

ARTICLE

LE PROJET DE LOI VISANT À SÉCURISER L'ESPACE NUMÉRIQUE (SREN) DÉFINITIVEMENT ADOPTÉ

IT et données personnelles | 17/04/24 | Florence Chafiol Alexandra Antalis

Le projet de loi SREN, adopté le 10 avril 2024 par l'Assemblée nationale, a pour objectif de mieux réguler l'espace numérique et de protéger davantage les internautes. Il adapte le droit français au Règlement sur les services numériques (*Digital Services Act* en anglais – DSA), au Règlement sur les marchés numériques (*Digital Markets Act* en anglais – DMA) et au Règlement sur la gouvernance des données (*Data Governance Act* en anglais – DGA).

Plusieurs députés ont d'ores et déjà annoncé qu'ils allaient saisir le Conseil constitutionnel concernant certaines dispositions de la loi. Une fois la question de la constitutionnalité du texte étudiée, sa version finale devra ensuite être notifiée à la Commission européenne qui décidera si le texte est promulgué ou non.

Quelles sont les mesures clés ? Que faut-il en retenir ? L'équipe IT/DATA décrypte les principaux apports.

- En matière de données à caractère personnel

> **Extension du champ d'application de la Loi Informatique et Libertés** : en principe, la Loi Informatique et Libertés s'applique (i) aux responsables du traitement ou sous-traitants établis sur le territoire français et (ii) aux traitements mis en œuvre par un responsable de traitement ou un sous-traitant établi hors de l'Union européenne dès lors que ces traitements sont liés à l'offre de biens ou de services à des personnes situées en France ou au suivi du comportement de ces personnes. La loi SREN vient étendre le champ d'application des titres I et II de la Loi Informatique et Libertés (ces titres concernant notamment les traitements relevant du Règlement général sur la protection des données (RGPD)) aux traitements (i) mis en œuvre par un responsable de traitement ou un sous-traitant établi hors de l'Union européenne et (ii) consistant à suivre le comportement des personnes situées sur le territoire français, notamment par la collecte de leurs données à caractère personnel en vue de leur rapprochement avec des données liées à leur activité en ligne. A noter que le rapprochement de données, qui constitue un traitement au sens du RGPD[1], consiste à mettre en relation des informations provenant d'ensembles de données distincts.

Ainsi, au sens du législateur français, le rapprochement de données en ligne de personnes situées en France doit systématiquement s'analyser comme un suivi des personnes au sens de l'article 3 du RGPD. Cela va pourtant à l'encontre de la position du Comité européen de la protection des données (CEPD) qui considère que la collecte ou l'analyse en ligne de données à caractère personnel relative à des personnes situées dans l'Union européenne ne doit pas être automatiquement considérée comme un « suivi » au sens de l'article 3 du Règlement général sur la protection des données[2].


L'objectif d'Eric Bothorel, qui a déposé l'amendement proposant la modification du champ d'application de la Loi Informatique et Libertés, était de « combler un vide juridique »[3] et de « préciser le champ d'applicabilité du RGPD »[4]. C'est chose faite puisqu'avec ces modifications, le RGPD s'applique désormais à des sociétés qui, comme LUSHA SYSTEMS INC., réalisent des rapprochements de données en ligne de personnes situées en France. Cela fait en effet écho à une délibération en date du 20 décembre 2022[5] aux termes de laquelle la formation restreinte de la CNIL, contrairement à la position du rapporteur, avait considéré que le RGPD n'était pas applicable à la société LUSHA SYSTEMS INC. qui commercialise une extension sur les navigateurs web permettant de récupérer les coordonnées professionnelles de profils visités sur LinkedIn ou sur Salesforce.com. En effet, la formation restreinte de la CNIL avait considéré que le simple rapprochement entre des données de contact professionnelles et l'identité de personnes dont le profil est visité en ligne ne pouvait s'assimiler à une opération de suivi du comportement des personnes au sens de l'article 3 du RGPD.

> Nouveaux pouvoirs pour la CNIL

- Tenue du registre des organisations altruistes en matière de données (article 26 du Règlement sur la gouvernance des données (DGA)). Les organisations altruistes sont des organismes du secteur public ou des personnes morales sans but lucratif qui mettent à disposition du public des données. Une fois reconnu et publié sur le registre tenu par la CNIL comme une organisation altruiste (moyennant le respect de certaines obligations comme la sécurité et la transparence), l'organisme pourra utiliser un logo commun conçu par l'Union européenne.
- Pouvoir de supervision et pouvoir de sanction s'agissant du respect des obligations prévues aux articles 26.1.d, 26.3 et 28.2 du Règlement sur les services numériques (DSA), à savoir l'interdiction des publicités fondées sur le profilage de mineurs ou réalisé à partir de données sensibles au sens de l'article 9 du RGPD et l'obligation renforcée d'information sur les publicités diffusées sur les plateformes en ligne.

- En matière de droit des nouvelles technologies





> **Renforcement des sanctions pénales en matière de haine en ligne, cyberharcèlement ou d'autres infractions graves** (pédopornographie, proxénétisme, dérives sectaires, menaces contre des élus, etc.)

- **Nouvelle peine de suspension des réseaux sociaux** : le juge peut désormais prononcer une peine complémentaire de suspension des réseaux sociaux pour six mois (voire un an en cas de récidive). Le réseau social qui ne bloquerait pas le compte suspendu encourt une amende de 75 000 euros.
- **Création d'un nouveau délit d'« outrage en ligne »** pour la diffusion de propos qui portent atteinte à la dignité d'une personne, présentent un caractère injurieux, dégradant ou humiliant, ou qui créent une situation intimidante, hostile ou offensante. La publication en ligne d'un montage à caractère sexuel réalisé avec les paroles ou l'image d'une personne (*deepfake*), sans son consentement est plus sévèrement réprimée (jusqu'à deux ans d'emprisonnement et 60 000 euros d'amende).

> **Modification du Code de la consommation et ajout d'un délit pénal pour les fournisseurs de place de marché (*marketplaces*) qui ne respecteraient pas leurs obligations issues du Règlement sur les services numériques (DSA)** (conception, organisation ou exploitation de l'interface, traçabilité des professionnels utilisant la plateforme, information des consommateurs) : un tel manquement peut être puni de deux ans d'emprisonnement et d'une amende de 300 000 euros (le montant de l'amende pouvant atteindre jusqu'à 6% du chiffre d'affaires mondial de la place de marché, de manière proportionnée aux avantages tirés du délit).

En cas d'infraction, la DGCCRF peut demander au juge d'enjoindre la place de marché à se mettre en conformité avec une astreinte journalière ne pouvant excéder 5% du chiffre d'affaires mondial hors taxes journalier de ladite place de marché. Le texte crée également une peine complémentaire d'interdiction d'exercice d'une profession commerciale ou industrielle pour les personnes physiques pour une durée maximale de cinq ans.

En application du Règlement sur les services numériques (DSA), l'ARCOM est désignée comme « coordinateur des services numériques ». L'ARCOM est donc chargée de la coordination entre les différentes autorités nationales compétentes (CNIL, DGCCRF) pour (i) assurer la mise en œuvre du Règlement sur les services numériques (DSA) au niveau national, (ii) siéger au sein d'un Comité européen des services numériques[6] et (iii) participer à la surveillance des très grandes plateformes en ligne et des très grands moteurs de recherche soumis aux obligations du Règlement européen.

> **Meilleur encadrement des escroqueries en ligne et les tentatives d'accès frauduleux aux coordonnées personnelles ou bancaires en application du Règlement sur les marchés numériques (DMA)** : la loi prévoit un dispositif de cybersécurité anti-arnaques qui consiste à faire afficher par le navigateur internet un message d'alerte qui avertira les utilisateurs lorsque, après avoir reçu un SMS ou un courriel frauduleux, ils s'apprentent à se diriger vers un site malveillant. Ce message renverra vers un site officiel de l'État.

Par ailleurs, la DGCCRF se voit dotée de pouvoirs pour mettre en demeure l'éditeur du site malveillant, notifier aux navigateurs internet l'adresse électronique du site et en cas d'impossibilité de contacter le site malveillant, enjoindre aux fournisseurs de services d'accès à internet ou aux fournisseurs du nom de domaine de bloquer l'accès au site pour une durée maximale de trois mois.

> **Encadrement des jeux à objets numériques monétisables (Jonum), à titre expérimental pour une durée de trois ans** : il s'agit des jeux vidéo qui fonctionnent grâce à la blockchain et aux NFT, dans lesquels l'achat d'objets numériques permet de jouer, de progresser dans le jeu et de gagner de nouveaux objets numériques et pour lesquels il n'existait jusqu'à présent pas de régime juridique. La loi introduit une définition de ces nouveaux types de jeux. Les éditeurs de Jonum soumis au cadre expérimental devront notamment déclarer leurs offres de jeux à l'Autorité nationale des jeux, vérifier l'âge des joueurs (l'accès aux mineurs étant interdit), prévenir l'addiction des joueurs et conserver les données relatives aux joueurs afin d'identifier les fraudes, lutter contre le blanchiment d'argent et le financement du terrorisme. Les récompenses et les objets numériques gagnés sont encadrés et ne peuvent être cédés à l'entreprise de jeu qui les a émis.

- **En matière de communication audiovisuelle**

> **Renforcement des pouvoirs de l'ARCOM en matière de régulation des contenus pornographiques, de contenus présentant des actes de torture et de barbarie et en matière de lutte contre la désinformation**

- En matière de régulation des contenus pornographiques : afin d'empêcher l'accès aux mineurs à ces contenus, l'ARCOM a la charge d'élaborer un référentiel général déterminant les exigences techniques auxquelles devraient répondre les systèmes de vérification d'âge sur des sites donnant accès à des contenus pornographiques, tout en respectant la vie privée des utilisateurs. En cas de non-respect de ce référentiel, l'ARCOM disposerait d'un pouvoir de mise en demeure et de sanction pécuniaire à l'encontre des éditeurs de sites pornographiques. L'ARCOM a le pouvoir de bloquer et de déréférencer, sans décision judiciaire préalable, tout site pornographique ainsi que le téléchargement de toute application, ne vérifiant pas l'âge des internautes français.
- En matière de régulation des contenus présentant des actes de torture et de barbarie : l'ARCOM a le pouvoir, à titre expérimental et pour une durée de deux ans, d'ordonner le retrait rapide, le blocage ou le

déréférencement par une plateforme en ligne de contenus présentant des actes de torture et de barbarie.

- En matière de lutte contre la désinformation : l'ARCOM pourra notamment enjoindre à de nouveaux opérateurs de stopper sous 72 heures la diffusion sur internet d'un média étranger frappé par des sanctions européennes (tels que Sputnik ou Russia Today France). En cas de manquement, l'ARCOM dispose d'un pouvoir de sanction lui permettant d'ordonner le blocage du site concerné et infliger une amende pouvant aller jusqu'à 4% du chiffre d'affaires de l'opérateur ou 250 000 euros.

> Nouvelles obligations pour les hébergeurs de contenus pornographiques

- **Obligations de retirer les contenus pornographiques en cas de signalement par une personne figurant dans ces vidéos**, en raison d'une violation des conditions contractuelles conclues entre un acteur et un producteur.
- **Obligation d'afficher un message d'avertissement avant et pendant la diffusion de contenus** simulant un viol, une agression sexuelle ou de la pédopornographie, rappelant le caractère illégal des comportements ainsi présentés.

[1] [Article 4, paragraphe 2 du RGPD](#).

[2] CEPD, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3) (page 22).

[3] A noter que l'amendement initial prévoyait un champ d'application beaucoup plus étendu de la Loi Informatique et Libertés puisqu'il était prévu que les titres I et II de la Loi Informatique et Libertés s'appliquent aux traitements de données de personnes qui se trouvent sur le territoire français par un responsable du traitement ou un sous-traitant établi en dehors de l'Union européenne qui réalise des traitements lorsque les données sont collectées sur le territoire français, en particulier s'il s'agit de données stockées sur des équipements terminaux de personnes physiques résidant sur ce territoire et que ces traitements ont pour finalité de mettre ces données à disposition de tiers, à titre onéreux ou gratuit.

[4] <https://www.assemblee-nationale.fr/dyn/16/amendements/1674/AN/190>

[5] Délibération de la formation restreinte n°SAN-2022-024 du 20 décembre 2022 concernant la société LUSHA SYSTEMS INC.

[6] Le Comité européen pour les services numériques est un groupe consultatif indépendant composé des coordinateurs pour les services numériques et de la Commission européenne. Il veille à l'application du DSA de manière cohérente dans l'ensemble de l'Union européenne. Il édicte des lignes directrices, publie des rapports annuels sur les principaux risques systémiques et les bonnes pratiques en matière d'atténuation de ces risques.

