



Berne le 16.01.2026

Interconnexion de banques de données au regard de la protection des données

Rapport du Conseil fédéral
donnant suite au postulat 19.4567 Flach du
20 décembre 2019



Interconnexion des banques de données de la Confédération et des cantons

Table des matières

Résumé	4
1 Introduction	6
1.1 Mandat	6
1.2 Délimitations du mandat	6
1.3 Structure du rapport	7
2 Organisation des travaux	7
2.1 Déroulement	7
2.2 Résumé du rapport d'experts	8
3 Contexte	11
3.1 Stratégies de la Confédération	12
3.1.1 Stratégie Suisse numérique	12
3.1.2 Stratégie Administration numérique suisse	12
3.1.3 Stratégie Administration fédérale numérique	13
3.1.4 Stratégie pour le développement et la gestion commune des données de base de la Confédération	13
3.1.5 Écosystème de données suisse	14
3.2 Principe « <i>Once-Only</i> »	14
4 Mise en relation de banques de données	15
4.1 Notions	15
4.1.1 Interconnexion	15
4.1.2 Interface de programmation applicative ou interface électronique (API)	16
4.1.3 Interopérabilité et normes	17
4.1.4 Sécurité et contrôle des accès	18
4.2 Architectures d'interconnexion	19
4.2.1 Liaison directe	19
4.2.2 Consolidation	19
4.2.3 Fédération	20
4.2.4 Technologie des registres distribués (DLT)	21
4.2.5 Espaces partagés	22
5 Interconnexion de banques de données avec les cantons	22
5.1 Conditions	23
5.1.1 Du point de vue juridique	23
5.1.2 Du point de vue technique	24
5.1.3 Du point de vue de la sécurité	25
5.2 Exemple du Référentiel cantonal fribourgeois	26
6 Enjeux sociétaux	27
6.1 Équilibre entre mutualisation et fédéralisme	27
6.2 Transparence, confiance et acceptabilité sociale	27
7 Cadre juridique	28
7.1 Constitution	28
7.1.1 Structure fédérale de la Suisse	28

Interconnexion des banques de données de la Confédération et des cantons

7.1.2	Droits fondamentaux.....	29
7.1.3	Dispositions importantes qui fixent des règles de droit.....	29
7.2	Loi sur la protection des données.....	30
7.2.1	Dispositions générales.....	30
7.2.2	Communication de données personnelles	31
7.2.3	Traitements de données personnelles conjoints et sous-traitance.....	32
7.2.4	Analyse d'impact relative à la protection des données.....	33
7.2.5	Dispositions d'exécution	34
7.3	Loi sur la sécurité de l'information	35
7.4	Loi sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités.....	36
8	Étude de cas et exemples en Suisse	36
8.1	VOSTRA.....	37
8.2	SYMIC.....	37
8.3	POLAP.....	38
9	Constat général et mesures d'amélioration envisagées.....	40
9.1	Sous l'angle juridique.....	40
9.2	Sous l'angle technique et sémantique	41
9.3	Sous l'angle de la sécurité	41
10	Conclusion	42
	Liste des abréviations.....	44



Résumé

L'interconnexion des banques de données administratives désigne la mise en relation de systèmes d'information permettant à différentes autorités d'échanger automatiquement ou de partager des données de manière électronique. Ce phénomène en progression vise à améliorer l'efficacité et la qualité de l'administration, ainsi qu'à en réduire ses coûts de fonctionnement. En libérant certaines autorités de la nécessité de constituer et gérer leurs propres bases de données, l'interconnexion permet de rationaliser les ressources, d'éviter les redondances, d'accélérer les processus décisionnels et administratifs et de renforcer la qualité des données.

Ce développement s'inscrit dans une dynamique plus large portée par le principe Once-Only, consacré par la déclaration de Tallinn. Selon ce principe, une donnée ne devrait être collectée qu'une seule fois par l'administration, puis mise à disposition des autres entités publiques compétentes. Le principe Once-Only constitue une forme avancée d'interconnexion supposant la capacité juridique, technique et organisationnelle d'échanger des données de manière automatisée. Il offre des gains substantiels en termes de simplification administrative et de qualité des services publics. Toutefois, il comporte également des risques : renforcement de l'État central, dilution des responsabilités, perte de contrôle sur les finalités des traitements, problème de proportionnalité des quantités de données échangées et accroissement de l'exposition aux risques. Si des données présentant des besoins de protection limités peuvent être traitées selon le principe Once-Only sans difficultés (p. ex. des données d'identification des entreprises), il n'en va pas de même des données confidentielles ou soumises à un autre devoir de protection à l'instar des données personnelles sensibles. Plus les données concernées présentent un besoin de protection accru, plus l'application du principe Once-Only devra être limitée à des catégories de données et un cercle d'acteurs limités et déterminés, ou à tout le moins déterminable.

Le rapport distingue quatre principaux modèles d'interconnexion. La liaison directe consiste dans le fait de relier entre eux deux systèmes d'information afin de leur permettre d'échanger des données de manière automatisée. La consolidation repose sur la centralisation des données dans un registre commun spécialement créé. La fédération permet d'interconnecter des systèmes distincts via des interfaces normalisées tout en maintenant l'hébergement, la gestion et l'entretien des données auprès des organes responsables. Les registres distribués reposent sur une architecture décentralisée dans laquelle chaque participant détient une copie synchronisée du registre et contribue à sa mise à jour selon des mécanismes de consensus. Enfin, les espaces partagés correspondent à l'usage d'infrastructures mutualisées, pouvant aussi être fournies par des prestataires externes. Ces modèles sont toutefois présentés à titre indicatif. En pratique, ils peuvent se décliner en une multitude de sous-modèles ou peuvent même se combiner entre eux selon les contextes ou pour répondre à des besoins spécifiques.

Juridiquement, toute forme d'interconnexion incluant le traitement de données personnelles constitue une communication de données au sens de la loi fédérale sur la protection des données, ce qui implique un fondement légal clair et explicite. La principale difficulté réside dans la nécessité d'assurer concordance et cohérence entre, d'une part, les bases légales qui régissent l'activité de l'organe qui communique les données et, d'autre part, les bases légales

Interconnexion des banques de données de la Confédération et des cantons

qui régissent l'activité de l'organe qui reçoit les données (interopérabilité juridique). En plus des exigences juridiques, l'interconnexion requiert également la capacité à harmoniser de manière cohérente les architectures techniques, les processus organisationnels et les modèles de données afin de garantir une interopérabilité technique, organisationnelle et sémantique. Toute interconnexion suppose finalement l'application de règle de sécurité harmonisée entre chaque participant à l'interconnexion.

Dans un État fédéral comme la Suisse, chacun de ces aspects sont soumis à des contraintes supplémentaires. En raison de la répartition des compétences entre la Confédération et les cantons, chaque collectivité publique dispose d'une large autonomie pour régler dans son droit et son organisation internes les conditions de mise en relation de ses systèmes d'information. En matière de bases légales, il appartient aux cantons d'édicter leur droit, sans que la Confédération n'intervienne généralement dans ce processus. Il en va de même s'agissant des aspects techniques, organisationnels et sémantiques, chaque entité restant à ce jour libre de définir ses propres exigences. Des efforts de coordination sont néanmoins menés dans ce domaine au travers de l'organisation Administration numérique suisse (ANS). En matière de sécurité informatique, finalement, la Confédération peut imposer des mesures aux cantons lorsqu'ils accèdent à ses propres ressources ou à des fins limitées de sécurité nationale (p. ex. la détection et la gestion de cyberattaques contre des infrastructures critiques). Pour le reste, la coordination repose sur des initiatives volontaires, notamment dans le cadre de la stratégie nationale de cybersécurité.

Afin d'améliorer la situation, le Conseil fédéral envisage trois types de mesures fondées sur un renforcement de la coopération aux trois niveaux de l'État. Sous l'angle juridique, il a demandé d'étudier la possibilité de compléter le guide de législation en matière de protection des données en y intégrant des indications d'ordre général sur la manière de mieux rédiger les bases légales nécessaires à la mise en place d'interconnexions, en fonction du type d'interconnexion envisagé. Ces compléments qui pourront aussi servir aux cantons devront tenir compte de la jurisprudence du Tribunal fédéral et du principe de neutralité technologique. Ils s'appliqueront en plus des exigences émises par le PFPDT dans ce domaine. Compte tenu des évolutions rapides dans le domaine de la digitalisation de l'administration, le Conseil fédéral reconnaît la nécessité d'engager une révision constitutionnelle afin de permettre la mise en place de normes communes contraignantes aux trois échelons du fédéralisme. Il a donné mandat au DFJP de proposer une révision de la Constitution dans ce sens. Sous l'angle de la sécurité, il est préconisé de se concentrer sur la mise en œuvre de la LSI et de consolider la coopération mise en place dans le cadre de la cyberstratégie nationale ou d'autres initiatives sectorielles.

Interconnexion des banques de données de la Confédération et des cantons

1 Introduction

1.1 Mandat

Le 20 décembre 2019, le conseiller national Beat Flach a déposé le postulat 19.4567 « Banques de données de la Confédération et des cantons et protection des données. Une vue d'ensemble s'impose », dont le contenu est le suivant :

Texte déposé

Le Conseil fédéral est chargé de présenter dans un rapport les problèmes qui se posent au regard de la protection des données dans le contexte de l'interconnexion et de la performance croissantes des banques de données de la Confédération et des cantons. Il indiquera également si des mesures, législatives ou autres, s'imposent dans ce domaine.

Développement

La Confédération et les cantons gèrent aujourd'hui une infinité de données, registres, listes, banques de données et fichiers, qui vont bien au-delà des numéros AVS et du registre de l'état civil. Aucune vue d'ensemble ne permet actuellement d'établir la nature, le volume et l'interconnexion des données traitées, quels services ont accès à quelles données et comment la protection des données est assurée dans ce foisonnement d'applications. Le rapport doit donner une vue d'ensemble des banques de données existantes et mettre en lumière les défis liés à l'avancée du numérique.

Dans son avis du 19 février 2020, le Conseil fédéral a proposé au Conseil national de rejeter le postulat. D'une part, la Confédération n'est en principe pas compétente en ce qui concerne les bases de données cantonales. D'autre part, un recensement des banques de données existant actuellement, au niveau fédéral ou cantonal, ne permettrait pas de tirer de conclusions quant aux défis que ces banques de données posent pour la protection des données. Le Conseil national a néanmoins décidé d'adopter le postulat le 30 septembre 2021.

1.2 Délimitations du mandat

Le postulat Flach 19.4567 charge le Conseil fédéral d'établir un rapport sur l'interconnexion des données et des banques de données de la Confédération et des cantons, plus particulièrement sur le fait qu'un ensemble de données puisse être utilisé comme source d'informations pour un autre ensemble de données au moyen d'interfaces développés dans ce but. Il demande à ce que la situation juridique du point de vue de la protection des données concernant ces interactions entre banques de données soit clarifiée, et aussi que les risques et les défis engendrés par cette interconnexion soient identifiés. Il requiert également qu'une vue d'ensemble des banques de données existantes soit établie.¹

Le présent rapport traite de l'*interconnexion* de banques de données, à savoir l'échange automatisée d'informations provenant de sources de données ou de banques de données distinctes. Afin de présenter le phénomène de l'interconnexion de manière aussi complète que possible, le présent rapport ne se limite pas à une analyse uniquement juridique de la question sous l'angle de la protection des données, mais mentionne en plus certains aspects supplémentaires relatifs à la technique, à l'organisation, à la sémantique et à la sécurité. Pour les

¹ Voir BO 2021 CN 2029-2030 : <https://www.parlament.ch/fr> > Travail parlementaire > Bulletin officiel > Conseil national > Session d'automne 2021 > Treizième séance > 30.09.21 08h00 > 19.4567.

Interconnexion des banques de données de la Confédération et des cantons

besoins du présent rapport et par souci de simplification, les dimensions techniques, organisationnelles et sémantiques sont néanmoins généralement réunies sous la seule dimension « technique² ».

Comme indiqué dans l'avis du Conseil fédéral du 19 février 2020, la Confédération n'est en principe pas compétente s'agissant des banques de données cantonales ou des traitements de données effectués par des autorités cantonales. Conformément au principe du fédéralisme, la manière dont chaque canton collecte et communique des données doit être réglée dans le droit cantonal. Le présent rapport examine donc la problématique essentiellement du point de vue des données ou banques de données de la Confédération et des différents accès accordés à celles-ci. Il met toutefois en évidence les défis posés par une communication de données entre la Confédération et les cantons, et inversement.

Enfin, ce rapport ne présente pas de vue d'ensemble complète des banques de données de la Confédération et des cantons, ni de leurs interconnexions, car une telle vue d'ensemble ne permettrait pas de tirer d'enseignements utiles en matière de protection des données. Au-delà de la difficulté à recenser tous les systèmes d'information existants, une cartographie figerait une réalité en constante évolution, produirait une vision vite dépassée, et risquerait de révéler des dépendances sensibles qui doivent rester confidentielles, notamment pour des raisons de sécurité et de souveraineté. À la place, le rapport fournit quelques cas d'étude offrant une vue spécifique sur certains cas d'interconnexion.

1.3 Structure du rapport

Le présent rapport suit la structure suivante. Il fait tout d'abord état de la manière dont se sont organisés les travaux menés préalablement à la rédaction du présent rapport (2.). Puis, le rapport présente le contexte dans lequel prend place l'interconnexion de banques de données dans le contexte de l'administration publique (3) et fournit des explications plus techniques sur les différents modèles d'architecture existants (4). La problématique de l'interconnexion des banques de données entre la Confédération et les cantons est ensuite abordée sous l'angle juridique, technique et sécuritaire (5). Le phénomène de l'interconnexion est par la suite examiné sous un angle plus sociétal (6) avant de faire l'objet d'un examen juridique plus approfondi (7). Le rapport poursuit ensuite avec trois études de cas portant sur les systèmes VOSTRA, SYMIC et POLAP (8). Sur cette base, le rapport dresse un constat général et envisage trois mesures d'amélioration possibles du point de vue juridique, technique et sécuritaire (9). Le rapport se termine par une brève conclusion (10).

2 Organisation des travaux

2.1 Déroulement

Les travaux ont été conduits par un groupe de travail formé de quatre représentantes de l'OFJ et d'une représentante du secrétariat général du DFJP. Le préposé à la protection des données du canton de Bâle-Campagne et deux représentants du PFPDT ont également été impliqués en tant que consultants.

Au mois de mars 2023, l'OFJ a décidé de faire appel à un bureau externe afin d'examiner certaines questions soulevées dans le postulat. Il a ainsi attribué à BEG Impact AG un mandat de gré à gré pour l'élaboration d'une étude sur la communication de données, du point de vue

² P. ex. aux § 5.1.2 et 9.2.

Interconnexion des banques de données de la Confédération et des cantons

technique, entre la Confédération et les cantons via leurs banques de données, illustrée au moyen d'exemples concrets.

Le rapport de BEG Impact AG « Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen » a été finalisé le 14 septembre 2024 ; il peut être consulté sur le site web de l'OFJ³. Le rapport a été élaboré par des experts indépendants. Les appréciations et conclusions qui y figurent reflètent le point de vue des experts et non celui de l'Office fédéral de la justice.

2.2 Résumé du rapport d'experts

Le rapport d'expert de BEG Impact AG expose comment, à l'ère de la numérisation, s'effectue d'un point de vue technique la communication de données personnelles entre la Confédération et les cantons, au sens de l'*interconnexion* entre des systèmes d'information (banques de données) fédérales et cantonales.

Le rapport présente tout d'abord quelques concepts fondamentaux au regard du droit de la protection des données, tels que l'interconnexion ou la communication de données⁴. Le cadre légal général établi par la LPD en cas de traitement de données personnelles est ensuite exposé⁵. Certains de ces aspects sont abordés dans les chapitres suivants du présent rapport.

Sont ensuite abordés les aspects techniques ainsi que les scénarios envisageables en matière d'interconnexion de données⁶. Du point de vue technique, l'accès à des données, aux fins de les ouvrir, lire, copier, supprimer ou déplacer, par un utilisateur ou un autre système informatique s'effectue par trois niveaux différents : le niveau de la présentation, le niveau de l'application et le niveau des données. L'échange de données entre deux ou plusieurs applications au moyen d'une interface de programmation d'application (Application Programming Interface : API) ou d'autres formes d'intégration de données au niveau de l'application peut s'opérer selon quatre modèles :

- L'intégration manuelle des données (*manuelle Datenintegration*) est une solution relativement ancienne, bien que toujours valide. Elle permet d'échanger des données entre une application A et une application B grâce à des scripts rédigés sur mesure, en particulier si seuls quelques systèmes sont reliés entre eux. La connexion entre deux systèmes est directe et exclusive, ce qui permet de définir précisément quels composants et quels utilisateurs peuvent y accéder ainsi que ce qui est échangé entre les applications.
- La consolidation des données (*Datenkonsolidierung*) consiste à convertir dans un format adéquat les données provenant de plusieurs sources et à les transférer dans une base de données centralisée.
- La virtualisation des données (*Datenvirtualisierung*) agit comme un pont entre les consommateurs de données et les systèmes sources, en interrogeant directement ces derniers via une couche intermédiaire dite « virtuelle ». Elle permet d'accéder aux données

³ Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 06.03.2026 > L'interconnexion des bases de données de la Confédération et des cantons requiert une coordination rigoureuse.

⁴ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 4 ss.

⁵ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 12 ss.

⁶ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 19 ss.

Interconnexion des banques de données de la Confédération et des cantons

demandées et d'en restituer le contenu en temps réel, sans qu'il soit nécessaire de les déplacer ou de les répliquer physiquement.

- Les registres distribués (*Distributed Ledger*) représentent une base de données répartie sur plusieurs nœuds d'un réseau, dans laquelle chaque participant détient une copie décentralisée, synchronisée et validée de l'ensemble des enregistrements. La « Blockchain » en constitue une mise en œuvre concrète. Elle organise les données en blocs, chaque bloc étant lié au précédent par une signature cryptographique. Cette structure peut ainsi être utilisée comme un registre partagé, infalsifiable, consultable et validé par toutes les personnes disposant des droits d'accès nécessaires, sans nécessité d'un tiers validateur.

Lors de la communication de données entre la Confédération et les cantons, la responsabilité du traitement doit être déterminée clairement afin de garantir la protection et la sécurité des données. Dans le cadre des quatre scénarios mentionnés, il en résulte les considérations suivantes :

- Dans l'intégration manuelle des données (*manuelle Datenintegration*), chaque autorité impliquée est responsable de la protection des données stockées dans son propre système et doit s'assurer que seules les données requises par la loi soient transmises et traitées au bon destinataire. En cas de flux transversaux de données entre les autorités, il convient de conclure les accords correspondants ou d'édicter les réglementations nécessaires.
- En cas de consolidation des données (*Datenkonsolidierung*) dans un registre central, il doit être établi quelles autorités sont responsables de la consolidation et à qui incombe la responsabilité des données sources, ainsi que les bases légales sur lesquelles se fondent le traitement et le stockage des données dans le registre central. La finalité des données peut poser un défi particulier. Il convient donc de déterminer le type ainsi que l'origine des données qui peuvent être reçues ou communiquées au registre central. Pour ce faire, des accords entre les différentes parties impliquées sont requis.
- Pour la virtualisation des données (*Datenvirtualisierung*) et le *ledger* distribué (*Distributed Ledger*), le droit applicable ainsi que les compétences en matière de communication des données ne peuvent pas être directement reliés à une seule application (et au stockage de données qu'elle contient). Ainsi, la relation entre tous les systèmes et entités impliquées doit être définie clairement. Les systèmes ainsi que les processus doivent être établies afin de garantir la protection et la sécurité des données.

En plus des aspects liés à la communication des données entre les entités concernées, le rapport d'experts soulève également le besoin de régler, en fonction des besoins, les questions de responsabilité, les processus visant à préserver les droits des personnes concernées, la gestion des incidents de sécurité, la surveillance ainsi que la mise en place de mesures techniques et organisationnelles.

Un autre point important du rapport d'experts concerne les différentes évolutions politiques et techniques en cours, susceptibles d'influencer la communication des données en général et plus particulièrement celle intervenant entre la Confédération et les cantons⁷. Un accent particulier est mis sur le principe *Once-Only* en vertu duquel des données identiques ne devraient

⁷ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 32 ss.

Interconnexion des banques de données de la Confédération et des cantons

être saisies qu'une seule fois au sein de l'administration. Bien que ce principe constitue un objectif stratégique de la Confédération en matière de digitalisation, son application n'est pas encore très répandue en raison de l'absence de bases légales adéquates. Sa mise en œuvre comporte toutefois certains risques comme la diffusion d'erreurs à grande échelle, des problèmes de respect de la finalité annoncée ainsi que des risques de sécurité, particulièrement pour les gros volumes de données. Le rapport insiste sur la nécessité de mettre en place des mesures de sécurité et de protection des données appropriées, notamment des méthodes d'authentification fortes.

À l'avenir, le *Big Data*, le *Cloud Computing*, l'intelligence artificielle et l'informatique quantique élargiront considérablement les capacités de traitement et de mise en relation des données, tout en soulevant de nouveaux défis. En particulier, l'exploration et la réutilisation des données grâce au *Big Data* entre en tension directe avec les principes de finalité et de minimisation des données, de même qu'avec l'obligation d'effacer les données pour lesquelles la finalité a été atteinte. L'intelligence artificielle pose des enjeux de traçabilité, car ses résultats ne sont pas toujours explicables. Le *cloud* offre des produits standardisés et utiles à l'administration, qui sont généralement sécurisés au moyen de dispositifs avancés. Il réduit toutefois le contrôle direct que l'administration a sur ses propres données. Enfin, le développement de l'informatique quantique pourrait à terme compromettre les systèmes de chiffrement actuels assurant la confidentialité des données, si des nouvelles solutions de chiffrement post-quantiques ne sont pas rapidement développées en parallèle.

Afin de mettre le thème de l'interconnexion en contexte, le rapport d'expert a examiné en détail l'organisation et le fonctionnement de deux systèmes d'information de l'administration fédérale choisis sur la base de critères de représentativité : le système d'information sur les casiers judiciaires (VOSTRA) et le système d'information central sur la migration (SYMIC)⁸. L'examen s'est basé sur des entretiens avec des membres du personnel de l'administration fédérale chargés de l'exploitation de VOSTRA et de SYMIC, ainsi que sur divers documents disponibles. Il a porté notamment sur le type d'architecture utilisée, le type de données échangées, les bases légales existantes, la répartition des responsabilités, la surveillance et les mesures techniques et organisationnelles mises en place. Les conclusions de cet examen figurent aux sections 8.1 et 8.2 du présent rapport.

Le rapport d'expert poursuit ensuite avec une analyse des principaux défis que soulève l'interconnexion de banques de données sous l'angle de la législation en matière de protection des données, en particulier lorsque cette interconnexion a lieu entre des banques de données fédérales et cantonales⁹. Le rapport d'experts parvient à la conclusion que lorsque les risques liés à la protection des données sont examinés à un stade précoce et que les dispositions légales correspondantes sont adoptées et appliquées en connaissance de cause, l'interconnexion de données entre la Confédération et les cantons ne présente généralement pas de risques supplémentaires non maîtrisables. Il importe toutefois de correctement maîtriser les spécificités techniques et organisationnelles propres à chaque situation afin de lui apporter des réponses appropriées tant sous l'angle juridique que technique.

Le rapport d'expert se conclut par huit recommandations¹⁰ dont le but est de permettre aux décideurs de mieux appréhender tout nouveau projet d'interconnexion :

⁸ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 38 ss

⁹ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 57 ss.

¹⁰ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 71 ss

Interconnexion des banques de données de la Confédération et des cantons

- 1) adopter une perspective inter-organisationnelle, inter-processus ou inter-flux de données ;
- 2) adresser sans détour les potentiels conflits entre le principe *Once-Only*, le Big Data et la protection des données ;
- 3) analyser les risques suffisamment tôt ;
- 4) prévoir des responsabilités et une coopération claires ;
- 5) mettre en place une collaboration multidisciplinaire et inter-niveaux ;
- 6) assurer une surveillance de bout en bout ;
- 7) mettre à disposition les ressources nécessaires ;
- 8) institutionnaliser l'amélioration continue des processus.

3 Contexte

La transformation numérique de l'administration publique s'accompagne d'une exigence croissante d'efficacité, de coordination et de transparence. Dans ce contexte, l'interconnexion des banques de données publiques constitue un des leviers permettant de simplifier les processus, d'éviter les redondances et de renforcer l'efficacité de l'administration. Toutefois, l'interconnexion soulève aussi des enjeux importants d'ordre juridique, technique et sécuritaire. Sur le plan juridique, elle exige notamment de porter une attention particulière au principe de légalité et aux exigences découlant de la législation sur la protection des données¹¹. Sur le plan technique, elle implique une harmonisation des solutions et des processus. Sur le plan de la sécurité, elle implique notamment de sécuriser les données tant au repos qu'en transit, ainsi que l'application d'une gestion rigoureuse des droits d'accès.

Dans un État fédéral comme la Suisse, la répartition des compétences entre la Confédération, les cantons et les communes constitue également un facteur déterminant. Conformément à l'art. 47 al. 2 Cst., les cantons disposent d'une autonomie dans leur organisation interne. Cette répartition des compétences crée un paysage institutionnel fragmenté, dans lequel les projets d'interconnexion peuvent se heurter à des divergences technologiques, juridiques et parfois même culturelles. En l'absence d'une architecture uniforme des systèmes d'information à l'échelle nationale, la digitalisation de l'administration aux trois niveaux du fédéralisme nécessite de recourir à des mécanismes complexes, fondés sur des bases légales croisées, la reconnaissance de standards techniques communs et des accords négociés entre les différents échelons de l'État.

Sur le plan fédéral, l'interconnexion des banques de données est soutenue par plusieurs initiatives parlementaires. Au total, trois motions demandent la mise en place ou le développement d'interfaces électroniques destinés à faciliter les flux de données. La motion VONLANTHEN 18.4276 « Faciliter l'échange d'informations en créant des interfaces électroniques au sein de l'administration fédérale » et la motion GRÜTER 18.4238 « Mettre en place des interfaces électroniques au sein de l'administration fédérale pour simplifier l'échange d'informations » réclament la possibilité d'échanges de données directs entre les entreprises et les personnes physiques. La motion de la COMMISSION DES FINANCES DU CONSEIL NATIONAL 20.4260 « Pour une infrastructure de données et une gouvernance des données durables dans l'administration fédérale » complète les deux précédentes. Elle demande l'instauration d'interfaces en temps réel (microservices et interfaces de programmation d'applications) interopérables, lisibles par machine et basées sur des normes ouvertes afin d'améliorer les échanges sous forme numérique

¹¹ Voir infra § 7.

Interconnexion des banques de données de la Confédération et des cantons

entre les autorités fédérales et les autorités d'autres niveaux de l'État, l'économie et la société civile.

Le Parlement a accepté les trois motions. Le Conseil fédéral a d'ores et déjà posé les jalons nécessaires pour y donner suite dans différentes stratégies. Le présent rapport vient compléter ces stratégies par une analyse structurée, combinant une approche juridique et technique des enjeux relatifs à l'interconnexion. L'objectif est double : identifier les conditions de faisabilité de telles interconnexions et formuler des recommandations assurant leur conformité juridique ainsi que leur faisabilité technique.

3.1 Stratégies de la Confédération

3.1.1 Stratégie Suisse numérique

La Stratégie suisse numérique est la stratégie faîtière dans le domaine numérique en Suisse. Elle donne un cadre à la stratégie Administration fédérale numérique de la Confédération, à la stratégie Administration numérique suisse et à plusieurs stratégies sectorielles. La Stratégie suisse numérique fixe des lignes directrices pour la transformation numérique de la Suisse en donnant aux acteurs de la numérisation, publics et privés, un cadre sur lequel s'appuyer¹². Elle est contraignante pour l'administration fédérale. Adoptée et mise à jour chaque année par le Conseil fédéral, elle définit trois thèmes prioritaires pour l'année qui suit¹³.

L'augmentation du nombre d'API constituait l'un des trois thèmes prioritaires de la stratégie Suisse numérique 2024. Il s'agit d'une concrétisation de l'art. 13 L META, selon lequel les autorités fédérales doivent s'efforcer de développer des interfaces électroniques permettant d'échanger des données avec d'autres autorités fédérales, cantonales et communales. La mise à disposition et l'augmentation d'interfaces standardisées a pour objectif d'assurer l'intégration et l'interopérabilité des systèmes numériques et l'échange de données à l'échelle de l'administration suisse. Dans le rapport de suivi de la stratégie 2024, la ChF a relevé des progrès importants survenus durant l'année écoulée en matière d'API, notamment la publication de plusieurs documents de référence sur les bonnes pratiques à adopter et la sécurité¹⁴. De l'avis de la ChF, le nombre d'API reste cependant encore insuffisant. Les raisons à cela sont notamment une culture API insuffisante auprès des acteurs concernés et une certaine insécurité liée à l'interprétation de la législation en matière de protection des données, en particulier les possibilités de connecter deux systèmes d'information entre eux¹⁵. Tenant compte de ce constat, le présent rapport vise à apporter certains éléments de réponse afin de concilier le phénomène de l'interconnexion avec la législation sur la protection des données¹⁶.

3.1.2 Stratégie Administration numérique suisse

La Stratégie Administration numérique suisse 2024-2027¹⁷ est une stratégie commune de la Confédération, des cantons, des villes et des communes. Pilotée par l'organisation « Administration numérique suisse » (ANS), elle fixe la marche à suivre pour faire avancer la transformation numérique des administrations aux trois échelons de la Suisse dans un contexte fédéral.

¹² Art. 7 let. b ONum.

¹³ Stratégie numérique 2025, in : FF 2025 31.

¹⁴ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération > Interfaces / API.

¹⁵ Cf. infra § 7.2.

¹⁶ Cf. infra les recommandations formulées au § 4.2 et les explications juridiques exposées au § 7.2. Ces explications pourront, dans la mesure du possible, être complétées par des recommandations d'ordre légistique. Voir à ce sujet le § 9.1.

¹⁷ Stratégie Administration numérique suisse 2024-2027, in : FF 2024 45.

Interconnexion des banques de données de la Confédération et des cantons

Fondée sur la coopération, la Stratégie fixe cinq principes communs à respecter en vue de développer une administration numérique fonctionnant en réseau. Un de ces principes est l'interopérabilité et la réutilisation : les solutions doivent être conçues de manière à être interopérables, les données de l'administration peuvent être utilisées à plusieurs reprises pour les prestations administratives numériques et les données sont saisies conformément au principe de saisie unique¹⁸.

Parmi les six champs d'action définis par la Stratégie pour la période 2024-2027, le champ « Bases légales » constitue un prérequis fondamental pour concrétiser la transformation numérique de l'administration. Il prévoit l'adaptation ou la création de normes permettant notamment la fourniture de prestations numériques, la communication électronique sécurisée, l'exploitation des technologies en nuage, ainsi que la gestion partagée et la réutilisation des données¹⁹. Ces fondements juridiques sont indispensables à la mise en œuvre du champ d'action « Offres numériques », qui vise à développer des prestations sans rupture de média et à instaurer des API permettant à l'administration d'agir en tant que système global au-delà des limites institutionnelles²⁰.

3.1.3 Stratégie Administration fédérale numérique

La stratégie Administration fédérale numérique²¹ adoptée par le Conseil fédéral en 2023 se concentre sur le développement de la cyberadministration à l'échelon de l'administration fédérale. Elle entend transformer en profondeur le fonctionnement de l'administration en favorisant une administration connectée, modulaire et centrée sur les utilisateurs. Elle s'articule autour de huit axes reprenant notamment le cadre d'action de l'OCDE sur l'administration numérique (OECD Digital Government Policy Framework, DGPF)²².

Selon le premier axe, l'administration fédérale est appelée à penser et à aménager l'administration numérique en réseau. Pour ce faire, la stratégie prévoit que l'administration fédérale exploite les synergies existantes et en crée de nouvelles, en développant ses prestations sous la forme de réseaux de création de valeur, accessibles via des interfaces standardisées facilitant leur réutilisation. Dans cette logique, les unités administratives sont appelées, dans la mesure du possible, à mettre à disposition leurs prestations numériques de manière ouverte et à les rendre disponibles sur des plateformes communes. L'usage de données et de solutions fondées sur des standards partagés est encouragé afin de garantir l'interopérabilité entre services. En outre, une identité numérique fiable, dotée d'un mécanisme de gestion des droits d'accès, doit être mise à disposition de tous les acteurs et intégrée systématiquement dans les processus administratifs.

3.1.4 Stratégie pour le développement et la gestion commune des données de base de la Confédération

Adoptée par le Conseil fédéral en décembre 2018, la stratégie pour le développement de la gestion commune des données de base²³ est une stratégie sectorielle visant à permettre une gestion partagée et cohérente d'un socle limité de données dites « de base » entre la Confédération, les cantons et les communes, conformément au principe *Once-Only*. Elle repose sur

¹⁸ Sur ce principe plus en détail : par. 3.2 ci-dessous.

¹⁹ Stratégie Administration numérique suisse 2024–2027, in : FF 2024 45, p. 10.

²⁰ Idem, p. 12.

²¹ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Administration numérique.

²² www.oecd.org > Publications > The OECD Digital Government Policy Framework.

²³ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Stratégies et stratégies partielles > SB018 – Stratégie pour le développement de la gestion commune des données de base de la Confédération.

Interconnexion des banques de données de la Confédération et des cantons

trois champs d'action : organisation (gouvernance), droit (bases légales) et informatique (architecture et plateformes techniques).

Les données de base – entretemps renommées en données « de référence²⁴ » – sont définies comme des informations stables et indispensables à l'activité administrative, portant sur des objets centraux tels que les entreprises, les personnes ou les bâtiments. Nombre d'unités administratives en ont besoin pour leurs tâches respectives. Leur gestion commune vise à éviter les saisies redondantes, à améliorer l'efficacité de l'administration et à alléger la charge des citoyens et des entreprises.

La stratégie a conduit à la publication de trois rapports définissant une compréhension commune des données de référence dans les domaines des entreprises²⁵, des personnes physiques et du bâti. Ces documents précisent le périmètre des données de référence dans chacun de ces domaines et les modalités de leur gestion partagée entre registres fédéraux, cantonaux et communaux, conformément à la législation applicable.

3.1.5 Écosystème de données suisse

Même s'il reste relativement ouvert et appelé à être précisé, le concept d'« écosystème de données Suisse²⁶ » traduit la volonté de favoriser la réutilisation intersectorielle et interorganisationnelle des données en Suisse dans un cadre de confiance. L'objectif est de partager des données présentant une utilité particulière pour l'administration ou l'économie via des espaces de données (*data spaces*) définis par des règles communes de gouvernance, d'interopérabilité (juridique, organisationnelle, technique et sémantique) et de fiabilité (transparence, contrôle, équité, efficacité). Il s'agit de créer une infrastructure décentralisée et modulable, alignée sur des standards internationaux, pour améliorer l'efficacité publique, stimuler l'innovation économique et scientifique, et renforcer la souveraineté numérique. La concrétisation de l'« écosystème de données Suisse » s'inscrit en parallèle des travaux législatifs menés dans le cadre de la motion de la Commission de la science, de l'éducation et de la culture du CE 22.3890 « Élaboration d'une loi-cadre sur la réutilisation des données ».

3.2 Principe « Once-Only »

Le principe *Once-Only* (une fois pour toute) qu'on retrouve dans plusieurs stratégies de la Confédération constitue un élément phare de la Déclaration de Tallin relative à la cyberadministration²⁷, que la Suisse a signée en 2017. Il postule qu'une information (à caractère personnel) ne devrait pas être collectée plus d'une fois auprès d'un individu ou d'une entreprise. Une fois cette information récoltée par l'administration, cette dernière devrait prendre les mesures nécessaires pour qu'elle puisse être partagée et réutilisée en interne entre les différents organes autorisés dans le respect de la législation applicable. Le principe *Once-Only* permet ainsi d'alléger la charge administrative pesant sur les particuliers et l'économie, de réduire les coûts de fonctionnement de l'administration et d'augmenter la qualité et l'efficacité des services publics.

²⁴ Voir, par exemple, les art. 2a let. d OREE et 2 let. f ORegBL.

²⁵ OFS, *Données de base sur les entreprises*, 2020 ; OFS, *Données personnelles de référence*, 2022 ; OFS, *Données de référence des bâtiments et des logements*, 2022. Ces documents sont disponibles à l'adresse : www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération > Données de registre.

²⁶ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > écosystème de données suisse > Document « Vision et objectifs écosystème de données suisse » du 11 juin 2025.

²⁷ Tallin Declaration on eGovernment. Disponible à l'adresse www.admin.ch > Documentation > Communiqués > 6.10.2017 > La Suisse signe la déclaration européenne relative à la cyberadministration.

Interconnexion des banques de données de la Confédération et des cantons

Actuellement, la plupart des administrations publiques disposent de leurs propres banques de données qu'elles développent et gèrent de façon indépendante. Cette forme d'organisation favorise toutefois la duplication des données et engendre un travail redondant pour l'administration et les administrés, une même donnée devant être collectée, saisie et gérée de multiples fois. Elle conduit également à la présence fréquente de données obsolètes, contradictoires ou incomplètes, faute d'une saisie et d'une mise à jour coordonnées et optimales. Or, du point de vue de la protection des données, l'exploitation de données personnelles inexactes est contraire au principe d'exactitude ancré à l'art. 6 al. 5 LPD. En interconnectant entre elles plusieurs banques de données, il est possible de comparer leur contenu en vue de détecter les données erronées et de les corriger via des processus automatisés ou par un contrôle humain selon les cas. La tâche de récolter, de saisir, d'ordonner et de maintenir certaines données peut être centralisée auprès d'un organe unique ou d'un petit nombre d'acteurs, ce qui permet aux autres organes d'être déchargés de cette responsabilité et de consacrer leurs ressources à des tâches à plus forte valeur ajoutée. Le travail de l'administration s'en retrouve rationalisé grâce à une gestion plus cohérente et efficiente des données.

Le principe *Once-Only* n'est cependant pas absolu et connaît de nombreuses variations comme de nombreuses limites. Du point de vue technique, son application dépend fortement du degré d'interopérabilité entre les systèmes, de la qualité des données et de la maturité des infrastructures en place comme des organisations qui en sont responsables. Sous l'angle juridique, toute donnée ne se prête pas non plus de la même manière à une utilisation selon le principe *Once-Only*. L'application du principe *Once-Only* au traitement de données personnelles, en particulier, doit respecter les exigences de la protection des données. Elle requiert l'élaboration de nouvelles dispositions légales dont le rang et la densité normative tiennent compte de la nature des données, de leur quantité, des possibilités d'usage, du cercle des utilisateurs potentiels et des risques concrets que leur accès facilité fait peser sur les droits fondamentaux des personnes concernées²⁸.

Dans la mesure où il implique plusieurs traitements automatisés de données personnelles, la mise en œuvre du principe *Once-Only* requiert l'adoption de bases légales appropriées autorisant la réutilisation des données pour des fins nouvelles. Bien que fréquemment évoqué comme solution, le recours au consentement soulève de nombreuses questions d'ordre juridique. Outre les questions liées au caractère libre et éclairé du consentement dans le cadre de rapports administratifs, le recours au consentement ne peut pas non plus sans autre remplacer la nécessité d'une base légale conformément au principe de légalité (cf. art. 5 et 36 Cst.). À tout le moins, son rôle demeure subsidiaire en droit public et son utilisation requiert dans tous les cas un examen attentif et systématique des conditions de validité du consentement (liberté de décision, information suffisante, absence de contrainte contextuelle, finalité suffisamment claire). Dans le cadre du présent rapport, l'application du principe *Once-Only* est envisagée à travers l'adoption de bases légales ad hoc.

4 Mise en relation de banques de données

4.1 Notions

4.1.1 Interconnexion

Les technologies de l'information et de la communication (TIC) permettent une mise en relation accrue des données. Dans ce cadre, l'interconnexion désigne la mise en relation de systèmes d'information distincts permettant à différentes autorités d'échanger automatiquement

²⁸ Cf. infra, § 4.2.1 à 4.2.4 et 7.2.

Interconnexion des banques de données de la Confédération et des cantons

ou de partager des données de manière électronique. Elle repose sur des interfaces, notamment des API, qui assurent la communication entre systèmes et garantissent la sécurité des échanges. Du point de vue juridique, l'interconnexion de systèmes d'information contenant des données personnelles en provenance de différentes sources fédérales et/ou cantonales correspond généralement à une communication de données personnelles (art. 5, let. e LPD et 36 al. 1 LPD)²⁹. Une telle communication n'a pas lieu « dans un cas d'espèce » mais de manière systématique et sans contrôle préalable de l'organe détenteur des données (principe du libre-service).

4.1.2 Interface de programmation applicative ou interface électronique (API)

Une API est une interface logicielle qui permet à deux systèmes (logiciels) de communiquer et d'échanger des données conformément à un ensemble de règles et de protocoles. Ainsi, lorsqu'un système de la partie 1 envoie une requête selon une structure particulière, le système de la partie 2 y répond conformément aux conditions définies. La manière de fonctionner d'une interface dépend du respect de règles communes par toutes les parties ou par tous les systèmes concernés. Selon la configuration, ces règles et les mécanismes visant à les faire respecter peuvent être prévus tant dans le droit public que dans des contrats privés. Dans le contexte de l'administration publique, c'est en priorité le droit public qui détermine ces règles et leurs mécanismes de mise en œuvre.

Conformément à l'art. 13 al. 1 LMETA, les autorités fédérales veillent à promouvoir autant que possible l'échange de données par interfaces électroniques. L'administration fédérale compte ainsi de nombreuses API. Elles permettent d'échanger des données entre deux administrations qu'elles soient fédérales, cantonales ou communales, entre une administration et un particulier ou entre une administration et une entreprise. Certaines API sont en libre accès, ce qui veut dire que les données sont ouvertes et publiques (API publiques)³⁰. D'autres API sont en accès restreint et ne peuvent être utilisées que par des entités ou des utilisateurs autorisés, selon des modalités prédéfinies (API partenaires ou privées)³¹. En raison des nombreuses possibilités de paramétrages offertes par les API, ces dernières ne sont pas uniquement considérées comme un moyen technique d'échanger de l'information, mais peuvent aussi constituer un moyen de réguler les flux de données dans les espaces numériques³².

Dans le cadre de la stratégie numérique de la Confédération 2020-2023, le secteur TNI de la Chancellerie fédérale a adopté l'Architecture API de la Confédération³³. Réunissant un ensemble de principes architecturaux et une architecture de référence, son objectif est de normaliser et de promouvoir l'accès numérique aux services publics dans l'environnement fédéral afin que les entreprises, l'administration et les personnes puissent bénéficier de la communication de machine à machine. Les travaux relatifs à cet objet se poursuivent aujourd'hui dans le cadre de la stratégie Administration numérique suisse.

²⁹ À ce sujet, infra § 7.2.

³⁰ C'est le cas, par exemple, de api.geo.admin.ch, l'application qui permet d'utiliser les données géographiques disponibles sur le portail geo.admin.ch.

³¹ C'est le cas, par exemple, de UPIViewer, la solution permettant à un utilisateur autorisé de consulter la base de données UPI contenant le numéro AVS.

³² VACCARI L. *et alii*. *Application programming interfaces in government : why, what et and how*, EUR 30227 EN, Publications Office of the European Union, Luxembourg, 2020.

³³ www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération > Interfaces / API.

Interconnexion des banques de données de la Confédération et des cantons

4.1.3 Interopérabilité et normes

L'interopérabilité est la capacité de systèmes hétérogènes (p. ex., développés par des fournisseurs différents, utilisant des technologies différentes) à collaborer ou à interagir ensemble. Elle se décline en plusieurs niveaux : technique (spécification d'interfaces, services d'interconnexion, protocoles de communication sécurisés...), sémantique (compatibilité des formats et description commune des données), organisationnel (alignement des processus métiers) et juridique (conformité au cadre légal)³⁴. L'interopérabilité est considérée comme un enjeu essentiel du développement de l'administration numérique et fait partie à ce titre des principes fondamentaux de la Stratégie Administration numérique suisse 2024-2027³⁵.

Les normes sont pour leur part des instructions de nature généralement technique qu'une organisation recommande de suivre dans l'accomplissement d'une certaine tâche. En prescrivant une manière de procéder, l'usage d'un certain protocole ou une façon de décrire des données, elles favorisent l'interopérabilité au niveau organisationnel, technique et sémantique entre des systèmes et des solutions informatiques autonomes. L'État peut les intégrer dans sa législation soit en les reprenant directement, soit en y faisant référence³⁶. Se fondant sur l'art. 12 LMETA, la ChF a, p. ex., déclaré diverses normes de l'association eCH contraignantes pour l'ensemble de l'administration fédérale³⁷. Dans le domaine de l'exécution du droit fédéral, on trouve déjà ponctuellement des normes contraignantes également pour les cantons et qui, de ce fait, assurent l'interopérabilité entre les différents niveaux de l'État³⁸.

Dans le secteur public, l'élaboration et l'adoption de normes est néanmoins plus complexe que dans le secteur privé. Loin de se limiter à la simple désignation d'un format de données ou à la spécification d'une API, elles affectent la structure et les processus internes des organisations concernées. C'est pourquoi l'élaboration et l'adoption de normes communes applicables aux trois échelons du fédéralisme inclut en plus une composante politique exigeant des mécanismes formalisés de concertation et de coordination.

Aujourd'hui, ces mécanismes sont formalisés pour l'essentiel dans la Convention-cadre de droit public concernant l'Administration numérique suisse (ANS)³⁹. La coopération entre la Confédération, les cantons et les communes au sein de l'ANS a permis de grandes avancées dans le domaine de l'interopérabilité et des normes. Cette coopération basée à l'heure actuelle sur l'harmonisation volontaire connaît toutefois des limites, lesquelles ont été mises en évidence tant au niveau politiques⁴⁰ que dans le cadre de l'évaluation 2025 de l'Administration numérique suisse⁴¹. Dans le cadre de sa réponse au postulat 23.3050 « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », le Conseil fédéral s'est prononcé en faveur

³⁴ Plus en détails : CONSEIL FÉDÉRAL, Rapport en exécution du postulat 23.3050 du 6 mars 2023 déposé par le Groupe du Centre « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », 19 septembre 2025, p. 7. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025. Également : eCH-0279 – Vision de l'architecture 2050, p. 13 ss.

³⁵ Stratégie Administration numérique suisse 2024–2027, in : FF 2024 45, p. 7 et 11.

³⁶ MÜLLER Georg / UHLMANN Felix / HÖFLER Stefan, *Elemente einer Rechtssetzungslehre*, Zürich 2024, n° 525 ; cf. p. ex. l'art. 31 al. 2, let. b de la loi sur les télécommunications (LTC ; RS 784.10).

³⁷ Une liste est disponible sous : www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives.

³⁸ Cf. Norme e-LP visée à l'art. 5 de l'ordonnance du DFJP concernant la communication électronique dans le domaine des poursuites (RS 281.112.1).

³⁹ FF 2021 3030.

⁴⁰ Postulat du groupe LE CENTRE 23.3050 « Définir des normes contraignantes pour le paysage de l'Administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? » du 6 mars 2023 ; Motion WÜRTH 24.4045 « Numérique. Création d'un article constitutionnel » du 26 septembre 2024 ; Initiative du canton de Saint-Gall 24.312 « Unir les forces à l'échelle du pays pour aborder la transition numérique ».

⁴¹ DELOITTE, *Évaluation externe de l'Administration numérique suisse – Rapport d'évaluation*, 29 janvier 2025.

Interconnexion des banques de données de la Confédération et des cantons

d'un renforcement de la coopération fédérale à travers l'adoption d'une nouvelle norme constitutionnelle en matière de digitalisation⁴². Il s'est engagé à associer étroitement les cantons les villes et les communes dans ce processus. Un message relatif à la révision de la Constitution devrait être présenté durant l'année 2028⁴³.

4.1.4 Sécurité et contrôle des accès

Dès lors qu'elle élargit la surface d'exposition des systèmes d'information, l'interconnexion implique une vigilance accrue en matière de sécurité informatique. Des mesures adaptées et proportionnées aux enjeux propres à chaque interconnexion et à chaque jeu de données concerné doivent être définies et mises en place.

Un premier élément essentiel à prendre en compte en matière d'interconnexion concerne la gestion des droits d'accès. Ceux-ci doivent être définis selon le principe du « Need-to-know », de manière à limiter l'accès aux seules personnes ou entités pour lesquelles il est nécessaire. Plus les données concernées présentent un haut degré de confidentialité, plus leur partage sera soumis à une gestion stricte des droits d'accès. En principe, l'attribution des droits d'accès devrait passer par un système d'autorisation, dont l'organisation et le fonctionnement devrait être réglé au niveau d'une loi et/ou d'une ordonnance. La confidentialité des données doit être assurée en complément par des mesures organisationnelles et par des dispositifs techniques. Le chiffrement, tant au repos que lors des transferts, constitue un élément central pour éviter toute divulgation non autorisée.

D'autres mesures doivent être prises dans le but d'assurer l'intégrité des données ainsi que la traçabilité et l'authenticité des opérations qu'elles subissent. L'intégrité impose que toute donnée stockée soit protégée contre toute altération volontaire ou accidentelle, ce qui suppose des mécanismes de contrôle d'intégrité et de détection des anomalies, mais aussi de limiter le nombre d'individus ou d'entités habilités à modifier les données. La traçabilité, quant à elle, exige, là où cela est nécessaire, la mise en place de journaux d'événements permettant de documenter l'ensemble des opérations effectuées sur les données (consultation, modification, suppression). Une telle traçabilité n'a pas seulement une fonction de sécurité technique. Elle est également un outil de responsabilisation et de conformité, permettant d'apporter la preuve du respect des obligations légales et de faciliter la détection d'éventuelles utilisations abusives. L'authenticité, enfin, garantit que l'origine des opérations est vérifiable et imputable à un acteur déterminé.

Sur le plan technique, la gestion des identités et des droits d'accès aux services numériques de la Confédération sont gérés par les systèmes IAM en application de l'OIAM. Les systèmes IAM offrent différents services d'identité permettant aux administrations fédérales mais aussi cantonales de se connecter de manière sécurisée à des bases de données centralisées de l'administration fédérale (notamment FED-LOGIN, AGOV). En revanche, il n'existe pas encore de solution similaire permettant de se connecter de façon unifiée aux services cantonaux ou communaux, chaque canton ou commune disposant de ses propres systèmes d'accès, sans interconnexion avec les systèmes IAM de la Confédération.

⁴² CONSEIL FÉDÉRAL, Rapport en exécution du postulat 23.3050 du 6 mars 2023 déposé par le Groupe du Centre « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », 19 septembre 2025. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

⁴³ CONSEIL FÉDÉRAL, Avis sur le modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique, 19 septembre 2025. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

Interconnexion des banques de données de la Confédération et des cantons

4.2 Architectures d'interconnexion

L'interconnexion entre plusieurs banques de données peut être réalisée au moyen de différents modèles d'architecture exposés dans le rapport d'expert⁴⁴. Les modèles décrits ci-après représentent les principaux modèles existants. Mais chacun d'eux peut se décliner en plusieurs sous-modèles ou même se combiner avec d'autres modèles. Leur présentation a donc avant tout une valeur didactique et indicative ; elle ne prétend pas à l'exhaustivité ni à l'établissement d'un cadre décisionnel unique. Chaque modèle soulève des enjeux distincts et appelle une analyse au cas par cas permettant d'identifier les conditions nécessaires à sa mise en œuvre, notamment en matière de bases légales, de responsabilité, de technologie, de flux et de sécurité.

4.2.1 Liaison directe

Une liaison directe⁴⁵ (ou connexion point à point) désigne une interconnexion établie entre deux systèmes via des interfaces, sans recourir à un intermédiaire. Dans le cas d'une liaison directe, un registre source détenu par un organe de l'administration (organe détenteur) met des données à disposition d'un ou plusieurs autres organes de l'administration (organes consommateurs), qui peuvent interroger ce registre en temps réel pour accomplir leurs tâches. Les données mises à disposition peuvent être simplement consultées mais aussi intégrées aux données des organes consommateurs dans leurs propres banques de données. Dans ce deuxième modèle, le registre de l'organe détenteur ne remplace donc pas les banques de données des organes consommateurs mais vient uniquement les alimenter.

Pour accorder à un organe une liaison directe à un registre contenant des données personnelles détenu par un autre organe, il est essentiel de vérifier dans la législation applicable, d'une part, que l'organe consommateur des données est autorisé à traiter les données concernées et, d'autre part, que l'organe détenteur des données est autorisé à les communiquer. La base légale autorisant la communication doit énoncer au minimum les données ou les catégories de données concernées ainsi que les finalités pour lesquelles elles peuvent être communiquées. Il doit en outre ressortir clairement qu'il s'agit d'un mode de communication automatisé. En droit fédéral, le rang de la base légale à adopter se déduit des art. 34 et 36 LPD. Une base légale au sens formel est dans tous les cas nécessaire pour la communication automatisée de données sensibles, la tenue d'activité de profilage ou lorsque la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (cf. art. 34 al. 2 LPD). Dans les autres cas, une base légale au sens matériel uniquement peut être suffisante.

4.2.2 Consolidation

La consolidation consiste à regrouper dans un registre central les données provenant de plusieurs organes producteurs de données. Concrètement, les données sont versées régulièrement ou en temps réel depuis plusieurs banques de données distinctes dans le registre central à l'aide de processus d'extraction et de consolidation, ou via des flux de données événementiels. Elles peuvent à cette occasion subir un processus de nettoyage par comparaison avec les données similaires provenant des différents organes producteurs de données. L'objectif est de disposer via un point d'accès unique de données homogènes et de qualité

⁴⁴ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 24 ss. Un résumé de ce rapport est disponible *supra* § 2.2.

⁴⁵ Dans le rapport BEG Impact, cette forme d'architecture est nommée sous l'expression « intégration manuelle » (en allemand : « Manuelle Dateintegration »). Selon notre compréhension, l'intégration manuelle correspond cependant à une forme de traitement consistant à intégrer dans une banque de données le contenu d'une autre banque de données. Une intégration manuelle peut ainsi intervenir suite à la mise en place d'une liaison directe.

Interconnexion des banques de données de la Confédération et des cantons

pour un ensemble d'organes à partir de quelques banques de données spécialement sélectionnées⁴⁶.

Comme le registre central est une infrastructure distincte des banques de données sources, il convient de régler juridiquement son existence et son fonctionnement de manière séparée. Les éléments à régler concernent notamment l'institution du registre central, l'organe responsable, la liste des organes contributeurs, le catalogue des données personnelles partagées, les règles de gestion du registre central, des règles de gestion à la source, les finalités pour lesquelles les données peuvent être communiquées et exploitées, la procédure et les droits d'accès ainsi que les règles de conservation et de sécurité des données. La question de savoir si la création d'un registre central requiert obligatoirement l'adoption d'une base légale au niveau de la loi ou si elle peut avoir lieu au niveau d'une ordonnance est complexe et dépend de différents facteurs. En plus des critères prévus aux art. 34 et 36 LPD, il convient de prendre en considération l'importance d'une telle infrastructure dans le fonctionnement et l'organisation de l'administration ainsi que les effets qu'elle déploie sur les particuliers et l'administration (cf. art. 164 al. 1 et 36 al. 2 Cst.⁴⁷).

De ce point de vue, l'introduction d'un registre central réunissant les données d'une très large partie de la population afin de les mettre à disposition de l'ensemble ou d'un très large éventail d'organes publics peut requérir l'adoption d'une base légale au sens formel, quand bien même le registre central ne traiterait aucune donnée sensible. Lorsque l'adoption d'une base légale au sens formel est nécessaire, l'ensemble des éléments décrits plus haut n'a cependant pas besoin d'être réglé au niveau de la même loi mais peuvent être répartis entre plusieurs actes (p. ex. la communication des données des registres sources vers le registre central peut être réglée dans les lois gouvernant les registres sources, tandis que la communication des données du registre central vers les organes consommateurs peut être réglée dans l'acte qui traite du registre central), y compris de rang différent (p. ex. certains aspects plus techniques peuvent être réglés au niveau d'une ordonnance).

4.2.3 Fédération

La fédération⁴⁸ consiste dans la mise en réseau de plusieurs banques de données distinctes dans un modèle décentralisé où chaque organe producteur de données conserve la maîtrise et la responsabilité de ses propres données. Au lieu de regrouper les informations sous un même toit, l'approche fédérée laisse les données d'une organisation là où elles se trouvent, mais offre un point de consultation unique grâce à une banque de données virtuelle. En d'autres termes, la fédération des données permet d'interroger des informations provenant de plusieurs systèmes comme si elles résidaient toutes dans un seul registre de données harmonisé mais sans les déplacer. Ce modèle élimine le besoin de créer un registre supplémentaire et de gérer l'intégration des données vers un système centralisé comme avec la consolidation. Les données sont consultées via une interface mais directement à la source, sans stockage intermédiaire ou réplication⁴⁹.

⁴⁶ On peut citer à titre d'exemple le projet de service national des adresses (SNA) actuellement en discussion au Parlement fédéral (objet [23.039](#)). Ce registre est élaboré à partir des données provenant notamment du registre des habitants des cantons et des communes suisses et d'autre registre fédéraux (SYMIC, Ordipro, UPI, RegBL et répertoires officiels).

⁴⁷ À ce sujet : infra 7.1.3.

⁴⁸ Dans le rapport BEG Impact, l'expression fédération (Datenföderation) est utilisée, semble-t-il, comme synonyme de virtualisation (Datenvirtualisierung). Bien qu'ils présentent certaines similitudes, il s'agit toutefois de deux modèles qui ne sont pas totalement identiques. La virtualisation des données va un cran plus loin dans la fédération, en créant une couche d'abstraction logique au-dessus des sources de données. Elle masque ainsi la complexité des schémas, des formats et des emplacements, offrant une vue unifiée des données.

⁴⁹ On peut citer à titre d'exemple l'index central des raisons de commerce (Zefix) prévu aux articles 928b CO et 14 ORC. Les données relatives aux entreprises restent gérées dans les systèmes cantonaux, Zefix renvoie vers les données cantonales originales.

Interconnexion des banques de données de la Confédération et des cantons

À l'inverse du modèle consolidé, le modèle fédéré n'implique pas la création d'un registre distinct dans lequel l'entier des données des registres sources seraient répliqué. Il n'en demeure pas moins que la mise en réseau de plusieurs systèmes d'informations va permettre la réalisation de nombreux flux de données entre entités distinctes dans un environnement où chaque flux n'est plus contrôlé individuellement. À défaut d'un système centralisé, c'est donc la mise en réseau qui doit être prévue au moyen de bases légales appropriées. Les éléments pertinents à prendre en compte concernant ici notamment l'existence et l'organisation du réseau, la liste des organes contributeurs de données, le catalogue des données, les règles de gestion à la source, les finalités pour lesquelles les données peuvent être communiquées et exploitées, la procédure, les droits et le mode d'accès ainsi que les règles de sécurité des données. Comme les données restent gérées à la source, la durée de conservation des données n'a, en revanche, pas besoin d'être traitée séparément, mais continue de dépendre des règles générales applicables à ces données. Concernant le rang de la base légale attendue, on peut appliquer à la fédération les mêmes considérations que celles valant pour la consolidation.

4.2.4 Technologie des registres distribués (DLT)

Un registre distribué, également appelé registre partagé (en anglais *Distributed Ledger-Technologie* ; *DLT*), est un registre décentralisé, hébergé et synchronisé simultanément sur un ensemble de machines connectées à un réseau. Le fonctionnement du registre repose sur un réseau pair-à-pair⁵⁰ et des algorithmes de consensus qui garantissent la fiabilité du registre. Le registre évolue par l'ajout de nouvelles informations, préalablement validées selon des règles prédéfinies. L'objectif principal est d'assurer l'immuabilité et la sécurité des données validées. Contrairement à une base de données centralisée, un registre distribué peut fonctionner sans autorité responsable. Toutefois, dans certains modèles où seuls des acteurs identifiés et autorisés participent au réseau (DLT dites privées ou permissionnées), une forme de gouvernance coordonnée peut être maintenue afin d'assurer la cohérence et la confiance entre les participants. La blockchain constitue une forme particulière de registre distribué où les données sont organisées en blocs, liés les uns aux autres de manière séquentielle et cryptographiquement sécurisée, formant une chaîne inaltérable.

En raison des spécificités propres aux registres distribués (p. ex. difficulté à identifier le responsable du traitement, problèmes liés à l'effacement et à la modification des données), leur usage est réservé à des cas très particuliers où l'intégrité des données dans le temps, une haute traçabilité et/ou éventuellement l'absence d'autorité centrale sont spécifiquement recherchés. Il convient alors de s'assurer que ces caractéristiques soient prises en compte et encadrées par la législation applicable⁵¹. Dans un contexte institutionnel tel que celui de l'État, un registre trop décentralisé peut cependant sembler inadapté aux exigences de gouvernance administrative. L'absence de mécanisme de gouvernance clairs compliquent la répartition des responsabilités et crée des difficultés pour assurer la conformité avec les normes juridiques en vigueur. Il est généralement préférable d'opter pour des registres distribués permissionnés ou privés, qui permettent d'imposer des politiques d'accès, de garantir l'identification des entités intervenant dans le traitement et d'assurer, dans toute la mesure du possible, une gouvernance conforme aux règles établies.

⁵⁰ Un réseau pair-à-pair ou *peer-to-peer* est une architecture décentralisée dans laquelle chaque nœud du réseau agit simultanément comme client et serveur, partageant directement des ressources ou des données avec les autres nœuds sans passer par un serveur central.

⁵¹ Voir, p. ex., l'art. 973d CO sur les droits-valeurs inscrits.

Interconnexion des banques de données de la Confédération et des cantons

4.2.5 Espaces partagés

Le recours à des espaces partagés ne constitue pas à proprement parler une forme d'interconnexion. Il est toutefois pertinent de l'examiner, car plusieurs entités administratives peuvent accéder à un même espace et y échanger par ce biais des données personnelles. Les espaces partagés désignent une zone de stockage ou de collaboration à laquelle plusieurs utilisateurs ou entités peuvent accéder simultanément pour consulter, modifier ou traiter des informations en commun. Ces zones de stockage ne sont pas liées à une architecture particulière. Elles englobent aussi bien des espaces hébergés en interne que proposés dans le *cloud*. Les espaces partagés se prêtent particulièrement bien aux formes de travail agiles et collaboratives, dans lesquelles plusieurs utilisateurs ou entités doivent accéder à une même ressource pour accomplir conjointement une tâche, souvent depuis des organisations ou des lieux distincts.

Contrairement à des environnements de données plus structurés où les flux sont organisés, normalisés et gouvernés selon des règles précises, les espaces partagés offrent une plus grande souplesse d'utilisation, chacun pouvant, en théorie, y déposer librement ce qu'il souhaite. En l'absence d'une gouvernance claire, cela peut néanmoins conduire à y placer des données inadaptées ou qui ne répondent pas aux mêmes exigences de protection. Lorsque l'espace partagé se situe dans le *cloud*, d'autres paramètres supplémentaires doivent être pris en considération comme la localisation des données ou les modalités contractuelles d'hébergement (cf. art. 9 LPD). La stratégie d'informatique en nuage de la Confédération prévoit à cet égard une approche différenciée, fondée sur quatre niveaux d'utilisation (nuage public, nuage public suisse, nuage privé Confédération, nuage privé sécurisé Confédération)⁵². En principe, le recours à une solution *cloud* relève de l'administration auxiliaire (*Bedarfsverwaltung*) et ne requiert généralement pas de base légale spécifique en tant que telle⁵³. Qu'il s'agisse d'espaces partagés hébergés en interne ou situés dans le *cloud*, tout échange de données personnelles entre entités juridiquement distinctes qui résulterait de l'usage d'un espace partagé doit en revanche faire l'objet d'un examen de sa légalité et, le cas échéant, être prévu comme tel conformément à l'art. 36 LPD.

5 Interconnexion de banques de données avec les cantons

La complexification croissante des politiques publiques et l'imbrication toujours plus étroite des compétences entre la Confédération et les cantons impliquent une intensification des échanges de données entre les différents niveaux de l'État. La Confédération détient généralement des données spécialisées (p. ex. économiques, fiscales, policières, douanières ou encore statistiques) que les autorités cantonales ou communales ne produisent pas elles-mêmes. À l'inverse, du fait de leur proximité avec la population, ce sont les cantons et plus encore les communes qui disposent souvent des données de base les plus à jour sur les personnes et les entreprises. Il existe donc un intérêt réciproque évident à collaborer en matière de gestion des données. Pareille collaboration doit cependant avoir lieu dans un cadre délimité assurant des échanges de données sécurisés et conformes aux règles établies.

⁵² www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération > Informatique en nuage.

⁵³ ChF, *Cadre juridique de l'utilisation de services d'informatique en nuage public dans l'administration fédérale*, mars 2025, p. 12. Disponible à l'adresse : www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Architecture de la Confédération Informatique en nuage. Également : OBERSON ABELS SA, *Enquête administrative « Fuite de donnée »*, Rapport du 28 mars 2024 à l'attention de l'organe de coordination (SG-DFF), n° 492. Disponible à l'adresse : www.admin.ch > Documentation > Communiqués > 1.05.2024 > Clôture de l'enquête administrative concernant la cyberattaque contre Xplain SA : le Conseil fédéral adopte des mesures.

Interconnexion des banques de données de la Confédération et des cantons

5.1 Conditions

5.1.1 Du point de vue juridique

Sous l'angle juridique, les traitements des données par la Confédération et les cantons sont soumis à différentes règles transversales et sectorielles. Tandis que la Confédération est exclusivement soumise à la législation fédérale et respecte la LPD en matière de protection des données, les cantons sont soumis en fonction de l'activité en cause soit au droit fédéral, soit au droit cantonal et, à quelques exceptions près, appliquent les règles de la législation cantonale applicable sur la protection des données.

Même si des différences existent, on peut néanmoins raisonnablement considérer que les diverses lois fédérales et cantonales révisées sur la protection des données en Suisse sont globalement équivalentes. Ainsi rares sont les cas dans lesquels un traitement autorisé en vertu d'une loi deviendrait illicite en application d'une autre loi. Le cadre posé par la LPD, la Directive UE 2016/680 sur la protection des données dans le secteur de la police et de la justice pénale, et la Convention STE 108+ ont facilité l'adoption de règles largement harmonisée à l'échelle de la Suisse. Cela garantit non seulement un niveau de protection des données homogène mais assure également une certaine sécurité juridique aux échanges de données qui ont lieu.

C'est plutôt dans la législation sectorielle qui détermine les traitements de données autorisés en fonction des domaines d'activités concernés que des différences plus importantes peuvent survenir. Qu'il s'agisse d'activités liées à la police, à l'aménagement du territoire, à la fiscalité, ou à l'éducation, toutes ces activités impliquent des échanges réguliers ou ponctuels de données entre la Confédération et cantons. En l'absence d'une compétence fédérale globale, ces échanges de données doivent ainsi reposer sur des bases légales qu'il revient au législateur de chaque collectivité d'adopter et d'insérer dans son droit interne. Or tous les législateurs travaillent selon des méthodes et ont des sensibilités en matière de protection des données, qui ne sont pas équivalentes. Il peut donc arriver qu'un échange de données entre collectivités ne puisse pas avoir lieu parce que l'une d'entre elles n'a pas correctement adapté son propre droit ou interprète une disposition légale différemment de l'autre collectivité.

Dans le cas d'échange de données entre cantons, l'autre collectivité ne dispose d'aucun moyen d'intervenir dans le processus législatif de la collectivité concernée⁵⁴. Dans le cas d'échanges de données entre la Confédération et les cantons, la situation varie selon le domaine d'activité en cause et le type de compétences correspondantes. Lorsque la Confédération dispose d'une compétence globale, elle peut elle-même fixer l'entier du déroulement et des conditions applicables à un échange de données. Une intervention du législateur cantonale n'est dès lors en principe par requise, bien qu'elle ne soit pas non plus totalement exclue. Selon un ancien avis du PFPDT, en l'absence de bases légales prévues par le droit fédéral, la compétence d'exécution reconnue aux cantons peut suffire à leur permettre d'édicter dans leur droit interne les bases légales supportant une interconnexion entre une banque de données cantonales et une banque de données fédérale, pour autant qu'une telle interconnexion soit nécessaire à l'accomplissement des tâches prescrites par le droit fédéral⁵⁵.

Lorsque la Confédération n'a qu'une compétence limitée ou n'a pas de compétence, elle peut uniquement fixer dans son droit interne les conditions que les cantons doivent respecter au

⁵⁴ Voir pour un exemple : ch. 7 ci-dessous.

⁵⁵ JAAC 62.44.

Interconnexion des banques de données de la Confédération et des cantons

moment de légiférer pour obtenir un accès à une base de données fédérale⁵⁶, mais elle ne peut, en principe, pas vérifier préventivement que ces exigences ont été correctement appliquées⁵⁷. Dans ce cas, le législateur fédéral peut néanmoins introduire un mécanisme d'annonce doté d'un effet déclaratoire. Ainsi, l'organe cantonal n'est en droit de demander un accès à la base de données concernée qu'après avoir créé les bases légales nécessaires dans son droit interne et officiellement annoncé celles-ci à l'organe fédéral compétent pour accorder l'accès. Bien que ce dernier n'ait pas forcément pour tâche de vérifier les bases légales en question, cette procédure peut néanmoins inciter le législateur cantonal à tenir compte du mieux possible des exigences du droit fédéral⁵⁸.

5.1.2 Du point de vue technique

Afin d'assurer une gestion administrative efficace à l'échelle nationale, les différentes administrations devraient, dans le respect du cadre juridique en vigueur, privilégier le développement de synergies et de solutions communes, plutôt que de fonctionner en silos et de reproduire vingt-sept fois la même solution. Dans ce contexte, une étroite collaboration entre la Confédération et les cantons est indispensable pour mettre en commun les ressources, partager les connaissances et fournir des solutions interopérables servant un même objectif commun.

En 2021, la Confédération et les cantons ont conclu la Convention-cadre concernant l'Administration numérique suisse⁵⁹. Cette dernière définit les règles de collaboration entre la Confédération et les cantons dans le domaine de la transformation numérique de leurs administrations. Elle a abouti le 1^{er} janvier 2022 à la création de l'organisation « Administration numérique suisse » (ANS) dont le but est d'encourager la transformation numérique des administrations en Suisse. L'un des moyens retenus consiste à développer des normes.

L'adoption de normes communes à la Confédération et aux cantons joue un rôle central dans le développement de la cyberadministration. Cela permet à des systèmes issus de collectivités distinctes de communiquer de manière fiable en s'appuyant sur des formats de données, des interfaces techniques et des référentiels sémantiques partagés plutôt que chaque collectivité ne développe ses propres solutions de manière isolée. Grâce à cette standardisation, des processus peuvent être automatisés de bout en bout, les coûts et les redondances sont limités et la fiabilité des échanges est renforcée.

Actuellement, les normes relatives à la cyberadministration sont principalement définies par l'association eCH, au sein d'un partenariat public-privé. Ces normes n'ont cependant aucune force obligatoire sur le plan juridique, leur portée demeurant ainsi essentiellement indicative. Seules les collectivités publiques sont habilitées à leur conférer un caractère contraignant

⁵⁶ P. ex., l'ancien art. 50e al. 3 LAVS selon lequel les cantons qui souhaitaient utiliser systématiquement le numéro AVS en dehors du domaine des assurances sociales devaient pour cela obligatoirement adopter une base légale au sens formel habilitant les organes cantonaux à traiter cette donnée dans l'accomplissement de leurs tâches légales uniquement. Voir aussi sur la question des compétences : infra 7.1.1.

⁵⁷ Selon l'art. 186 al. 2 Cst., un tel contrôle n'est possible qu'en présence de compétences cantonales d'exécution.

⁵⁸ Une telle solution a, p. ex., été mise en œuvre aux art. 50e al. 3 et 50g LAVS, et 134ter al. 2, let. a RAVS dans leur version jusqu'au 1^{er} janvier 2022, avant que le législateur fédéral n'autorise lui-même intégralement l'utilisation systématique du numéro AVS pour les autorités publiques fédérales, cantonales et communales.

⁵⁹ Convention-cadre de droit public concernant l'Administration numérique suisse, in : FF 2021 3030.

Interconnexion des banques de données de la Confédération et des cantons

dans leur propre sphère de compétence⁶⁰. Le 19 septembre 2025, le Conseil fédéral a approuvé⁶¹ le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique, dont l'un des axes vise précisément à rendre la coopération fédérale plus contraignante dans le domaine de la numérisation⁶². Il s'est dans ce sens prononcé en faveur de l'inscription d'un nouvel article dans la Constitution permettant d'édicter des normes contraignantes relative à la numérisation pour toutes les collectivités en Suisse⁶³. Afin de garantir une prise en compte adéquate des intérêts des cantons, des villes et des communes, une commission tripartite réunissant des représentants de chaque échelon a été constituée pour déterminer la meilleure manière d'avancer⁶⁴.

5.1.3 Du point de vue de la sécurité

L'interconnexion croissante des infrastructures et des systèmes informatiques de la Confédération et des cantons renforce inévitablement le risque de voir des vulnérabilités présentes dans les systèmes d'une autorité se répercuter sur les systèmes d'autres autorités. Conformément aux règles du fédéralisme, les cantons répondent eux-mêmes de leur sécurité de l'information. Toutefois, la Confédération a un intérêt direct à ce que les cantons garantissent une protection équivalente lorsqu'ils traitent des informations protégées de la Confédération ou recourent à ses moyens informatiques.

L'art. 9 LSI énonce que lorsque des autorités fédérales collaborent avec des tiers, ce qui inclut aussi les cantons, elles font en sorte que les exigences et mesures prévues par la LSI soient consignées dans les accords et contrats correspondants et veillent à ce que ces mesures soient contrôlées de manière adéquate. L'art. 3 LSI déclare, en outre, que les règles fédérales en matière de sécurité de l'information s'appliquent aux cantons dans deux situations définies : d'une part, lorsqu'ils traitent des informations classifiées de la Confédération, et d'autre part, lorsqu'ils accèdent à des moyens informatiques appartenant à celle-ci. Cette application est cependant subsidiaire par rapport au droit cantonal. Si le droit cantonal assure un niveau de sécurité équivalent à celui exigé par la Confédération, les règles fédérales cessent de s'appliquer au profit des règles cantonales. L'objectif est d'imposer un socle minimal de protection dans les cas d'interaction directe avec des ressources de la Confédération, tout en respectant l'autonomie cantonale, lorsque celle-ci garantit un niveau de sécurité comparable.

Finalement, la Confédération dispose d'une compétence implicite en matière de préservation de la sûreté intérieure et extérieure de la Suisse⁶⁵, lui ayant permis d'édicter, par exemple, une réglementation relative aux cyberattaques dirigées contre des infrastructures critiques.

⁶⁰ Sur le sujet : CONSEIL FÉDÉRAL, Rapport en exécution du postulat 23.3050 du 6 mars 2023 déposé par le Groupe du Centre « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », 19 septembre 2025, p. 12. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

⁶¹ CONSEIL FÉDÉRAL, *Avis sur le modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique*, 19 septembre 2025. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

⁶² ANS, *Développement de l'Administration numérique suisse (ANS) – Rapport sur la future coopération fédérale dans le domaine de l'administration numérique*, 13 mars 2025, pp. 22 ss. Document disponible à l'adresse Internet : www.administration-numerique-suisse.ch > À propos de nous > Administration numérique suisse > Administration numérique suisse > Mise en place par étape de l'Administration numérique suisse.

⁶³ CONSEIL FÉDÉRAL, Rapport en exécution du postulat 23.3050 du 6 mars 2023 déposé par le Groupe du Centre « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », 19 septembre 2025. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

⁶⁴ Conseil fédéral, Rapport en exécution du postulat 23.3050 du 6 mars 2023 déposé par le Groupe du Centre « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », 19 septembre 2025. Document disponible : www.admin.ch > Documentation > Communiqués > Communiqués du Conseil fédéral > 19.09.2025 > Le Conseil fédéral approuve le projet de modèle cible relatif à la future coopération fédérale dans le domaine de l'administration numérique.

⁶⁵ ATF 117 Ia 202, consid. 4a, b et d.

Interconnexion des banques de données de la Confédération et des cantons

Selon l'art. 74b LSI, les autorités cantonales et communales sont identifiées comme des infrastructures critiques. À ce titre, ils sont tenus de signaler les cyberattaques contre leurs moyens informatiques auprès de l'OFCS. En contrepartie, ils bénéficient d'un soutien de ce dernier contre les cybermenaces. Ce soutien consiste en particulier dans la fourniture d'informations techniques et de recommandations sur les cybermenaces, de même que la mise à disposition d'instruments techniques de détection des cyberincidents. Une intervention plus importante de la Confédération dans ce domaine n'est pas envisagée à ce stade, la Confédération ne disposant pas des compétences lui permettant d'intervenir dans l'organisation interne des cantons, ce qui inclut les aspects liés à leur sécurité informatique. Le renforcement de la sécurité informatique peut toutefois également s'opérer au travers de l'adoption de normes techniques de sécurité via l'ANS ou dans le cadre de la cyberstratégie nationale à laquelle participent la Confédération et les cantons⁶⁶.

5.2 Exemple du Référentiel cantonal fribourgeois

Le canton de Fribourg vient d'adopter une modification de sa loi sur la cyberadministration⁶⁷ visant à compléter, après une phase pilote, les bases légales nécessaires à l'exploitation d'un Référentiel cantonal de données⁶⁸. Il s'agit d'un registre centralisé réunissant les données de référence nécessaires à l'identification des personnes physiques, des personnes morales et autres organisations reconnues, ainsi que des données liées au bâti.

Le Référentiel cantonal correspond à une architecture de type « consolidation⁶⁹ » dotée d'une gouvernance centrale. Il est alimenté par différentes banques de données de la Confédération, du canton et des communes. Ces données sont centralisées puis croisées afin de détecter les éventuelles divergences et de procéder à leur correction. Une fois ce processus achevé, les données sont ensuite mises à disposition des organes publics selon une logique Once-Only pratiquée à l'échelon cantonal, conformément à une autorisation d'accès individuelle octroyée par l'organe en charge du Référentiel cantonal.

En plus des données issues des banques de données cantonales et communales du canton de Fribourg, le Référentiel cantonal traite des données provenant de plusieurs registres fédéraux (Infostar, RegBL, UPI, SYMIC, REE, IDE). Différentes dispositions de la loi rappellent dans ce sens que le traitement des données provenant des registres fédéraux doit pleinement respecter le droit fédéral (art. 17e al. 1, 2e phr., art. 19 al. 2 et 22 al. 4 LCyb). C'est le cas, notamment, du traitement systématique du NAVS, soumis aux exigences des art. 153b ss LAVS. Bien qu'ils n'aient en soi aucune portée normative propre dès lors que le droit fédéral prime de toute manière le droit cantonal, ces rappels soulignent néanmoins les interdépendances entre les législations fédérales et cantonales dans le domaine des projets numériques à large échelle. Ils peuvent aussi servir à rappeler plus immédiatement aux organes cantonaux l'existence de dispositions fédérales. Sous l'angle technique, l'interopérabilité est assurée par l'utilisation de formats d'échange standardisés (normes eCH). En plus des bases légales, les modalités et la sécurité des échanges de données sont précisées dans des conventions fixant clairement les droits et les obligations de chaque partie.

⁶⁶ www.ncsc.admin.ch > Stratégie CSN > Cyberstratégie nationale CSN.

⁶⁷ Loi du canton de Fribourg du 18 décembre 2020 sur la cyberadministration (LCyb ; RSF 184.1).

⁶⁸ Loi du 4 septembre 2025 modifiant la loi sur la cyberadministration (Référentiel cantonal ; ROF 2025_066).

⁶⁹ *Supra* 4.4.2.

Interconnexion des banques de données de la Confédération et des cantons

6 Enjeux sociétaux

6.1 Équilibre entre mutualisation et fédéralisme

Dans un État fédéral comme la Suisse, l'interconnexion des systèmes entraîne des conséquences sur les relations qu'entretiennent les collectivités publiques entre elles. Si la mutualisation des systèmes d'information et des données vise à améliorer l'efficacité des services publics, elle peut aussi favoriser une forme de centralisation de l'État fédéral au détriment de l'autonomie cantonale ou communale, en particulier si les dépendances techniques entre systèmes se traduisent par des asymétries de contrôle et de ressources⁷⁰.

Pareil effet s'explique notamment par les interdépendances techniques qu'engendre l'interconnexion des systèmes. Lorsqu'un canton ou une commune devient dépendant d'une plateforme centrale, d'un service partagé ou d'un standard technologique piloté à un autre niveau, son autonomie décisionnelle et opérationnelle peut s'en trouver restreinte. Cette limitation est d'autant plus marquée si les ressources financières, les compétences techniques ou la capacité d'influence ne sont pas équitablement réparties entre les entités concernées.

Il est donc essentiel d'inscrire dès le départ toute interconnexion dans une logique de coopération équilibrée, où chaque entité conserve un pouvoir effectif sur ses ressources informationnelles tout en s'insérant dans un cadre commun d'interopérabilité. Cela suppose non seulement une répartition claire des compétences, mais aussi le développement de formes de collaboration respectueuses des prérogatives propres à chaque échelon et qui incluent la possibilité pour les autorités concernées de participer à la définition des standards techniques et des mécanismes de gouvernance partagés.

6.2 Transparence, confiance et acceptabilité sociale

La circulation accrue des données entre administrations publiques via des processus automatisés peut générer des préoccupations quant au risque de profilage administratif, à l'éventuelle réutilisation des données à des fins vagues ou non prévues initialement, ou encore à l'asymétrie d'information entre l'administration et les citoyens. Ces préoccupations peuvent être d'autant plus fortes que contrairement à d'autres activités de l'État, le traitement des données est une activité largement invisible pour les citoyens.

Certes, le traitement des données est généralement réglementé par la loi et donc, dans une certaine mesure, public. Néanmoins, il est aujourd'hui très difficile sinon impossible pour quiconque d'avoir une vue d'ensemble des traitements de données le concernant. Même quand une base légale peut être identifiée, celle-ci n'est pas toujours rédigée d'une manière totalement claire et compréhensible pour les citoyens. Cette opacité peut renforcer le sentiment de perte de contrôle sur l'usage des données personnelles et générer un sentiment de surveillance diffus auprès de la population.

Pour assurer un niveau de transparence suffisant, d'autres instruments de publicité que la loi pourraient être utilisés dans le futur. En 2021, l'ANS a commandé une étude de faisabilité concernant la mise en place d'un « modèle de traçabilité de l'utilisation des données personnelles » permettant à chaque personne de voir qui a consulté ses données personnelles. L'étude conclut que la mise en place d'un tel modèle est techniquement réalisable à long terme, mais qu'une mise en œuvre à large échelle est actuellement peu faisable en raison de la complexité du paysage informatique suisse et du manque d'éléments facilitateurs (comme une E-ID nationale ou des standards harmonisés). L'étude préconise à la place une mise en

⁷⁰ Voir : E-PIAF, The Road to Automated Democracy – Monitor demokratikompatible Digitalisierung des Staates 2025, p. 44 ss.

Interconnexion des banques de données de la Confédération et des cantons

œuvre partielle et graduelle en commençant avec un petit nombre de registres ou de portails sélectionnés.⁷¹

7 Cadre juridique

7.1 Constitution

7.1.1 Structure fédérale de la Suisse

La transformation numérique met à l'épreuve le fédéralisme suisse en réinterrogeant certains fondements classiques de l'organisation étatique, tels que la souveraineté des cantons, la répartition des compétences et le principe de subsidiarité (art. 3, 5a, 43a et 47 Cst.). En vertu de ces principes, la Confédération ne dispose pas d'une compétence générale qui lui permettrait de régler tout échange de données avec les cantons. Une telle compétence ne peut pas non plus être déduite de la combinaison de ses différentes compétences sectorielles. Dans de nombreux domaines, les compétences fédérales et cantonales régissant le traitement des données personnelles sont en effet fortement enchevêtrées.

Le passage à l'administration numérique, en particulier sous l'angle de l'interconnexion des banques de données, est néanmoins susceptible d'affecter directement la manière dont les différents niveaux de l'État collaborent et exercent leurs compétences respectives. Tandis que les exigences techniques liées à la digitalisation appellent une harmonisation croissante des normes, de la sémantique et des interfaces aux trois échelons de l'État, le fonctionnement et l'organisation de l'administration demeure largement différenciés selon qu'on se situe à l'échelle de la Confédération ou de chaque canton. Sans nullement remettre en question le principe du fédéralisme, ce décalage structurel peut néanmoins constituer une source de tension entre la logique de coordination inhérente à la transition numérique et l'autonomie organisationnelle reconnue par la Constitution à chaque canton.

Au-delà de ces aspects, l'interopérabilité juridique doit aussi être attentivement examinée. Lorsque la Confédération n'a pas la compétence nécessaire pour tout régler dans le droit fédéral, un échange de données entre collectivité ne peut intervenir qu'à la condition que chaque collectivité (Confédération, canton ou commune) dispose dans son droit interne des bases légales nécessaires tant pour le traitement que pour la communication des données concernées. Cette exigence de double légalité rend les interconnexions complexes à piloter du point de vue législatif. En l'absence de mécanisme préventif formel de vérification des projets législatifs entre collectivités, il n'existe aucun contrôle systématique de la cohérence normative entre les différents systèmes juridiques.

Le seul contrôle réellement opérant en la matière reste à ce jour celui exercé par les tribunaux. Il s'agit cependant d'un contrôle *a posteriori*, qui intervient seulement une fois l'acte législatif en question adopté ou entré en vigueur. À titre d'exemple, le Tribunal fédéral a déjà déclaré illicite par trois fois l'introduction d'un système cantonal de recherche automatisée de véhicules et de surveillance du trafic (RVS) nécessitant l'interconnexion de banques de données fédérales et cantonales. À chaque fois, la collectivité concernée n'était pas parvenue à créer des bases légales suffisamment précises pour autoriser le traitement souhaité⁷². Cet

⁷¹ <https://www.administration-numerique-suisse.ch/fr/plan-de-mise-en-oeuvre-de-la-cyberadministration/elaborer-un-modele-de-tracabilite-de-lutilisation-des-donnees-personnelles> > Synthèse en français de l'étude de faisabilité "modèle de tracabilité de l'utilisation des données personnelles".

⁷² ATF 146 I 11, consid. 3.3 ; ATF 149 I 218, consid. 8 et ATF 151 I 137, consid. 3.

Interconnexion des banques de données de la Confédération et des cantons

exemple peut révéler le besoin de fournir certains outils afin d'aider les collectivités concernées dans l'élaboration de leurs bases légales sans toutefois empiéter sur leurs prérogatives en matière de législation⁷³.

7.1.2 Droits fondamentaux

L'interconnexion croissante des banques de données administratives renforce les capacités de traitement, de croisement et d'accès à l'information détenue par les autorités. Si elle peut améliorer l'efficacité de l'action publique, elle peut aussi soulever certaines préoccupations au regard du droit fondamental à la vie privée, à la protection des données personnelles et à l'autodétermination informationnelle (art. 10 al. 2 et 13 Cst.).

En particulier, la mise en place de solutions électroniques permettant un accès direct et en temps réel à de multiples banques de données, sans contrôle individuel préalable, accentue les possibilités de surveillance et la constitution de profils de la personnalité des individus. La jurisprudence du Tribunal fédéral relève parfois dans ce sens le risque d'un *chilling effect*, soit d'un effet dissuasif pouvant amener un individu à s'auto-censurer par crainte d'une possible réutilisation ultérieure, non prévue, de ses données par les autorités⁷⁴. Pour cette raison, l'interconnexion de plusieurs banques de données requiert à chaque fois un examen attentif de l'intérêt public poursuivi, des effets négatifs possibles et de son caractère proportionné.

En fonction des résultats de cet examen, une intervention plus ou moins importante du législateur devra être envisagée. En l'absence de risque particulier (p. ex. pour l'accès à des données comme le nom, le prénom, l'adresse, la date de naissance à un nombre restreint d'acteurs), la communication automatisée des données peut être réglée soit dans une loi au sens matériel, soit dans une loi au sens formel, le choix entre l'un ou l'autre pouvant être dicté par différents motifs. En revanche, lorsque l'interconnexion envisagée porte sur des données sensibles, sert à des activités de profilage ou soulève d'autres risques particuliers (p. ex. un volume particulièrement important de données, un nombre très élevé d'utilisateurs potentiels et/ou un contexte jugé délicat), elle devra en principe être expressément prévue dans une loi au sens formel et faire l'objet d'une description suffisamment précise et détaillée (art. 36 al. 1, 2^e phr. Cst. *cum* art. 34 al. 2 LPD). En tel cas, il est toutefois possible de répartir la réglementation entre la loi qui fixe les principes essentiels et une ordonnance qui précise les aspects secondaires.

7.1.3 Dispositions importantes qui fixent des règles de droit

En vertu de l'article 164 al. 1 Cst., toutes les dispositions importantes qui fixent des règles de droit doivent être édictées sous la forme d'une loi adoptée par le Parlement. Cette disposition réserve de manière générale à l'Assemblée fédérale le soin d'adopter les dispositions les plus importantes qui fondent l'activité de l'État à l'exclusion du Conseil fédéral. La Constitution énumère une série de dispositions jugées importantes, parmi lesquelles figurent les règles fondamentales relatives à l'organisation et à la procédure des autorités fédérales (let. g). Selon la doctrine, cela inclut notamment les règles relatives au traitement des affaires à l'interne, de même que l'établissement de relations ou de collaborations avec d'autres autorités⁷⁵.

⁷³ Cf. infra 9.1.

⁷⁴ ATF 146 I 11, consid. 3.2 ; ATF 149 I 218, consid. 8.11.2 et ATF 151 I 137, consid. 3.3.1. Voir aussi : décision de l'ancienne Commission fédérale de la protection des données et de la transparence n° 09/05 du 15 février 2006, in : ZBI : 108/2007 392, p. 397.

⁷⁵ DUBEY Jacques, in : Dubey Jacques / Martenet Vincent (édit.), CoRo Cst., Bâle 2021, ad. art. 164 Cst., n° 46.

Interconnexion des banques de données de la Confédération et des cantons

En pratique, il est vrai que l'exigence de légalité formelle pour les règles d'organisation ne s'est pas systématisée avec la même intensité que pour les autres catégories de normes importantes citées par la Constitution. On admet généralement qu'en tant qu'autorité exécutive le Conseil fédéral est plus apte à régler l'organisation et le fonctionnement de l'administration fédérale que ne l'est probablement le Parlement (art. 178 Cst. *cum* art. 8 LOGA)⁷⁶. Il n'empêche que les normes d'organisation sont loin d'être neutres tant du point de vue de l'État de droit que des effets qu'elles déploient sur les citoyens. Car en organisant l'administration et en décidant des outils à sa disposition, elles influent directement sur les capacités d'action de l'État⁷⁷.

Il est désormais largement admis que la transformation numérique modifie en profondeur le fonctionnement et l'organisation de l'État. Reste à déterminer quelles conclusions en tirer du point de vue du droit. Si l'introduction de nouvelles technologies numériques peut être souhaitable, elle fait également apparaître des modes de gestion et d'organisation totalement inédits au sein de l'État. L'interconnexion des bases de données a, par exemple, redéfini en des termes nouveaux le problème classique de la centralisation et de la décentralisation en rendant plus facilement accessibles à l'État central des données en provenance de la périphérie et inversement.

Il ne s'agit pas de considérer que chaque projet d'interconnexion nécessite sur ce fondement systématiquement une base légale formelle, mais ce phénomène ne peut pas non plus être réduit à un simple ajustement technique. À ce titre, au-delà des critères posés par l'art. 36 Cst. et la LPD, tout nouveau projet d'interconnexion devrait également faire l'objet d'un examen à la lumière de l'article 164 al. 1 Cst., tenant compte de son impact global sur l'organisation et le fonctionnement de l'État, ainsi que de ses effets sur l'administration et les citoyens.

7.2 Loi sur la protection des données

7.2.1 Dispositions générales

Le traitement des données personnelles effectué par des organes fédéraux est régi par la LPD. Son but est de protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement (art. 1 LPD).

En principe, les organes fédéraux ne sont en droit de traiter des données personnelles que si une base légale les y autorise (art. 6 al. 1 et 34 LPD). Le traitement des données doit être conforme aux principes de la bonne foi et de la proportionnalité (art. 6 al. 2 LPD). Les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée, et doivent être traitées ultérieurement de manière compatible avec ces finalités (art. 6 al. 3 LPD).

Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données. Il le fait de manière proactive, dès la conception du traitement (art. 7 al. 1 LPD). Les mesures techniques et organisationnelles doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées (art. 7 al. 2 LPD). Il revient au responsable du traitement ainsi qu'à ses sous-traitants

⁷⁶ BIAGGINI Giovanni, in : BV Kommentar, 2e éd., Zurich 2017, ad art. 164 Cst., n° 7 et ad art. 178 Cst., n° 15. Également : FF 2007 5499, p. 5550.

⁷⁷ MONTAVON Michael, *Cyberadministration et protection des données*, thèse Fribourg, Genève / Zurich / Bâle 2021, p. 351.

Interconnexion des banques de données de la Confédération et des cantons

d'assurer par des mesures techniques et organisationnelles appropriées, un niveau de sécurité adéquat par rapport au risque encouru (art. 8 al. 1 LPD). Au plan fédéral, tous les organes fédéraux sont tenus de déclarer leurs traitements au PFPDT (art. 12 al. 4 LPD). Ces traitements sont enregistrés et peuvent être consultés sur la page internet <https://data-reg.edoeb.admin.ch/search>.

En offrant un accès en libre-service à des données provenant de systèmes tiers, l'interconnexion peut entrer en tension avec les principes de proportionnalité et de finalité, notamment en permettant un changement de finalité ou en limitant la possibilité de restreindre la transmission des données au strict nécessaire. Lorsqu'il est prévu par une disposition légale ou qu'il découle d'une modification législative émanant du même législateur, la survenance d'un changement horizontal de finalité n'est en principe pas contraire au droit de la protection des données⁷⁸. La légitimation démocratique du législateur fonde la licéité du nouveau traitement, tandis que la publicité des normes en assure la prévisibilité⁷⁹. La situation est différente en cas de changement vertical de finalité. En vertu du principe du parallélisme des formes, le législateur cantonal ne pourrait, en effet, pas, p. ex., modifier de sa propre initiative la finalité des données qui lui sont communiquées conformément au droit fédéral en vue de l'accomplissement d'une tâche spécifique.

Sous l'angle de la proportionnalité, l'étendue des données échangées au moyen d'une interconnexion ne peut, il est vrai, généralement pas être ajustée avec une précision absolue pour correspondre strictement au minimum requis dans chaque cas d'espèce. Une première analyse doit ainsi intervenir au moment de choisir l'interconnexion comme moyen de communication, en tenant compte du risque que certaines communications puissent s'accompagner de données éventuellement superflues. Si, en dépit de ce risque, le recours à l'interconnexion se révèle justifié, une seconde analyse doit être menée afin de déterminer cette fois l'étendue des données pouvant être partagées. À ce stade, un certain niveau de généralisation est néanmoins inévitable. Un équilibre raisonnable doit être trouvé entre, d'une part, le but et l'étendue de l'interconnexion et, d'autre part, l'atteinte portée aux droits fondamentaux des personnes concernées.

Dans son aide-mémoire du 18 juin 2024 sur l'obligation de prévoir et de motiver les accès en ligne⁸⁰, le PFPDT énumère les exigences qualitatives et quantitatives qu'il impose à l'administration fédérale dans le cadre de ses activités de conseil et de surveillance en matière de planification et de justification des projets correspondants de l'administration fédérale.

7.2.2 Communication de données personnelles

La communication de données consiste dans le fait de transmettre des données personnelles ou de les rendre accessibles (art. 5 let. e LPD). Les organes fédéraux ne sont en droit de communiquer des données personnelles que si une base légale le prévoit (art. 36 al. 1 LPD). La base légale exigée doit être de rang formel lorsque la communication porte sur des don-

⁷⁸ Arrêt du TF 6B_346/2024 du 8 novembre 2024, consid. 2.2.1. Dans cet arrêt, le TF a jugé illicite la réutilisation de données collectées sur la base d'une loi pour l'exécution d'une tâche déterminée, afin d'accomplir une autre tâche prévue par une loi différente. « *Die gestützt auf [das genannte Gesetz] erhobenen Daten dürften nur für den vorgesehenen Zweck verwendet werden. Eine Zweckänderung bedürfte einer gesetzlichen Grundlage* ».

⁷⁹ MEIER Philippe / TSCHUMY Nicolas, in : Meier Philippe / Météille Sylvain (édit.), CoRo LPD, Bâle 2023, ad art. 6 LPD, n° 55 et les références citées ; HELD Thomas / BRÖNNIMANN Markus, in : Bieri Adrian / Powell Julian (édit.), OFK DSG, Zurich 2023, ad art. 36 LPD, n° 12. Plus nuancée : EPINEY Astrid / ROVELLI Sophia, *Once-only et le principe de l'État de droit - Avis de droit établi sur mandat de privatim, la Conférence des préposés(e)s suisses à la protection des données*, in : digma n° 11 2022, n° 79 et 87.

⁸⁰ <https://www.edoeb.admin.ch/fr> > Actualités > Brèves > 2024 > 18.06 Aide-mémoire sur les accès en ligne.

Interconnexion des banques de données de la Confédération et des cantons

nées sensibles, qu'elle sert à des activités de profilage ou que la finalité ou le mode du traitement est autrement susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (art. 34 al. 2 let. a et c LPD).

Selon la LPD de 1992, la communication de données par procédure d'appel ou au moyen d'une liaison en ligne (« *durch ein Abrufverfahren* » en allemand) faisait l'objet de règles spécifiques. Ainsi, les organes fédéraux n'étaient en droit de rendre des données personnelles accessibles en ligne que si cela était prévu expressément ; les données sensibles ou les profils de la personnalité ne pouvaient être rendus accessibles en ligne que si une loi au sens formel le prévoyait expressément (art. 19 al. 3 aLPD).

Les règles spéciales sur les liaisons en ligne n'ont pas été reprises dans le cadre de la révision de la LPD 2020. Il n'en découle cependant aucune différence par rapport à la pratique qui prévalait sous la LPD de 1992. Selon le guide de législation en matière de protection des données, une communication de données par procédure d'appel ou au moyen d'une liaison en ligne constitue un mode de communication qui, comme tel, doit être prévu par la loi⁸¹.

« L'accès en ligne selon le principe du self-service est particulièrement susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée, il doit être prévu dans une loi au sens formel en tout cas lorsqu'il porte sur des données sensibles ou des données basées sur des profilages. Il peut figurer dans une loi au sens matériel si le responsable du traitement donne un accès en ligne à des données non sensibles et que la probabilité d'atteinte grave aux droits fondamentaux est réduite. De plus, le principe de finalité exige qu'un lien étroit soit établi entre l'accès en ligne et chaque tâche de l'autorité pour lesquelles il est requis. Par exemple, une autorité x a accès en ligne aux catégories de données y pour exécuter une tâche prévue à l'art. z de telle loi. Une autre autorité a accès en ligne aux catégories de données b pour accomplir une tâche c prévue à l'art. d de telle loi. Les bases légales nécessaires pour prévoir un accès en ligne seront d'autant plus précises que le risque d'atteinte aux droits fondamentaux est élevé. La gravité de l'atteinte doit être examinée en tenant compte non seulement de la nature des données mais aussi et en particulier du but du traitement. »⁸²

Ces explications pourraient toutefois être complétées afin de mieux tenir compte des caractéristiques propres aux différents modèles d'architecture existants⁸³. En l'état, la notion de procédure d'appel ou de liaison en ligne semble surtout se référer à l'établissement d'une liaison directe. Tout en conservant une approche technologiquement neutre, le guide de législation pourrait fournir des indications plus précises sur la manière d'élaborer des bases légales pour chaque modèle d'architecture en tenant compte de ses caractéristiques et des risques spécifiques qu'il soulève.

7.2.3 Traitements de données personnelles conjoints et sous-traitance

Un responsable du traitement est une personne ou un organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (art. 5, let. j, LPD).

⁸¹ Voir aussi : COSSALI SAUVAIN Monique, in : Benhamou Yaniv / Cottier Bertil (édit.), *Petit commentaire LPD*, Bâle 2023, ad art. 36, n° 24 ss.

⁸² OFFICE FÉDÉRAL DE LA JUSTICE, *Guide de législation en matière de protection des données*, version actualisée de mars 2024, p. 16 s. Disponible à l'adresse : www.bj.admin.ch > Etat & Citoyen > Légistique > Instruments de légistique.

⁸³ Cf. *infra* 9.2.

Interconnexion des banques de données de la Confédération et des cantons

Lorsqu'une autorité collecte et traite des données pour accomplir les tâches que la loi lui confie, elle est en principe seule responsable de ce traitement. Si elle communique ces données à un autre organe, sa responsabilité s'étend à l'acte de communication, mais non à l'usage que le destinataire fera ensuite des données. Ce principe s'applique aussi aux échanges entre autorités fédérales et cantonales. Ainsi, une autorité fédérale qui transmet des données à un organe cantonal doit respecter les bases légales fédérales applicables, y compris en matière de communication. En revanche, dès réception, le traitement ultérieur relève de la seule responsabilité de l'autorité cantonale, qui agira sur la base du droit cantonal ou fédéral en fonction de la matière.

La situation devient plus complexe en cas d'interconnexion de plusieurs bases de données. Dans ce cas, les rôles et les responsabilités des différents acteurs peuvent se superposer ou s'entrelacer. Lorsque plusieurs autorités ont un accès direct et continu à des données via une infrastructure partagée, la distinction classique entre responsable de la communication et responsable du traitement ultérieur tend à s'estomper. Il devient alors essentiel de clarifier les bases légales qui fondent chaque traitement ainsi que la portée de la responsabilité de chaque acteur, tant en matière d'accès aux données que de leur entretien ou de leur usage. Afin de garantir que chaque traitement reste conforme au cadre juridique applicable à l'autorité concernée, il est nécessaire de mettre en place une organisation appropriée, incluant des règles précises sur la gestion des droits d'accès, la traçabilité des consultations et les finalités autorisées. L'art. 33 LPD énonce dans ce sens qu'en présence d'un traitement conjoint de données avec d'autres organes fédéraux, avec des organes cantonaux ou avec des organes privés, le Conseil fédéral règle les procédures de contrôle et les responsabilités en matière de protection des données. Cette disposition est précisée par l'art. 6 OPDo, lequel exige que les traitements automatisés de données impliquant plusieurs ensembles de données interconnectés ou l'exploitation conjointe de systèmes d'information ou d'ensembles de données, soient encadrés par un règlement de traitement.

Le traitement conjoint de données doit être distingué de la sous-traitance. Contrairement aux responsables du traitement, le sous-traitant ne traite pas des données pour son propre compte mais pour le compte d'un ou plusieurs tiers, qui assument le rôle de responsables du traitement (voir art. 5 let. k LPD). Le recours à un sous-traitant est typique des solutions cloud mais peut aussi intervenir, par exemple, lorsque la gestion et l'entretien d'une plateforme est confiée à une entreprise privée ou même suivant les cas à un autre organe public. Il requiert d'accorder une attention particulière à l'encadrement contractuel de la relation de sous-traitance (art. 9 LPD).

7.2.4 Analyse d'impact relative à la protection des données

En vertu de l'art. 22 LPD, lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles (AIPD). L'AIPD est un outil important pour identifier, évaluer et mitiger à temps les risques propres à un nouveau traitement et prendre des mesures appropriées en vue de les minimiser.

L'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement (art. 22 al. 2 LPD). Même si on ne peut pas présumer que toute interconnexion de plusieurs bases de données entraîne *per se* à chaque fois un risque élevé pour les droits fondamentaux, cela peut néanmoins se produire dans certaines configurations. Tel

Interconnexion des banques de données de la Confédération et des cantons

peut être le cas, par exemple, lorsque l'interconnexion aboutit au traitement de données sensibles à grande échelle, qu'elle permet l'élaboration de profils de la personnalité, qu'elle produit des inférences non souhaitées, qu'elle favorise grandement la réutilisation de données pour des finalités secondaires imprévisibles et néfastes ou qu'elle instaure une surveillance généralisée.

La réalisation d'une AIPD peut être particulièrement difficile à mener en présence d'architectures complexes reliant plusieurs systèmes. Il est nécessaire de comprendre parfaitement le fonctionnement de chaque système non seulement individuellement mais aussi collectivement dans ses interactions avec les autres systèmes. Les personnes qui disposent des connaissances nécessaires à cette fin sont souvent réparties dans différents offices, voire dans des collectivités différentes. Il en résulte le besoin d'instituer dès les premières étapes du projet une coordination et une collaboration étroite entre les acteurs concernés.

Pour aider les organes publics à apprécier les risques d'un nouveau traitement et préparer les bases légales nécessaires à cette fin, le Conseil fédéral a adopté les Directives AIPD⁸⁴, lesquelles ont été complétées par différents outils développés par l'OFJ⁸⁵. Les Directives AIPD assurent la coordination entre, d'une part, la procédure d'évaluation des risques au sens de la LPD et, d'autre part, la procédure normative et la méthode de gestion de projet HERMES que l'administration fédérale applique notamment pour la conduite de projets informatiques.

7.2.5 Dispositions d'exécution

En plus de la LPD, des dispositions plus précises concernant la sécurité des données personnelles ont été introduites dans l'OPDo.

Tout nouveau traitement de données personnelles doit faire l'objet d'un examen préalable dont le but est d'établir le besoin de protection des données et de déterminer les mesures techniques et organisationnelles appropriées à prendre par rapport au risque encouru (art. 1 OPDo). En fonction du besoin de protection, le responsable du traitement est tenu de prendre des mesures pour assurer la confidentialité, l'intégrité et la disponibilité des données ainsi que la traçabilité des opérations de traitement (art. 2 et 3 OPDo). Les mesures à mettre en place peuvent concerner, à titre d'exemple, la gestion des droits d'accès, le chiffrement des données au repos et en transit, la journalisation des accès et des opérations inter-systèmes ou encore la mise en place d'un plan de continuité.

En présence de certains traitement automatisés de données, l'OPDo requiert en plus l'élaboration d'un règlement de traitement (art. 6 OPDo). Le but de ce document est de formaliser, documenter et encadrer du point de vue de l'organisation, de la conformité juridique et de la sécurité technique les traitements de données automatisés présentant un risque particulier. Sont notamment visés les systèmes d'information offrant des accès aux cantons, aux autorités étrangères, aux organisations internationales ou aux personnes privées, les systèmes d'informations constitués d'ensembles de données interconnectés ou encore l'exploitation d'un système d'information en commun avec d'autres organes fédéraux (art. 6 al. 1, let. d à f). Le règlement comprend, en particulier, des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir

⁸⁴ Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD), in : FF 2023 1882.

⁸⁵ www.bj.admin.ch > Etat & Citoyen > Protection des données > Informations destinées aux organes fédéraux.

Interconnexion des banques de données de la Confédération et des cantons

la sécurité des données. Il doit être mis à jour régulièrement et tenu à la disposition du conseiller à la protection des données (art. 6 al. 2 et 3).

La législation fédérale sur la protection des données prévoit que les organes publics de l'administration fédérale qui envisagent de créer de nouveaux accès en ligne doivent signaler les projets correspondants au PFPDT à un stade précoce (art. 31 OPDo). Cela lui permet dans le cadre de ses tâches légales de conseil et de surveillance d'influencer en temps utile l'élaboration des bases juridiques et la documentation des risques découlant des interconnexions prévues pour les droits fondamentaux de la population concernée. Le PFPDT exige des organes fédéraux responsables de tels projets qu'ils documentent la nécessité et l'étendue de la mise en place d'une interconnexion. Dans le cas d'interconnexions préexistantes, il exige une comparaison entre la situation actuelle et la situation souhaitée. Le PFPDT exige en outre que les offices fédéraux responsables déclarent et justifient les interconnexions nouvelles ou supplémentaires également aux organes politiques compétents pour l'approbation des bases légales. Dans l'aide-mémoire précité, il énumère les exigences qu'il pose dans sa pratique par rapport à la planification et à la justification des projets correspondants de l'administration fédérale.

7.3 Loi sur la sécurité de l'information

La sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques au sens large sont réglées dans la LSI. La loi prévoit des règles sur la gestion des risques (art. 8), la collaboration avec les tiers (art. 9), la classification des informations et leur accès (art. 11 ss), la sécurité des moyens informatiques (art. 16 ss LSI) ainsi qu'une obligation de signaler les cyberattaques (art. 74a). Les règles applicables sont précisées dans l'OSI. Cette dernière prévoit en particulier :

- la mise en place d'un système de management de la sécurité de l'information (SMSI ; art. 5) ;
- l'obligation pour chaque unité administrative de tenir une liste des bases légales et des obligations contractuelles lui étant applicables en matière de sécurité de l'information (art. 6) ;
- l'établissement d'un inventaire des objets à protéger, y compris les collections d'informations traitées dans le but d'exécuter un processus d'affaires de la Confédération, mentionnant notamment si l'objet à protéger est partagé avec des tiers (art. 7) ;
- des mesures en matière d'évaluation et de gestion des risques (art. 8 OSI) ;
- la mise en place de formation et de sensibilisation en matière de sécurité de l'information (art. 11) ;
- la définition d'un plan de gestion des incidents (art. 12) ;
- la planification de contrôles et d'audits (art. 13).

En cas de traitement de données personnelles, les dispositions de la LSI et de l'OSI s'appliquent à titre complémentaire à la LPD s'agissant des mesures techniques et organisationnelles (art. 4 al. 2 LSI). Pour les cantons, la LSI et l'OSI s'appliquent à titre subsidiaire,

Interconnexion des banques de données de la Confédération et des cantons

lorsqu'ils exploitent des informations classifiées de la Confédération ou des moyens informatiques de cette dernière sans disposer de règles équivalentes dans leur droit interne (art. 3 LSI).

7.4 Loi sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités

La collaboration entre les autorités, y compris provenant de différentes collectivités, en matière d'utilisation des moyens électroniques est régie par la LMETA.

La loi encourage la mutualisation de moyens informatiques à l'intérieur de l'administration fédérale et avec les cantons (art. 11 LMETA), la reconnaissance de normes et l'usages d'interfaces communes (art. 12 et 13 LMETA) ainsi que la conclusion de convention avec d'autres collectivités publiques en Suisse afin de régler la collaboration nécessaire à l'usage partagé de moyens électroniques (art. 4 LMETA). Afin de simplifier la mise en œuvre de ces objectifs, la LMETA prévoit en outre la mise à disposition d'une plateforme en ligne fournissant des informations relatives aux jeux de données de l'administration fédérale, aux interfaces permettant leur utilisation ainsi qu'aux prestations des autorités disponibles sous forme électronique (plateforme d'interopérabilité I14Y⁸⁶ ; art. 14 LMETA).

Des dispositions plus précises figurent en supplément dans l'ONum. Elles consistent notamment dans :

- la mise à disposition centralisée de moyens informatiques (art. 11 ONum) ;
- l'harmonisation des données et des interfaces en fonction de leur cycle de vie (art. 15 ss ONum) ;
- l'élaboration de directives notamment en matière de processus, d'architecture d'entreprise et de normes (art. 40 ONum).

Vu le rôle de législation auxiliaire de la LMETA, la loi prévoit qu'elle est subsidiaire aux autres lois de la Confédération, notamment en matière de protection des données et de sécurité de l'information (art. 2 al. 4 LMETA). Compte tenu de l'opposition formée par les cantons dans le cadre de la consultation, le Conseil fédéral avait à l'époque expressément renoncé à faire figurer dans la LMETA des règles qui lui aurait permis d'imposer unilatéralement l'utilisation de services administratifs en ligne ou de normes⁸⁷.

8 Étude de cas et exemples en Suisse

Comme indiqué en introduction, le présent rapport ne fournit pas une vue d'ensemble complète des banques de données de la Confédération ni des interconnexions entre l'administration fédérale et les administrations cantonales ou communales. Au-delà de l'extrême difficulté à établir une telle cartographie dans le cadre de ce rapport, celle-ci fournirait uniquement un résultat figé qui risquerait d'être rapidement dépassé. À défaut, il a été demandé aux experts mandatés d'approfondir deux exemples concrets, sélectionnés sur la base de critère de pertinence et de représentativité. Le choix des experts s'est porté sur les systèmes VOSTRA et

⁸⁶ <https://i14Y.admin.ch>

⁸⁷ Voir à ce sujet la version initiale de l'art. 2, al. 2, AP-LMETA et le commentaire de l'art. 2 révisé P-LMETA, ainsi que les explications du CF in : FF 2022 804, p. 18.

Interconnexion des banques de données de la Confédération et des cantons

SYMIC⁸⁸. Une jurisprudence récente du Tribunal fédéral a conduit à ajouter l'exemple du système POLAP, qui illustre de manière concrète les difficultés juridiques liées à l'interconnexion entre systèmes fédéraux et cantonaux.

8.1 VOSTRA

VOSTRA est le système électronique d'information sur les casiers judiciaires géré par la Confédération. Il soutient les autorités en leur donnant accès à des extraits de casiers judiciaires individuels, en contenant des données actuelles sur les jugements pénaux et les procédures pénales en cours et en facilitant l'établissement d'extraits de casiers judiciaires. Il sert de source d'information pour différentes autorités suisses autorisées et permet aux particuliers de consulter leur propre historique pénal. VOSTRA a fait l'objet d'un examen approfondi dans le cadre de l'expertise réalisée par BEG Impact AG⁸⁹.

Sur le plan de l'architecture, VOSTRA possède plusieurs interfaces avec des banques de données et des applications spécialisées de différents offices fédéraux et autorités cantonales. Il repose sur une architecture de type « consolidation » incluant une opération de comparaison avec la base de données UPI contenant le NAVS gérée par la CdC.

Sur le plan juridique, la gestion de VOSTRA et donc le traitement des données personnelles ainsi que leur communication sont réglés de manière exhaustive dans la LCJ et l'OCJ ainsi que dans le règlement de traitement y relatif. Aucune lacune n'a été identifiée par les experts. La responsabilité de VOSTRA incombe à l'OFJ, mais d'autres organes participent également à la tenue du registre en y saisissant des données (SERCO cantonaux et militaire) ou en fournissant les infrastructures nécessaires à son exploitation (CSI-DFJP, OFIT). Dans la mesure où des données de VOSTRA sont communiquées à des autorités cantonales en vue de leur traitement ultérieur, le droit cantonal est applicable et les autorités cantonales sont compétentes en matière de surveillance.

Sur le plan de la sécurité, de nombreuses mesures techniques et organisationnelles sont prévues pour protéger les données, en particulier la gestion des accès et des autorisations ainsi que la journalisation des accès. Ces mesures sont ancrées au niveau de la loi et font l'objet de contrôle par les autorités fédérales. Il n'a toutefois pas été possible dans le cadre de l'expertise menée de savoir dans quelle mesure les différentes autorités cantonales prévoient des mesures similaires pour les données reprises par VOSTRA. Le rapport d'expert suggère qu'il serait envisageable de préciser ces aspects dans une convention avec les cantons en application de l'art. 4 LMETA.

8.2 SYMIC

SYMIC est le système d'information central sur la migration et sert d'instrument de travail pour les domaines des étrangers, de l'asile et de la nationalité en Suisse. Il est le principal registre de personnes pour les ressortissants étrangers qui vivent ou séjournent en Suisse. SYMIC est utilisé aux trois échelons du fédéralisme par plus de 36 000 collaborateurs. Comme pour VOSTRA, SYMIC a fait l'objet d'un examen approfondi dans le cadre de l'expertise réalisée par BEG Impact⁹⁰.

⁸⁸ La méthode et les critères ayant conduit aux choix des deux exemples sont expliqués dans BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 38 et 76.

⁸⁹ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 38 ss.

⁹⁰ BEG Impact, *Schlussbericht Studie – Datenvernetzung zwischen Bund und Kantonen*, Schaffhouse 2024, p. 51 ss.

Interconnexion des banques de données de la Confédération et des cantons

Sur le plan de l'architecture, SYMIC est relié à plus de 30 systèmes tiers. Il repose principalement sur une architecture de type consolidation, bien que certaines données puissent être intégrées manuellement au moyen de liaisons directes entre SYMIC et certaines banques de données cantonales et communales.

Sur le plan juridique, les principales bases légales relatives à SYMIC figurent dans la LDEA et dans l'ordonnance SYMIC mais on trouve aussi certaines normes spéciales concernant SYMIC dans la LEI, la LAsi et la LN. Selon le rapport d'expert, l'ordonnance SYMIC fournit une bonne vue d'ensemble des ayants droits. Il pourrait cependant s'avérer nécessaire de la réviser dans le cadre du renouvellement de l'application. La responsabilité de SYMIC incombe au SEM, tandis que son développement et son exploitation sont confiés au CSI-DFJP. En cas de communication de données de SYMIC à des autorités cantonales, le droit cantonal est applicable et les autorités cantonales sont compétentes en matière de surveillance.

Sur le plan de la sécurité, les droits d'accès sont gérés au moyen d'un modèle de rôles et les accès sont attribués manuellement par le SEM. Les accès aux données sont journalisés et font l'objet d'un contrôle périodique. Une analyse détaillée des mesures techniques et organisationnelles mises en place n'a toutefois pas pu être réalisée dans le cadre de l'expertise. Comme pour VOSTRA, le rapport d'expert relève la possibilité de préciser ces aspects dans une convention avec les cantons en application de l'art. 4 LMETA.

8.3 POLAP

Le projet de plateforme nationale de recherche policière (POLAP) trouve son origine dans la motion 18.3592 de la conseillère nationale Corina Eichenberger. Il a pour objectif de permettre l'interconnexion des systèmes d'information de la Confédération, des cantons et de l'Union européenne au moyen d'un point d'accès centralisé, en permettant la mise en réseau des systèmes d'information de police existants. L'introduction de POLAP à l'échelle de la Suisse est cependant rendue compliquée en raison de l'interdépendance des bases légales entre le droit fédéral et le droit cantonal, ce qu'illustre un arrêt récent du tribunal fédéral⁹¹.

En raison de la souveraineté des cantons en matière de police, la mise en place d'un tel dispositif ne saurait, en effet, reposer uniquement sur des bases légales fédérales. À ce jour, trois options sont envisagées pour permettre l'introduction de POLAP :

- la conclusion d'une convention intercantonale avec la Confédération, permettant d'établir un cadre uniforme de traitement et d'échange des données policières ;
- une révision de la Constitution fédérale afin de conférer à la Confédération la compétence de régir l'accès aux données policières à l'échelon suisse ;
- l'adoption, canton par canton, de bases légales propres autorisant la participation au système POLAP.

En principe, la priorité est aujourd'hui donnée à l'option 1, fondée sur une convention intercantonale avec la Confédération. Toutefois, différents événements ont conduit à retarder l'adoption d'une telle convention. Dans l'intervalle, certains cantons ont opté pour l'option 3.

⁹¹ ATF 151 I 137, consid. 6.3-6.7.

Interconnexion des banques de données de la Confédération et des cantons

Ils ont choisi de légiférer unilatéralement afin de permettre une participation anticipée au système. C'est le cas du canton de Lucerne qui a procédé au moyen de l'art. 4^{octies} LPol/LU⁹², dont la teneur est la suivante :

§ 4^{octies} * Polizeilicher Informationssystem-Verbund des Bundes und der Kantone

¹Die Luzerner Polizei kann sich zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie zur Kriminalitätsbekämpfung an Systemen des Bundes und der Kantone beteiligen, um Daten über Personen, Fahrzeuge, Sachen und deren Vorgänge sowie über Vorermittlungen und Ermittlungen innerhalb von Strafverfahren auszutauschen.

²Sie kann die Daten gemäss Absatz 1, einschliesslich besonders schützenswerter Personendaten, mit anderen Behörden des Bundes und der Kantone im Abrufverfahren austauschen. Der Datenaustausch ist zu protokollieren.

³Der Regierungsrat regelt das Nähere, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die ausgetauscht werden können.

Saisi d'un recours contre cette nouvelle base légale, le Tribunal fédéral a commencé par déclarer qu'il ne voit pas bien comment un système d'information de police commun à la Confédération et aux cantons pourrait reposer sur une pluralité de bases légales cantonales distinctes et potentiellement divergentes. Considérant que l'art. 4^{octies} LPol/LU devait de toute manière être abrogé pour d'autres raisons, il a cependant laissé cette question ouverte.⁹³

Pour le Tribunal fédéral, la principale difficulté réside dans l'utilisation envisagée d'une procédure d'appel permettant un accès direct aux données policières, sans passer par une demande d'entraide administrative. Un tel mode de communication des données complique non seulement leur contrôle, mais augmente aussi significativement le risque d'échanges disproportionnés et de détournements de finalité. Il en découle ainsi un risque accru d'abus et d'atteintes graves au droit à l'autodétermination informationnelle, en particulier lorsque des données sensibles sont concernées.

Conformément à l'article 36 Cst., pareil traitement de données ne peut être admis qu'en présence d'une base légale claire au sens formel, de l'existence d'un intérêt public prépondérant, et dans le respect du principe de proportionnalité. Or, de l'avis du Tribunal fédéral, l'art. 4^{octies} LPol/LU ne répond pas à ces exigences. Il est formulé de manière trop vague, couvre l'ensemble des données issues de l'activité policière – y compris les données sensibles et celles issues d'enquêtes pénales – et autorise leur consultation par des autorités non spécifiées, sans définir concrètement les finalités ni les catégories de données concernées. En outre, il renvoie de manière générale à une ordonnance d'exécution pour des modalités jugées néanmoins essentielles. Du point de vue du Tribunal fédéral, l'art. 4^{octies} LPol/LU ne satisfait ainsi pas aux exigences de densité normative requises pour un tel traitement de données. Il doit donc être abrogé.⁹⁴

Le Tribunal fédéral conclut en indiquant que si la volonté du législateur lucernois avait été d'autoriser l'échange sans condition et sans restriction de toutes les données policières au moyen d'une procédure d'appel, peu importe la manière dont il s'y serait pris, la disposition

⁹² Modification G 2023-001 du 24 octobre 2022 de la Gesetz über die Luzerner Polizei du 27 janvier 1998 (PolG ; SRL 350).

⁹³ ATF 151 I 137, consid. 6.6.

⁹⁴ ATF 151 I 137, consid. 6.6.1 et 6.7.

Interconnexion des banques de données de la Confédération et des cantons

violerait dans tous les cas l'exigence d'un intérêt public prépondérant et le principe de proportionnalité. Rien ne saurait, en effet, selon lui, justifier un accès aussi large incluant aussi les cas mineurs.⁹⁵

L'exemple de POLAP illustre parfaitement bien la problématique de l'interconnexion des banques de données entre la Confédération et les cantons. En raison de la répartition des compétences qui prévaut dans le domaine policier, les cantons doivent également disposer de leurs propres bases légales pour être raccordés à POLAP. La Confédération ne dispose pas des compétences législatives suffisantes pour régler elle-même intégralement l'échange de données policières au niveau suisse⁹⁶.

9 Constat général et mesures d'amélioration envisagées

Le Conseil fédéral estime que, compte tenu de la complexité du sujet, l'interconnexion des bases de données au sein de l'administration fédérale est globalement bien maîtrisée. Il reconnaît certes qu'il existe un potentiel d'optimisation, mais ne constate aucune lacune majeure, y compris dans la collaboration avec les cantons. Le rapport d'experts arrive à la même conclusion et ne constate aucun besoin d'action manifeste dans ce domaine. Dans un souci d'amélioration continue, le Conseil fédéral examine néanmoins des mesures d'optimisation ciblées après avoir pris connaissance des recommandations générales du rapport.

9.1 Sous l'angle juridique

Chaque interconnexion devant faire l'objet d'un examen individualisé, le Conseil fédéral ne voit pas de nécessité d'intervention législative pour améliorer la situation en matière d'interconnexion des banques de données. Toutefois, il pourrait être utile de compléter et de préciser le guide de législation en matière de protection des données⁹⁷. Tout en veillant à respecter le principe de neutralité technologique, des indications plus précises pourraient être fournies dans le but de mieux décrire les éléments essentiels à faire figurer dans un acte législatif en cas d'interconnexion en tenant compte des différents types d'architecture possibles. Cela pourrait également inclure des éléments à destination des cantons afin de les aider à édicter leurs propres bases légales lorsque ces derniers veulent s'interconnecter à des moyens informatiques de la Confédération. Pour les accès à des systèmes fédéraux contenant des données particulièrement sensibles, il serait également possible de prévoir ponctuellement un mécanisme d'annonce selon lequel l'organe cantonal désirant accéder à une base de données fédérale devrait notifier à l'organe fédéral responsable les bases légales sur lesquelles repose la demande d'accès. Pareille mesure devrait toutefois rester réservée à des cas justifiés et requerrait dans tous les cas d'être prévue au moyen d'une base légale dans la législation concernée.

Vu la diversité des modèles d'interconnexion envisageables⁹⁸, la possibilité d'élaborer des recommandations générales sur la manière de rédiger les bases légales nécessaires à l'interconnexion n'est toutefois pas certaine. Cette question devra faire l'objet d'une analyse plus approfondie afin d'en évaluer la possibilité et d'identifier d'éventuelles pistes de solution.

⁹⁵ ATF 151 I 137, consid. 6.6.2.

⁹⁶ Conseil fédéral, Message concernant l'approbation et la mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive (UE) 2023/977 relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil (Développement de l'acquis de Schengen) du 4 septembre 2024, in FF 2024 2359, p. 16 s.

⁹⁷ Document disponible à l'adresse : www.bj.admin.ch > Etat & citoyen > Légistique > Instruments de légistique > Guide de législation en matière de protection des données.

⁹⁸ Cf. *Supra* § 4.2.

Interconnexion des banques de données de la Confédération et des cantons

9.2 Sous l'angle technique et sémantique

Les normes relatives notamment à la sémantique, à l'organisation et à la technique sont à l'heure actuelle élaborées principalement par l'association eCH, dans le cadre d'un partenariat public-privé. Les normes eCH ne sont cependant pas juridiquement contraignantes et n'ont donc qu'un caractère de recommandation. Seules les collectivités publiques peuvent déclarer ces normes contraignantes dans leur domaine de compétence respectif. À la suite de l'approbation du modèle cible relatif à la future collaboration fédérale dans le domaine de l'administration numérique et de la réponse au postulat Le Centre 23.3050 « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? », le Conseil fédéral a démarré les travaux de révision de la Constitution visant à créer une nouvelle compétence fédérale en matière de digitalisation.

La faculté de fixer de normes contraignantes, qui requiert de modifier la Constitution, complètera les instruments existants dans le domaine de la coopération fédérale. La majorité des représentants professionnels des trois échelons de l'État interrogés dans le cadre de l'évaluation de l'ANS est favorable à un tel changement, à condition de garantir que tous les niveaux soient fortement impliqués. Ces résultats coïncident d'ailleurs avec les expériences faites par d'autres pays (entre autres l'Allemagne et l'Autriche). L'objectif est d'inscrire dans la Constitution une compétence fédérale prévoyant des règles spécifiques relatives à la participation des cantons et des communes. Les normes à adopter seront ainsi dès le départ développées dans le cadre d'une coopération technique entre tous les échelons de l'État, de manière à permettre aux organes cantonaux et communaux compétents de prendre position sur le plan politique à des moments opportuns.

L'interconnexion durable des systèmes ne repose pas uniquement sur des normes techniques et des bases légales cohérentes, mais également sur une compréhension sémantique commune. Les autorités doivent utiliser des concepts et des définitions harmonisés afin d'éviter des divergences d'interprétation qui pourraient nuire à la sécurité juridique, à la qualité des données ou à leur réutilisation dans l'administration. L'élaboration de modèles de données de référence ainsi que la mise en place de catalogues de métadonnées, en s'appuyant sur les travaux menés au sein de l'Administration numérique suisse, permettraient de soutenir la cohérence des échanges. L'interopérabilité sémantique représente ainsi un complément essentiel aux dimensions juridique et technique, et constitue une condition préalable pour une mise en œuvre efficace du principe de saisie unique.

9.3 Sous l'angle de la sécurité

Sur le plan de la sécurité, la répartition des compétences entre la Confédération et les cantons limite les possibilités d'intervention de la Confédération en matière de sécurité informatique au niveau cantonal. La Confédération dispose certes d'une compétence implicite en matière de sécurité intérieure et extérieure, mais cette compétence ne lui permet qu'une marge d'action restreinte. La seule possibilité effective d'action qu'a la Confédération réside dans la fixation de règles minimales que les cantons doivent respecter lorsqu'ils accèdent à des ressources fédérales ou les utilisent.

Il est clair cependant que la sécurité informatique est un enjeu national et qu'une coordination et une collaboration sont nécessaires entre les trois échelons du fédéralisme. Si les cantons doivent définir de manière autonome leur organisation en matière de sécurité informatique, ils peuvent néanmoins se référer à plusieurs instruments pour les aider dans cette tâche. Le Réseau national de sécurité (RNS) a par exemple adopté à cet effet des « Recommandations

Interconnexion des banques de données de la Confédération et des cantons

de mise en œuvre des organisations cantonales pour la cybersécurité ». Sur le plan national, la Confédération et les cantons collaborent dans le cadre de la Cyberstratégie nationale (CSN) de 2023⁹⁹. Un comité de pilotage assure la planification et la coordination de la mise en œuvre de la stratégie et élabore un plan d'action en collaboration avec les principaux acteurs.

Finalement, la question se pose également de savoir si la Confédération devrait plus systématiquement prévoir des mesures de sécurité concrètes ainsi que leur suivi dans des conventions avec les cantons et/ou les communes en cas d'interconnexion. Mise en avant dans le cadre du rapport d'expert, la mise en œuvre d'une telle mesure semble toutefois relever davantage d'analyses au cas par cas que d'une approche globale, chaque situation étant différente. Le cas échéant, le besoin de prévoir des mesures concrètes de sécurité peut être identifié dans le cadre de la réalisation de l'analyse d'impact relative à la protection des données. Conformément au principe de la protection des données dès la conception (cf. art. 7 al. 1 LPD), le responsable du traitement doit de manière proactive intégrer, dès la phase de conception du projet d'interconnexion, des mesures techniques et organisationnelles appropriées visant à garantir un niveau de sécurité des données adapté aux risques identifiés.¹⁰⁰

10 Conclusion

Le phénomène de l'interconnexion des banques de données au sein de la Confédération et avec les cantons tend à se généraliser. Cette évolution promet des avantages considérables, tels qu'une administration plus efficace, mieux coordonnée et moins coûteuse, ainsi qu'un allègement sensible de la charge pesant sur les citoyens. Elle contribue ainsi de manière significative à l'objectif général de modernisation de l'action de l'État, qui repose sur une meilleure gestion de l'information.

Dans le même temps, cette évolution s'accompagne aussi de risques accrus, liés à l'accès facilité à des volumes importants de données en temps réel. En présence de données personnelles, elle peut aussi entrer en tension avec le respect du principe de proportionnalité, la limitation des finalités du traitement et la maîtrise des échanges tels qu'exigés par la législation sur la protection des données. Le Conseil fédéral est toutefois d'avis que ces risques peuvent être maîtrisés grâce à un travail législatif soigné et l'introduction proactive de mécanismes de sécurité et de contrôle adaptés.

Du point de vue juridique, chaque collectivité demeure compétente pour définir son propre cadre juridique dans les domaines qui ne relèvent pas du droit fédéral. La Confédération ne peut pas s'immiscer dans les processus législatifs des cantons ou seulement de manière marginale (p. ex. en prévoyant ponctuellement la nécessité d'un mécanisme d'annonce pour l'accès à des ressources informatiques de la Confédération). Afin de favoriser une approche plus harmonisée et cohérente des bases légales dans la législation et de faciliter la rédaction des bases légales futures en matière d'interconnexion (interopérabilité juridique), le Conseil fédéral a néanmoins demandé au DFJP d'examiner d'ici à la fin de l'année 2026 si des recommandations d'ordre légistique peuvent être établies sous l'angle légistique en complément de l'aide-mémoire du PFPDT et, dans l'affirmative, de compléter le guide de législation en matière de protection des données. Le cas échéant, ces recommandations devront tenir

⁹⁹ www.ncsc.admin.ch > Stratégie CSN > Cyberstratégie nationale CSN

¹⁰⁰ Supra § 7.2.1 et 7.2.4.

Interconnexion des banques de données de la Confédération et des cantons

compte de la jurisprudence du Tribunal fédéral et respecter le principe de neutralité technologique.

En plus des aspects juridiques, l'interconnexion requiert des efforts soutenus d'harmonisation des pratiques, des solutions techniques et de la sémantique (interopérabilité organisationnel, technique et sémantique), ce qui suppose la reconnaissance et l'application de normes communes. À l'heure actuelle, de tels efforts reposent sur des mécanismes de collaboration volontaire. L'adoption d'un futur article constitutionnel permettant de rendre ces normes contraignantes à tous les échelons du fédéralisme devrait toutefois faciliter et accélérer la transformation numérique de la Suisse dans le cadre d'une collaboration renouvelée et renforcée entre la Confédération, les cantons, les villes et les communes. Le Conseil fédéral s'est expressément prononcé en faveur d'une telle solution dans sa réponse au postulat Le Centre 23.3050 « Définir des normes contraignantes pour le paysage de l'administration numérique suisse. Faut-il inscrire la numérisation dans la Constitution fédérale ? » et il a donné mandat au DFJP de lui soumettre un projet de révision constitutionnelle.

Enfin, en matière de sécurité, la Confédération ne peut imposer de mesures directes aux cantons que dans un cadre limité, soit lorsqu'elle peut se prévaloir de sa compétence implicite de préserver la sécurité intérieure et extérieure de la Suisse, soit, en se fondant sur la LSI, lorsque des organes cantonaux ou communaux accèdent à ses propres ressources ou utilisent ces dernières. Dans le second cas, non seulement la Confédération peut fixer les règles de sécurité applicables à ces ressources mais la sécurité des échanges de données entre bases de données fédérales et cantonales ou communales pourrait encore être renforcée par la conclusion plus systématique de conventions précisant les exigences de sécurité propres à chaque interconnexion. Pour le reste, Confédération, cantons et communes doivent continuer de collaborer pour assurer une cohérence durable et stratégique des exigences de sécurité et de leur mise en œuvre.

Interconnexion des banques de données de la Confédération et des cantons

Liste des abréviations

AIPD	Analyse d'impact relative à la protection des données
aLPD	Ancienne loi fédérale sur la protection des données de 1992
API	Application Programming Interface
ANS	Administration numérique suisse
BO	Bulletin officiel
CdC	Centrale de compensation
ChF	Chancellerie fédérale
CN	Conseil national
CO	Code des obligations
CSI-DFJP	Centre de services informatiques du Département fédéral de justice et police
Cst.	Constitution fédéral
IDE	Numéro d'identification des entreprise
DFJP	Département fédéral de justice et police
Infostar	Registre informatisé de l'état civil
FF	Feuille fédérale
JAAC	Jurisprudence des autorités administratives de la Confédération
LAVS	Loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (RS 831.10)
LAsi	Loi du 26 juin 1998 sur l'asile (RS 142.31)
LCJ	Loi du 17 juin 2016 sur le casier judiciaire informatique VOSTRA (RS 330)
LDEA	Loi du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (RS 142.51)
LEI	Loi du 16 décembre 2005 sur les étrangers et l'intégration (RS 142.20)
LMETA	Loi du 17 mars 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (RS 172.019)
LN	Loi du 20 juin 2014 sur la nationalité (RS 141.0)
LOGA	Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (RS 172.010)
LPD	Loi du 25 mars 2020 sur la protection des données (RS 235.1)
LSI	Loi du 18 décembre 2020 sur la sécurité de l'information (RS 128)
NAVS	Numéro d'assuré assurance-vieillesse et survivants
OCDE	Organisation de coopération et de développement
OCJ	Ordonnance sur le casier judiciaire informatique VOSTRA (RS 331)
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFS	Office fédéral de la statistique
OIAM	Ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM ; RS 172.010.59)
ONum	Ordonnance du 2 avril 2025 sur les services numériques et la transformation numérique dans l'administration fédérale (Ordonnance sur la numérisation ; RS 172.019.1)
OPDo	Ordonnance du 31 août 2022 sur la protection des données (RS 235.11)
Ordipro	Système d'information du Département fédéral des affaires étrangères
OREE	Ordonnance du 30 juin 1993 sur le registre des entreprises et des établissements (RS 431.903)

Interconnexion des banques de données de la Confédération et des cantons

ORegBL	Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements (RS 431.841)
OSI	Ordonnance du 8 novembre 2023 sur la sécurité de l'information dans l'administration fédérale et l'armée (Ordonnance sur la sécurité de l'information ; RS 128.1)
PFPDT	Préposé fédéral à la protection des données et à la transparence
POLAP	Plateforme nationale de recherche (de l'allemand Polizeiliche Abfrage-plattform)
RAVS	Règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants (RS 831.101)
RGPD	Règlement général européen sur la protection des données
SEM	Secrétariat d'État aux migrations
SERCO	Services de coordination cantonaux chargés du casier judiciaire et des profils d'ADN
SERCO militaire	Service de coordination de la justice militaire
SYMIC	Système d'information central sur la migration
VOSTRA	Casier judiciaire
REE	Registre des entreprises et des établissements
UE	Union européenne
UPI	Unique Person Identification
RegBL	Registre fédéral des bâtiments et des logements
TIC	Technologies de l'information et de la communication