LIVRABLE 1 - DEFINITION DE LA DONNEE SENSIBLE

Sous-Groupe.1 du GT3 du Comité Stratégique de Filière

Synthèse : les recommandations du Sous-Groupe 1 du CSF

1. Identifier les données sensibles pour mieux les protéger. Les organismes, publics comme privés, doivent se doter des outils nécessaires pour identifier et qualifier les données sensibles qu'ils détiennent. Cette démarche suppose un niveau de maturité suffisant en matière de gouvernance des données, ainsi qu'une cartographie régulière de leur patrimoine informationnel.

2. Dépasser la définition issue du droit des données personnelles. La notion de donnée sensible ne saurait se limiter aux catégories particulières de données visées à l'article 9 du règlement (UE) n° 2016/679 du 27 avril 2016 (RGPD). Elle doit englober l'ensemble des données, personnelles et non personnelles, dont la divulgation ou l'altération serait susceptible de porter atteinte aux intérêts des individus, des entreprises ou de la nation. La définition retenue par le Sous-Groupe 1 s'inscrit dans le cadre plus large du règlement (UE) 2023/2854 du 13 décembre 2023 (dit « Data Act »), et tient compte des évolutions en cours dans le cadre de la proposition de de règlement « Digital Omnibus » de la Commission européenne.

3. Adopter une approche industrielle fondée sur les flux de données. La qualification d'une donnée sensible ne peut faire abstraction des trois flux structurant le traitement des données au sein d'un organisme : les flux entrants (données reçues), la gestion interne (données traitées) et les flux sortants (données transmises à des tiers). Cette approche par les flux constitue le socle d'une qualification contextualisée.

4. Intégrer la temporalité dans la gouvernance des données sensibles. La sensibilité d'une donnée évolue dans le temps. Plus une donnée est divulguée tôt, plus le risque peut être élevé. Certaines données perdent ainsi progressivement leur caractère sensible à mesure qu'elles deviennent obsolètes. Cette réalité impose une gouvernance active : les données sensibles doivent faire l'objet d'un suivi tout au long de leur cycle de vie, avec des durées de conservation adaptées aux obligations réglementaires sectorielles applicables.

5. Prendre en compte la combinaison et la destination des données Des données anodines prises isolément peuvent devenir sensibles par leur combinaison ou par leur destination. L'effet mosaïque – illustré notamment par les cas Strava et data.gouv.fr – en est un bon exemple. Cette réalité conduit à reconsidérer certaines logiques d'Open Data, non pour les remettre en cause, mais pour y intégrer des garde-fous proportionnés aux risques identifiés.

6. Mettre en œuvre des mesures de protection adaptées et proportionnées. La qualification de donnée sensible entraîne l'obligation de mettre en œuvre des mesures techniques, opérationnelles et organisationnelles proportionnées aux risques. Parmi ces mesures, l'anonymisation occupe une place centrale – comme en témoignent le décret n° 2025-840 du 22 août 2025 et les débats sur la caviardisation des décisions de justice.

7. Recourir à des acteurs souverains pour le traitement des données sensibles. Le traitement et l'hébergement de données sensibles appellent le recours à des acteurs offrant des garanties d'immunité vis-à-vis des législations étrangères à portée extraterritoriale. La loi SREN a posé ce principe pour les organismes publics, en lien avec le référentiel SecNumCloud de l'ANSSI. Le Sous-Groupe 1 recommande d'étendre cette exigence aux organismes privés traitant des données sensibles, en retenant la qualification de la donnée comme critère déclencheur.

8. Structurer une gouvernance et développer les compétences dédiées. La gestion des données sensibles ne peut reposer sur le seul délégué à la protection des données. Elle appelle des compétences spécialisées et une gouvernance intégrée au sein des organisations. Le développement de ces profils

constitue par ailleurs un véritable gisement d'emplois, à la hauteur des enjeux que représente la donnée sensible dans l'économie numérique.

Introduction

La donnée occupe désormais une place centrale dans les stratégies économiques et les politiques publiques. La protection des données les plus sensibles constitue, dans ce contexte, un impératif croissant. Encore faut-il que les organismes qui les détiennent disposent des outils nécessaires pour les identifier et les qualifier.
C'est l'objet du présent livrable, élaboré par le Sous-Groupe 1 du GT3 du Comité Stratégique de Filière : proposer une définition claire et opérationnelle de la « donnée sensible », conciliant sécurité juridique et conditions favorables à l'innovation.

La définition retenue est volontairement restrictive, afin de ne pas soumettre à ce régime un trop grand nombre de données et d'éviter ainsi tout effet de blocage sur les échanges et l'innovation.

Le présent document (1) propose une définition de la « donnée sensible » et (2) précise, terme par terme, les choix opérés pour cette définition.

1. Proposition de définition de la « donnée sensible »

À l'issue de ses travaux, le Sous-Groupe 1 du CSF retient la définition suivante :

> « *On entend par donnée sensible une donnée tant personnelle que non personnelle qui par sa nature, sa destination ou par combinaison, peut nécessiter un consentement des personnes qui en sont titulaires. Les données sensibles nécessitent d'être protégées pendant tout leur cycle de vie par les acteurs publics et privés en particulier contre l'occurrence d'un risque significatif en mettant en œuvre des mesures techniques, opérationnelles et organisationnelles* ».

2. Précisions sur la définition de la donnée sensible

3.1 Avant-propos : qualifier la donnée sensible pour mieux la protéger

La notion de donnée sensible souffre d'une définition incertaine et peu stabilisée, source d'insécurité juridique pour les acteurs qui y sont soumis. Si la tentation est grande de recourir à une énumération – données RH, brevets, actifs de R&D, actifs numériques stratégiques – cette approche se heurte à une difficulté plus fondamentale : de nombreuses organisations méconnaissent l'étendue réelle de leur patrimoine de données. Le cloisonnement interne et le faible niveau de maturité de certains organismes en matière de gouvernance des données expliquent en partie ces angles morts. Les audits de données, qu'elles soient sensibles ou non, demeurent encore trop rares.

Il ressort des travaux du Sous-Groupe 1 que les acteurs de l'écosystème partagent trois préoccupations consubstantielles à la notion de donnée sensible :

1. la protection contre l'application de législations à portée extraterritoriale ;
2. la protection contre les risques cyber ;
3. la protection contre les risques de dépendance et de rupture de service.

Le présent document vise à fournir aux industriels un cadre concret pour qualifier leurs données et déterminer les conditions appropriées de leur traitement et de leur stockage.

3.2 « une donnée tant personnelle que non personnelle » : une notion qui dépasse le cadre des données à caractère personnel

Il serait réducteur de limiter la notion de donnée sensible aux seules données à caractère personnel. Le règlement UE n°2016/679 du 27 avril 2016 (dit « RGPD ») définit certes, en son article 9, paragraphe 1, une catégorie de données dites « sensibles » – *données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques, biométriques, de santé ou relatives à la vie sexuelle ou à l'orientation sexuelle* – dont le traitement est en principe interdit, sauf à relever de l'une des exceptions prévues à l'article 9, paragraphe 2.

Mais cette définition, centrée sur la personne physique, ne couvre pas l'ensemble des données qui méritent, en pratique, d'être qualifiées de sensibles et protégées en conséquence.

Le Sous-Groupe 1 a donc retenu une acception plus large, s'inscrivant dans le cadre du règlement (UE) n° 2023/2854 (dit « Data Act »), qui définit la donnée comme « *toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* ». Cette approche permet d'englober l'ensemble du patrimoine de données des organisations, indépendamment de leur nature personnelle ou non personnelle. Elle tient également compte des évolutions en cours dans le cadre de la proposition de règlement « Digital Omnibus » présentée par la Commission européenne, qui esquissent une possible révision de la définition de la donnée à caractère personnel.

À titre d'illustration, pourraient ainsi accéder à la qualification de donnée sensible :

- les données commerciales : informations relatives à l'activité économique d'une entreprise dont la divulgation est susceptible de nuire à sa réputation ou à ses relations clients ;
- les données industrielles : informations techniques telles que des secrets de fabrication dont la divulgation est susceptible de porter atteinte à la compétitivité de l'entreprise ;
- les données protégées par la propriété intellectuelle, eu égard à l'importance stratégique de leur protection.

3.3 « qui par sa nature, sa destination ou par combinaison » : sur l'approche par cercle concentrique[1]

À l'issue de ses travaux, le Sous-Groupe 1 a convergé vers une approche industrielle de la donnée sensible structurée autour des trois flux de données de l'organisme :

- **Flux entrants (input)** : données sensibles reçues par l'organisme – données RH, fiscales, comptables, données issues de l'INPI, etc. Il s'agit de données sensibles par destination ;
- **Gestion interne** : données sensibles traitées en interne – portefeuille clients, données de R&D, etc. ;
- **Flux sortants (output**) : données sensibles transmises dans le cadre des relations avec des tiers – données contractuelles, données couvertes par un accord de confidentialité (NDA), données déclarées auprès d'administrations telles que l'URSSAF, etc.

Elle suppose, de la part de l'organisme, un niveau de maturité suffisant en matière de gouvernance des données. Cette exigence est d'autant plus pressante que les volumes traités sont appelés à croître considérablement sous l'effet du développement de l'intelligence artificielle.

Des données anodines prises isolément peuvent devenir sensibles par leur combinaison ou par leur destination. Les deux illustrations suivantes permettent d'en mesurer concrètement la portée.

> *Illustration – Données sensibles par destination : l'Open Data et le projet de Jumeau numérique présenté par l'IGN, le Cerema, Inria et 1Spatial France*
>
> Au Salon des Maires de novembre 2025, l'IGN, Inria, le Cerema et 1Spatial France ont annoncé le développement d'un jumeau numérique territorial, dont le déploiement est prévu fin 2026[2]. Inscrite dans la stratégie européenne des « *Local Digital Twins* », cette initiative vise à faciliter la prise de décision des collectivités en leur ouvrant un accès élargi à la donnée géographique.
> Cette annonce illustre une tension inhérente à la notion de donnée sensible par destination. Une donnée cartographique, anodine à l'échelon local, peut devenir sensible dès lors qu'elle est agrégée ou accessible à un tiers malveillant – qu'il s'agisse de préparer une attaque cyber ou de porter atteinte à la sécurité physique d'un site ou d'une personne. C'est précisément le principe de l'OSINT (*Open Source Intelligence*) : l'exploitation de données publiques, combinées entre elles, peut produire des renseignements opérationnels à des fins malveillantes.
> Des mesures techniques telles que la restriction d'accès par adresse IP ont été envisagées, mais leur efficacité reste limitée – l'usage d'un VPN suffit à les contourner. L'Open Data n'est pas en cause en tant que telle ; c'est son accessibilité sans distinction d'origine qui soulève la question. Ce cas illustre précisément ce que la définition retenue par le Sous-Groupe 1 entend couvrir :

[1] La doctrine recourt fréquemment à l'image des cercles concentriques pour représenter cette gradation. Au centre se trouvent les données intrinsèquement liées à la personne physique, dont la violation porterait atteinte à la dignité humaine. S'y articulent ensuite les données générées par les interactions de l'individu avec les institutions - état civil, éducation nationale, documents d'identité, autorisations administratives - dont la protection revêt une importance particulière, comme en témoigne la recrudescence des attaques par rançongiciel ciblant les collectivités territoriales, notamment durant et après la période pandémique.

[2] Source : IGN, « Jumeau numérique de la France et de ses territoires : présentation au Salon des maires 2025 », communiqué de presse, 18 novembre 2025, disponible sur : https://www.ign.fr/institut/espace-presse/jumeau-numerique-de-la-france-et-de-ses-territoires-presentation-au-salon-des-maires-2025 (consulté le 24 mars 2026).

une donnée peut ne pas être sensible par nature, mais le devenir par destination ou par combinaison.

Illustration – L'effet mosaïque : des données anodines devenant sensibles par combinaison

L'application Strava, utilisée par plus de 150 millions de personnes, en fournit une illustration saisissante. Les données de géolocalisation partagées publiquement par les gardes du corps de dirigeants politiques ont permis d'inférer la tenue de réunions confidentielles, révélant des déplacements à finalité politique qui auraient dû demeurer secrets[3]. Ce risque a été formellement identifié dans un mémo du Pentagone[4]. Il ne s'agit pas ici d'une violation de données au sens technique du terme, mais de paramètres de confidentialité insuffisamment protecteurs dont les détenteurs n'avaient pas mesuré les implications.

3.4. « Les données sensibles nécessitent d'être protégées pendant tout leur cycle de vie par les acteurs publics et privés » : gouvernance et temporalité

La sensibilité d'une donnée n'est pas une caractéristique figée : elle évolue dans le temps. Plus une donnée est divulguée tôt, plus le risque d'atteinte à sa valeur ou à son intégrité est élevé. Un brevet ou un secret d'affaires susceptible d'influer sur un cours boursier perd progressivement de sa portée au fil des évolutions technologiques. La temporalité constitue donc un facteur déterminant dans l'appréciation du risque.

Cette réalité appelle une gouvernance active de la donnée. Il ne s'agit pas de constituer un stock figé, mais un corpus vivant, régulièrement mis à jour et purgé selon les besoins. Cette approche demeure aujourd'hui l'apanage d'un nombre encore limité d'organismes disposant d'une maturité suffisante en matière de gestion des données.

À l'instar des données à caractère personnel au sens du RGPD, les données sensibles ne peuvent être conservées indéfiniment. Lorsqu'elles portent sur un savoir-faire devenu obsolète, leur protection accrue du fait de leur statut n'est plus justifiée. Certains secteurs imposent toutefois des durées de conservation spécifiques, répondant à des impératifs réglementaires distincts. Ainsi, un prestataire de vérification d'identité à distance (PVID) pratiquant le KYC peut conserver certaines données jusqu'à six ans au titre du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT). Dans le secteur bancaire, cette durée peut atteindre dix ans, les données étant couvertes par le secret bancaire institué par loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit (dite « loi bancaire »).

[3] M. UNTERSINGER, « Strava, une histoire émaillée de failles de sécurité », *Le Monde*, 27 octobre 2024, disponible sur : https://www.lemonde.fr/pixels/article/2024/10/27/strava-une-histoire-emaillee-de-failles-de-securite_6361676_4408996.html (consulté le 24 mars 2026).

[4] Mémo du Secrétaire adjoint à la Défense Patrick M. Shanahan, *Use of Geolocation-Capable Devices, Applications and Services*, Département de la Défense des États-Unis, 3 août 2018.

Illustration – Directive NIS2 et gestion du cycle de vie des données techniques

Un opérateur de services essentiels dans le secteur de l'énergie subit une intrusion sur son système d'information. En application de la directive (UE) 2022/2555 du 14 décembre 2022 (dite « NIS2 »), il est tenu de notifier l'incident à l'autorité compétente dans des délais stricts et de conserver les journaux d'événements et données techniques associés aux fins d'analyse post-incident. Ces données, hautement sensibles au moment de l'incident, voient leur sensibilité décliner progressivement une fois les mesures correctives déployées et l'incident clôturé. Leur conservation au-delà du délai réglementaire, sans réévaluation de leur niveau de protection, constitue précisément le type de risque que la gouvernance active du cycle de vie vise à prévenir.

3.5 « Contre l'occurrence d'un risque significatif » : le risque, une notion contextuelle et plurielle

Sur les risques significatifs

La notion de risque significatif ne se laisse pas définir de manière abstraite et universelle : elle est par nature contextuelle et varie selon les cadres réglementaires et les objectifs qu'ils poursuivent. Le risque au sens de la directive NIS2 – centré sur la continuité des services essentiels et la résilience des infrastructures critiques – ne recouvre pas la même réalité que le risque au sens du règlement (UE) 2023/2854 du 13 décembre 2023 (dit « Data Act »), qui s'attache davantage aux conditions d'accès et de partage des données. Cette hétérogénéité reflète également la pluralité des niveaux d'exposition : le risque peut affecter la nation dans son ensemble, les entreprises dans leur compétitivité ou leur continuité d'activité, ou les individus dans leurs droits fondamentaux et leur sécurité physique.

Le Sous-Groupe 1 du CSF n'entend pas, dans le cadre de ce premier livrable, proposer une définition exhaustive du risque significatif. Il renvoie sur ce point aux travaux qui seront menés dans la suite de ses réflexions.

Sur les définitions du droit positif français

Le Sous-Groupe 1 n'est pas le seul à avoir engagé une réflexion sur la définition de la donnée sensible. L'article 31 de la loi n° 2024-449 (dite « loi SREN ») en offre une illustration notable :

> *« 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. »*

À l'instar de la définition retenue par le Sous-Groupe 1, la loi SREN retient une acception de la donnée sensible qui ne se limite pas aux données à caractère personnel. Le raisonnement des rédacteurs s'articule ensuite en arborescence, prenant en compte les risques liés à l'ordre public, à la santé, à la propriété intellectuelle et à la vie des personnes.

Le Sous-Groupe 1 a, dans cette même veine, insisté sur la nécessaire prise en compte de l'État de droit. La protection des données sensibles ne saurait servir de prétexte à des mesures qui viendraient affaiblir des principes cardinaux tels que le chiffrement de bout en bout – principe réaffirmé à plusieurs reprises ces derniers mois, aussi bien dans les débats sénatoriaux relatifs à la transposition de la directive NIS2 et de la directive (UE) 2022/2557 du 14 décembre 2022 (dite « REC ») qu'à la mise en œuvre du règlement (UE) 2022/2554 du 14 décembre 2022 (dit « DORA ») via le projet de loi Résilience, que dans les discussions sur le projet de loi de lutte contre le narcotrafic, où la question de l'installation d'une backdoor à des fins de lutte contre la criminalité a suscité de vifs débats.

> *Illustration – Protocole MCP et accès aux données publiques : data.gouv.fr*
>
> Depuis le 25 février 2026, data.gouv.fr dispose d'un serveur MCP expérimental permettant à tout système d'IA d'interroger des jeux de données publics français[5]. La plateforme elle-même reconnaît que ce type d'outil est difficile à auditer. Le risque ne tient pas à l'accès aux données publiques en tant que tel, mais à l'impossibilité d'identifier le fournisseur du modèle d'IA qui y accède. L'autorité de protection des données luxembourgeoise a ainsi alerté, dès février 2025, sur les risques associés au modèle DeepSeek[6] : absence de représentant légal dans l'Union européenne, déficit de garanties au regard du RGPD, et implication potentielle d'acteurs étatiques dans le traitement des données. Or, rien dans le protocole MCP ne permet aujourd'hui d'empêcher un tel modèle d'accéder au serveur de data.gouv.fr. Dès lors que cet accès est étendu à des données sensibles, les risques se trouvent significativement démultipliés. du RGPD, et implication potentielle d'acteurs étatiques dans le traitement des données. Or, rien dans le protocole MCP ne permet aujourd'hui d'empêcher un tel modèle d'accéder au serveur de data.gouv.fr. Dès lors que cet accès est étendu à des données sensibles, les risques se trouvent significativement démultipliés.

3.6 « en mettant en œuvre des mesures techniques, opérationnelles et organisationnelles »

À l'instar de la notion de risque significatif, les mesures de protection des données sensibles ne peuvent être définies de manière universelle : elles sont contextuelles et proportionnées aux risques identifiés. Elles se déclinent en trois registres complémentaires:

- Les mesures techniques recouvrent les dispositifs technologiques de protection – par exemple chiffrement, anonymisation, contrôle des accès, journalisation.
- Les mesures opérationnelles concernent les procédures et processus mis en place au quotidien pour encadrer le traitement des données – par exemple gestion des incidents, plans de continuité, audits réguliers.
- Les mesures organisationnelles renvoient quant à elles à la gouvernance interne – par exemple politiques de sécurité, formation des équipes, répartition des responsabilités, désignation de référents.

[5] Direction interministérielle du numérique (DINUM), « Expérimentation autour d'un serveur MCP pour datagouv », *data.gouv.fr*, 25 février 2026, disponible sur : https://www.data.gouv.fr/posts/experimentation-autour-dun-serveur-mcp-pour-datagouv (consulté le 24 mars 2026).

[6] Commission nationale pour la protection des données (CNPD), « DeepSeek et protection des données : les recommandations de la CNPD », 3 février 2025, disponible sur : https://cnpd.public.lu/fr/actualites/national/2025/02/deepseek.html (consulté le 24 mars 2026).

Illustration – Les bénéficiaires effectifs et la cryptomonnaie

Le décret n° 2025-840 du 22 août 2025 illustre concrètement le recours à l'anonymisation comme mesure de protection. Après que le guichet unique des entreprises eut rendu publiques les coordonnées des bénéficiaires effectifs dans une logique d'Open Data, ce décret est venu restreindre cet accès, dans un contexte marqué par la multiplication des séquestrations et agressions physiques visant des dirigeants d'entreprises actives dans le secteur des cryptomonnaies. L'anonymisation s'impose ici non comme une contrainte réglementaire abstraite, mais comme une réponse directe à un risque physique identifié.

Illustration – La caviardisation des décisions de justice

Un arbitrage similaire se pose s'agissant de l'anonymisation des décisions de justice. Afin de protéger magistrats, greffiers et avocats face à des menaces croissantes, un décret a été envisagé pour anonymiser leurs noms dans les décisions publiées. Cette mesure a toutefois suscité des réserves : en l'absence d'un accès granulaire réservé à la profession juridique, elle prive les praticiens de la possibilité d'identifier et de contacter des confrères dans le cadre de leurs activités professionnelles – pour échanger sur une stratégie procédurale ou partager des bonnes pratiques dans un domaine spécialisé. Cet exemple illustre une tension récurrente : toute mesure de protection des données sensibles doit être calibrée pour ne pas produire d'effets collatéraux disproportionnés sur les usages légitimes.

Illustration – L'affaire Ashley Madison : les conséquences d'une absence de mesures de protection adaptées

La violation de données sensibles peut, dans les cas les plus graves, avoir des conséquences létales pour les personnes concernées. L'affaire Ashley Madison, régulièrement citée dans la littérature universitaire, en offre une démonstration concrète. La société exploitait une plateforme de rencontres extraconjugales. Lorsque des hackers ont menacé de divulguer les données de ses utilisateurs, l'entreprise n'a pas réagi. Les données ont été publiées, parmi lesquelles des informations relatives à l'orientation sexuelle des utilisateurs – catégorie expressément visée à l'article 9 du règlement (UE) n° 2016/679.

La Federal Trade Commission a par la suite sanctionné la société pour absence de mesures de sécurité proportionnées, et lui a enjoint de mettre en place un programme de bug bounty, soulignant la pertinence d'une démarche d'amélioration continue en matière de sécurité des données. Cet exemple illustre de manière saisissante pourquoi les mesures techniques, opérationnelles et organisationnelles ne constituent pas une simple obligation de conformité, mais une nécessité dont l'absence peut avoir des conséquences irréversibles.

3.7 Le recours à un acteur souverain : une exigence croissante pour le traitement des données sensibles

La question de la souveraineté numérique est indissociable de celle de la protection des données sensibles. Confier le traitement ou l'hébergement de données sensibles à un acteur soumis à une législation étrangère à portée extraterritoriale – tels le Cloud Act américain (*Clarifying Lawful Overseas Use of Data Act)* ou les dispositions de la législation chinoise en matière de renseignement – expose les organisations à un risque certain : celui de voir ces données accessibles à des autorités étrangères.

Le législateur français a commencé à tirer les conséquences de ce constat. La loi SREN impose ainsi aux organismes publics, lorsqu'ils traitent des données d'une sensibilité particulière dans un environnement cloud, de recourir à des prestataires offrant des garanties de protection contre tout accès non autorisé par des autorités publiques d'États tiers. Cette exigence se traduit concrètement par le référentiel SecNumCloud de l'ANSSI, qui conditionne la qualification des prestataires de services cloud à des critères stricts d'immunité vis-à-vis des législations extraterritoriales.

Cette démarche, encore limitée au secteur public, gagnerait à être étendue. Les organismes privés traitant des données sensibles – qu'il s'agisse de données industrielles, de secrets d'affaires, de données de santé ou de données couvertes par des obligations réglementaires sectorielles – sont exposés aux mêmes risques. Or, en l'absence d'obligation symétrique, le recours à des acteurs non souverains demeure la norme dans de nombreuses organisations, souvent par méconnaissance des risques ou par défaut de maturité en matière de gouvernance des données.

Le Sous-Groupe 1 considère que la notion de donnée sensible telle que définie dans le présent document devrait constituer le critère déclencheur d'une obligation de recours à un acteur souverain ou, à tout le moins, à un prestataire offrant des garanties équivalentes. Cette approche par la qualification de la donnée présente l'avantage d'être à la fois proportionnée – elle ne s'applique qu'aux données justifiant une protection renforcée – et opérationnelle, en offrant aux organisations un critère clair pour orienter leurs choix d'infrastructure.

À terme, une extension du cadre posé par la loi SREN aux acteurs privés traitant des données sensibles apparaît souhaitable, selon des modalités adaptées à la diversité des secteurs et des organisations concernées.

3.8 Conclusion

La notion de donnée sensible est appelée à évoluer. À mesure que les usages numériques se complexifient et que les capacités de croisement et d'exploitation des données progressent, le périmètre de ce qui mérite d'être qualifié de sensible s'élargira inévitablement. Les critères retenus par le Sous-Groupe 1 – nature, destination, combinaison – constituent un cadre opérationnel, non un inventaire figé. Ils devront être régulièrement réévalués à l'aune des évolutions technologiques, réglementaires et géopolitiques.

Cette réévaluation implique également de reconsidérer la notion de risque. La donnée n'est pas seulement un actif stratégique et une opportunité de création de valeur : elle est aussi un vecteur de menaces, dont la matérialisation peut affecter les individus, les entreprises et la nation. C'est précisément de cette double nature que découle la nécessité d'une gouvernance des données robuste et structurée – non comme une contrainte supplémentaire, mais comme une condition de la confiance et de la compétitivité.

Cette gouvernance suppose enfin de muscler les compétences internes des organisations. La gestion des données sensibles ne saurait reposer sur le seul délégué à la protection des données. Elle appelle des profils spécialisés – chief data officers, data stewards, experts en sécurité des systèmes d'information – dont le développement constitue par ailleurs un véritable gisement d'emplois. Le traitement parcellaire et cloisonné qui prévaut aujourd'hui dans de nombreuses organisations doit céder la place à une approche intégrée, à la hauteur des enjeux.

Annexe 1 - Bibliographie

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 (RGPD).

Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (Data Governance Act).

Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de leur utilisation (Data Act).

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (IA Act).

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, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive NIS 2).

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN).

Direction interministérielle du numérique (DINUM), *Vade-mecum sur la sensibilité des données au sens de l'article 31 de la loi SREN*, disponible sur : numerique.gouv.fr

HEXATRUST / FNTC-Numérique, *Guide sur les données externalisées – Comprendre, évaluer et maîtriser les risques des réglementations extraterritoriales*, coord. A. MINESI (AFNOR Normalisation), février 2026, disponible sur : fntc-numerique.com

CAPOTOSTO (J.), « The mosaic effect : the revelation risks of combining humanitarian and social protection data », *ICRC Humanitarian Law & Policy Blog*, 9 février 2021, disponible sur : blogs.icrc.org/law-and-policy

MHALLA (A.), *Cyberpunk – Le nouveau système totalitaire*, Seuil, 2025.