans le cadre de ce texte d'application de règlements européens.

M. Olivier Gérard, coordonnateur du pôle « médias – usages numériques » de l'Union nationale des associations familiales. – Nous échangeons aujourd'hui sur un texte qui s'inscrit dans un foisonnement d'initiatives parlementaires et réglementaires, ce qui manifeste une volonté forte des pouvoirs publics d'agir en vue d'apaiser la situation dans l'espace numérique. C'est une priorité pour les familles que nous représentons. Cette impulsion politique est nécessaire pour que nous puissions collectivement faire bouger les lignes. En effet, les modifications législatives ne suffiront pas, et il faudra que l'ensemble des parties prenantes unissent leur action.

L'étude de l'Arcom a conforté les données figurant dans le rapport d'information sur l'industrie de la pornographie que le Sénat a publié l'an dernier. Les chiffres concernant l'accès des mineurs aux sites pornographiques sont édifiants et il faut garder à l'esprit que cet accès passe en premier lieu par le smartphone. L'étude montre en effet que dans 95 % des cas, l'accès aux sites pornographiques se fait par ce biais et dans 75 % des cas exclusivement par le smartphone.

Quant au cyberharcèlement, la situation est également inquiétante. Le rapport du Sénat sur le sujet citait un ordre de grandeur : entre 800 000 et un million d'enfants sont victimes de harcèlement scolaire chaque année. En outre, les violences en ligne et les propos haineux s'inscrivent aussi dans le champ du cyberharcèlement.

Selon la dernière étude que nous avons menée, les parents considèrent le harcèlement comme le principal sujet d'inquiétude en matière de santé des enfants. Ils souhaitent que l'on prévoie un accompagnement et un soutien et que des mesures soient prises pour lutter contre ce phénomène. Au-delà des mesures législatives, ils attendent aussi davantage d'information sur ce sujet.

Les mesures sur la protection de l'enfance que le projet de loi prévoit dans ses premiers articles étaient nécessaires. Toutefois, un certain nombre de dispositions qui s'inscrivent dans le champ du numérique souffrent du délai nécessaire à leur mise en œuvre opérationnelle. Par exemple, les articles relatifs à la protection des mineurs du règlement général sur la protection des données (RGPD), qui prévoyaient notamment le consentement des parents dans le cas des enfants âgés de 13 à 15 ans, n'ont pas été mis en œuvre, cinq ans après la mise en place du règlement. De plus, la loi de mars 2022 visant à renforcer le contrôle parental sur les

moyens d'accès à Internet n'entrera en vigueur qu'à la fin du premier semestre 2024.

Pourtant, les attentes sont fortes de la part des familles, et l'enjeu est de santé publique. Dans l'univers numérique, les évolutions sont très rapides et il est difficile de justifier de tels délais auprès des parents.

Les articles 1er et 2 relatifs à l'accès à la pornographie prévoient le renforcement du rôle confié à l'Arcom pour réduire les délais d'intervention. Avec l'Open, nous avions saisi l'Arcom dès la fin de 2020. Or les décisions judiciaires n'ont toujours pas été rendues, ce qui montre la nécessité de repenser le dispositif pour le rendre plus réactif et plus utile compte tenu de l'urgence du problème. L'Arcom pourra donc prendre des décisions administratives, qu'il s'agisse de bloquer les sites, de les déréférencer, voire de prononcer des sanctions pécuniaires, dans le respect de la procédure contradictoire. Nous espérons que cela permettra de lever l'incompréhension dont nous font part les parents sur la lenteur des interventions.

Le texte est plutôt positif à nos yeux. Toutefois, il met l'accent sur les sites de communication en ligne, notamment pornographiques. Or l'accès des mineurs aux contenus pornographiques passe aussi par les réseaux sociaux, par les messageries privées ou par la transmission de contenus *via* les téléphones portables. La mesure prévue dans le texte ne suffira donc pas à résoudre toutes les questions.

L'article 1er porte sur les recommandations techniques, notamment les dispositifs de vérification d'âge, ce qui représente pour nous une avancée importante. En effet, durant ces derniers mois, les débats ont essentiellement porté sur l'absence d'un cadre référentiel, même si un certain nombre de solutions techniques sont déjà proposées sur le marché pour faire en sorte de respecter des principes comme l'anonymat. La proposition de mettre en place rapidement des recommandations techniques est une belle avancée, d'autant que le référentiel sera contraignant.

Toutefois, le texte ne fixe pas de délai pour la mise en œuvre de ce référentiel, de sorte que celui-ci ne semble pas avoir d'obligation de résultat.

Sur la lutte contre le cyberharcèlement, l'article 5 vise à sanctionner ceux qui l'exercent par une peine complémentaire de suspension des comptes. Il s'agit là d'une avancée positive dans la protection des victimes, qui permettra d'éviter que les pratiques ne se poursuivent au-delà des décisions rendues. La mesure vise ainsi à lutter contre tout sentiment d'impunité, ce qui est, selon nous, tout à fait nécessaire.

Le texte prévoit de bloquer l'utilisation de la plateforme incriminée et éventuellement l'ensemble des comptes de la personne mise en cause. Toutefois, le cyberharcèlement peut passer par plusieurs plateformes et il faudrait sans doute prévoir des mesures de suspension en cascade pour que la sanction concerne l'ensemble des canaux auxquels le harceleur a eu recours.

Même si ce n'est pas l'objet de la loi, il faut rappeler que la lutte contre le cyberharcèlement passe par la sanction des auteurs, par la sensibilisation de l'ensemble des parties prenantes et par l'accompagnement des victimes et de leur famille. Or les moyens alloués pour cela restent insuffisants. Nous menons des actions en ce sens sur notre réseau et nos services sont saturés, ce qui nous empêche d'accompagner les familles de manière satisfaisante.

Qu'il s'agisse de la lutte contre l'accès à la pornographie, de celle contre le cyberharcèlement ou de la protection des enfants en ligne, les enjeux éducatifs pèsent lourd. Il convient de renforcer les dispositifs de prévention et d'éducation auprès des jeunes, de manière qu'ils adoptent de nouveaux réflexes quant aux comportements acceptables ou non en ligne. Il faut aussi continuer d'accompagner les parents et la famille, qui jouent un rôle essentiel. Nous venons ainsi de lancer un dispositif de labellisation des actions de parentalité numérique et nous considérons qu'il faut continuer de développer ce type d'initiative. En effet, c'est en développant une approche complémentaire que nous pourrons faire face à ce fléau.

Enfin, le cyberharcèlement passe beaucoup par le smartphone, qui reste le grand absent de ce projet de loi. Les jeunes sont pourtant équipés de manière très précoce, avec les mêmes outils que les adultes, alors qu'ils n'ont pas forcément la maturité suffisante pour les utiliser. Nous devrions nous interroger sur la place du smartphone dans notre société. Si nous voulons lutter contre les dérives et mieux protéger les enfants, c'est une réflexion qu'il nous faudra mener.

M. Arthur Melon, délégué général du Conseil français des associations pour les droits de l'enfant. – Le Cofrade se félicite du fait que les pouvoirs publics se saisissent du sujet de l'exposition des mineurs à la pornographie.

Toutefois, à la lecture des articles du texte, j'ai ressenti davantage de colère que de soulagement. En effet, le Parlement vote des lois qui sont bien faites, mais ne sont pas appliquées : on ajoute de nouvelles lois pour trouver prétexte à ne pas appliquer des dispositions législatives qui existent bel et bien et qui sont parfaitement suffisantes. Ainsi, l'article 227-24 du code pénal prévoit une sanction à l'encontre des personnes mettant à disposition des contenus pornographiques susceptibles d'être vus par des mineurs. De plus, il est déjà prévu dans la loi que l'Arcom et la justice ont la possibilité de déréférencer et de bloquer les sites qui contreviendraient à ces dispositions.

L'arsenal législatif en vigueur est donc suffisant pour s'attaquer au cœur du problème, que l'enquête de l'Arcom a bien identifié : 60 % des contenus pornographiques consommés par les mineurs proviennent de cinq plateformes. Une section entière de ce projet de loi leur est consacrée, les autres plateformes pornographiques qui font payer leurs contenus ne posant pas de problème particulier en matière d'exposition des mineurs à la pornographie. Par conséquent, est-il bien nécessaire de prévoir un chapitre

dans un nouveau projet de loi pour contraindre cinq plateformes à se conformer à la loi, alors même qu'elles font l'objet de deux procédures judiciaires, l'une au pénal et l'autre au civil, par l'intermédiaire des fournisseurs d'accès Internet.

La plainte au pénal a été engagée en 2018 sur le fondement de l'article 227-24 du code pénal, à la suite de la plainte déposée par le Cofrade et par l'Open. Au bout de cinq ans, nous n'avons reçu aucune nouvelle de cette plainte déposée devant le ministère public.

Quant à l'autre procédure, elle a été lancée auprès de l'Arcom, à la fin de l'année 2020. Or, à force de manœuvres dilatoires, on constate toujours en 2023 des millions de visites de mineurs sur des sites pornographiques, dont les responsables n'ont visiblement pas l'intention de prendre la moindre mesure pour respecter la loi et protéger les mineurs.

Pourtant, la Cour de cassation a rappelé dans un arrêt récent que la loi était claire et constitutionnelle. Rien ne s'oppose donc à ce que le tribunal prenne la décision de demander aux fournisseurs d'Internet de couper l'accès à ces sites.

À l'article 1er, l'alinéa 2 prévoit que l'Arcom veillera à ce que les contenus pornographiques mis à disposition par un service de communication au public en ligne ne puissent pas être accessibles aux mineurs. L'Arcom deviendrait ainsi l'autorité de référence dans la protection des mineurs. Toutefois, n'est-ce pas plutôt aux fournisseurs de veiller à ce que les contenus pornographiques qu'ils diffusent sur Internet ne soient pas accessibles aux mineurs ? Ne faudrait-il pas plutôt préciser que le rôle de l'Arcom est de veiller à ce que les fournisseurs de contenus pornographiques s'assurent de leurs obligations légales ?

Le troisième alinéa prévoit l'élaboration par l'Arcom de lignes directrices pour que les plateformes pornographiques puissent savoir comment protéger les mineurs de leurs contenus.

Cet alinéa s'inscrit en fait dans la ligne stratégique de défense de ces plateformes, lesquelles expliquent depuis plusieurs mois ne pas pouvoir se conformer à la loi parce que celle-ci n'est pas claire et que ni l'Arcom ni la Commission nationale de l'informatique et des libertés (Cnil) ne leur indiquent comment assurer la protection des mineurs. Dès lors, elles considèrent que la loi est anticonstitutionnelle, ne respectant pas le principe de légalité des délits et des peines. Or, je le rappelle, pour la Cour de cassation, elle est parfaitement claire, et les plateformes doivent prendre elles-mêmes les mesures qui s'imposent pour rendre leurs contenus inaccessibles aux mineurs. J'attire donc votre attention sur le fait que cette mesure, en suggérant que les pouvoirs publics doivent un certain nombre d'explications, donne raison aux plateformes.

Par ailleurs, l'article 227-24 et la loi prévoyant le déférencement des sites Internet par le biais de l'Arcom et du tribunal judiciaire posent une

obligation de résultat : si une plateforme est dans l'incapacité de s'assurer que ses contenus pornographiques ne sont pas accessibles aux mineurs, elle n'a pas le droit d'en faire trafic. Ce que je crains avec ce troisième alinéa, c'est que l'on passe d'une obligation de résultat à une obligation de moyens. Les plateformes pornographiques allégueront s'être conformées aux lignes directrices de l'Arcom et, en cas de problème avec leurs solutions techniques, demanderont que l'on se retourne vers l'autorité indépendante. Or les technologies du numérique évoluent très vite, et l'on ne sait pas comment, demain, l'âge des mineurs sera vérifié ou comment ceux-ci pourront dissimuler leur âge véritable. Autrement dit, on demande à l'Arcom d'entrer dans une course sans fin d'adaptation de lignes directrices à des évolutions extrêmement rapides.

Les plateformes pornographiques essaient aujourd'hui de nous faire croire que, si les contenus sont accessibles aux mineurs, c'est du fait de la législation et du manque de technologies adéquates. Il faut inverser la réflexion et considérer que, si la technologie ne permet pas de contrôler l'âge des mineurs, la plateforme ne peut pas faire commerce de ses contenus. On ne peut sacrifier l'intérêt de l'enfant sur l'autel de solutions techniques qui se font toujours attendre !

Par ailleurs, je ne vois pas, au regard des chiffres d'affaires des plateformes, comment l'amende prévue au sixième alinéa pourrait être dissuasive. S'agissant de plateformes qui ne sont pas domiciliées fiscalement en France, quelles procédures seront engagées pour recouvrir 75 000 euros à l'étranger ? Cela vaudra-t-il le coup pour le contribuable français ?

Enfin, même si, comme Olivier Gérard l'a rappelé, les procédures judiciaires sont beaucoup trop longues par rapport à l'urgence de la situation et que je comprends parfaitement l'idée de permettre à l'Arcom de prendre seule la décision de suspension des sites, je pose la question de la constitutionnalité d'une telle mesure. Les plateformes ne se gêneront pas pour lancer une nouvelle question prioritaire de constitutionnalité (QPC) et bloquer une décision de l'Arcom dans ce sens.

À l'article 3, relatif à la pénalisation en cas de non-retrait de contenus à caractère pédopornographique, il est indiqué le cas d'une plateforme ne pouvant se conformer à une demande de retrait « pour des motifs tenant à la force majeure ou à une impossibilité de fait qui ne lui sont pas imputables ». J'aimerais bien avoir un exemple de tels cas… Pour quelles raisons une plateforme, sommée par l'Arcom de retirer un contenu à caractère pédopornographique, pourrait justifier d'une impossibilité de le faire ?

En outre, le projet de loi s'en tient au seul retrait des contenus à caractère pédopornographique, comme s'il n'y avait pas, derrière, des auteurs de pédocriminalité et des victimes. Nulle part il n'est fait mention d'enquêtes qui devraient être automatiquement lancées pour les identifier et

s'assurer que les victimes reçoivent l'assistance dont elles ont besoin et que les auteurs soient traduits devant la justice.

Mme Angélique Gozlan, membre du comité d'experts de l'Observatoire de la parentalité et de l'éducation numérique. – Je précise qu'outre ma qualité d'expert de l'Open je suis également docteur en psychopathologie et psychologue clinicienne, ce qui inscrit mes propos dans un courant de pensée particulier par rapport aux enfants et aux adolescents.

Saluant le travail engagé, qui marque un tournant symbolique et législatif quant à la protection des mineurs sur Internet, l'Open tient néanmoins à souligner plusieurs points.

Je ne serai pas longue sur la question de la pornographie, car nous rejoignons totalement les remarques qui viennent d'être exposées par Arthur Melon. Se posent, d'une part, la question de l'effectivité des pouvoirs accordés à l'Arcom et, d'autre part, celle de l'application des mesures en matière de sanctions pénales et administratives des sites donnant accès à des contenus pornographiques à des mineurs, dont beaucoup dépendent d'entreprises opacifiées, hébergées dans des paradis fiscaux.

S'agissant des exigences de contrôle d'âge soumises au respect de la vie privée, il est absolument nécessaire de veiller à ne pas sacrifier la protection de l'enfant à la protection des données : on procède bien au contrôle des cartes d'identité des mineurs lorsqu'ils veulent acheter de l'alcool dans un supermarché. En l'absence de solutions techniques permettant d'opérer une corrélation entre le contrôle de l'âge et la protection des données, l'Open propose d'appliquer le système de la carte bleue, facile et rapide à mettre en place.

Nous soutenons bien évidemment la volonté de régulation des sites pornographiques, mais nous insistons pour que cette régulation se fasse au nom de la cohérence éducative. Or, il n'y a rien dans ce projet de loi sur l'éducation des mineurs et des adultes !

Il faut promouvoir l'obligation d'une éducation aux médias et au numérique auprès des enfants et des adolescents, ainsi qu'une éducation sexuelle abordant, non pas uniquement la santé sexuelle et la prévention des risques, mais aussi les questions du consentement, du plaisir sexuel, de la connaissance de son corps au regard du corps de l'autre, de la relation sexuelle, de la condition de l'homme et de la femme. Ainsi, on leur offrira la possibilité de se construire un regard critique et d'aller vers une vie sexuelle dans le respect d'autrui.

Il faut par ailleurs impliquer et soutenir les adultes pour qu'ils puissent accompagner les enfants et les adolescents dans l'utilisation des espaces numériques, en prenant en considération le risque d'exposition aux images pornographiques. Nous sommes, je le rappelle, la première génération de parents à devoir construire une éducation numérique.

Raisonner seulement par le prisme de l'évitement des risques n'est donc pas suffisant ; il est absolument nécessaire de penser prévention, éducation et accompagnement.

Sur le cyberharcèlement, l'option retenue dans le texte – une peine complémentaire de suspension du compte sur la plateforme pour les utilisateurs condamnés pour une durée maximale de six mois – pose plusieurs questions.

Sachant que tout utilisateur peut créer maints comptes et changer d'adresse IP, comment une telle mesure sera-t-elle techniquement possible ?

Il est par ailleurs précisé dans l'étude d'impact que « *la peine de suspension des comptes ne concerne que les services de plateforme en ligne ayant été utilisés pour commettre l'infraction* ». Or, comme le montrent les études sur le cyberharcèlement, un cyberharceleur n'opère pas à partir d'un réseau social unique ; il utilise divers canaux. En imaginant qu'après une suspension de compte sur un site donné, il poursuive son harcèlement à partir d'un compte ouvert ailleurs, que prévoit le projet de loi pour faciliter le parcours juridique de la victime ?

Les « témoins en ligne » sont les grands absents de ce texte. Comment définit-on la notion de témoins en ligne du cyberharcèlement, dont la particularité est d'être présents en masse ? Comment qualifie-t-on des actes comme *liker* ou repartager une publication harcelante ? Que prévoit le texte pour ces témoins en ligne ?

Toujours dans l'étude d'impact, on peut lire que « cette peine complémentaire de suspension de compte dissuade les utilisateurs dont les comptes ont déjà été suspendus à récidiver et également d'autres utilisateurs qui pourraient être tentés de se livrer à des comportements similaires ». Cet effet de dissuasion est relatif au profil psychologique de la personne et ne peut pas être généralisé.

Enfin, « l'obligation pour les plateformes d'empêcher la création de nouveaux comptes par ces utilisateurs récidivistes prévient d'autant plus de tels comportements et protège les utilisateurs de contenus néfastes et préjudiciables ». J'attire votre attention sur le fait qu'on ne peut penser la prévention des comportements de cyberharcèlement et la protection des utilisateurs par la seule voie législative – une interdiction n'empêche pas la transgression – et que l'usage fait des réseaux sociaux constitue juste une mise en lumière de comportements préexistants. Or – question fondamentalement absente du projet de loi –, que prévoit-on pour l'accompagnement des personnes condamnées ? Les harceleurs sont en souffrance et en difficulté – ce sont soit d'anciens harcelés soit des personnes se construisant en leaders négatifs pour réparer une faille narcissique – et, dans le cas de mineurs, ils manifestent en outre une banalisation de leurs actes et une déréalisation. « *Ce n'est pas la vraie vie, on est sur numérique* », vont-ils dire… Un suivi doit donc impérativement être associé à ces mesures

et l'on pourrait s'inspirer, ici, de pratiques déjà existantes, notamment les injonctions de soins à destination des acteurs de violences sexuelles.

On pourrait donc imaginer une injonction de soins en aval de l'acte commis – avec prise en charge individuelle ou en groupe – et, en amont, une sensibilisation plus forte des enfants et des adolescents à l'être ensemble et au collectif. Cela implique d'intégrer aux programmes scolaires, avec une progression de la maternelle au secondaire, des modules d'éducation aux médias et au numérique, comprenant notamment une sensibilisation à l'impact émotionnel des images, l'intégration progressive d'une notion de « citoyen en ligne », une déculpabilisation à l'acte de signalement, une sensibilisation aux phénomènes de groupe et une information associée à la responsabilisation de leurs actes.

Cela me permet de rebondir sur un point de l'étude d'impact qui m'a particulièrement interloquée : les impacts sur la jeunesse y sont qualifiés par le terme « néant ». Je n'ai pas les codes pour savoir ce que sous-tend, dans le cadre d'un projet de loi, la notion d'impacts sur la jeunesse, mais pour la psychologue que je suis, ce terme m'apparaît comme un non-sens. L'article 5 du projet de loi doit évidemment avoir un impact sur la jeunesse ! La sanction qu'il porte doit avoir valeur d'apprentissage ; elle doit affirmer la centralité de la loi et des règles, que ce soit dans l'espace public réel ou dans l'espace numérique, ce qui favorisera le vivre ensemble et la société ; elle doit permettre de rendre un sujet responsable, à même d'assumer les conséquences de ses actes. Il doit donc y avoir un « après la sanction », c'est-à-dire un accompagnement qui n'oublie personne : harceleurs, témoins et victimes.

Mme Catherine Morin-Desailly, présidente. – La question éducative est effectivement essentielle, mais il faut distinguer ce qui relève de la loi et ce qui relève de son application par décret, puis au travers de l'élaboration des programmes éducatifs. Aujourd'hui, ces sujets sont déjà inscrits au cœur du code de l'éducation. De longue date, le Sénat a légiféré en ce sens. Ainsi, en 2011, nous avons instauré une obligation de formation et de sensibilisation des élèves aux risques et aux menaces de l'Internet. Puis nous avons de nouveau amendé la loi du 26 juillet 2019 pour une école de la confiance afin de spécifier ce que doit être la formation des formateurs dans ce domaine très précis. Maintenant, nous devons contrôler l'application de la loi. Aidez-nous à le faire !

M. Loïc Hervé, rapporteur. – Les interventions ayant été très complètes et fouillées, je souhaiterais plutôt livrer une réflexion.

Nous sommes bien conscients de la période dans laquelle s'inscrit notre travail : un accord vient d'être trouvé en commission mixte paritaire sur la majorité numérique ; nous attendons une décision de justice ; le *Digital Markets Act (DMA)* et le *Digital Services Act (DSA)* entreront sous peu dans l'ordre juridique français ; de nouveaux textes européens sont en cours de

négociation ; certains textes de loi entrent à peine en vigueur, avec des effets juridiques qui pourront seulement être mesurés après quelques mois ou quelques années.

À vous entendre, si je schématise, il faudrait se contenter d'appliquer les dispositions existantes, attendre et voir si cela fonctionne… Il me semble au contraire qu'il faut accélérer et « massifier » le dispositif car, en réalité – toutes les auditions le montrent –, rien n'est réglé. Non seulement les affaires portées devant l'autorité judiciaire tardent à obtenir un jugement, mais elles sont également très peu nombreuses. Cela me fait penser à l'excision : des milliers de jeunes filles vivant en France sont concernées, mais aucune affaire n'est portée devant les tribunaux !

L'idée de confier à l'Arcom la définition d'un cahier des charges précis des techniques par lesquelles on pourrait tenter de contrôler l'âge des personnes consultant des sites pornographiques est donc une tentative et, dans un contexte où il faut « massifier », essayons de rendre la rédaction plus opérationnelle, mais ne tournons pas le dos à cette nouvelle tentative. Je le dis sans méconnaître les difficultés techniques posées, ni aucune des difficultés liées aux messageries instantanées, à la double anonymisation ou encore au simple fait que, dans certaines familles, les enfants ont accès aux cartes bancaires.

Notre commission spéciale ne fait que saisir une occasion. Ce texte aurait pu ne pas exister – les règlements européens ne l'exigent pas forcément –, mais certains points devaient être précisés et le Gouvernement a tenu à insérer les premiers articles du texte. Je vois difficilement comment le Parlement, en particulier le Sénat, ne pourrait pas saisir cette occasion pour progresser sur ce sujet, fondamental pour la jeunesse de notre pays.

Mme Laurence Rossignol. – Je pense, comme vous, monsieur Melon, que l'efficacité des trois premiers articles du texte est sujette à caution. Vous dites même que le dispositif envisagé pourrait s'avérer contre-productif. Cependant, quel autre dispositif pourrions-nous mettre en œuvre ? À mon sens, la pornographie est toxique pour tous, non pour les seuls mineurs. Idéalement, nous devrions être capables d'imposer la fermeture d'un site Internet en cas de non-respect de la disposition de la loi du 30 juillet 2020 concernant l'accès de ses contenus aux mineurs. Nous ne devrions pas avoir à nous engager dans des séries de référentiels ou de procédures comme celles que prévoit le texte. Vous avez raison par ailleurs de souligner que l'on n'entend dire par aucune autre entité, comme on l'entend de la part des grandes entreprises de l'industrie pornographique, qu'elle ne respecte pas la loi parce que l'État ne lui donne pas les moyens de le faire.

Nous butons toujours sur le même sujet : le postulat du nécessaire respect de l'anonymat et de la vie privée des consommateurs de pornographie. En réalité, il existe des *continuums* entre la pornographie,

la pédocriminalité et le viol. Un article paru aujourd'hui dans *Le Monde* fait ainsi état d'une affaire criminelle survenue dans le Vaucluse, au cours de laquelle cinquante personnes ont été mises en examen pour viol, dans les ordinateurs desquelles des milliers d'images de viols et d'images pédopornographiques ont été retrouvées. Ces *continuums* ne sont, bien sûr, pas systématiques, mais il faut les avoir à l'esprit.

Or nous butons toujours sur la même question : qu'est-ce qui justifie que les consommateurs de pornographie aient droit à l'anonymat qu'aucun autre usager d'Internet ne revendique par ailleurs ? Pourquoi ce qui fonctionne pour les sites de jeux en ligne ne peut-il pas s'appliquer aux sites pornographiques ? Je n'ai toujours pas compris cela. Nous pourrons poser cette question au Conseil constitutionnel à l'occasion d'une QPC.

En l'état, le texte suscite une grande frustration, car nous avons l'impression de vider la mer à l'aide d'une petite cuillère.

Mme Marie Mercier. – Je partage ce qui a été dit : au travers de ce texte, nous avons l'impression de radoter. Une loi impose le contrôle de l'âge pour le visionnage de sites pornographiques. Nous savons contrôler l'âge dans l'univers numérique. Or cela ne fonctionne pas ! Certes, l'anonymat est demandé par les usagers sur les sites gratuits, mais qu'en est-il des sites pornographiques payants ? Pourquoi butons-nous sur le problème du contrôle de l'âge, alors qu'il ne se présente pas pour le cas des sites de jeux en ligne ? Il y a là des raisons qui nous échappent.

Un nouveau texte vient donc s'ajouter aux lois existantes. Il est déjà obligatoire de s'assurer que des contenus réservés aux adultes ne tombent pas sous les yeux des enfants. Or nous n'arrivons pas à effectuer ce contrôle, et ce texte ne nous permettra pas d'y arriver davantage.

L'article 15 du texte m'a par ailleurs beaucoup ennuyée : on ne voit pas pourquoi le Gouvernement réussirait davantage avec des ordonnances là où la loi échoue concernant le contrôle des jeux comportant l'achat, l'usage ou le gain d'objets numériques monétisables.

M. Patrick Chaize, rapporteur. – Il est hors de question que nous laissions cet article en l'état.

Mme Catherine Morin-Desailly, présidente. – Nous l'avons dit d'emblée au ministre délégué chargé de la transition numérique et des télécommunications.

M. Loïc Hervé, rapporteur. – Les contenus payants font l'objet d'un contrat. C'est l'existence de ce dernier et du paiement associé qui crée l'identification de la personne qui y accède. L'enjeu du texte est de fournir une réglementation et une régulation en l'absence de contrat, pour des contenus non soumis à une identification préalable.

Mme Annick Billon. – Lorsqu'Alexandra Borchio Fontimp, Laurence Cohen, Laurence Rossignol et moi-même avons démarré les

travaux relatifs à notre rapport d'information intitulé *Porno : l'enfer du décor*, en janvier 2022, le regard porté sur l'industrie pornographique était assez édulcoré. Depuis, la situation a évolué. Nous avons mis en avant le fait que ces images étaient consultées par de très nombreux mineurs, et l'existence d'une porosité entre la pornographie, le proxénétisme, et la prostitution. Nos travaux ont suscité des réactions.

Le texte qui nous occupe ne va peut-être pas assez loin, mais il a l'avantage de présenter quelques propositions. Nous devons tout mettre en œuvre pour rendre la vie impossible aux entreprises de ce secteur, qui ne respectent pas la loi quand elle existe. Une véritable éducation au corps est par ailleurs nécessaire, car les enfants sont exposés à des images pornographiques dès l'âge de huit ou neuf ans.

Il faut que vous nous aidiez à améliorer ce texte pour rendre la vie impossible à ces entreprises, souvent hébergées dans des paradis fiscaux et qui génèrent beaucoup d'argent, en leur imposant de lourdes sanctions.

Vous avez tous mentionné l'importance de mobiliser des moyens pour faire respecter la loi. Il revient aux entreprises de l'industrie pornographique de se mettre en conformité avec la loi. Ce n'est pas à un organisme extérieur, *a fortiori* à l'État, de les aider à le faire. Il incombe à ces entreprises de faire en sorte que les images qu'elles véhiculent ne soient pas accessibles aux mineurs, et que toutes les images qui contreviennent à la loi – images de viols, à caractère raciste, ou relevant de la pédocriminalité – soient bloquées.

Nous sommes intéressés par toutes les pistes que vous pourriez proposer pour renforcer en la matière la protection des mineurs et de toute la société, car ces images ne sont pas nuisibles seulement pour les mineurs.

Mme Toine Bourrat. – Quelle est votre position sur la levée de l'anonymat et du pseudonymat sur Internet, sachant que le second permet de multiplier les comptes à l'infini ?

Mme Alexandra Borchio Fontimp. – Que pensez-vous de la possibilité de fusionner les plateformes d'appel 3018 et 3020, évoquée dans le cadre de la proposition de loi visant à instaurer une majorité numérique et à lutter contre la haine en ligne, dont j'étais rapporteure ? Cette possibilité avait été envisagée pour améliorer leur visibilité.

Quel est votre point de vue concernant l'idée, portée par cette proposition de loi, de replacer l'autorité parentale au cœur de la famille pour responsabiliser les enfants, et la création d'un « permis d'Internet » ? Une meilleure éducation à la sexualité est en effet indispensable.

Enfin, j'envisage de présenter un amendement visant à responsabiliser les boutiques d'applications et les systèmes d'exploitation, qui concourent également à l'accès aux contenus pornographiques. Ces sociétés doivent se montrer vigilantes en ce domaine, car elles disposent des données permettant de le faire.

Mme Catherine Morin-Desailly, présidente. – Cet amendement, sur lequel j'avais travaillé avec Annick Billon et vous-même pour un texte antérieur, trouvera toute sa place dans le projet de loi dont nous discutons.

André Reichardt a été co-rapporteur de la proposition de résolution européenne visant à prévenir et combattre les abus sexuels sur les enfants. Le sujet est pris très au sérieux en Europe, où l'on s'interroge sur une législation *ad hoc*.

M. André Reichardt. – À titre informatif, outre les données chiffrées relatives aux consultations des sites pornographiques gratuits, connaissons-nous les chiffres des consultations des sites pornographiques payants ?

Par ailleurs, l'obligation faite à l'Arcom dans le texte de fournir des lignes directrices pour contrôler la majorité des personnes qui visionnent des contenus pornographiques risque d'avoir peu d'effet. Existe-t-il une autre façon de procéder que l'on pourrait inscrire dans le projet de loi, pour parvenir à un contrôle obligatoire efficace de cette majorité ?

M. Olivier Gérard. – La disposition contenue dans l'article 15 du texte nous a également surpris, la voie d'ordonnance ne nous semblant pas appropriée compte tenu de l'importance des enjeux relatifs à la protection de l'enfance sur Internet.

Mme Catherine Morin-Desailly, présidente. – Il n'est pas question de laisser cette partie du texte en l'état. Le Sénat aime peu les ordonnances de toute façon.

M. Olivier Gérard. – La simplification des plateformes d'appel est une demande que l'on entend beaucoup sur le terrain. On se perd en effet dans les numéros existants, et l'on renvoie à l'enfant ou au parent concerné la responsabilité de choisir entre l'un ou l'autre. Une simplification est donc nécessaire pour clarifier et faciliter l'accès du grand public aux plateformes d'appel – *via* un guichet unique, par exemple.

Il est important par ailleurs de redonner une place aux parents, afin qu'ils exercent véritablement leur rôle auprès de leurs enfants. Des dispositifs d'accompagnement et de sensibilisation pourraient être envisagés. Une réflexion est en outre en cours autour d'une certification « Pix parents », reprenant les compétences requises pour accompagner les enfants sur Internet, qui doit aboutir fin 2024 ou début 2025.

Je n'ai pas d'informations par ailleurs sur les chiffres des consultations des sites pornographiques payants.

M. Arthur Melon. – Nous sommes les premiers à déplorer la longueur des délais de justice. Celle-ci tient toutefois à des manœuvres dilatoires engagées par les plateformes concernées. Une nouvelle procédure a en outre dû être lancée en raison d'un vice de procédure imputable à

l'Arcom, qui a entraîné un retard de plusieurs mois pour la citation des fournisseurs d'accès à Internet devant le tribunal judiciaire.

L'injonction de médiation prononcée durant la première audience entre l'Arcom, les fournisseurs d'accès à Internet et les plateformes pornographiques nous a par ailleurs surpris, car elle revenait à demander à un régulateur chargé de faire respecter la loi de négocier avec des structures qui ne la respectent pas.

Un arrêt du Conseil constitutionnel découlant d'une QPC et rendu au printemps explique également la longueur de la procédure judiciaire engagée.

Faire passer les décisions par le juge prend donc du temps. Toutefois, rien ne garantit que l'Arcom fasse le travail plus rapidement que les magistrats, du fait des incertitudes sur les moyens qui lui seraient alloués dans ce cadre.

Mme Catherine Morin-Desailly, présidente. – La question des moyens n'est pas neuve. L'Arcom se voyant octroyer plus de missions, des amendements seront déposés lors de l'examen du prochain projet de loi de finances pour augmenter, de manière générale, les moyens alloués aux autorités de régulation.

M. Arthur Melon. – Le Cofrade, l'Open et l'Unaf ont saisi l'Arcom fin août à l'encontre de Twitter, qui laisse des contenus pornographiques, pédopornographiques et zoophiles sur sa plateforme. À ce jour, aucune suite n'a été donnée à cette saisine.

Il est assez curieux par ailleurs de voir combien les plateformes pornographiques bénéficient d'une sorte de régime d'exception concernant le respect de la vie privée. Quand il s'agit de connaître la religion, l'orientation sexuelle ou politique de quelqu'un sur les réseaux sociaux, cela ne pose pas problème. Or dès qu'il est question de pornographie, cela devient très important. Pourquoi un tel régime d'exception ? Je rappelle que la Cour de cassation a estimé que la loi actuelle avait des moyens proportionnés par rapport à l'exigence de protection des mineurs. Nous devrions donc être moins regardants sur la protection des données personnelles lorsqu'il s'agit de protéger des mineurs.

M. Loïc Hervé, rapporteur. – Le texte prévoit la définition d'un cahier des charges technique, qui fera l'objet d'une délibération de l'Arcom après avis de la Cnil. Des opérations de vérification du contrôle de l'âge pour le visionnage d'images pornographiques seront ensuite effectuées, assorties d'un régime de sanctions. Il ne s'agit donc pas simplement d'affirmer une obligation. Confier cette tâche à l'Arcom est un choix politique qui sera posé ou non au travers de ce texte de loi. Il faudra évidemment renforcer les moyens qui lui sont alloués.

Par ailleurs, il n'est pas certain que le fait de passer par une autorité administrative indépendante plutôt que par le juge judiciaire fournisse une réponse plus efficace et plus massive au problème dont nous parlons. Ce choix devra être posé par le législateur. Il reste qu'en l'absence d'un tel choix nous en resterons au droit actuel, dans le cadre duquel très peu d'affaires sont portées devant les tribunaux, et les délais de jugement sont très longs.

L'expression « manœuvres dilatoires » relève du jugement de valeur. La juridiction judiciaire repose en effet sur la base du contradictoire. Toutefois, l'opération de médiation ordonnée par le juge m'a également surpris, mais cela s'est fait dans le respect du fonctionnement ordinaire des juridictions judiciaires.

M. Arthur Melon. – L'enquête de Médiamétrie commandée par l'Arcom montre que 60 % des contenus pornographiques consommés par les mineurs proviendraient de cinq plateformes gratuites. Je ne sais pas comment se répartissent les 40 % de contenus restants entre les plateformes gratuites et payantes, mais je pense que les premières sont majoritaires.

Si le tribunal demande le 7 juillet prochain aux fournisseurs d'accès de suspendre les plateformes pornographiques, gageons qu'elles trouveront tout de suite une solution technique pour se mettre en conformité avec la loi et pouvoir republier leurs contenus. La question des difficultés techniques relève plutôt du prétexte. Je serais d'ailleurs curieux de voir, une fois qu'une décision de sanction aura été prise à l'encontre de l'une d'entre elles, la créativité que déploieront les autres plateformes pour trouver des solutions permettant de contrôler l'âge des internautes.

Mme Toine Bourrat. – Je rappelle ma question sur le pseudonymat sur Internet ?

Mme Angélique Gozlan. – Il s'agit d'un enjeu important, car l'usage de pseudonymes favorise la levée des inhibitions et augmente le nombre d'inconduites sur les réseaux sociaux. Il participe en outre aux pratiques agressives et aux diffamations en masse comme le *trolling* et les raids. Cependant, derrière le pseudonyme se trouve toujours une adresse IP. On rejoint ici la question de la protection des données personnelles. Néanmoins, une levée du pseudonymat pourrait être envisagée en cas de cyberharcèlement.

Mme Catherine Morin-Desailly, présidente. – Le texte qui nous occupe est un texte d'application d'au moins trois règlements européens, auxquels s'ajoute le *Data Act*, par anticipation. Il a fait l'objet de négociations entre les États membres.

Une solution extrême au problème de l'accès des mineurs aux contenus pornographiques consisterait à responsabiliser les plateformes en leur conférant un troisième statut, entre hébergeur et éditeur, et en remettant en cause leur modèle économique. C'est celui-ci en effet qui rend possibles ces dérives, car elles sont rémunératrices. En l'occurrence, le texte propose

un compromis, et constitue à ce titre une étape vers une possible amélioration de la situation.

Les crimes qui ont été évoqués restent condamnables, par une justice qui demeure trop lente. Cependant, le sujet principal reste notre difficulté à avoir prise sur ces plateformes, que l'on a laissé prospérer. Une étape comme celle-ci est nécessaire pour tenter de reprendre la main. Si le texte n'est pas parfait, il a le mérite de construire une prise de conscience collective pour que tout le monde se mette en ordre de marche dans cette direction.

La commission spéciale n'en est encore qu'à l'étape des auditions. Vous entendre aujourd'hui nous a permis de rappeler l'importance de faire valoir les dispositions qui existent déjà dans la loi, et le travail considérable qu'il nous faut mener sur les moyens dédiés à l'évaluation et au contrôle réguliers, par le Parlement, de leur application. Merci de votre éclairage. Nous serons attentifs à tout cela.

Ce texte s'appliquera uniformément dans tous les États membres. Cela est d'autant plus important que les réseaux pédopornographiques sont souvent transfrontaliers. Il faut appréhender cette question de façon transnationale, d'où l'importance d'un socle minimal de législation harmonisé au niveau européen.

LISTE DES PERSONNES ENTENDUES

Auditions plénières

M. Jean-Noël Barrot, ministre délégué auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargé de la transition numérique et des télécommunications

OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITÉ LIÉE AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (OCLCTIC)

Mme Cécile Augeraud, commissaire divisionnaire, cheffe de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

SOUS-DIRECTION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

M. Pierre-Yves Lebeau, chef de l'état-major

Mme Clara Timsit, conseillère juridique rattachée à l'état-major

PÔLE D'EXPERTISE DE LA RÉGULATION NUMÉRIQUE (PEREN)

M. Lucas Verney, directeur adjoint

EUROPOL

M. Jean-Philippe Lecouffe, directeur exécutif adjoint des opérations

<u>Table ronde des régulateurs</u>

AUTORITÉ DE RÉGULATION DE LA COMMUNICATION AUDIOVISUELLE ET NUMÉRIQUE (ARCOM)

M. Roch-Olivier Maistre, président

M. Guillaume Blanchot, directeur général

AUTORITÉ DE RÉGULATION DES COMMUNICATIONS ÉLECTRONIQUES, DES POSTES ET DE LA DISTRIBUTION DE LA PRESSE (ARCEP)

Mme Laure de La Raudière, présidente

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

Mme Marie-Laure Denis, présidente

Table ronde des sociétés d'informatique en nuage (clouders) européennes

OVHCLOUD

Mme Solange Viegas Dos Reis, directrice juridique et membre du Comité exécutif

DOCAPOSTE

Mme Séverine Denys, directrice des relations institutionnelles

NUMSPOT

M. Alain Issarni, directeur général

EUCLIDIA

M. Jean-Paul Smets, vice-président

OUTSCALE

M. Thibault de Tersant, directeur général adjoint de Outscale, secrétaire général de Dassault Systems

M. Grégory Abate, secrétaire général adjoint de Dassault Systems

SCALEWAY

M. Damien Lucas, directeur général de Scaleway

M. Lucas Buthion, responsable des affaires publiques au sein du Groupe Iliad-Free

Table ronde des opérateurs du numérique

FACEBOOK - META FRANCE

M. Anton'Maria Battesti, directeur des affaires publiques

Mme Béatrice Oeuvrard, responsable des affaires publiques

GOOGLE FRANCE

M. Benoît Tabaka, secrétaire général

M. Frédéric Géraud de Lescazes, directeur des politiques publiques de Google Cloud France

AMAZON

M. Arnaud David, directeur des affaires publiques européennes d'Amazon Web Services

M. Yohann Bénard, directeur des affaires publiques d'Amazon

Table ronde sur la protection de l'enfance

CONSEIL FRANÇAIS DES ASSOCIATIONS POUR LES DROITS DE L'ENFANT (COFRADE)

M. Arthur Melon, délégué général

UNION NATIONALE DES ASSOCIATIONS FAMILIALES (UNAF)

M. Olivier Gérard, coordonnateur du pôle « médias – usages numériques »

OBSERVATOIRE DE LA PARENTALITÉ ET DE L'ÉDUCATION NUMÉRIQUE (OPEN)

Mme Angélique Gozlan, membre du comité d'experts

Auditions menées par Patrick Chaize, rapporteur

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE - DIRECTION GÉNÉRALE DES ENTREPRISES

M. Loïc Duflot, chef du service de l'économie numérique

M. Pierre Serra, chef de projet économie de la donnée

Mme Chantal Rubin, cheffe du pôle régulation des plateformes numériques

DIRECTION GÉNÉRALE DE LA CONCURRENCE, DE LA CONSOMMATION ET DE LA RÉPRESSION DES FRAUDES (DGCCRF)

Mme Nadine Mouy, sous-directrice services réseaux et numérique

Mme Axelle Bulle, cheffe du bureau du soutien juridique

Mme Hélène Bonnet, adjointe au bureau Médias, communications électroniques, culturel, économie de la donnée

GROUPEMENT D'INTÉRÊT PUBLIC ACTION CONTRE LA CYBERMALVEILLANCE (ACYMA)

M. Jérôme Notin, directeur général

CONSEIL NATIONAL DU NUMÉRIQUE (CNNUM)

M. Jean Cattan, secrétaire général

Mme Joëlle Toledano, professeure des universités, associée à la chaire gouvernance et régulation de Dauphine, membre du CNNum

Table ronde « Navigateurs Internet »

GOOGLE CHROME

Mme Floriane Fay, responsable des relations institutionnelles et politiques publiques

M. Olivier Esper, responsable des relations institutionnelles

MOZILLA FIREFOX

M. Tasos Stampelos, responsable politique publique européenne

M. Sylvestre Ledru, directeur de l'ingénierie et responsable France

APPLE SAFARI

Mme Julie Lavet, responsable des relations avec le Parlement

Table ronde « Télécommunications »

FÉDÉRATION FRANÇAISE DES TÉLÉCOMMUNICATIONS (FFT)

M. Olivier Riffard, directeur général adjoint de la FFT

M. Alix de Montesquieu, responsable des affaires institutionnelles d'Altice Group

Mme Carole Gay, responsable des affaires institutionnelles d'Orange

M. Corentin Durand, responsable affaires publiques de Bouygues Télécom

ILIAD-FREE

M. Sylvain Lemaire, chargé des affaires publiques

M. Lucas Buthion, responsable des affaires publiques

Table ronde « Jeux à objets numériques monétisables (Jonum) »

AUTORITÉ NATIONALE DES JEUX (ANJ)

M. Rémi Lataste, directeur général

SYNDICATS DES ÉDITEURS DE LOGICIELS DE LOISIRS (SELL)

M. Nicolas Vignolles, délégué général

ASSOCIATION FRANÇAISE DES JEUX EN LIGNE (AFJEL)

Mme Isabelle Djian, déléguée générale

Mme Audrey Herblin-Stoop, présidente du groupe de travail « Affaires institutionnelles »

M. Adrian Julian, président du groupe de travail « Lutte contre le jeu illégal »

SYNDICAT NATIONAL DU JEU VIDÉO (SNJV)

Mme Anne Dévouassoux, présidente

M. Lévan Sardjeveladze, premier vice-président des affaires publiques

M. Julien Villedieu, délégué général

AIRBNB

Mme Diane Prebay, responsable des affaires institutionnelles

UFC-QUE CHOISIR

M. Benjamin Recher, chargé des relations institutionnelles

M. Frithjof Michaelsen, chargé de mission numérique

NUMEUM

Mme Marine Gossa, déléguée aux Affaires publiques

Mme Anissa Kemiche, chargée des affaires européennes

ALLIANCE DIGITALE

M. Pierre Devoize, directeur général adjoint en charge des affaires publiques.

FÉDÉRATION DU E-COMMERCE ET DE LA VENTE À DISTANCE (FEVAD)

M. Marc Lolivier, délégué général

Mme Marie Audren, responsable affaires publiques

AUTORITÉ DE LA CONCURRENCE

M. Benoît Coeuré, président

M. Yann Guthmann, chef du service de l'économie numérique

Auditions menées par Loïc Hervé, rapporteur

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE - DIRECTION GÉNÉRALE DES ENTREPRISES (DGE)

M. Loïc Duflot, chef du service de l'économie numérique

Mme Chantal Rubin, cheffe du pôle régulation des plateformes numériques

MINISTÈRE DE LA JUSTICE - DIRECTION DES AFFAIRES CRIMINELLES ET DES GRÂCES

Mme Sophie Macquart-Moulin, adjointe au directeur

AUTORITÉ DE RÉGULATION DE LA COMMUNICATION AUDIOVISUELLE ET NUMÉRIQUE (ARCOM)

M. Roch-Olivier Maistre, président

M. Guillaume Blanchot, directeur général

Mme Laurence Pécaut-Rivolier, personnalité qualifiée en charge des contenus pédopornographiques et terroristes

Mme Lucile Petit, directrice des plateformes en ligne

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

M. Louis Dutheillet de Lamothe, secrétaire général

Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles

CONSEIL NATIONAL DU NUMÉRIQUE (CNNUM)

M. Jean Cattan, secrétaire général

Mme Margot Godefroi, rapporteure

Table ronde des juridictions

CONSEIL D'ÉTAT

M. Thierry-Xavier Girardot, secrétaire général

M. Sylvain Humbert, secrétaire général adjoint, chargé des juridictions administratives et du numérique

COUR DE CASSATION

Première présidence

Mme Elisabeth Pichon, secrétaire générale

Mme Estelle Jond-Necand, secrétaire générale adjointe

Mme Caroline Azar, chargée de mission

Parquet général

Mme Audrey Prodhomme, secrétaire générale

COUR DES COMPTES

Mme Maïa Wirgin, secrétaire générale

Mme Gwladys de Castries, secrétaire générale adjointe

M. Antoine Pavamani, chargé de mission relations institutionnelles

Mme Marie Dussol, directrice des affaires juridiques

Table ronde d'associations

LIGUE DES DROITS DE L'HOMME

Mme Maryse Artiguelong, membre du Bureau national et responsable du groupe de travail « Libertés et technologies de l'information et de la communication »

LA QUADRATURE DU NET

M. Bastien Le Querrec, juriste, doctorant en droit, membre

Table ronde des acteurs des réseaux sociaux

GOOGLE / YOUTUBE

M. Olivier Esper, directeur des relations institutionnelles

SNAPCHAT

Mme Sarah Bouchahoua, responsable des affaires publiques France

FACEBOOK FRANCE / META FRANCE

M. Anton'Maria Battesti, directeur des affaires publiques

Mme Béatrice Oeuvrard, responsable des affaires publiques

LISTE DES CONTRIBUTIONS ÉCRITES

- Alliance française des industries du numérique (Afnum)
- Alliance française des places de marché (AFPDM)
- Amnesty international France
- Act Up-Paris
- Association des casinos indépendants de France (Acif)
- Association des maires de France et des présidents d'intercommunalité (AMF)
- Association pour le développement des actifs numériques (Adan)
- Casinos de France
- Cigref
- Cloud Infrastructure Services Providers in Europe (Cispe)
- Conseil supérieur du notariat (CSN)
- Criteo
- Doctrine
- Open Internet Project
- Eurocloud
- Fédération nationale des courses hippiques
- Fédération nationale des syndicats d'exploitants agricoles (FNSEA)
- Fédération Parapluie Rouge (FPR)
- Groupe Barrière
- Groupe Tranchant
- IBM France
- LOV Group
- Ministère des armées – Direction générale du numérique et des systèmes d'information et de communication
- Mouvement des entreprises de France (Medef)
- Oracle
- Qarnot Computing
- Sorare
- Twitch
- Unibet
- Union des marques
- Vivendi

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

https://www.senat.fr/dossier-legislatif/pjl22-593.html