



GOUVERNEMENT

*Liberté
Égalité
Fraternité*

Vade-mecum sur la sensibilité des données au sens de l'article 31 de la loi SREN

Ce vade-mecum a pour objet de préciser la notion de données d'une sensibilité particulière au sens de la loi visant à sécuriser et à réguler l'espace numérique du 21 mai 2024, dite loi SREN. Les dispositions de cette loi ne s'appliquent que lorsqu'un système d'information a recours à un service d'informatique en nuage (cloud) commercial. Lorsque les données d'un service ou d'un opérateur de l'Etat sont hébergées ou traitées sur hébergement en nuage commercial, le recours à une offre dite « de confiance » n'est pas systématiquement obligatoire. Une analyse doit être réalisée au cas par cas par l'administrateur de ces données afin de déterminer si elles relèvent ou non du champ d'application de l'article 31 de la loi SREN¹. Des exemples concrets sont ici proposés afin d'éclairer autant que possible cette analyse. La mise en œuvre de ce vade-mecum fait l'objet d'un accompagnement par la DINUM.

I. Rappel du cadre législatif et réglementaire

L'[article 31 de la loi n°2024-449 du 21 mai 2024](#) visant à réguler et sécuriser l'espace numérique (loi SREN) prévoit que dans le cas où « les administrations de l'État, ses opérateurs dont la liste est annexée au projet de loi de finances ainsi que les groupements d'intérêt public comprenant les administrations ou les opérateurs mentionnés précédemment et dont la liste est fixée par décret en Conseil d'Etat », ont recours à un service d'informatique en nuage commercial, les systèmes informatiques, incluant les éléments nécessaires à leur résilience, doivent respecter le cadre suivant :

« Si le système ou l'application informatique concerné traite de données d'une sensibilité particulière, qu'elles soient à caractère personnel ou non, et si leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle, l'administration veille à ce que le service d'informatique en nuage fourni par le prestataire privé mette en œuvre des critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre ».

¹ L'article 31 s'applique lors du recours à un prestataire privé uniquement, les autres situations sont décrites dans la circulaire d'utilisation de l'informatique en nuage par l'Etat du 31 mai 2023

Le décret d'application de l'article 31 précité vient préciser les critères de sécurité et de protection applicables. A cet effet, la France dispose de la qualification nationale dénommée SecNumCloud, attribuée par l'ANSSI aux prestations de services d'informatique en nuage, comprenant notamment des exigences visant à assurer une protection adéquate contre les lois non européennes à portée extraterritoriale. Une certification européenne d'un niveau au moins équivalent, attestant de la mise en œuvre des mesures et procédures nécessaires à cette conformité, pourra également être utilisée lorsqu'une telle certification sera adoptée au niveau européen. Les solutions répondant à ces exigences sont dénommées dans le document « cloud de confiance ».

Pour aller plus loin :

Le document « [Recommandations pour l'hébergement des SI sensibles dans le cloud | ANSSI](#) » précise, en fonction du type de système d'information, de la sensibilité des données et du niveau de la menace, les types d'offres cloud à privilégier. L'utilisation d'un hébergement de confiance ne dispense pas de se conformer aux autres réglementations applicables dans le cadre d'une politique de sécurité des données.

II. Analyse à mener

Pour les administrations concernées (administrations de l'État, opérateurs de l'État, GIP listés par décret), **cette obligation ne concerne que des données soumises à deux conditions cumulatives** :

1. Elles présentent une sensibilité particulière, c'est-à-dire que les données qui :

« relèvent de secrets protégés par la loi, notamment au titre des [articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration](#) » (cf. Annexe) ;

ou sont « nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes. »

2. L'impact de leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes, ou à la protection de la propriété intellectuelle.

La satisfaction de cette double condition doit faire l'objet d'une analyse au cas par cas dans la continuité de la circulaire du 31 mai 2023 relative à l'actualisation de la doctrine d'utilisation de l'informatique en nuage par l'Etat qui précise notamment qu'une violation de données « *devra être évaluée sous chaque angle des critères de sécurité élémentaires, à savoir : la confidentialité, l'intégrité, la disponibilité, voire la traçabilité. Il pourra être pris en compte dans cette analyse différentes natures d'impacts possibles et par exemple : impacts opérationnels, politiques, économiques, juridiques, environnementaux, patrimoniaux* ».

Une violation de données peut concerner en pratique de nombreuses situations, au-delà du seul accès aux données par des autorités publiques d'États tiers non autorisés. Ainsi, la Commission nationale de l'informatique et des libertés précise, s'agissant des données personnelles, qu'une violation de données « *se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée à des données [...] transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à des données de manière accidentelle ou illicite* », et que cela peut inclure « *tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité* » des données.

Ainsi, à titre d'illustration, et sans prétention d'exhaustivité, **toute action tendant à rendre indisponibles des données, bloquer ou empêcher le fonctionnement d'un système d'information ou l'altération des données est susceptible de constituer une violation des données**. L'analyse au cas par cas doit ainsi porter, d'une part, sur la nature des données traitées (cf. annexe, notamment les données personnelles), et d'autre part, sur l'impact d'une éventuelle violation pour déterminer si celle-ci est **susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle**. A ce titre, l'analyse de l'impact d'une violation de données doit intégrer la capacité à détecter cette violation, à les corriger dans des délais suffisamment courts dans le cas d'une altération ou à rendre de nouveau les données accessibles en cas de données rendues indisponibles.

Ce risque d'atteinte doit être suffisamment caractérisé, et non simplement hypothétique, et constituer la conséquence directe de la violation des données sensibles contre laquelle il est entendu se prémunir.

Un tel risque peut être lié à l'accès, par des autorités de pays tiers non habilitées, à des échanges ou documents relatifs à des missions relevant de la souveraineté nationale, dès lors qu'un tel accès pourrait faire naître des risques pour l'ordre public ou la sécurité nationale.

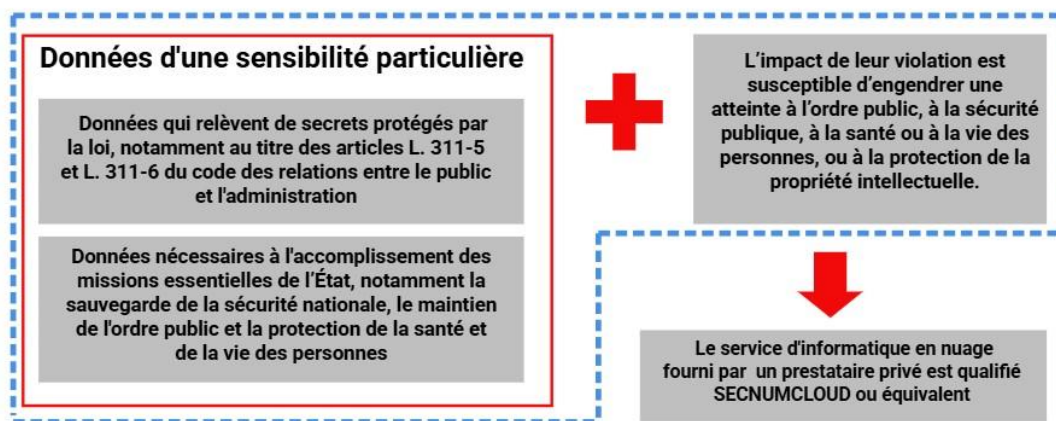
L'atteinte peut également porter sur un risque pour la santé ou la vie des personnes (par exemple, des risques pour la sécurité des approvisionnements de santé en particulier pour les produits figurant sur la liste de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) soumis à des obligations particulières, la divulgation massive de données de santé, etc.).

Enfin, les atteintes à la protection de la propriété intellectuelle sont également concernées. Sur ce point, le Conseil d'État identifie, dans son étude annuelle de 2024 sur la souveraineté, trois catégories de risques, liés en particulier à la propriété industrielle et plus largement la protection du patrimoine scientifique et technique de la Nation, portant sur des actions malveillantes d'espionnage et de sabotage, la captation de la propriété intellectuelle et du travail scientifique opéré par les universités et centres de recherche, et la prise de contrôle du capital de certaines entreprises stratégiques.

Nota bene - Extension de l'exigence de protection des données sensibles au système d'information dans son ensemble

Dès que lors que certaines données traitées remplissent les deux conditions précitées, l'ensemble des données localisées sur la même infrastructure et traitées par le système d'information concerné doit faire l'objet d'un hébergement conforme aux dispositions de l'article 31, sous réserve qu'un cloisonnement efficace des données ne puisse être techniquement, ou sans remettre en cause l'équilibre économique du contrat, mis en œuvre.

En résumé :



III. Exemples de systèmes d'information analysés au regard de l'obligation résultant de l'article 31 de la loi SREN

1. Des SI pour lesquels l'analyse conduit à la nécessité du recours au cloud de confiance

Il est notamment impératif, au titre des dispositions de l'article 31 de la loi SREN, de protéger de manière adéquate les SI qui traitent des données d'une sensibilité particulière telles que définies précédemment si leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle. Cela peut comprendre par exemple :

- Les SI contenant des données nécessaires à l'exercice des missions régaliennes de l'État, particulièrement au sein des services du Premier ministre, des ministères de **l'Intérieur, des Armées, de la Justice, de l'Economie et des Finances ou de l'Europe et des Affaires étrangères**. Tous les systèmes d'information de ces ministères ne sont toutefois pas, par nature, inclus dans le champ d'application de la loi mais toutes les données concourant à l'exercice de leurs missions régaliennes et assurant leur continuité devront dans ce cas respecter les exigences de la loi.

- Les SI des ministères contenant des données utilisées pour une **activité relevant de la sécurité nationale ou de la protection de la santé et la vie des personnes**, s'ils traitent des données d'une sensibilité particulière, et notamment s'agissant des domaines suivants :
 - o Chaînes d'**alertes sanitaires** du ministère chargé de l'agriculture et de l'alimentation
 - o Chaînes d'alertes sur les **dangers environnementaux** (pollution, radioactivité...) du ministère chargé de l'environnement
 - o Systèmes d'information liés au **secours** (SAMU, antipoison...) du ministère chargé de la santé et des solidarités.

- Les **messageries et outils collaboratifs des administrations**, ceux-ci étant susceptibles de contenir des données nécessaires à l'accomplissement des missions essentielles de l'État et/ou relevant de secrets protégés par la loi, et que leur violation est susceptible d'engendrer une atteinte à l'ordre public, soit par la divulgation des données qu'elles contiennent (dans le corps du mail ou dans les pièces jointes), soit par le blocage de l'accès à ces données, empêchant ainsi la continuité de l'action publique.

- **Outils d'élaboration d'actes réglementaires et de décisions administratives**, qui sont essentiels à l'accomplissement d'une mission essentielle de l'Etat et dont l'altération ou l'indisponibilité pourrait engendrer un trouble à l'ordre public en empêchant une décision par exemple .

- **Outils comportant des données sur la conduite de négociations internationales dont la violation par divulgation conduirait à un affaiblissement de la position française et in fine une décision défavorable entraînant un trouble à l'ordre public.**

- Systèmes d'information relatifs à **la paye des agents publics** dans la mesure où ils contiennent des données à protéger (adresse des agents exerçant des missions régaliennes par exemple) et leur arrêt ne permettrait plus d'assurer la continuité du service public.

2. Des SI pour lesquels l'analyse ne conduit pas à la nécessité du recours au cloud de confiance

Certains SI des administrations, en raison de la nature non sensible des données traitées ou, si elles sont sensibles, de l'absence de trouble à l'ordre public de leur violation, n'apparaissent pas de nature à relever de l'obligation prévue à l'article 31 de la loi SREN. Toutefois, il convient de rappeler que toutes les autres obligations de protection des données telles que celles imposées par le RGPD ou la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, continuent de s'appliquer. L'analyse des systèmes d'information qui ne seraient pas soumis aux dispositions de l'article 31 de la loi SREN relève *in fine* de la responsabilité du ministre concerné.

A titre d'exemple de SI n'étant a priori pas soumis à l'obligation posée par l'article 31 de la loi SREN, on pourrait citer les SI de **diffusion d'informations institutionnelles (portail, API) à destination du public**, en dehors de ceux qui sont utilisés pour la communication de crise ou d'alertes mettant en jeu la sûreté des biens et des personnes.

Il convient de souligner que, même en dehors du champ d'application de la loi SREN, il est nécessaire, si cela est justifié au cas par cas, d'introduire dans les appels d'offres portant sur l'achat de solutions numériques, des critères/clauses liés à la sécurité et la souveraineté.

Exemples d'analyse de différents cas d'usage au regard de l'art. 31 de la loi SREN

Nature des données	1er critère : données particulièrement sensibles	2ème critère : risque d'atteinte à la sécurité ou à l'ordre public, à la santé ou à la vie des personnes, ou à la protection de la propriété intellectuelle	Cloud de confiance requis
<p>Données des applications d'aide au traitement des dossiers judiciaires en matière criminelle (exemple : solution d'IA pour le Parquet national antiterroriste)</p> <p><i>> Données sensibles, et dont la violation par divulgation pourrait entraîner la nullité des procédures et une atteinte à l'ordre public</i></p>	<p>Oui (secrets protégés / missions essentielles)</p>	<p>Oui</p>	<p>Oui</p>
<p>Données des applications d'aide au traitement des dossiers judiciaires en matière civile (exemple : solution d'IA pour assister les juges aux affaires familiales)</p> <p><i>> Données sensibles, et dont la violation par divulgation pourrait entraîner la nullité des procédures et une atteinte à l'ordre public</i></p>	<p>Oui (secrets protégés / missions essentielles)</p>	<p>Oui</p>	<p>Oui</p>
<p>Données des portails de communication institutionnelle à destination du grand public</p> <p>Exemple : données du site www.viepublique.fr</p> <p><i>> Données non sensibles</i></p>	<p>Non</p>	<p>Non</p>	<p>Non</p>
<p>Données des applications de régulation des interventions du SAMU (ministère de la Santé)</p> <p><i>> Données sensibles, dont la violation par indisponibilité entraînerait un risque d'atteinte à la santé des populations</i></p>	<p>Oui (secrets protégés / missions essentielles)</p>	<p>Oui</p>	<p>Oui</p>

<p>Données relatives à la paye des agents publics (interministériel) <i>> Données sensibles, et dont la violation (blocage du versement) engendrerait un trouble probable à l'ordre public</i></p>	Oui (secrets protégés / missions essentielles)	Oui	Oui
<p>Données relatives aux bulletins de note des établissements scolaires (ministère EN) <i>> Données sensibles mais dont la violation n'engendrerait pas de manière certaine une atteinte à la sécurité ni à l'ordre public, ni à la santé ou à la vie des personnes, ni à la propriété intellectuelle</i></p>	Oui (secrets protégés)	Non	Non
<p>Données des administrations contenant des informations stratégiques en matière de propriété intellectuelle. (exemples : résultat des recherches de l'INSERM, brevets de l'INPI) <i>> Données sensibles dont la violation par divulgation entraînerait une atteinte à la propriété intellectuelle</i></p>	Oui (secrets protégés)	Oui	Oui
<p>Données relatives au plan cadastral (DGFIP) <i>> Données sensibles mais dont la violation n'engendrerait pas de manière certaine une atteinte à la sécurité ni à l'ordre public, ni à la santé ou à la vie des personnes, ni à la propriété intellectuelle</i></p>	Oui (secrets protégés)	Non	Non
<p>Données relatives au contrôle de légalité exercé par les préfetures sur les délibérations des collectivités locales (ministère de l'Intérieur) <i>> Données sensibles mais dont la violation n'engendrerait pas de manière certaine une atteinte à la sécurité ni à l'ordre public, ni à la santé ou à la vie des personnes, ni à la propriété intellectuelle</i></p>	Oui (secrets protégés / missions essentielles)	Non	Non
<p>Données des systèmes d'information répertoriant les crimes et délits (ministère de l'Intérieur) <i>> Données sensibles, et dont la violation par divulgation engendrerait une atteinte à la sécurité et à l'ordre public</i></p>	Oui (secrets protégés / missions essentielles)	Oui	Oui
<p>Données issues des systèmes d'information mis en œuvre dans les chaînes d'alerte sanitaire et de secours <i>> Données sensibles, dont la violation par indisponibilité ou altération entraînerait un risque d'atteinte à la santé des populations</i></p>	Oui (secrets protégés / missions essentielles)	Oui	Oui

ANNEXE

Données relevant de secrets protégés par la loi, notamment au titre des [articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration](#)

Ces données sont notamment celles qui sont couvertes par les secrets protégés par la loi suivants :

- secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;
- secret de la défense nationale ;
- secret de la conduite de la politique extérieure ;
- secret lié à la sûreté de l'Etat, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations ;
- secret lié à la monnaie et au crédit public ;
- secret des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ;
- secret de la recherche et de la prévention d'infraction ;
- sous réserve de l'[article L. 124-4 du code de l'environnement](#), aux autres secrets protégés par la loi, notamment le secret statistique, la protection de l'environnement ;
- secret médical ;
- protection de la vie privée ;
- secret des affaires.