



Berne, le 12 février 2025

Rapport sur l'application d'une science des données respectueuse de la vie privée

Solutions techniques de gestion de la confidentialité pour l'utilisation commune des données au sein de l'administration fédérale

Numéro du dossier : 031.21-688/6/7/1



Table des matières

1	Introduction	5
2	Concepts clés	8
2.1	Notions de base	8
2.2	Confidentialité des inputs et des outputs	10
3	Technologies d'amélioration de la confidentialité	15
3.1	Environnement d'exécution fiable	15
3.2	Chiffrement homomorphe	16
3.3	Calcul multipartite sécurisé	17
3.4	Apprentissage distribué.....	18
3.5	Preuve à divulgation nulle de connaissance	19
3.6	Confidentialité différentielle	20
3.7	Données synthétiques.....	22
4	Cas pratique 1 : Plateforme pour la pratique confidentielle de la science des données sans transfert de données	24
4.1	Contexte et objectifs.....	24
4.2	Principe	26
4.3	Limites et Défis.....	28
5	Cas pratique 2 : Enrichissement sécurisé de données par appariement confidentiel	30
5.1	Contexte et objectifs.....	30
5.2	Principe	33
5.3	Limites et Défis.....	36
6	Cadre légal et gouvernance	37
6.1	Traitement de données identifiantes – Revue du cadre légal.....	37
6.2	Limites du cadre légal existant.....	39
6.2.1	État de l'art des attaques d'extraction de données identifiantes : l'anonymisation mise en échec.....	39
6.2.2	Conséquences pour la législation encadrant la valorisation des données détenues par l'État	40
6.3	Les « Five Safes » : un cadre de gouvernance pour une science des données respectueuse de la vie privée	41
7	Recommandation pour l'administration fédérale	44

Résumé exécutif

Le Conseil fédéral a mandaté l'élaboration d'un concept sur l'application de la science des données respectueuse de la vie privée au sein de l'administration fédérale reposant sur l'utilisation des technologies d'amélioration de la confidentialité. Ces techniques ouvrent de nouvelles opportunités de création de connaissance à partir des données détenues par l'administration tout en respectant la protection des données. En effet, elles permettent d'appliquer les techniques de la science des données sur des données relatives à des individus sans que ces dernières ne soient vues ou transférées, tout en contrôlant le risque de divulgation lié au partage des résultats. Afin de faire face à la demande toujours croissante en livraison et appariement de données détenues par l'administration fédérale, par l'intermédiaire du Data Science Competence Center (DSCC), l'Office fédéral de la statistique (OFS) évalue le potentiel de ces technologies afin de simplifier, accélérer et surtout limiter la charge administrative et technique nécessaire à la fourniture de ces services tout en garantissant les plus hauts standards en termes de protection de la vie privée.

Ce rapport est aligné sur plusieurs initiatives internationales, comme un décret présidentiel aux États-Unis sur l'utilisation sûre de l'IA, et les travaux de l'ONU en partenariat avec les fournisseurs de statistiques internationaux sur les technologies d'amélioration de la confidentialité. Afin d'illustrer l'impact de ces technologies sur une utilisation commune des données détenues par l'administration fédérale, ce rapport se concentre sur deux cas pratiques standards dont les applications touchent l'ensemble de la société suisse. Le premier décrit le principe, et offre une implémentation, d'une plateforme permettant l'application confidentielle et sécurisée de la science des données sans transfert de données à travers un accès distant. Ce cas pratique offre une solution technique standardisée et automatisée, et implémentant le principe de « Privacy-by-design » permettant de remplacer la livraison de données. Le plein potentiel des données détenues par l'administration n'est toutefois réalisable qu'avec la contribution du second cas pratique qui permet de mutualiser plusieurs sources de données afin de les enrichir. Ce service d'appariement confidentiel de données se positionne comme une alternative moderne et économe en ressources à l'appariement tel qu'il existe aujourd'hui. Le recours aux technologies d'amélioration de la confidentialité assure que les données au niveau individuel sont protégées tout en permettant leur utilisation commune. Ces cas pratiques ouvrent la voie d'une réutilisation plus efficace et plus large des données entre offices fédéraux mais aussi avec des acteurs externes tels que la recherche académique, les organisations (inter-)gouvernementales, non-gouvernementales et même le secteur privé tout en respectant la protection de la sphère privée.

La mise en perspective du cadre juridique actuel face aux avancées techniques, en particulier l'essor des technologies d'amélioration de la confidentialité, révèle toutefois certaines limites notamment l'impossibilité technique de garantir le caractère irréversible de l'anonymisation. De plus, à travers une implémentation stricte du principe de finalité, la réutilisation de données n'est permise en général qu'aux organes fédéraux à des fins ne se rapportant pas à des personnes, telles que la statistique, la planification et la recherche. Dans ce cadre, les technologies d'amélioration de la confidentialité offrent un nouvel ensemble d'outils permettant de garantir le respect de la sphère privée dans un contexte plus large que celui couvert par le cadre légal actuel. Cet élargissement nécessite toutefois la création d'un cadre de gouvernance fondé sur l'évaluation du risque et permettant d'assurer le respect de l'État de droit dans son ensemble. De cette manière, une plus large réutilisation des données est susceptible d'être politiquement et socialement acceptée, car veillant à ce que les avantages qu'elle apporte ne se fassent pas au détriment des citoyens, des ménages et des entreprises suisses.

Les technologies d'amélioration de la confidentialité offrent ainsi de nouvelles opportunités de gain en efficience pour l'administration fédérale ainsi que de création de valeur au profit du bien commun. Il est donc important que l'administration fédérale s'assure de disposer de l'infrastructure informatique ainsi que de l'expertise technique permettant l'utilisation de ces technologies. Combinées à un cadre juridique et de gouvernance adéquats, ces technologies joueront un rôle déterminant dans l'accomplissement toujours plus efficace des tâches de la Confédération au profit de l'ensemble de la société suisse dans le respect de sa constitution. Leur mise en œuvre doit venir soutenir l'administration fédérale dans ses

tâches sans porter atteinte à celles existantes, notamment celles de l'administration militaire et du Service de renseignement de la Confédération (SRC).

1 Introduction

Dans le cadre de la mise en œuvre de la stratégie de la Confédération en matière de science des données (DSStB), le Conseil fédéral (CF) a donné le mandat au DFI (OFS) d'élaborer un concept présentant des solutions techniques de gestion de la confidentialité pour l'utilisation commune des données au sein de l'administration fédérale et de rédiger le présent rapport sur l'application d'une science des données respectueuse de la vie privée (Chiffre 6 de la décision du CF du 2 décembre 2022 ; EXE 2022.2746).

Afin de répondre aux défis auxquels fait face aujourd'hui la société suisse dans des domaines tels que la santé, le climat, la mobilité, ou encore l'environnement, et pour prendre des décisions éclairées, l'État peut recourir toujours plus à l'élaboration de politiques publiques fondées sur les données. Toutefois, la systématisation de cette pratique n'est rendue possible que par une pleine exploitation du potentiel des données collectées par les différentes unités administratives. En effet, ces dernières se distinguent par leur qualité, leur exhaustivité et surtout leur fiabilité ce qui constitue un gigantesque potentiel de génération de valeur ajoutée pour le bien commun. Toutefois sa réalisation est aujourd'hui limitée et appelle à une facilitation des collaborations transversales à l'intérieur et à l'extérieur de l'administration fédérale, sans pour autant compromettre les préoccupations légitimes de protection des données des individus, entreprises, ménages suisses. L'administration fédérale se doit donc de développer une pratique pour une science des données respectueuse de la vie privée permettant de garantir le respect de l'état de droit lors de l'utilisation des données que les administrés lui confient.

La mise en place de conditions cadres afin de tirer pleinement profit des données détenues par l'administration y compris des méthodes issues du domaine de l'intelligence artificielle (IA), bénéficierait à l'économie et la société suisse. Elle fait écho à la volonté du Conseil fédéral de promouvoir des espaces de données fiables et l'autodétermination numérique, conscient du fait que « l'interconnexion des données offre un grand potentiel pour la société, l'économie, la science et les administrations »¹. La motion 22.3890 CSEC-E du 22.08.2022 qui demande l'élaboration d'une loi-cadre sur la réutilisation des données² souligne également la nécessité de trouver des solutions qui permettent la valorisation de toutes les données (et pas seulement des données ouvertes).

Au niveau international, le décret présidentiel (« Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence »)³ récemment promulgué aux États-Unis par l'administration Biden insiste sur le développement des conditions cadres du contrôle des risques de divulgation de données personnelles des citoyens américains par les systèmes d'IA. En Europe, le « Input Privacy-Preservation Techniques Project »⁴ réalisé dans le cadre de la Commission économique pour l'Europe des Nations unies illustre la pertinence des technologies d'amélioration de la confidentialité pour les

¹ <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-87780.html>

² <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20223890>

³ <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>

⁴ <https://unece.org/sites/default/files/2021-11/November%20workshop%202021%20HLG-MOS-PPT%20%281%29.pdf>

organisations statistiques. En particulier, l'« Office for National Statistics » au Royaume-Uni évalue la possibilité d'utiliser ces technologies pour protéger les données de mortalité⁵.

Dans le cadre de la DSSStB, le rapport « Science des données pour le bien commun - cas d'application dans l'élaboration des politiques »⁶ a montré qu'exploiter pleinement le potentiel des données est un défi complexe qui nécessite l'implication de multiples parties prenantes et la mise en place de nombreuses compétences (organisationnelles, éthiques, légales, techniques). Au centre des problématiques liées à l'application de la science des données, il est nécessaire de mettre en place un cadre de gouvernance des données couvrant l'ensemble du cycle de vie des données (création, collecte, stockage, sécurité, accès, suppression etc.) autour de trois axes principaux :

- 1) L'infrastructure informatique : est notamment adressée dans le cadre du développement d'un concept pour une plateforme collaborative pour la science des données (Chiffre 4 de la décision du CF du 2 décembre 2022 ; EXE 2022.2746) et fait l'objet d'un rapport séparé.
- 2) La gestion des jeux de données : avec le programme de la Gestion nationale des données (NaDB ; EXE 2023.1946)⁷, le Conseil fédéral encourage l'utilisation multiple des données à long terme à travers le « Once-Only principle » soutenu par des initiatives d'harmonisation et la standardisation des métadonnées telles que la plateforme d'interopérabilité I14Y⁸ mise en place par le DFI (OFS) et les services Linked Data LINDAS proposés par le DFI (AFS)⁹. La libération du plein potentiel des données détenues par l'administration publique repose sur ces projets qui inventorient les données collectées par l'administration et en assurent leur interopérabilité. Outre la délimitation précise du patrimoine de l'administration fédérale en matière de données, les métadonnées sont aussi essentielles à l'application d'une science des données respectueuse de la vie privée.
- 3) La gestion de la confidentialité : afin de satisfaire aux attentes des administrés en termes de respect de la vie privée, l'exploitation des données détenues par l'administration fédérale est aujourd'hui principalement encadrée soit par une stricte non-réutilisation à d'autres fins que celle de la collecte, soit par une obligation d'anonymisation notamment dans la publication de données en tant que « Open Government data ». Au vu des avancées scientifiques des vingt dernières années, en particulier dans le domaine des attaques permettant d'extraire des informations personnelles de publications statistiques ou de modèles d'intelligence artificielle, l'anonymisation apparaît malheureusement comme une promesse techniquement inaccessible. Afin de maintenir la confiance des administrés envers l'État et de rendre possible la réutilisation des données qu'il détient, le cadre de gouvernance de la confidentialité des données doit être renouvelé. De nouveaux instruments légaux soutenus par des technologies d'amélioration de confidentialité doivent être mis en place afin d'assurer que les « Five Safes »¹⁰, c-à-d « Safe People », « Safe Project », « Safe Setting », « Safe Data » et « Safe Output », soient encadrés lors de toute réutilisation de données détenues par l'administration fédérale.

⁵ <https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/deaths/methodologies/applyingdifferentialprivacyprotection-toonsmortalitydatapilotstudy>

⁶ [Science des données pour le bien commun - cas d'application dans l'élaboration des politiques - | Publication](#)

⁷ <https://www.bfs.admin.ch/bfs/fr/home/nadb/nadb.html>

⁸ <https://www.i14y.admin.ch/>

⁹ <https://lindas.admin.ch/>

¹⁰ <https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/>

La collaboration de nombreux acteurs, aussi bien dans le domaine informatique que législatif, est donc nécessaire pour réaliser le plein potentiel des données détenues par l'administration fédérale au profit de l'ensemble des acteurs de la société suisse. Le présent rapport se concentre sur la description de solutions techniques permettant l'implémentation d'un cadre de gouvernance de gestion de la confidentialité. Il inclut aussi des exemples de leur mise en pratique pour opérationnaliser la gestion de la confidentialité dans le contexte de la gouvernance des données. Il explicite notamment le potentiel des technologies d'amélioration de la confidentialité (Privacy-Enhancing-Technologies, PET) pour de nouvelles possibilités de valorisation des données tout en respectant leur confidentialité. Les technologies d'amélioration de la confidentialité favorisent notamment l'analyse collaborative de données qui seraient autrement trop sensibles pour être partagées avec des tiers ou réutilisées pour une autre fin que celle pour laquelle elles ont été collectées.

Dans le cadre des Nations unies, le Comité d'experts des Nations unies sur le Big Data et la science des données pour les statistiques officielles (UNCEBD) a créé en 2018 un groupe de travail chargé de soutenir les offices statistiques nationaux dans l'utilisation des technologies d'amélioration de la confidentialité (UNTask Team on Privacy-Enhancing-Technologies). Ce dernier a publié un guide sur le sujet¹¹. En effet, la gestion de la confidentialité, et plus particulièrement le contrôle du risque de divulgation, est un sujet de prédilection des offices statistiques qui doivent assurer la confidentialité des données qui leurs sont confiées afin de satisfaire au principe 5 du code de bonne pratique de la statistique publique¹². L'OCDE a quant à elle publié un rapport destiné à aider les décideurs politiques à mieux comprendre comment ces technologies d'amélioration de la confidentialité peuvent être utilisées pour améliorer la protection de la vie privée tout en facilitant le partage de données ou d'informations¹³. L'ordre exécutif de l'administration Biden mentionné plus haut identifie d'ailleurs clairement les technologies d'amélioration de la confidentialité comme élément technique clé pour une utilisation sûre et efficace des données au sein de l'administration fédérale.

Dans cette perspective, ce rapport s'applique à proposer des concepts techniques qui puissent avoir la plus grande portée possible, à la fois au niveau fédéral, national et international. Ces concepts doivent donc être portables, doivent pouvoir être exportés, réutilisés et compatibles avec des initiatives de standardisation de métadonnées, avec la plateforme I14Y, et de promotion d'un vocabulaire commun grâce aux ontologies proposées par les services LINDAS.

Après une définition des notions de base et des acteurs en présence lorsqu'on parle d'utilisation commune de données identifiantes, diverses technologies d'amélioration de la confidentialité sont présentées, avec leurs avantages et leurs faiblesses respectives pour une utilisation dans le contexte de l'administration fédérale.

Deux cas pratiques sont ensuite présentés, avant de passer en revue les bases légales existantes et comment les technologies d'amélioration de la confidentialité peuvent contribuer à la mise en œuvre des principes fondamentaux de protection de la vie privée et enfin proposer des recommandations pour la mise en place d'un cadre de gouvernance pour la gestion de la confidentialité utilisant au mieux les technologies présentées dans ce rapport tout en respectant le cadre légal de la protection des données. Ce cadre de gouvernance se doit d'assurer que ces technologies soutiennent l'administration fédérale dans ses tâches sans toutefois porter atteinte à celles existantes, notamment celles de l'administration militaire et du SRC.

¹¹ <https://unstats.un.org/bigdata/task-teams/privacy/guide/>

¹² <https://unstats.un.org/unsd/dnss/docs-ngaf/National%20Code%20of%20Good%20Practice.pdf>

¹³ https://www.oecd-ilibrary.org/science-and-technology/emerging-privacy-enhancing-technologies_bf121be4-en

2 Concepts clés

2.1 Notions de base

Avant de présenter en détail les différentes technologies permettant de mettre en place une science des données pour une utilisation commune des données au sein de l'administration fédérale, il est nécessaire de préciser la signification des concepts utilisés dans ce rapport. En effet, la protection des données est par nature interdisciplinaire et fortement dépendante du contexte d'utilisation des données. Ainsi il est nécessaire de préciser le sens des termes employés dans le cadre de ce rapport. Les définitions choisies sont déterminées premièrement par le cas pratique que nous examinons, c'est-à-dire l'utilisation commune de données détenues par l'administration fédérale, et deuxièmement pour assurer une compatibilité avec le standard international de langue anglaise : la version anglaise de chaque concept est précisée en parenthèse afin de faciliter les liens avec la littérature scientifique de référence.

Dans ce rapport, une **unité identifiable** (identifiable unit), aussi appelée **unité de confidentialité** (Privacy unit), fait référence à toute personne physique ou morale, ou tout groupement de ces dernières, comme un ménage, générant des informations ne faisant pas partie du domaine public et dont le contenu doit être protégé. Pour les personnes physiques, une unité identifiable est aussi appelée personne concernée (Data subject). La généralité adoptée dans ce rapport est nécessaire car, d'un point de vue technique, assurer la protection d'un groupe d'individus, comme un ménage, demande des mesures plus importantes que d'assurer la protection de chaque personne physique qui le compose.

Ainsi, le terme « **données identifiantes** » fait référence à toutes les informations collectées sur une, ou un ensemble de personne(s) identifiable(s). La nature d'une donnée ne déterminant pas son caractère identifiant, toute donnée associée à une unité identifiable doit être considérée comme identifiante. En effet, les techniques modernes de réidentification ne reposent pas sur la valeur d'une donnée prise individuellement mais sur leur combinaison : c'est sur ce principe que repose les attaques par appariement, voir section 6.2 pour plus de détails.

Si l'unité identifiable est une personne physique, comme dans le cadre des lois sur la protection des données comme la Loi fédérale sur la protection des données ([Art. 5 let. a LPD ; RS 235.1](#)), on parle alors de **données personnelles** (personal data). Lorsqu'il s'agit de personnes morales, la législation utilise le terme de **données concernant des personnes morales** (LOGA, [RS 172.010](#)). L'application de la science des données respectueuse de la vie privée dépasse le cadre de ces lois couvrant, par exemple, aussi l'ordonnance concernant l'exécution des relevés statistiques fédéraux ([RS 431.012.1](#)) qui dispose que « les résultats des relevés seront rendus accessibles au public sous une forme qui exclut toute identification des personnes, des ménages, des entreprises ou des établissements interrogés ». Cet exemple, incluant aussi bien la protection de personnes physiques, de personnes morales et de leur groupement, motive le choix de distinguer dans ce rapport les données personnelles des données identifiantes.

Un **produit de données** (Data Product) désigne tout produit dérivé de données identifiantes et développé grâce à l'application de la science de données. Ces produits tombent en général dans trois grandes catégories :

- Les micro-données : les jeux de données donnant des informations au niveau d'une / des personnes concernées (ou unité de confidentialité).
- Les résultats d'analyses de données : cette catégorie inclut par exemple la production de statistiques et plus généralement toutes informations concernant un groupe d'unités de confidentialité. Ces indicateurs objectifs sont particulièrement utiles pour l'élaboration de politiques publiques.

- Les modèles d'apprentissage machine et d'intelligence artificielle : ces derniers peuvent en effet être entraînés sur des données identifiantes avec un risque que ces dernières soient divulguées aussi bien lors du processus d'entraînement que lors de l'utilisation du modèle.

L'application d'une science des données respectueuse de la vie privée s'assure donc que les données identifiantes utilisées pour la génération de produits soient protégées. Dans ce cadre, il est nécessaire de distinguer deux objectifs différents :

- **La protection de la vie privée** (Privacy) qui a pour but de s'assurer que les produits de données satisfont un ensemble de standards. Ces derniers sont directement influencés non seulement par les lois mais aussi par la réalité sociale et culturelle contemporaine. Ces derniers déterminent ce qui est, ou n'est pas, acceptable au moment de la création du produit de données. Par exemple, la notion de sensibilité des données attachée à la protection de la vie privée est contextuelle, ne peut et ne doit pas être anticipée. En effet, à titre d'illustration, le genre d'un individu physique est souvent considéré comme une information non sensible car de notoriété publique. Toutefois, rendre public que la composition du genre d'un foyer a changé d'une année à l'autre, constitue la révélation d'une information considérée comme sensible, à savoir un changement de genre. Tous ces cas de figures ne peuvent pas être anticipés lors de la production d'un produit de données, d'autant plus que la sensibilité d'une information est le résultat d'un jugement de valeur tributaire de l'état de la société à un moment de son histoire.
- **La confidentialité** (Confidentiality) qui regroupe l'ensemble des mesures visant à maintenir secrètes des données identifiantes. La notion de confidentialité est donc objective, résistant au temps et beaucoup plus forte et difficile à mettre en place techniquement.

Dans ce rapport, l'objectif d'une science des données respectueuse de la vie privée est d'assurer la confidentialité des données identifiantes de chaque unité de confidentialité et non pas uniquement de se limiter à vérifier la conformité des produits avec les standards actuels. Cela a pour objectif de formuler un cadre formel indépendant de l'évolution des normes et dont le but peut être évalué objectivement. Ce choix s'inspire de la position du Bureau du Censu américain qui est tenu juridiquement d'assurer la confidentialité des personnes physiques dans l'ensemble des produits de données qu'il met à disposition¹⁴.

La confidentialité des données identifiantes doit être assurée autant durant le processus de production du produit de données que lors de sa mise à disposition et de son utilisation. Ainsi, en premier lieu il faut assurer la **sécurité des données**, c'est à dire empêcher l'accès non autorisé aux données identifiantes. Les principaux outils permettant d'assurer la sécurité des données reposent sur des techniques cryptographiques, d'authentification et de contrôle des droits d'accès. En second lieu, la confidentialité doit s'assurer que lors la mise à disposition du produit aucune donnée identifiable ne soit **divulguée**, c'est-à-dire ne soit rendue publique lors de la publication volontaire d'un résultat. Ces deux aspects de confidentialité sont complémentaires et définissent deux catégories de technologies qui seront décrites dans la section suivante.

¹⁴ <https://www.govinfo.gov/content/pkg/USCODE-2007-title13/pdf/USCODE-2007-title13.pdf>

Enfin, afin de positionner les objectifs d'une science des données respectueuse de la vie privée en fonction de la LPD (RS 235.1)¹⁵ et au Règlement Général sur la Protection des Données (RGPD¹⁶), nous rappelons la signification des termes suivants :

- **Anonymisation** : processus par lequel des informations identifiables sont modifiées de manière irréversible de telle sorte qu'elles ne puissent plus, ou au prix d'un effort démesuré, être attribuées, directement ou indirectement, à une personne identifiable.
- **Pseudonymisation** : la modification de données identifiantes afin qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données ne sont pas attribuées à une personne identifiable.

Il apparaît donc clairement qu'assurer la confidentialité des données identifiantes est équivalent au concept d'anonymisation et que toute technique tombant sous l'égide de la pseudonymisation sera donc considérée comme insuffisante pour garantir la confidentialité sans mesure organisationnelle et / ou contractuelle supplémentaire.

D'un point de vue purement technique, les récentes avancées scientifiques révèlent que ni l'anonymisation, ni l'absence de risque de divulgation de données identifiantes ne peuvent être garantis : la publication d'un produit de données, quelle que soit sa nature, s'accompagne toujours d'un risque non nul de divulgation de données identifiantes. Il est toutefois possible de contrôler ce risque à l'aide de solutions techniques. Ces technologies permettent de piloter ce qui est communément appelé le **compromis confidentialité-utilité** (privacy-utility trade-off). De manière intuitive, ce concept traduit qu'il n'est pas possible de publier un produit de données qui reflète exactement le jeu de données identifiantes tout en garantissant un haut niveau de confidentialité. Ainsi, limiter significativement le risque de divulgation vient au prix d'une perte d'utilité du produit, et vice versa. Les technologies d'amélioration de la confidentialité présentées dans le reste de ce chapitre, permettent de quantifier et donc de piloter ce compromis de manière éclairée. En revanche, le choix d'un niveau acceptable de risque de divulgation et / ou d'une utilité minimale est une question hautement politique et sociétale qui ne peut pas être résolue technologiquement.

2.2 Confidentialité des inputs et des outputs

La création d'un produit de données et sa distribution s'effectue selon une chaîne de valorisation des données identifiantes nécessitant l'implication des parties prenantes suivantes :

- La / les personne(s) identifiable(s) (Data Subject(s)) : unité de confidentialité qui génère les données identifiantes.
- Le(s) fournisseur(s) de données (Input party) : organisation qui collecte les données identifiantes et mandate leur valorisation par la création d'un produit de données. Par exemple, un office statistique national produisant une statistique comme l'indice du taux de pauvreté ou une entreprise collectant des données à partir d'objets connectés.
- Le(s) fournisseur(s) de calcul (Computing Party) : organisation qui fournit la puissance de calcul nécessaire à la création du produit de données. Les calculs sont en général exécutés sur des

¹⁵ <https://www.fedlex.admin.ch/eli/cc/2022/491/fr>

¹⁶ <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

serveurs distants, c'est-à-dire grâce à une infrastructure en nuage. Cette dernière peut être opérée soit par une organisation de confiance, par exemple un office fédéral, soit par une entreprise privée donnant accès à des serveurs partagés par l'ensemble des clients du prestataire et donc qualifiés de publics.

- Le(s) consommateur(s) du produit de données (Result Party) : cercle d'individus auquel est distribué le produit de données. Par exemple, pour une administration, tout produit de données de type « Open Government Data » est distribué sans restriction au public : ce cas constitue le cercle de distribution le plus large pour lequel le contrôle de la confidentialité doit être le plus strict car le risque d'extraction de données identifiantes est le plus élevé. La diffusion d'un produit peut aussi se limiter à des cercles plus restreints, comme par exemple les employés de l'administration fédérale, qui sont tous soumis au secret de fonction et donc pour lesquels le risque d'une tentative d'extraction de données identifiantes est plus limité que lors d'une diffusion au public.

Les **technologies d'amélioration de la confidentialité** (Privacy-Enhancing-Technologies, PETs) constituent un ensemble de solutions techniques permettant de contrôler le risque de perte de confidentialité des données identifiantes tout au long de leur chaîne de valorisation en fonction de la confiance que s'accordent les différentes parties prenantes. Le terme « confiance » est ici à comprendre au sens large du terme, c'est-à-dire n'importe quelle raison justifiant la non-divulgaration de données identifiantes à une autre partie. Cela inclut par exemple l'existence d'une loi interdisant l'échange de données identifiantes entre les parties, la défiance des personnes concernées envers la partie fournisseur de données, ou encore l'absence de cadre juridique ou de mesure organisationnelle limitant toute tentative d'extraire des données identifiantes. L'absence de relation de confiance entre deux ou plus de parties prenantes peut être comblée grâce au recours à des technologies d'amélioration de la confidentialité qui se divisent en deux grandes catégories :

- Les technologies assurant la **confidentialité des inputs** (Input Privacy) qui s'efforcent de permettre à deux ou plus de parties prenantes décrites ci-dessus de soumettre des données pour un calcul sans qu'une autre partie ne puisse accéder aux données identifiantes originales autres que celles qui lui appartiennent. Ces technologies se reposent la plupart du temps sur des techniques de cryptographie et font donc partie de solutions assurant la sécurité de données.
- Les technologies assurant la **confidentialité des outputs** (Output Privacy) qui visent à limiter la divulgation de données identifiantes à partir du produit de données. Dans ce cadre, le produit est diffusé volontairement par le fournisseur de données. Ce processus est également connu sous le nom de contrôle (statistique) de la divulgation, un domaine bien connu par les offices statistiques nationaux qui développent cette pratique depuis plusieurs années.

Ainsi en fonction des relations de confiance entre les différentes parties prenantes de la chaîne de valorisation de données identifiantes, l'organisation garante de la confidentialité, en général la partie fournisseur de données, aura recours à une combinaison de technologies assurant la confidentialité des inputs et des outputs. Les figures 1, 2, et 3 donnent des exemples de schémas de confiance permettant de localiser où, le long de la chaîne de valorisation des données identifiantes, les technologies de type confidentialité des inputs, respectivement des outputs, viennent combler un déficit de confiance entre les parties.

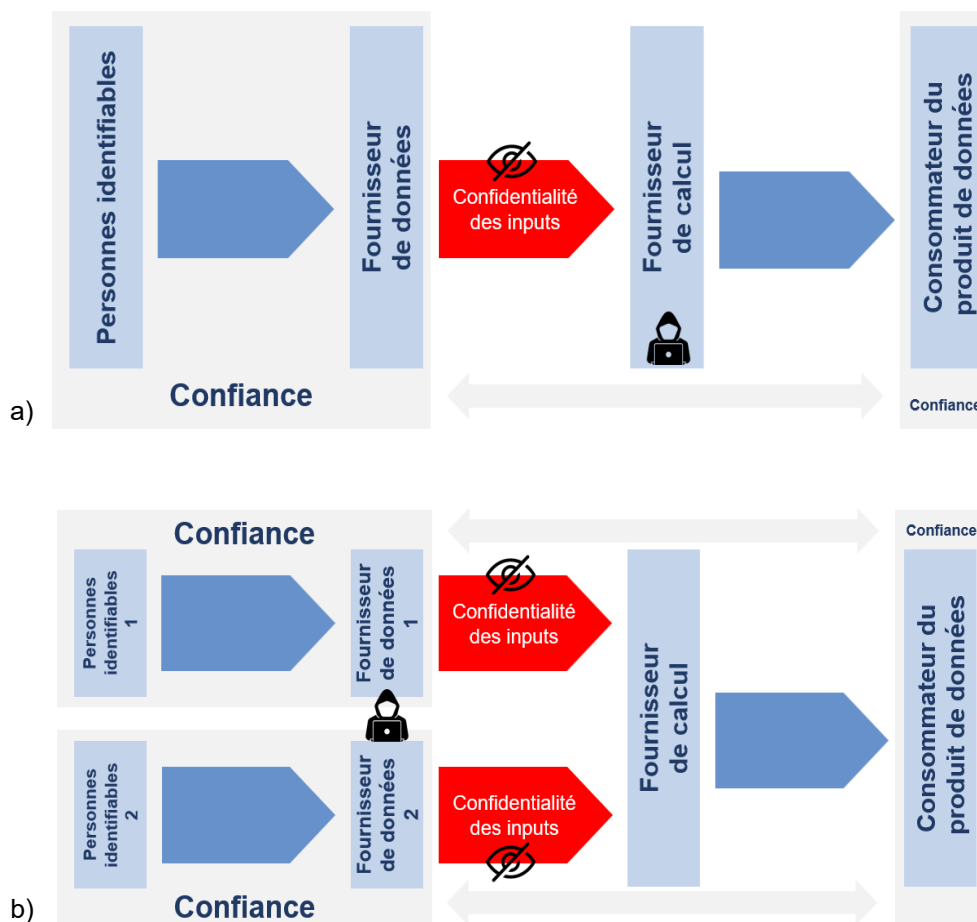


Figure 1 : Exemple de schéma de confiance pour l'utilisation de technologies d'amélioration de type confidentialité des inputs avec a) une unique partie fournisseur de données et b) deux parties fournisseurs de données. Dans les deux cas, les parties fournisseurs de données et le consommateur sont liés par une relation de confiance.

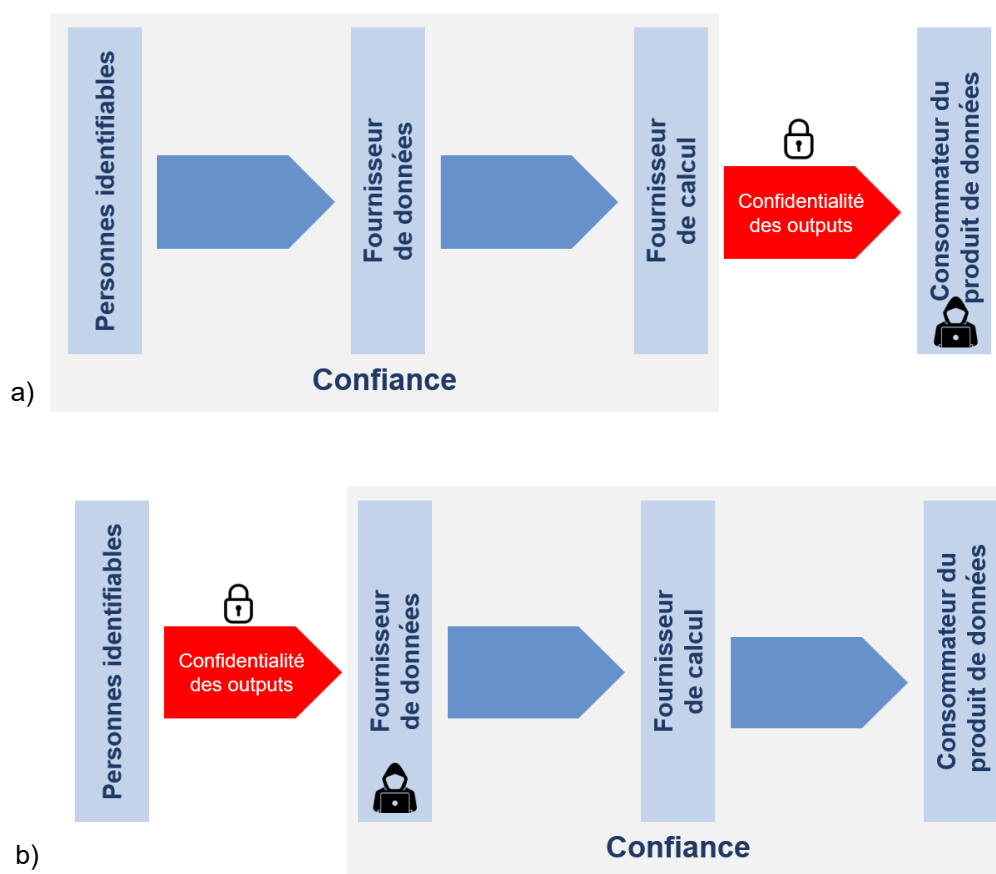


Figure 2 : Exemple de schéma de confiance pour l'utilisation de technologies d'amélioration de type confidentialité des outputs avec a) le schéma de référence pour les « Open Government Data » et b) le schéma lorsque les personnes (unités) identifiables ne font pas confiance au fournisseur de données.

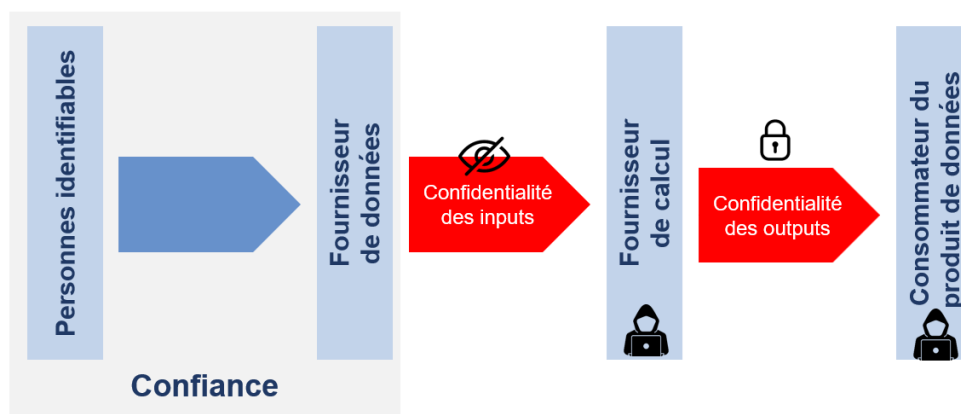


Figure 3 : Exemple de schéma de confiance nécessitant la combinaison de technologies d'amélioration de la confidentialité de type confidentialité des inputs et des outputs.

3 Technologies d'amélioration de la confidentialité

3.1 Environnement d'exécution fiable

Explication du principe

Un environnement d'exécution fiable (TEE ou Trusted Execution Environment), aussi appelé calcul confidentiel (Confidential Computing), a pour objectif de garantir la sécurité et l'intégrité du code et des données contre les attaques logicielles et physiques lors de l'exécution d'un programme informatique. Cette technologie permet l'exécution privée d'un programme informatique sur une infrastructure à distance, sans nécessiter que le fournisseur soit un tiers de confiance. Le TEE assure l'intégrité du code et protège les données contre toute manipulation à l'intérieur de l'environnement, en empêchant tout accès externe non autorisé. L'intégrité du code exécuté est garantie par une attestation d'exécution générée par le fournisseur grâce à une preuve d'authenticité cryptographique. La mise en place de ces environnements repose sur des composants matériels fournis par certains fabricants ou prestataires de services informatiques, généralement intégrés à des modèles particuliers de processeurs.

Limitations et risques

Un TEE est directement lié aux modèles de processeurs sur lesquels il peut être déployé, avec certaines implémentations parfois uniquement disponibles via un service en nuage spécifique, créant ainsi une dépendance à l'égard du fournisseur choisi. De plus, certains modèles de TEE souffrent d'une limitation au niveau de la mémoire de calcul disponible. Bien que quelques implémentations permettent de contourner cette limite, l'usage excessif de cette alternative est souvent considéré comme une mauvaise pratique.

De plus, la technologie étant directement liée au matériel, elle s'expose à des vulnérabilités techniques, qu'elles soient liées à un accès direct à la machine ou à la découverte ultérieure de failles de sécurité, rendant le système obsolète et impossible à mettre à jour. En outre, le fonctionnement varie significativement en fonction du fournisseur et de la technologie sous-jacente, ajoutant une couche supplémentaire de complexité au déploiement d'un TEE.

Dans un TEE, le code exécuté n'est pas nécessairement secret, puisqu'il peut être connu du responsable de l'administration du système. Bien que l'environnement offre une protection lors de l'exécution du code, la résilience du code lui-même face à des attaques externes (via les interfaces qu'il fournit) peut rester insuffisante. Cette situation expose potentiellement le système à des vulnérabilités face à des attaques par canal auxiliaire (side channel).

Promesses et maturité

L'environnement d'exécution fiable (TEE) est déjà adopté dans divers secteurs, notamment pour sécuriser l'exécution de code sensible sur les smartphones (considérés comme des dispositifs non-fiables). Les applications de services financiers recourent fréquemment à cette technologie pour assurer la sécurité des paiements et des identifications. Un avantage majeur de cette technologie réside dans sa facilité d'intégration avec d'autres technologies améliorant la confidentialité (PET), sans compromettre significativement les performances d'exécution du code.

De plus, de nombreux fournisseurs de services en nuage (Azure, AWS, etc.), offrent cette technologie au sein de leurs plateformes, simplifiant ainsi son intégration au sein des organisations. Les recherches actuelles se concentrent principalement sur l'identification des risques liés aux différentes attaques possibles sur cette technologie et sur la création d'une norme qui fait encore défaut dans le domaine. Néanmoins, certains acteurs tels que Globalplatform et Enarx s'efforcent de remédier à ce problème.

L'un des avantages notables qu'offrent certains TEEs par rapport à d'autres technologies améliorant la confidentialité est la flexibilité de portage d'algorithmes existants (tels que ceux utilisés pour l'analyse de

données) sur l'environnement sécurisé sans modification drastique du code source. Cela dépend fortement du cadre utilisé lors de l'implémentation d'un TEE et reste un domaine de recherche encore en pleine expansion.

En science des données, un TEE peut avoir diverses applications. Par exemple, un fournisseur (propriétaire d'un modèle d'apprentissage) peut mettre à disposition son modèle sur un TEE afin qu'un client (propriétaire de données) puisse l'utiliser tout en s'assurant que ses données y sont envoyées de façon sécurisée. Ainsi, le client ne dispose pas d'un accès direct au modèle tandis que le fournisseur n'a pas directement accès aux données.

3.2 Chiffrement homomorphe

Explication du principe

Le chiffrement homomorphe est une technique de cryptographie permettant de réaliser des opérations directement sur des données chiffrées, grâce à ses propriétés mathématiques. Ainsi, il n'est pas nécessaire de déchiffrer les données pour effectuer des analyses statistiques, des tests d'hypothèse ou des inférences avec des modèles d'IA.

Cette technique permet par exemple à un fournisseur de données sensibles (« A ») d'externaliser des traitements et stockage de données identifiantes à (« B »), un fournisseur de calcul dans une infrastructure en nuage. Par exemple, considérons le cas où « A » est un employé d'un office fédéral souhaitant utiliser le modèle d'apprentissage automatique servi par « B ». Ce modèle prédit un risque de fraude à partir de données identifiantes de déclarations fiscales. « A » chiffre les données de manière homomorphe et les transmet à « B ». Ce dernier fait passer les données chiffrées à travers le modèle et obtient un résultat également chiffré qu'il renvoie à « A ». Enfin, « A » déchiffre le résultat pour connaître le risque de fraude inféré, tandis que « B » n'a rien appris sur les données.

À la date d'écriture de ce rapport, le chiffrement homomorphe est la seule technologie permettant de maintenir les données chiffrées tout au long du processus, éliminant ainsi le besoin de faire confiance au fournisseur de calcul, qui n'a jamais accès aux données déchiffrées.

Le « Fully Homomorphic Encryption » (FHE) est la forme la plus avancée de chiffrement homomorphe, permettant d'effectuer un nombre illimité d'opérations mathématiques sur les données chiffrées, offrant ainsi des applications plus complexes telles que l'entraînement de réseaux de neurones profonds.

Limitations et risques

Le chiffrement homomorphe présente des risques similaires à ceux des autres techniques de chiffrement. Il nécessite notamment un stockage sécurisé des clés de chiffrement ainsi qu'une résistance aux attaques par force brute, cryptanalyse, canaux auxiliaires et interception de données.

La principale limitation du chiffrement homomorphe est son besoin considérable en ressources informatiques : les données chiffrées sont significativement plus volumineuses, ce qui entraîne un besoin accru en espace de stockage. De plus, les calculs sur les données chiffrées sont considérablement plus lents que sur des données en clair, ce qui rend le chiffrement homomorphe inadapté aux applications en temps réel.

Il faut aussi souligner que le chiffrement homomorphe est une technologie de confidentialité des inputs. Ainsi, bien que les données restent chiffrées chez les fournisseurs de calculs, il n'y a aucune garantie concernant le risque de divulgation une fois le produit de données déchiffré par son consommateur.

Enfin, et surtout, le chiffrement homomorphe n'offre qu'un nombre restreint d'analyses : seules les opérations linéaires sont calculables exactement, ce qui oblige à recourir à des approximations pour toute opération plus complexe. Par conséquent, la garantie de chiffrement s'effectue au prix de l'exactitude.

Promesses - Maturité

Le chiffrement homomorphe est appliqué avec succès dans la pratique et des bibliothèques en code source ouvert sont disponibles. Un de ces cas d'application est l'intersection privée de jeux de données (Private Set Intersection) permettant de trouver les éléments communs entre deux jeux de données identifiantes appartenant à des fournisseurs de données distincts, qui ne souhaitent pas partager leurs données mutuellement. De même, la mise à disposition de modèles d'apprentissage automatique, comme dans l'exemple de risque de fraude évoqué précédemment, est une autre application notable.

Le chiffrement homomorphe est un champ actif de recherche et la technologie qui a fait des progrès considérables les cinq dernières années, avec en particulier le développement de solutions matérielles spécialisées afin de réduire le temps de calcul et rendre la technologie viable. Si les progrès se poursuivent de manière significative, le chiffrement homomorphe pourra être utilisé dans de multiples applications, offrant ainsi un énorme potentiel dans divers domaines.

3.3 Calcul multipartite sécurisé

Explication du principe

Le calcul sécurisé multi-parties (Secure MultiParty Computation, MPC ou SMPC) est une forme de calcul sécurisé qui permet à un groupe d'effectuer conjointement un calcul, sans divulguer les inputs privés (données) des participants. Le MPC est une sous-branche de la cryptographie. Contrairement à la cryptographie classique, où l'attaquant se trouve à l'extérieur du système, le MPC vise à garantir la sécurité des données des participants les uns par rapport aux autres. Les participants conviennent d'un algorithme à appliquer, puis utilisent un protocole MPC pour calculer conjointement l'output de cet algorithme sur leurs inputs secrets, sans les révéler. Chaque participant n'apprend que ce qui peut être déduit de l'output. Le MPC garantit que les inputs de chaque partie restent privés (confidentialité des inputs) ainsi que l'intégrité du résultat obtenu.

Il existe deux principales catégories d'algorithmes MPC. La première catégorie permet l'exécution de tous types d'algorithmes, notamment des algorithmes permettant la création de produit de données. Dans cette catégorie, le concept de partage de secret est très largement utilisé : les inputs sont divisés en parts et répartis entre les parties. L'algorithme de MPC exécute ensuite les calculs sur les parts séparées, qui sont recombinaisonnées uniquement à la fin de l'exécution, de manière à maintenir secrets les inputs de chaque partie tout au long de l'exécution de l'algorithme. La seconde catégorie regroupe les algorithmes uniquement dédiés à la production de produits de données très spécifiques (p. ex. appariements de jeux de données privées) et sont hautement optimisés pour ceux-ci.

Limitations et risques

Les protocoles MPC offrent un niveau de sécurité élevé, avec une garantie formelle, mais impliquent généralement des opérations cryptographiques qui entraînent des coûts de calcul et de communication élevés. Cette technologie est donc adaptée pour des tâches spécifiques uniquement.

Il existe différents modèles de menace plus ou moins strictes pour le MPC incluant la possibilité de parties corrompues ou encore leur collusion. Par exemple, certains algorithmes sont sûrs même avec une majorité de parties corrompues. Il est donc important de définir un modèle de menace clair lors de l'utilisation de MPC, ainsi que de sélectionner avec précaution des algorithmes et des bibliothèques adaptés.

L'exécution d'algorithmes existants nécessite souvent une réécriture du code pour permettre le passage en MPC. De plus, les bibliothèques logicielles en code source ouvert pour le MPC n'offrent souvent pas le même éventail de fonctionnalités spécifiques à la science des données, ce qui nécessite un travail supplémentaire lors de l'adaptation d'un code pour le MPC.

Finalement, bien que le MPC limite la capacité de chaque partie à accéder aux données en entrée des autres participants, il n'assure pas la confidentialité dans le résultat calculé. En effet, le résultat du calcul permet parfois de révéler des informations sensibles. Ainsi, le MPC nécessite une réflexion approfondie sur les calculs à effectuer, et doit souvent être combiné avec des techniques préservant la confidentialité des outputs, telles que la confidentialité différentielle.

Promesses et maturité

Le MPC trouve des applications dans des scénarios où la confidentialité des inputs est critique, tels que l'analyse collaborative des données en santé, finance et d'autres domaines sensibles. Par exemple, des techniques de MPC ont été utilisées en Estonie pour réaliser une étude sur la corrélation entre l'activité professionnelle pendant les études universitaires et l'échec académique. Cette étude a nécessité des données de deux entités étatiques indépendantes qui n'ont pas les bases légales pour les partager. Ainsi, sans l'aide du MPC, cette étude n'aurait pas pu voir le jour.

Une grande majorité de projets utilisant des techniques de MPC font recours à des bibliothèques logicielles propriétaires. Il n'existe actuellement pas de bibliothèque en code source ouvert pour le MPC avec une maturité suffisante pour la mise en production. La recherche en cours se concentre sur l'optimisation des protocoles MPC pour atténuer la surcharge computationnelle et de communication. À mesure que les techniques cryptographiques progressent, l'efficacité du MPC devrait s'améliorer, le rendant plus viable pour un éventail plus large d'applications. La combinaison de MPC et de confidentialité différentielle (v. ci-dessous) pour préserver la confidentialité des outputs est également prometteuse mais en est pour l'instant au stade de la recherche.

3.4 Apprentissage distribué

Explication du principe

L'apprentissage distribué permet à plusieurs parties d'entraîner un algorithme d'apprentissage automatique, plus particulièrement un réseau de neurones, de façon à garantir la sécurité des données d'entraînement entre les parties (confidentialité des inputs). Les données restent stockées sur l'infrastructure de leur propriétaire et ne sont jamais échangées entre les parties. Seuls les paramètres du modèle, c'est-à-dire le résultat de l'apprentissage, sont partagés entre les parties. Ces techniques nécessitent un tiers fournisseur de calcul afin de coordonner le processus : celui-ci ne requiert jamais l'accès aux données d'input mais joue un rôle central dans l'agrégation et la distribution des paramètres d'entraînement aux différentes parties.

On distingue principalement deux approches d'apprentissage distribué : l'apprentissage fédéré et l'apprentissage fractionné. Dans l'apprentissage fédéré, les participants détiennent leur propre copie du modèle, qu'ils entraînent individuellement sur leurs données privées. Ensuite, les participants envoient les paramètres de leur modèle à un serveur central pour agrégation. Un modèle global est alors construit et redistribué à chaque participant pour une nouvelle itération d'entraînement. Dans l'apprentissage fractionné, le modèle est divisé de façon à permettre à chacun des participants d'entraîner sur son infrastructure une sous-partie distincte du modèle avec ses propres données. Chaque sous-partie du modèle produit une sortie intermédiaire. Pendant le processus d'entraînement, le serveur central entraîne lui aussi un modèle qui combine ces sorties intermédiaires. Contrairement à l'apprentissage fédéré, l'apprentissage fractionné doit nécessairement s'effectuer de manière séquentielle. L'apprentissage fractionné offre cependant une meilleure protection des données en input en masquant davantage d'informations sur les paramètres et l'architecture du modèle aux différentes parties, ce qui limite aussi pour ces dernières les possibilités d'inspection du modèle.

Limitations et risques

En comparaison avec l'approche classique d'entraînement centralisé des modèles d'apprentissage machine, l'apprentissage distribué génère un surcoût en termes de communication entre les parties et le

serveur central. Le temps d'apprentissage est également rallongé pour les techniques requérant une synchronisation entre les parties à chaque étape de l'algorithme d'optimisation du modèle. De manière générale, les modèles d'IA entraînés de façon distribuée sont moins performants que leurs modèles équivalents entraînés sur des données centralisées.

L'apprentissage distribué vise à garantir la confidentialité des données privées en input. Il est cependant possible que les paramètres du modèle transmis durant la phase d'apprentissage ainsi que le modèle résultant révèlent de l'information relative aux données des participants : c'est pourquoi il doit être combiné avec une technologie qui permet la confidentialité des outputs, afin de contrôler le risque de divulgation.

Enfin, l'apprentissage distribué est également vulnérable à la corruption d'une ou plusieurs parties ou du serveur d'agrégation. Un participant peut par exemple insérer de fausses données d'entraînement, afin de modifier le comportement du modèle de façon ciblée et servir ainsi son propre intérêt.

Promesses et maturité

L'apprentissage distribué favorise la collaboration entre plusieurs organisations en leur permettant d'entraîner de façon conjointe un modèle sans avoir à centraliser les données, ce qui résout certains problèmes de confidentialité des inputs. De plus, en tirant parti de la diversité des sources de données, l'apprentissage distribué favorise le développement de modèles plus robustes et performants. Par exemple, les données de santé ne sont pas toujours disponibles en quantité suffisante pour permettre l'entraînement de modèles d'IA performants pour le diagnostic médical. L'apprentissage distribué permet d'entraîner un modèle d'IA robuste grâce aux données provenant de plusieurs hôpitaux, tout en améliorant la confidentialité des inputs.

Il existe plusieurs bibliothèques open source qui permettent l'apprentissage distribué d'algorithmes d'IA. Celles-ci s'intègrent bien avec les bibliothèques d'apprentissage machine classique et rendent cette technologie accessible.

3.5 Preuve à divulgation nulle de connaissance

Explication du principe

Une preuve à divulgation de nulle connaissance (PDNC) (Zero Knowledge Proof) est un protocole cryptographique où un « fournisseur de preuve » prouve à un « vérificateur » qu'une affirmation est vraie sans révéler aucune information auxiliaire autre que sa véracité. Par exemple, une PDNC permet de vérifier la proposition suivante : un modèle d'apprentissage automatique de prédiction de solvabilité a été exécuté sur l'ensemble de l'historique financier de l'entreprise 'X' sans toutefois divulguer les détails spécifiques du modèle, ni les données financières de l'entreprise. Les PDNC sont de nature probabiliste, c'est-à-dire qu'il reste toujours un risque résiduel que l'affirmation soit qualifiée de fausse alors qu'elle est vraie. Ce risque peut toutefois toujours être réduit de manière arbitraire en engageant des capacités de calcul supplémentaires.

Les principaux domaines d'application des PDNC sont l'authentification, l'identification et les cryptomonnaies. En science des données, les PDNC peuvent faciliter le partage et la collaboration entre parties prenantes dans des scénarios où des informations identifiables doivent être protégées. Par exemple, on peut les utiliser pour vérifier la nature de données identifiantes sans les révéler directement ou encore vérifier l'identité de personne sans divulguer ses informations personnelles. Ainsi le flux de données est sécurisé contre les fuites et les parties prenantes ne partagent pas leurs données avec un potentiel fournisseur de calcul.

Limitations et risques

La vérification des PDNC est une tâche gourmande en ressources : elle nécessite soit de nombreuses communications entre le vérificateur et le fournisseur de preuve, soit une très grande capacité de calcul. Pour cette raison, les applications pratiques du PDNC sont actuellement limitées à des problèmes très simples pour être utilisables soit à grande échelle, soit en temps réel.

La création de nouveaux protocoles de PDNC est souvent un défi théorique car il est difficile de traduire un problème humain en énoncé mathématique. Leur implémentation nécessite donc non seulement des développeurs informatiques mais aussi des personnes avec des bonnes connaissances en mathématiques et cryptographie. A l'avenir, beaucoup de protocoles PDNC ne seront plus sécurisés avec l'arrivée de capacité de calcul de type quantique.

En plus d'être une technologie de type « confidentialité des inputs », les PDNC nécessitent souvent un certain niveau de confiance entre les fournisseurs des données et les fournisseurs de calculs limitant ainsi leur applicabilité à des schémas de confiance bien précis.

Promesses et maturité

La maturité de cette technologie est variable : certaines applications de PDNC sont déjà bien maîtrisées et appliquées tandis que d'autres restent encore au stade de la recherche. Étant nécessaire au fonctionnement des chaînes de blocs (blockchain), où les transactions peuvent être vérifiées sans partager de données identifiantes, les PDNC bénéficient de nombreux efforts visant à surmonter leurs limitations actuelles et des travaux sont en cours afin de développer une taxonomie et une standardisation.

Un exemple typique d'application des PDNC en science des données est de permettre d'attester de la bonne exécution d'un algorithme sans divulguer les données utilisées. En apprentissage automatique et IA, un propriétaire d'un modèle peut ainsi attester du résultat d'un modèle sans pour autant partager ce dernier. Les PDNC sont aussi centrales dans l'implémentation de systèmes de votes électroniques garantissant ainsi la validité des élections et l'anonymat des électeurs. Enfin, en février 2023, l'Union Européenne a approuvé une « identité numérique » utilisant les PDNC et permettant à tous les résidents et citoyens européens de s'identifier et d'attester des informations personnelles pour des services dématérialisés tels que louer un vélo ou payer ses impôts.

3.6 Confidentialité différentielle

Explication du principe

La confidentialité différentielle (Differential Privacy) ne désigne pas un outil ou algorithme unique, mais un cadre méthodologique définissant les propriétés mathématiques qu'un algorithme d'analyse statistique ou d'apprentissage automatique doit satisfaire afin de pouvoir quantifier mathématiquement le risque de divulgation associé au partage du produit de données associé. Il s'agit donc d'une technologie de contrôle de la confidentialité des outputs.

Plus précisément, la confidentialité différentielle repose sur la randomisation de l'output d'un algorithme afin de rendre non fiable toute tentative d'extraction de données identifiantes à partir du produit de données. En effet, un algorithme satisfaisant les conditions de la confidentialité différentielle garantit de contrôler précisément le risque de divulgation de données identifiantes indépendamment des informations auxiliaires et des moyens techniques disponibles à l'attaquant. Ce risque est quantifié par un paramètre appelé budget de perte de confidentialité (privacy-loss budget) dont le choix dépend de la sensibilité des données et de l'utilisation envisagée du produit de données protégé.

La confidentialité différentielle peut aussi être appliquée directement au jeu de données original ; on parle alors de confidentialité différentielle locale (local differential privacy). Cette approche vise à rendre les données non fiables en les perturbant aléatoirement de telle sorte qu'elles ne puissent pas être utilisées contre l'unité identifiable auxquelles elles appartiennent. Ce mécanisme appelé réponse aléatoire

(randomized response) est utilisé depuis plusieurs années par les offices statistiques nationaux, les instituts de sondage et plus récemment le secteur privé afin de s'assurer de l'honnêteté d'une réponse, ou plus simplement de l'acceptation de la collecte de données, sur des sujets sensibles comme les relations extra-conjugales ou la télémétrie (localisation, applications installées, enregistrement de frappe, etc.) des ordinateurs personnels.

Limitations-Risques

Les mécanismes de confidentialité différentielle nécessitent l'introduction d'une perturbation aléatoire dans l'algorithme. Ainsi il est nécessaire d'évaluer et de communiquer clairement dans quel cadre les produits de données, ou microdonnées, perturbés peuvent être utilisés et avec quel niveau de confiance. Cette évaluation se fait au cas par cas et nécessite une expertise technique poussée en confidentialité et statistiques mathématiques.

Actuellement de nombreuses initiatives visent à développer des standards ou simples lignes directrices pour calibrer l'ampleur de la perturbation en fonction du contexte et du degré de sensibilité du produit de données¹⁷. Toutefois, le choix du budget de perte de confidentialité, et donc l'ajustement du compromis utilité / confidentialité, reste un défi avant tout politique nécessitant une discussion étroite entre spécialistes de la confidentialité différentielle, régulateurs et décideurs politiques. Il n'y a pas de solution universelle car le choix de ce paramètre dépend du cadre de gouvernance de gestion de la confidentialité prenant en compte l'ensemble des « Five Safes »¹⁸. La gestion des attentes des destinataires, c-à-d les « Safe People » est particulièrement importante, car le degré de fiabilité du produit publié ne peut être assuré que pour des utilisations bien précises.

Il faut également souligner que la confidentialité différentielle requiert des compétences techniques pointues au-delà de l'expertise mathématique et statistique : l'implémentation est non triviale d'un point de vue de l'infrastructure informatique, car il faut notamment pouvoir assurer un suivi rigoureux du budget de perte de confidentialité et des versions des données utilisées dans les analyses.

Promesses – Maturité

La confidentialité différentielle, formellement introduite en 2006¹⁹, est un intense sujet de recherche académique et d'expérimentation. Elle s'inscrit dans une continuité de travaux sur le contrôle de la divulgation statistique et en réponse aux progrès des connaissances sur les attaques de divulgation de données identifiantes telles que la reconstruction, l'appariement et l'appartenance. Aujourd'hui, la confidentialité différentielle est déployée en production tant par des acteurs privés (Apple, Google, Microsoft) que par des institutions gouvernementales (Bureau du Censur américain). Ainsi, des librairies à code source ouvert sont disponibles avec un niveau suffisant de maturité et de fiabilité. La complexité d'un algorithme différentiellement confidentiel étant par ailleurs très marginalement plus élevée que celle d'un algorithme classique, le coût computationnel additionnel n'est pas une limitation.

La confidentialité différentielle en tant que technologie assurant la confidentialité des outputs est particulièrement prometteuse pour les raisons suivantes :

¹⁷ <https://www.nist.gov/news-events/news/2023/12/nist-offers-draft-guidance-evaluating-privacy-protection-technique-ai-era>

¹⁸ <https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/>

¹⁹ Dwork, C. (2006). Differential Privacy. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds) Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science, vol 4052. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11787006_1

- Une garantie mathématique de limite du risque d'extraction de données identifiantes à partir d'un produit de données dont la validité est assurée, quels que soient les informations auxiliaires et les moyens techniques dont dispose une partie tentant d'extraire ces informations. Cette garantie assure que toute tentative d'extraction ne peut être faite de manière fiable tout en fixant le niveau maximum de fiabilité qu'un potentiel attaquant peut atteindre.
- Le risque cumulatif de divulgation peut être quantifié même avec des publications successives et indépendantes de produits de données de différente nature.
- Le mécanisme d'ajout de bruit aux données peut être communiqué dans la plus grande transparence sans compromettre la garantie de confidentialité, ce qui permet un débat public ouvert sur le compromis confidentialité / utilité.
- La garantie du contrôle du risque de divulgation de données identifiantes qu'offre la confidentialité différentielle peut être utilisée pour rendre possible la réutilisation de données détenues par l'administration, soit au sein même de cette dernière, soit entre l'administration et le reste de la société suisse (recherche, secteur privé, société civile) sans partager ces données et tout en contrôlant le risque auquel les individus contribuant leur données sont exposés et en leur donnant l'assurance qu'aucune donnée identifiable ne peut être extraite de manière fiable. Le chapitre 2 expose en détail ce cas d'application ainsi que son grand potentiel de bénéfice sociétal.

3.7 Données synthétiques

Explication du principe

La génération de données synthétiques vise à créer un jeu de données alternatif dont la granularité se situe au niveau d'une / de personne(s) identifiable(s) mais ne divulguant pas de manière évidente les données identifiantes du jeu de données original. On distingue deux types de jeux de données synthétiques :

- Les données intégralement simulées, ou factices, reproduisant uniquement les caractéristiques des données originales. Plus précisément, ce type de jeu de données synthétiques partage uniquement les mêmes métadonnées (nom de variables, types de variables, valeurs possibles, etc.) que les données identifiantes mais contient que des informations générées aléatoirement. Ces dernières sont utilisées principalement pour tester les pipelines d'analyse de données.
- Les données sont générées afin de reproduire certaines propriétés statistiques du jeu de données original. La génération n'est donc pas purement aléatoire même si elle reste en partie stochastique. Dans ce cas, puisque des informations sur le jeu de données sont partagées, le risque de divulgation de données identifiantes est non nul et doit être contrôlé.

Les générateurs de données synthétiques de la première catégorie reposent en général sur de simples générateurs de nombre aléatoires. La deuxième catégorie recourt à des algorithmes plus complexes provenant des mathématiques appliqués et d'algorithmes d'apprentissage machine et d'intelligence artificielle (forêts aléatoires, réseau de neurones, réseaux antagonistes génératifs, etc.).

Limitations et Risques

Chaque jeu de données synthétiques est généré afin de reproduire certaines propriétés du jeu de données original. Il est donc nécessaire de communiquer clairement au consommateur la nature et la portée de ces propriétés afin qu'il puisse comprendre dans quel contexte et dans quel mesure le jeu de données peut être utilisé de manière fiable. Par exemple, un jeu de données synthétiques utilisé dans le cadre d'un projet de recherche doit pouvoir garantir que la découverte n'est pas due au hasard de sa génération mais bel et bien à un signal présent dans les données identifiantes d'origine.

D'un point de vue du contrôle de la divulgation, la plupart des générateurs de données synthétiques n'offrent pas de garantie formelle. Au contraire, les récents développements dans ce domaine montrent que ces générateurs sont sujets à des divulgations flagrantes de données identifiantes au même titre

que tout autre produit de données. Cette limitation peut être dépassée en combinant ces générateurs avec une technologie de contrôle de la confidentialité des outputs telle que la confidentialité différentielle.

Toute promesse de l'existence d'un jeu de données reproduisant l'intégralité des propriétés du jeu de données original tout en assurant la non divulgation de données identifiantes est erronée et techniquement impossible.

Promesses et Maturité

Les jeux de données synthétiques offrent la possibilité de diffuser des micro-données, en particulier au public, tout en limitant le risque de divulgation de données identifiantes. Cette solution est flexible, facile à mettre en place et ouvre de nombreuses nouvelles opportunités de valorisation de données identifiantes détenues par une administration. Cela ne peut être toutefois accompli qu'en combinant les générateurs de données synthétiques avec une technologie de contrôle de la confidentialité des outputs. La génération de données synthétiques est mature avec de nombreuses implémentations open source disponibles sous forme de package R ou Python. Les données simulées sont parfaitement utilisables en production au sein d'une administration, en revanche le second type de données synthétiques, reproduisant certaines propriétés statistiques des données identifiantes, nécessite que la recherche scientifique clarifie dans quelle mesure les données générées sont fiables d'utilisation. Cette incertitude rend leur utilisation encore discutable pour une administration.

4 Cas pratique 1 : Plateforme pour la pratique confidentielle de la science des données sans transfert de données

4.1 Contexte et objectifs

Les divers organismes de la Confédération possèdent une vaste quantité de données indispensables à l'exercice de leur mission d'intérêt public. L'administration fédérale consacre des investissements considérables en temps et en ressources pour collecter, sélectionner et consolider ces jeux de données, lesquels constituent une source d'information fiable et unique. Toutefois, malgré leur valeur intrinsèque, leur pleine exploitation au bénéfice du bien public demeure incomplète. Ces données, lorsqu'elle se rapportent à une personne physique ou morale, sont généralement réservées à l'usage pour lequel elles ont été recueillies, conformément aux réglementations sur la protection des données et le secret statistique. Leur réutilisation est toutefois possible pour des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique ([Art. 39 al. 1 LPD, RS 235.1](#)). Toute requête de ce type est soumise à un examen minutieux pour évaluer la légitimité de la demande et le risque de divulgation associé. En conséquence, dans ces cas, le processus administratif nécessaire pour obtenir l'accès à ces données est long et complexe.

Le plein potentiel des données collectées par l'administration fédérale ne peut donc être réalisé que par leur réutilisation dans divers domaines :

- Premièrement, les autres offices de la Confédération, et les autres unités administratives, peuvent exploiter ces données pour soutenir efficacement le processus d'élaboration de politiques publiques en s'appuyant sur des indicateurs objectifs. Par exemple, l'Office fédéral de la statistique (OFS) peut fournir des données démographiques et/ou de décès au niveau individuel afin de permettre à l'Office fédéral de la santé publique d'adapter ses décisions de manière proactive et au plus proche de la réalité. Dans le domaine de l'éducation, les données de trajectoires des étudiants détenues par l'OFS peuvent intéresser les cantons afin de pouvoir appréhender au mieux les besoins de formation au niveau national.
- Deuxièmement, les laboratoires de recherche peuvent utiliser ces données pour faire progresser la connaissance et renforcer la compétitivité de la Suisse par le biais de l'innovation. Par exemple, des chercheurs universitaires pourraient analyser les données détenues par les offices fédéraux pour développer des solutions innovantes pour lutter contre la pauvreté ou le décrochage scolaire.
- Troisièmement, le secteur privé peut tirer parti de ces données pour soutenir la vitalité économique de la Suisse. Par exemple, les entreprises suisses pourraient utiliser les données détenues par les offices fédéraux pour enrichir leurs propres données et prendre des décisions stratégiques en matière d'investissement ou de développement de produits.
- Enfin, ces données peuvent également être partagées avec d'autres États pour mieux faire face à des crises d'ampleur mondiale telles que celle du COVID-19. Par exemple, la Suisse pourrait partager des données épidémiologiques avec d'autres pays pour aider à coordonner une réponse mondiale efficace à la pandémie.

Cependant, il est impératif que cette réutilisation des données soit politiquement et socialement acceptée, en veillant à ce que les avantages qu'elle apporte ne se fassent pas au détriment des citoyens, des ménages et des entreprises suisses au risque de voir la confiance dans les statistiques fédérales ou la volonté de participer à des enquêtes significativement diminuer. Pour maintenir la confiance envers l'État, il est donc crucial de limiter le risque de divulgation de données identifiantes lors de leur utilisation à l'intérieur et à l'extérieur de l'administration fédérale.

Ce cas pratique explore la possibilité de réutiliser les données collectées tout en contrôlant le risque de divulgation de données identifiantes. Il est important de souligner que ce service nécessite que ces

données soient collectées par un service central de confiance. L'utilisation des technologies d'amélioration de confidentialité sert ici à maintenir, voire à accroître, la confiance des personnes qui ont confié leurs données à ce service, lors d'une possible réutilisation de leurs données. Assurer la confiance envers ce service central est une question de gouvernance interdisciplinaire comportant la mise en place non seulement de mesures techniques mais aussi juridiques et organisationnelles. La coordination de ces mesures est abordée dans la section 6.3 de ce rapport.

Ce projet se présente sous la forme d'une plateforme à laquelle les parties autorisées et désireuses de réutiliser les données peuvent se connecter à distance afin de créer des produits de données dont le risque de divulgation est contrôlé, sans que l'utilisateur ne voie les données originales à aucun moment. Ainsi, les données identifiantes ne circulent pas entre le détenteur et l'utilisateur des données. L'objectif final de cette plateforme est soit de donner l'opportunité de valoriser des données identifiantes par une seconde utilisation jugée trop risquée ou lorsque leur partage est prohibé par la loi, soit d'offrir la possibilité de rapidement développer des algorithmes d'analyse de données dans l'attente d'un processus formel de partage de données. L'utilisation de technologies d'amélioration de la confidentialité des outputs, telles que la confidentialité différentielle, permet de contrôler finement le risque de divulgation quel que soit l'usage fait des données identifiantes. La plateforme permet ainsi :

- de maintenir la confiance de la population envers l'État en assurant que le risque de conséquences néfastes au niveau individuel lors de la réutilisation de données identifiantes est limité;
- de donner un accès beaucoup plus rapide aux données protégées à des fins autres que celles pour lesquelles elles ont été collectées. Dans ce cas, la plateforme peut par exemple servir de solution transitoire en attendant qu'un laboratoire de recherche ait accès aux données originales. En effet, pour maintenir la confidentialité, les résultats des algorithmes sont perturbés avec des techniques de confidentialité différentielle. Avec une large perturbation, le risque de divulgation est marginal et l'accès à la plateforme peut être donné sur la base d'une réglementation juridique minimale. Les résultats obtenus sont donc sujets à un haut niveau d'incertitude ce qui limite leur utilité. Toutefois, cette opportunité reste précieuse car elle permet au chercheur de commencer à travailler rapidement en testant son code et son protocole expérimental.

La plateforme est similaire dans son principe à un services d'accès distant (remote access) mais se distingue des solutions classiques en premier lieu en assurant que les données identifiantes ne sont jamais divulguées à l'utilisateur et ensuite par l'absence de besoin d'une vérification humaine des algorithmes exécutés par l'utilisateur. En effet, pour ce dernier point, les plateformes d'accès distant nécessitent un contrôle systématique des résultats par des experts du risque de divulgation, ce qui est à la fois coûteux et lent. L'utilisation de la confidentialité différentielle permet donc d'automatiser l'ensemble du processus tout en assurant un contrôle du risque de divulgation grâce à une méthodologie mathématique de quantification résistante au temps et à l'évolution technologique.

Afin de souligner le potentiel de ce cas pratique pour l'administration fédérale, voici quelques exemples concrets d'application au sein du Département fédéral de l'intérieur :

- Statistique de décès : l'utilité des données collectées par l'OFS pour la statistique de décès dépasse la statistique car elle permet aussi d'estimer l'impact de certains facteurs, comme la crise du COVID19, sur la mortalité. L'université de Milan a par exemple réalisé une étude pour la population suisse grâce à la livraison de ces données qui sont à la fois personnelles et sensible. Cette dernière requiert l'élaboration et la signature d'un contrat de livraison qui transfère la responsabilité de la protection de données à l'université requérante ; cette mesure ne limite pas le risque réputationnel pour l'Administration en cas de fuite de données par l'université. L'utilisation de la plateforme décrite dans ce cas pratique permettrait de contrôler ce risque tout en simplifiant significativement la réalisation de ce type d'étude par la recherche en allégeant le fardeau administratif.

- Enquête suisse sur la structure des salaires : les données collectées dans le cadre de cette enquête sont d'un grand intérêt pour le public comme le souligne la large couverture de ce sujet par les médias. Dans ce cadre, au-delà de la production statistique conventionnelle, l'OFS a développé Salarium, une application web permettant aux utilisateurs d'obtenir des chiffres détaillés en fonction de critères tels que la région, le sexe, l'industrie et le nombre d'heures de travail hebdomadaires. Les résultats partagés sur cette page, qui est la plus visitée du site de l'OFS, sont utilisés par exemple pour les négociations salariales individuelles, pour les négociations entre partenaires sociaux et pour le contrôle des salaires usuels. Ces données sont d'une richesse inestimable pour la société suisse qui bénéficie directement de leur réutilisation, par exemple, par le monde de la recherche. En effet, ces données permettraient d'évaluer et d'adapter les mesures politiques sociales et économiques afin d'assurer leur efficacité et leur équité. Le cas pratique présenté ici permettrait de faciliter et d'accélérer la réalisation de ce potentiel dans le respect de la vie privée des administrés et contribuant ainsi à l'acceptation de cette réutilisation.
- Programme « Digisanté » : ce programme vise à promouvoir la transformation numérique du système de santé. Le volet 4 du projet se concentre sur deux objectifs : le premier concerne l'amélioration de l'utilisation des données détenues par le service public pour une meilleure planification et pilotage du système de santé par les autorités et les acteurs concernés. Le second objectif vise à faciliter l'accès à ces données aux chercheurs issus du milieu académique et de l'économie privée pour traiter les problématiques sanitaires. La cas pratique décrit dans ce chapitre offre une solution technique évidente à ce défi permettant d'assurer la confidentialité des données de santé lors de leur réutilisation et ainsi concrétiser la mise en place d'un « Espace de données pour la recherche sur la santé » respectueux de la vie privée.

En résumé, la plateforme présentée dans ce chapitre permet d'accroître le potentiel d'utilisation des données de l'administration suisse, de manière automatisée, tout en garantissant la confidentialité des données identifiantes, limitant ainsi le risque réputationnel pour l'administration et celui de subir des conséquences néfastes pour les administrés.

4.2 Principe

Parties et schéma confiance

L'architecture de la plateforme est élaborée pour maximiser l'utilisation des caractéristiques spécifiques des relations de confiance au sein d'une administration publique :

- Les unités de confidentialité transfèrent leurs données au fournisseur de données désigné, qui est généralement un office de la Confédération, dans le cadre d'une relation de confiance établie par une base légale existante.
- Chaque office de la Confédération peut faire appel à un fournisseur de calcul de confiance, tel que l'Office fédéral de l'informatique et des télécommunications, ce qui élimine la nécessité d'utiliser des technologies de contrôle de la confidentialité des inputs. Ce fournisseur est chargé de la sécurité des données, ce qui implique la mise en place des mesures nécessaires pour prévenir l'accès non autorisé aux données et à la plateforme. Il est également responsable de l'identification et de la légitimation des utilisateurs de la plateforme.
- Les parties consommatrices de données peuvent être diverses, allant des employés fédéraux d'autres offices au grand public. Dans tous les cas, il est supposé que l'office fournissant les données et le consommateur du produit de données ne sont pas liés par une relation de confiance. Par conséquent, l'utilisation d'une technologie de contrôle des outputs est nécessaire, en particulier la confidentialité différentielle, pour atténuer le risque de divulgation d'informations identifiables.

Ce modèle de confiance est courant dans les administrations publiques qui peuvent compter sur des capacités de calcul gérées directement par l'État.

Description du service

Le fonctionnement du service peut être appréhendé à travers la figure 4, laquelle met en lumière le scénario pratique où les données sont mises à la disposition d'un utilisateur autorisé. Du point de vue de l'utilisateur, le service opère de la manière suivante :

- 1) L'utilisateur se connecte à distance à la plateforme, accédant ainsi à un environnement virtuel conçu pour l'exécution des langages de programmation Python ou R. La maîtrise de ces langages est indispensable pour utiliser la plateforme, étant donné leur prédominance dans l'analyse de données tant dans le domaine privé qu'académique.
- 2) À l'aide d'une librairie, l'utilisateur peut consulter un catalogue exhaustif des jeux de données qui lui sont disponibles, ainsi que leurs nature et représentations (métadonnées), tout en prenant connaissance du budget de perte de confidentialité qui lui est alloué.
- 3) Une fois un jeu de données sélectionné, l'utilisateur peut télécharger dans son environnement de calcul un jeu de données factice entièrement simulé, mais reproduisant fidèlement les métadonnées du jeu de données original. Ce jeu de données factice peut être utilisé pour élaborer et tester des algorithmes d'analyse de données.
- 4) L'utilisateur peut ensuite transmettre son algorithme finalisé à un serveur distant de l'administration fédérale. Avant son exécution, l'algorithme est soumis à une analyse afin de vérifier la présence d'un mécanisme de contrôle de la confidentialité. En l'absence de ce mécanisme, l'exécution de l'algorithme est refusée. Ensuite, le serveur vérifie les droits d'accès de l'utilisateur au jeu de données ainsi que l'adéquation de son budget de perte de confidentialité.
- 5) Si les conditions d'accès et de confidentialité sont remplies, le serveur sécurisé récupère les données identifiantes à partir d'un espace de stockage sécurisé.
- 6) L'algorithme est alors appliqué de manière autonome au jeu de données original, et le résultat est calculé en préservant la confidentialité grâce à la méthode de confidentialité différentielle.
- 7) Le résultat protégé est enregistré et transmis à l'utilisateur. Cet enregistrement permet à l'utilisateur de consulter ses résultats antérieurs, évitant ainsi une répétition de la consommation de son budget pour une même analyse. L'archivage des algorithmes et des résultats associés permet également aux autorités de surveiller l'activité des utilisateurs ainsi que l'utilisation des différents jeux de données.

Cette approche permet à l'utilisateur d'exécuter des algorithmes sans accéder directement aux données identifiantes, tout en assurant à l'office fournissant les données que le risque de divulgation d'informations identifiables est limité.

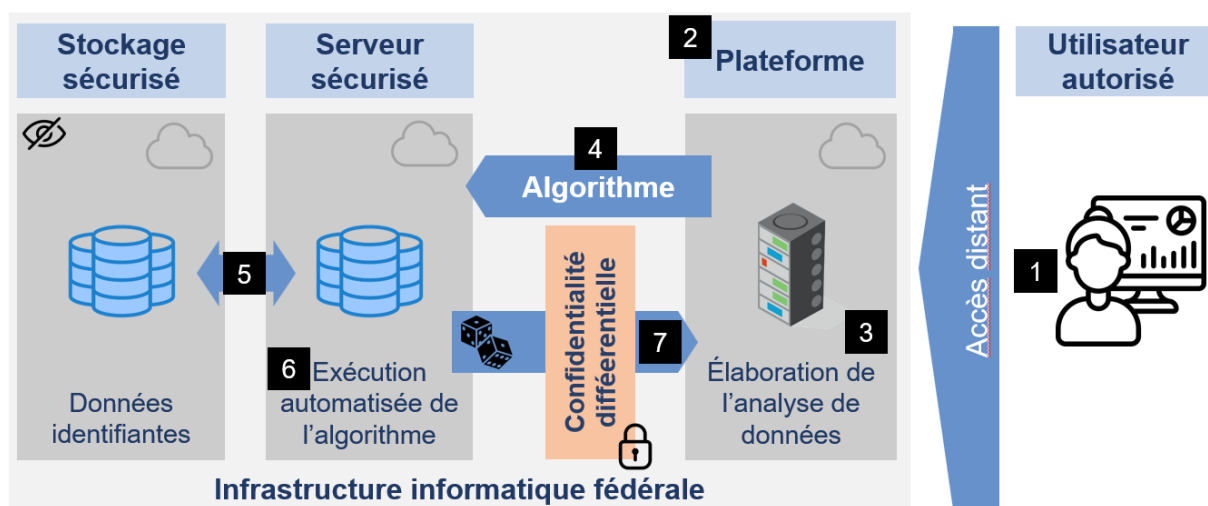


Figure 4 : Schéma de principe d'une plateforme permettant l'application confidentielle de la science des données sans transfert de données.

Pour qu'une analyse de données soit autorisée, il est impératif qu'elle intègre un mécanisme de contrôle de la divulgation, tel qu'un algorithme de randomisation basé sur la confidentialité différentielle. La plateforme ne développe pas ces algorithmes en interne, mais s'appuie sur des bibliothèques à source ouverte reconnues, notamment "OpenDP", "SmartnoiseSQL" pour la manipulation et la transformation de données, ainsi que "DiffPrivLib" pour l'apprentissage machine et l'intelligence artificielle, pour n'en citer que quelques-uns.

Le serveur sécurisé est lié directement à l'espace de stockage des jeux de données. Avec la démocratisation du « Once Only Principle », l'utilisation de la plateforme bénéficie des initiatives autour de la création de catalogues répertoriant les jeux de données détenus par l'administration et surtout listant leurs métadonnées. À titre d'exemple, la norme I14Y simplifie la génération de jeux de données factices destinés à évaluer les algorithmes d'analyse de données conçus par les utilisateurs. L'intégration directe de ces services, telle que celle permise par le package "fso-metadata" développé par l'OFS, permet de tirer pleinement parti de ces initiatives en les fusionnant, et ainsi, d'exploiter pleinement la valeur des données détenues par l'administration fédérale.

Afin de prouver la faisabilité d'une telle plateforme, une implémentation en **code ouvert** a été développée par le centre de compétence de la Confédération en science des données (DSCC) et est disponible sur son GitHub²⁰. **Ce projet, développé pour assurer sa portabilité sur une infrastructure informatique standard, est donc à disposition à toute entité de l'administration fédérale qui souhaiterait expérimenter, voir déployer en production, ce type de service.** Elle est accompagnée d'un rapport couvrant l'ensemble des détails techniques (<https://arxiv.org/abs/2406.17087>).

4.3 Limites et Défis

Ce cas pratique tire profit des caractéristiques spécifiques des relations de confiance au sein de l'administration fédérale. En collaborant avec un prestataire de calcul de confiance, l'accent est mis exclusivement sur la garantie de la confidentialité des résultats produits. Cette protection est mise en œuvre grâce à l'application de la confidentialité différentielle. Le principal défi associé à la confidentialité différentielle réside dans la détermination du budget de perte de confidentialité. Pour rappel, ce concept permet de réguler de manière précise le compromis entre l'utilité des données et le risque de divulgation, en définissant un seuil maximal de perte de confidentialité pour chaque utilisateur. Le choix de ce seuil est une

²⁰ <https://github.com/dscc-admin-ch/lomas>

question qui revêt une dimension politique et peut être formulé ainsi : "Quel est le niveau de risque maximal auquel les unités de confidentialité du jeu de données peuvent être exposées de manière acceptable ?" ou encore "Quel est le niveau minimal d'utilité requis pour garantir la fiabilité du jeu de données ?". Ces deux interrogations correspondent respectivement aux principes de "confidentiality first" et "utility first", permettant ainsi à un organisme de définir ses priorités et de choisir de manière éclairée et justifiable le budget de perte de confidentialité.

Dans cette optique, nous examinons à titre d'exemple l'utilisation des données dans le domaine de la recherche. Le processus actuel est caractérisé par sa lenteur et sa lourdeur lors de l'obtention d'accès à des données identifiantes, nécessitant un cadre juridique formel transférant la responsabilité de la protection des données au laboratoire de recherche qui les utilise. Ce processus, outre son coût administratif élevé, entraîne une considérable réduction de la vitesse de la recherche, une situation parfois incompatible avec des circonstances urgentes telles que la pandémie de Covid-19. Pour illustrer ce défi, nous présentons deux cas d'utilisation particulièrement pertinents de la plateforme :

- « Facilitation et/ou travaux préliminaires » : Cette approche vise à fournir rapidement des données à un chercheur pour lui permettre de démarrer ses travaux sans délai. Cela lui offre l'opportunité de vérifier la faisabilité de ses analyses et, si celles-ci sont validées, de préparer et de tester ses algorithmes en attendant la conclusion du processus administratif d'obtention des données originales. Les avantages sont doubles :
 - Pour l'utilisateur : accélération du projet de recherche.
 - Pour l'administration fédérale : économies de ressources lorsque les analyses s'avèrent non faisables.
- « Rendre possible » : Cette approche concerne la mise à disposition de données précédemment jugées trop sensibles, mais qui peuvent désormais être valorisées étant donné qu'elles ne sont jamais divulguées sous leur forme originale et que le risque de divulgation est maîtrisé. Les bénéfices sont les suivants :
 - Pour l'utilisateur : analyse de données normalement inaccessibles.
 - Pour l'administration fédérale : exploitation du plein potentiel des données collectées. De plus, cela entraîne des retombées réputationnelles positives car l'investissement financier dans la collecte et la consolidation des jeux de données est valorisé au-delà de l'organisme responsable.

Ces deux cas d'utilisation exigent un faible budget de perte de confidentialité pour compenser le risque, que ce soit en raison de la sensibilité des données ou de la nécessité d'une temporalité courte qui rend difficile la mise en place de contrôles étendus sur les utilisateurs potentiels ou la conclusion de contrats formels.

En dernier lieu, bien que le risque de divulgation soit évalué et maîtrisé pour chaque utilisateur grâce au budget de perte de confidentialité, aucune mesure technique ne prévient la possibilité pour plusieurs utilisateurs de s'associer afin de combiner leurs budgets individuels dans le but d'extraire des informations identifiables de la plateforme. Une telle collusion doit être explicitement interdite par règles juridiques régissant l'utilisation de la plateforme. Par conséquent, il est impossible de se soustraire entièrement à un cadre légal régissant l'utilisation de la plateforme. Tant que le budget de perte de confidentialité des utilisateurs reste limité, ce cadre est probablement moins contraignant que les accords requis pour le partage de données identifiantes. Cela se traduit par des économies de ressources et une plus grande facilité d'accès pour les utilisateurs. Au sein de l'administration fédérale suisse, le contrôle de l'identité et la traçabilité des utilisateurs peuvent être assurés grâce à des protocoles d'authentification tels que eIAM.

5 Cas pratique 2 : Enrichissement sécurisé de données par appariement confidentiel

5.1 Contexte et objectifs

La collecte systématique de données identifiantes et ses limites

La collecte systématique de données s'étend désormais à tous les domaines de la société, reflétant une évolution significative dans la manière dont les informations sont recueillies et utilisées. Dans le secteur privé, cette pratique est observée de manière notable au sein des institutions bancaires, qui collectent minutieusement des données sur les transactions financières et les habitudes de consommation des clients. De même, les fournisseurs de "smart devices" exercent une collecte de données intensive, notamment dans des domaines tels que la santé personnalisée, où des dispositifs connectés surveillent et enregistrent en temps réel les paramètres physiologiques des individus. Cette tendance s'étend également à des secteurs comme l'efficacité énergétique, où les capteurs intelligents mesurent et analysent la consommation d'énergie dans les bâtiments résidentiels et commerciaux, et la téléphonie mobile, où les opérateurs recueillent des données sur la mobilité des individus.

Dans le secteur public, et notamment le domaine médical, une collecte systématique est également entreprise, bien qu'encadrée par un cadre légal strict reposant souvent sur l'obtention d'un consentement explicite (Art. 7 al. 1 LRH). Par exemple, il est de plus en plus courant que, lors d'une hospitalisation, les patients soient interrogés afin d'autoriser l'utilisation de leurs données à des fins d'études cliniques ou épidémiologiques.

Les organisations non gouvernementales (ONG) jouent également un rôle majeur dans la collecte de données à des fins humanitaires et de développement. Elles recueillent des informations sur les flux migratoires pour mieux comprendre les mouvements de populations et identifier les besoins en termes d'assistance et de protection des migrants. De plus, elles mesurent le développement économique et social dans les pays en développement afin d'évaluer l'impact des programmes d'aide et d'orienter les politiques de développement. Enfin, elles interviennent dans la gestion des crises internationales, telles que les épidémies ou les catastrophes naturelles, en collectant des données pour évaluer les besoins humanitaires et coordonner les interventions d'urgence.

Cependant, il est important de souligner que la nature systématique de cette collecte engendre inévitablement des biais, des duplications et, de manière plus générale, des imprécisions. Par conséquent, leur utilisation dans des domaines sensibles, au-delà par exemple de la simple publicité ciblée, s'avère délicate et requiert une analyse et une modélisation approfondie ainsi que des mesures de sécurité et de protection de la vie privée.

D'un autre côté, l'administration fédérale consacre des investissements substantiels, à la fois en termes de temps et de ressources, pour la collecte, la sélection et la consolidation de jeux de données jugés fiables et dignes de confiance. Ces données représentent une source unique, comparable uniquement à certaines études cliniques dans le domaine de la santé. Néanmoins, certaines informations cruciales pour le fonctionnement de l'administration fédérale demeurent indisponibles ou non collectées en raison du manque de base légale ou de l'absence d'acceptation par la société, les considérant comme associées à un risque trop élevé pour les individus. L'enrichissement des données détenues aussi par différents organes de l'administration fédérale que par le monde de recherche, des ONG et du secteur privé avec celles détenues par le secteur public permet de réaliser pleinement leur potentiel. Ce processus d'enrichissement nécessite un appariement, qui consiste à combiner deux (ou davantage) sources de données en associant les informations relatives à la même personne identifiable. Il devient alors possible d'analyser les résultats de cet appariement ou de l'utiliser pour entraîner des modèles d'apprentissage automatique ou d'intelligence artificielle. Toutefois, il est impératif que cette pratique soit menée dans le strict respect de la confidentialité des unités identifiables dont les données sont utilisées.

L'appariement de données : opportunités pour le secteur public

L'appariement des données présente des avantages significatifs pour le secteur public. Tout d'abord, il permet l'enrichissement des données détenues par d'autres administrations, facilitant ainsi l'appariement entre différentes entités administratives telles que les offices fédéraux ou d'autres niveaux administratifs tels que les cantons et les communes. Par exemple, cela permet à des organismes tels que l'Office fédéral de la santé publique (OFSP) ou l'Office fédéral de l'environnement (OFEV) d'évaluer l'impact des politiques de santé publique ou environnementales sur la mortalité en utilisant les données collectées par l'Office fédéral de la statistique (OFS). De plus, l'enrichissement avec des données détenues en dehors de l'administration offre aussi des perspectives pour l'administration fédérale : les données provenant d'acteurs externes, tels que le secteur bancaire, permettraient par exemple une estimation plus précise des indicateurs économiques de consommation. De même, les données collectées par les fournisseurs d'énergie pourraient améliorer la gestion des programmes de développement de l'efficacité énergétique ou permettre l'élaboration de règles efficaces en cas de pénurie. Enfin, l'utilisation des données de mobilité détenues par les opérateurs de téléphonie mobile permet, par exemple, l'optimisation des moyens de transports ainsi que de leurs infrastructures et pourrait s'avérer cruciale lors de la gestion de crises nationales telles qu'une épidémie ou une catastrophe naturelle.

L'appariement des données offre également des avantages significatifs pour les acteurs non publics. Tout d'abord, dans le domaine de la recherche, en particulier dans le domaine de la santé, de multiples acteurs détiennent d'importants jeux de données qui peuvent présenter des biais dus à une mauvaise campagne de collecte. Enrichir ces ensembles de données avec des données fiables telles que celles détenues par l'OFS permet de corriger ces lacunes, rétablissant ainsi la crédibilité scientifique des résultats des études menées avec ces jeux de données imparfaits. Cette approche constitue une voie convaincante pour résoudre en partie le problème de reproductibilité auquel est confrontée la communauté scientifique contemporaine. Aujourd'hui, à l'OFS, ces appariements sont possibles à des fins de planification, statistique et recherche (art. 14a LSF) mais extrêmement coûteux en ressources aussi bien administratives que techniques. L'utilisation des technologies d'amélioration de la confidentialité offre une opportunité de proposer ce service à grande échelle tout en limitant le fardeau financier qu'il impose à l'administration fédérale.

De même, dans le domaine des ONG et des collaborations interétatiques, les institutions internationales s'efforcent de promouvoir le bien commun au-delà des frontières nationales. Cependant, l'échange de données à l'échelle internationale ou avec certaines organisations intergouvernementales est souvent entravé, ou d'une complexité incomparable, en raison de l'existence de réglementations strictes. Des domaines tels que le commerce international ou la migration pourraient bénéficier de l'utilisation de données identifiantes détenues par un ou plusieurs pays pour relever les défis mondiaux tels que le changement climatique.

En outre, dans le secteur privé, toute entreprise qui collecte de manière systématique des données identifiantes pourrait tirer parti d'un appariement avec les données détenues par l'administration fédérale pour les enrichir et les fiabiliser. Cette pratique nécessiterait un cadre légal clair et favoriserait le dynamisme de l'économie suisse en stimulant l'innovation par la validation des produits de données créés.

Il est impératif que ce type d'appariement, impliquant principalement des données identifiantes sensibles, soit accepté à la fois politiquement et socialement, tout en garantissant que les avantages découlant de leur utilisation ne se réalisent pas aux dépens des citoyens, des ménages et des entreprises suisses. Afin de maintenir la confiance envers l'État, il est nécessaire de prendre des mesures pour limiter le risque de divulgation de données identifiantes lorsqu'elles sont appariées, que ce soit à l'intérieur ou à l'extérieur de l'administration fédérale, et de garantir qu'il est impossible de tirer des conclusions fiables au niveau de l'unité de confidentialité.

Un service d'enrichissement sécurisé de données par appariement confidentiel

Ce cas pratique examine la possibilité d'apparier des données provenant de sources qui n'ont pas le droit, ou qui ne souhaitent simplement pas, partager des données identifiantes entre elles, mais qui cherchent néanmoins à créer un produit combinant les deux jeux de données. Ce scénario se matérialise sous la forme d'un service auquel les parties autorisées et intéressées par l'appariement de données peuvent se connecter à distance afin de mettre à disposition leurs données, les enrichir par le biais d'un appariement, puis créer des produits de données dont le risque de divulgation est contrôlé. Tout ce processus est exécuté sans que les contributeurs ne puissent accéder aux données identifiantes originales des autres à aucun moment. L'objectif principal de ce service est soit de permettre à l'administration fédérale d'enrichir ses propres jeux de données à l'aide de sources de données externes, soit de mettre à disposition les jeux de données détenus par l'administration fédérale afin de fiabiliser les données provenant de sources externes.

En d'autres termes, ce service facilite la collaboration entre deux fournisseurs de données qui ne se font pas mutuellement confiance, dans le but de mutualiser leurs données et de créer un produit de données exploitant les deux sources. L'absence de relation de confiance entre ces parties est essentielle, garantissant que la solution technique ne permettra pas aux différents acteurs d'accéder directement aux résultats de l'appariement : les données identifiantes ne sont jamais mises à disposition sous leur forme originale, seule la sortie du produit de données créé à partir du résultat de l'appariement est transmise au consommateur, après l'application d'une mesure de contrôle du risque de divulgation. Par conséquent, il est impératif de combiner une technologie d'amélioration de la confidentialité des "outputs", en particulier la confidentialité différentielle, avec une technologie de confidentialité des "inputs".

La confidentialité des inputs garantit que les parties impliquées n'accèdent jamais directement aux données originales identifiables utilisées pour l'appariement, et que le code exécuté par le service est bien celui convenu par les deux fournisseurs. En parallèle, la confidentialité des outputs permet de contrôler de manière précise le risque de divulgation lié à la création du produit de données utilisant les données enrichies. Cette dernière assure qu'aucune conclusion ne peut être tirée de manière fiable au niveau individuel à partir du résultat de l'appariement : seules des conclusions concernant les groupes de personnes sont possibles, toutefois leur bénéfice pour le bien commun doit être tout de même évalué en déterminant qui utilise ce résultat dans quel but. Il convient de souligner que toute tentative de profilage individuel, de ciblage ou simplement d'extraction d'information au niveau individuel est rendue non fiable grâce à la technologie de contrôle des sorties. L'architecture du service décrite dans la section suivante est sélectionnée afin de permettre une combinaison optimale de ces deux types de technologies d'amélioration de la confidentialité.

En raison de son rôle et de son architecture spécifique, le service assure plusieurs fonctions clés :

- Il contribue à maintenir la confiance de la population envers l'État en garantissant que les utilisateurs n'accèdent pas aux données originales, limitant ainsi le risque de conséquences néfastes au niveau individuel résultant de l'utilisation de données identifiantes.
- Il augmente l'efficacité de l'État dans l'accomplissement de ses tâches en lui permettant d'accéder à de nouvelles sources de données.
- Il favorise le bénéfice de l'ensemble de la société en mettant à disposition les sources de données fiables détenues par l'administration fédérale.

En résumé, le service facilite la mutualisation des données détenues par les différents acteurs de la société suisse, ce qui permet à chacun de tirer profit de ces ressources tout en garantissant la confidentialité des données identifiantes au niveau individuel et en contrôlant précisément le risque de subir des conséquences néfastes pour les administrés.

5.2 Principe

Parties et schéma confiance

L'architecture du service est définie par l'absence de relation de confiance entre les différents contributeurs et utilisateurs, comme illustré dans la figure 5.

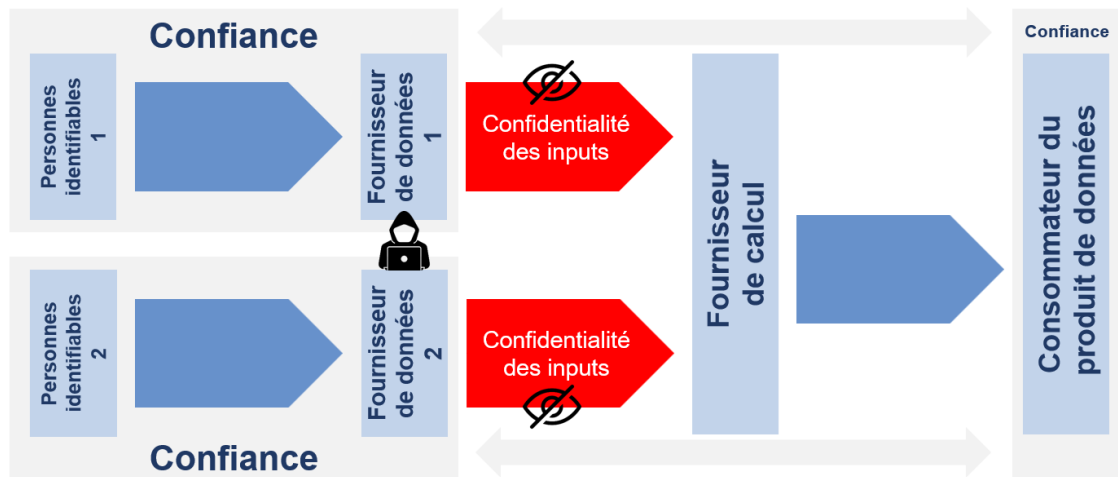


Figure 5 : Schéma de confiance présumé pour le cas pratique « Enrichissement sécurisé de données par appariement confidentiel ».

Les parties impliquées se distinguent comme suit :

- 1) Deux groupes, ou plus, de personnes identifiables, dont les données sont collectées par deux fournisseurs de données, ou plus, indépendants. Ces collectes sont distinctes, ne recouvrent pas les mêmes informations et incluent un sous-ensemble d'individus identifiables communs. L'un des fournisseurs souhaite combiner les informations provenant des deux collectes pour créer un produit de données enrichi par les deux sources.
- 2) Fournisseur de données : l'un des fournisseurs représente un organe de l'administration fédérale, tandis que le second peut appartenir à toute catégorie d'acteur de la société suisse ou internationale. Pour garantir la confidentialité des données identifiantes détenues par les deux parties, il est impératif d'imposer qu'aucun des deux fournisseurs de données n'accède aux données identifiantes de l'autre sans l'application d'une technique de contrôle de la divulgation.
- 3) Fournisseur de calcul : cette partie ne peut être considérée comme digne de confiance par les deux fournisseurs de données. Traditionnellement, dans le cadre d'une administration, l'OFIT ou tout prestataire informatique de la Confédération est considéré comme digne de confiance grâce aux règles légales applicables et des mesures de sécurité informatique. Cependant, dans un contexte multipartite, au moins l'un des deux fournisseurs n'est pas lié par une relation de confiance envers l'administration fédérale, ce qui impose que le fournisseur de calcul ne doit pas être techniquement en mesure d'accéder aux données des fournisseurs de données. Cette absence de confiance ne nécessite pas nécessairement de recourir à l'infrastructure de calcul gouvernementale ; le calcul peut également être externalisé vers des prestataires de services en nuage publics. Par conséquent, la solution technique de confidentialité des entrées doit offrir des garanties suffisantes en termes de sécurité et de confidentialité pour ce scénario.
- 4) Le consommateur : dans ce cas, le consommateur du produit de données est supposé être l'un des deux, ou les deux, fournisseurs de données. Étant donné que ces deux parties ne sont pas liées par une relation de confiance, il est donc nécessaire de protéger le produit à l'aide d'une technologie d'amélioration de la confidentialité assurant la **confidentialité des inputs**.

Choix des technologies d'amélioration de la confidentialité

La nature multipartite de ce cas pratique restreint le choix des technologies de confidentialité des inputs aux trois options suivantes : les environnements d'exécution fiables, le calcul multipartite sécurisé et le chiffrement homomorphe. Le choix de la technologie est guidé par plusieurs critères, notamment la compatibilité avec la technologie de confidentialité des outputs choisie (confidentialité différentielle), la disponibilité de solutions open-source pour limiter le risque de "vendor lock-in", ainsi que la facilité d'implémentation et de déploiement du service. Une analyse détaillée des avantages et des inconvénients de chaque technologie est fournie dans le chapitre 3. Nous expliquons brièvement ci-dessous la motivation derrière les choix de ce cas pratique en particulier :

- Le calcul multipartite sécurisé ne dispose pas encore d'implémentations open-source suffisamment matures pour être utilisées dans ce type d'application. De plus, la combinaison de la confidentialité différentielle avec des protocoles de calcul multipartite sécurisé pose encore certains défis, notamment la génération multipartite délocalisée de nombres aléatoires. Bien que quelques techniques existent, elles demeurent encore à un stade de recherche.
- Le chiffrement homomorphe bénéficie de solutions multipartites open-source, mais sa combinaison avec la confidentialité différentielle en l'absence d'une tierce partie de confiance nécessite un mécanisme de randomisation appliqué directement sur les données chiffrées pour décrypter le produit de données et appliquer la confidentialité différentielle. Cette tâche s'avère complexe et aucune solution mature n'est actuellement disponible.
- Les environnements d'exécution fiables permettent aujourd'hui de déployer des services comme décrit dans le cas pratique 1 avec un nombre limité de modifications. Il est ainsi possible de déployer ce cas pratique directement au sein d'une enclave, offrant une solution simple combinant les technologies de confidentialité des inputs et des outputs. De plus, des initiatives publiques-privées telles que Gramine²¹ offrent des solutions open-source et portables sur différents prestataires de services en nuage. Associés à un service d'attestation d'intégrité du code exécuté, les environnements d'exécution fiables constituent la solution la plus complète pour l'implémentation de ce cas pratique. Cependant, contrairement aux deux autres technologies, ces environnements ne fournissent aucune garantie mathématique de sécurité et nécessitent une confiance dans le fabricant de matériel, par exemple Intel ou AMD.

Pour ce cas pratique, les environnements d'exécution apparaissent comme une solution naturelle présentant de grandes synergies avec le cas pratique présenté dans le chapitre précédent, dont les composants peuvent être réutilisés directement pour la production de produits de données une fois l'appariement réalisé.

²¹ <https://gramineproject.io/>

Description du service

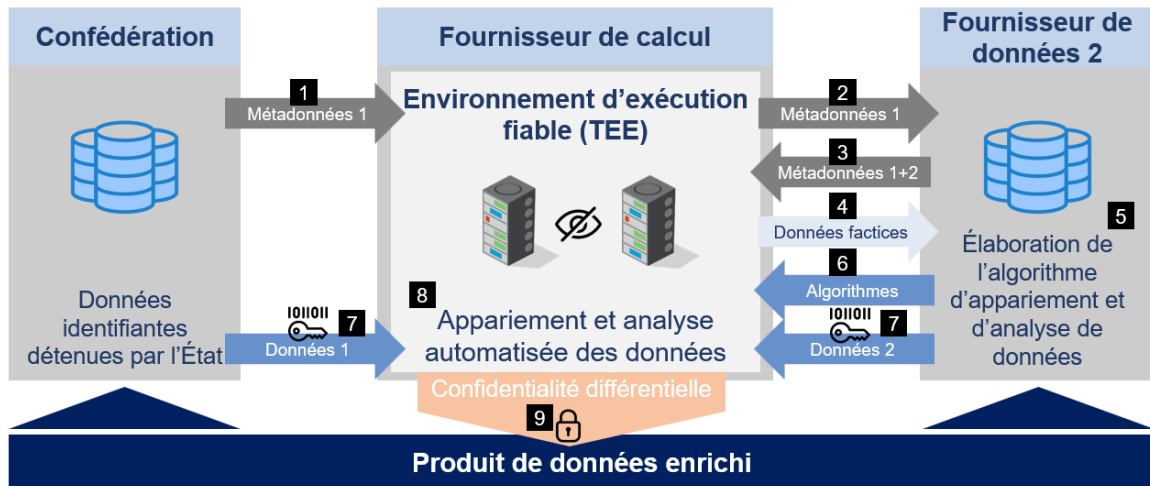


Figure 6 : Schéma de principe du service permettant la création de produits de données à partir de données enrichies à l'aide d'un appariement confidentiel tout en contrôlant le risque divulgation

Le fonctionnement du service est détaillé dans la figure 6. Par défaut, nous partons du principe que le fournisseur 1, représenté par la Confédération sur la figure 6, met à disposition ses jeux de données, tandis que le fournisseur 2 demande la création du produit de données en contribuant également ses propres données. Nous présumons que le fournisseur 1 et le fournisseur 2 ont préalablement convenu d'un budget de perte de confidentialité acceptable pour la création de ce produit, ainsi que pour la mise en commun de leurs bases de données respectives. Enfin, il est supposé que l'Administration fédérale soit chargée de l'exploitation du service, ce qui implique la mise en place des autorisations nécessaires, l'allocation du budget de perte de confidentialité et le déploiement de l'enclave.

Du point de vue du fournisseur 2, le fonctionnement du service se déroule selon les étapes suivantes :

- 1) Le fournisseur 1 télécharge ses métadonnées dans l'environnement d'exécution fiable.
- 2) Le fournisseur 2 récupère les métadonnées du jeu de données fourni par le fournisseur 1.
- 3) Le fournisseur 2 élargit le catalogue de métadonnées en y intégrant ses propres métadonnées, et standardise l'encodage de ses données en les alignant sur celui du fournisseur 1. Enfin, le fournisseur 2 télécharge dans l'environnement d'exécution fiable le catalogue de métadonnées consolidé.
- 4) Le catalogue de métadonnées consolidé est utilisé pour générer un jeu de données factice reproduisant les caractéristiques des jeux de données 1 et 2. Ce jeu de données factice est transmis au fournisseur 2 pour le développement et le test, local, de l'algorithme d'appariement et de création du produit.
- 5) Développement des règles de comparaison entre les jeux de données 1 et 2, ainsi que de l'algorithme de création du produit de données, sur le jeu de données factices.
- 6) Téléchargement des algorithmes d'appariement et d'analyse de données dans l'environnement d'exécution fiable. Test des algorithmes dans cet environnement sécurisé sur le jeu de données factices.
- 7) Téléchargement des deux jeux de données identifiantes détenus par chacun des fournisseurs dans l'environnement d'exécution fiable. Ce transfert est crypté pour empêcher tout accès non autorisé.
- 8) Vérification de la présence d'un mécanisme de confidentialité différentielle et de l'existence d'un budget de perte de confidentialité suffisant pour l'exécution de l'algorithme de création du produit de données.
- 9) Exécution automatique de l'appariement et de l'algorithme de création du produit de données. Le produit est ensuite envoyé, crypté, aux fournisseurs de données.

Les étapes 7, 8 et 9 sont similaires à celles décrites dans le cas pratique 1, reposant sur le déploiement du cas pratique décrit dans le chapitre 1 dans un environnement d'exécution fiable. Ainsi, grâce à ce processus, le fournisseur 2 peut créer son produit de données à partir du résultat de l'appariement sans jamais accéder aux données identifiantes, tout en garantissant au fournisseur 1 que le produit de données créé ne présente qu'un risque limité de divulgation d'informations identifiables.

5.3 Limites et Défis

Le cas pratique présenté ici repose fondamentalement sur l'harmonisation et la standardisation des métadonnées provenant des deux fournisseurs de données. Ces dernières sont supposées être partagées entre les deux fournisseurs de données, ce qui implique la divulgation des noms des colonnes, des descriptions de leur contenu, ainsi que l'ensemble des valeurs possibles à chaque fournisseur. Il est crucial de souligner que ni l'appariement ni l'utilisation automatisée des données personnelles ne sont réalisables sans cette étape préliminaire. Pour exploiter pleinement le potentiel des données détenues par l'administration fédérale, il est impératif que l'effort requis pour cette harmonisation soit réalisé et nous soulignons une fois de plus l'importance d'initiatives de standardisation telles que i14y pour exploiter pleinement le potentiel des données détenues par les services de l'État. Les technologies d'amélioration de la confidentialité (PETs) émergent comme une solution technique permettant la réutilisation de données détenues par l'administration fédérale de manière respectueuse de la vie privée une fois la standardisation achevée. Ces deux éléments, à savoir les PETs et l'harmonisation des métadonnées, sont fondamentaux pour la science des données moderne et donc indissociables et doivent être mis en œuvre conjointement pour réaliser la pleine valorisation des données détenues par la société suisse.

Ce deuxième cas pratique est directement fondé sur les outils exposés dans le cas pratique 1. Par conséquent, il rencontre les mêmes difficultés et défis, notamment en ce qui concerne le choix du budget de perte de confidentialité et la mise en place du cadre légal associé. Mais au-delà des défis juridiques et méthodologiques, ce cas pratique s'appuie sur l'utilisation de matériel informatique spécialisé, à savoir des puces de calcul permettant un cloisonnement strict des utilisateurs (TEE / confidential computing). Ces types de machines font aujourd'hui partie de l'offre de la plupart des fournisseurs de services en nuage publics tels qu'Azure, AWS, Google Cloud, etc. Cependant, ils ne sont pas encore proposés par les services informatiques de la Confédération. Leur mise en place nécessiterait un investissement en infrastructure et en ressources humaines pour offrir ce type de service au sein de l'administration. Toutefois, la nature sécurisée de ces services pourrait justifier de recourir directement aux prestataires externes susmentionnés plutôt que de réaliser un tel investissement en interne. Le choix de développer ces capacités en interne ou de s'appuyer sur des prestations en nuage publiques est donc une question politique liée à la gouvernance des données et à leur exploitation. Pour exploiter pleinement le potentiel des données détenues par l'État, il est donc nécessaire pour l'administration fédérale soit d'investir dans l'infrastructure nécessaire à leur mise à disposition grâce aux technologies décrites ci-dessus, soit d'accepter une perte de gouvernance et de créer les bases légales nécessaires à l'utilisation des services en nuage publics tels que les environnements d'exécution fiables. De nouvelles bases légales sont aussi nécessaires pour l'exploitation d'un service tel que décrit dans cette section.

6 Cadre légal et gouvernance

Ce chapitre illustre comment les technologies d'amélioration de la confidentialité (PETs) s'inscrivent dans le cadre légal existant et dans quelle mesure elles peuvent offrir des pistes de réflexion pour faciliter la réutilisation de données identifiantes tout en respectant la vie privée des individus. Cette revue du cadre légal n'a donc en aucun cas la prétention d'être exhaustive. En cas d'une mise en œuvre concrète des cas d'application décrits dans ce rapport, l'ensemble des dispositions relatives à la protection des données doit être appliqué, incluant notamment l'ordonnance sur la protection des données (RS 235.11, OPDo) ainsi que les impératifs de confidentialité inclus dans les instruments internationaux de l'assistance administrative en matière fiscale.

6.1 Traitement de données identifiantes – Revue du cadre légal

Le cadre légal existant en matière de traitement de données identifiantes (v. chapitre 2.1) distingue les données personnelles de personnes physiques des données concernant les personnes morales, et n'aborde qu'indirectement tout regroupement de ces dernières : la législation assure la protection d'un groupe en garantissant la protection de chaque individu composant ce groupe. Toutefois, d'un point de vue technique, protéger un groupe requiert des mesures spécifiques et plus contraignantes que celles assurant la protection de chaque individu qui le compose. Pour cette raison, ce rapport aborde les données identifiantes dans toute leur généralité, à savoir en tant qu'information attachées à une quelconque unité identifiable, voir section 2.1 pour les définitions exactes.

Il convient aussi de rappeler ici que la notion de **traitement** au sens de la loi (Art. 5 let. d LPD) couvre l'ensemble du cycle de vie des données et du processus d'une science des données respectueuse de la vie privée²², c'est-à-dire la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage et enfin la suppression. Ce traitement par l'administration fédérale repose en particulier sur deux principes clés :

- **L'anonymisation des données identifiantes** : le cadre légal existant est fondé sur le principe d'anonymisation, et de suppression, pour garantir la confidentialité des données identifiantes. Les données considérées comme anonymisées sortent du champ d'application de la législation sur la protection des données.
- **L'utilisation primaire des données** : le cadre légal existant restreint l'utilisation des données collectées par l'administration fédérale à celle prévue par la loi. En effet, une base légale explicite pour tout traitement de données, dont la finalité doit être clairement définie, est exigée. Toute réutilisation pour une autre finalité est en principe impossible sauf notamment à des fins de statistique, de planification ou de recherche ou si une base légale est créée pour autoriser le traitement de données déjà collectées à l'origine pour une autre fin.

L'anonymisation et la non-réutilisation reflètent les principes de **l'État de droit** (art. 5 de la Constitution suisse (Cst) ; RS 101), selon lesquels toute activité de l'État doit être fondée sur une base légale, répondre à un intérêt public et être proportionnée au but visé. Ces mesures assurent également la **protection de la sphère privée**, c'est-à-dire « que toute personne a le droit d'être protégée de l'emploi abusif des données qui la concernent » (Art. 13 Cst), et la réalisation des **droits fondamentaux** par l'État (Art 35 Cst). En conséquence les principes de **bonne foi, licéité, proportionnalité, finalité et d'égalité** orientent le cadre légal pour le traitement des données.

Concernant le traitement de données identifiantes de personnes physiques, c-à-d de **données personnelles**, la Loi fédérale sur la protection des données (LPD, RS 235.1) s'applique aussi bien aux acteurs

²² <https://www.bfs.admin.ch/bfs/fr/home/dsc/dsc.html>

privés qu'aux organes fédéraux. Cette dernière implémente les principes d'anonymisation et du principe de finalité de la manière suivante :

- Uniquement le traitement des données personnelles **non-anonymisées**, c-à-d de toute information concernant une personne physique identifiée ou identifiable (Art. 5 LPD), est encadré par la LPD. Toute donnée anonymisée sort donc du champ d'application de cette loi.
- La LPD exige explicitement l'existence d'une **base légale** pour le traitement de ces données personnelles par un organe fédéral (Art. 34 LPD). La nécessité d'une base légale au sens formel ou au sens matériel dépend notamment du degré de sensibilité des données, et de la finalité du traitement : si le traitement des données est susceptible de porter gravement atteinte aux droits fondamentaux d'une personne concernée, une loi formelle est exigée, tandis que si la finalité du traitement est indispensable à l'accomplissement d'une tâche de l'organe fédéral déjà définie dans une loi formelle, une loi au sens matériel peut suffire. La LPD couvre aussi le traitement conjoint de données personnelles par un organe fédéral avec d'autres organes fédéraux, ou avec des organes cantonaux ou même privés, comme décrit dans le cas pratique 2 de ce rapport, en précisant que dans ce cas le Conseil fédéral règle les modalités (procédures de contrôle et responsabilités ; art. 33 LPD).

Lorsqu'il s'agit du traitement de **données concernant les personnes morales** par un organe fédéral, une disposition transitoire de la nouvelle LPD (art. 71 LPD) s'applique. Mais c'est en principe la Loi sur l'organisation du gouvernement et de l'administration (LOGA, RS 172.010) qui entre en ligne de compte. Ces lois implémentent les principes d'anonymisation et d'utilisation primaire de la manière suivante :

- Par analogie avec l'article 5 LPD, les données concernant les personnes morales considérées comme anonymisées sortent du champ d'application de la loi.
- L'article 57r de la LOGA affirme la nécessité d'une finalité pour le traitement de données concernant les personnes morales, y compris des données sensibles, par les organes fédéraux. La finalité du traitement doit correspondre aux tâches de l'organe fédéral telles que définies dans une loi au sens formel.

Concernant les bases légales formelles spécifiques aux organes fédéraux, un exemple particulièrement pertinent dans le contexte de ce rapport est celui de la **statistique fédérale** :

- La loi sur la statistique fédérale (Art. 18 al. 3 LSF) exige l'**anonymisation** des produits de données, qui ne doivent plus contenir d'éléments d'identification des personnes, des ménages, des entreprises ou des établissements interrogés. Toute violation de ce principe engage potentiellement la responsabilité de la Confédération selon la Loi fédérale sur la responsabilité de la Confédération, des membres de ses autorités et de ses employés (LRCE, RS 170.32), pourrait si les conditions légales sont remplies entraîner des sanctions pénales et se répercuterait directement sur la réputation et l'image de l'administration fédérale.
- La statistique fédérale est soumise à la **Loi sur la statistique fédérale** (LSF, 431.01) et l'ordonnance sur les relevés statistiques (RS 431.012.1). Les données collectées par la statistique fédérale sont avant tout utilisées à des fins statistiques mais une base légale existe permettant leur réutilisation sous la forme d'une livraison de données ou d'un appariement à des fins de statistique, de planification et de recherche uniquement. L'application de cette base légale nécessite la signature d'un contrat avec, en général, un transfert de responsabilité en termes de protection des données au destinataire de la livraison. Le projet de nouvelle ordonnance sur la statistique fédérale favorise l'utilisation multiple de données à travers l'implémentation du principe « once-only » mais leur utilisation se limite notamment à des fins de statistique, de planification et de recherche.

Enfin, dans le domaine de la santé, la **Loi relative à la recherche sur l'être humain** (LRH, 810.30) protège les données qui ne sont pas considérées comme anonymisées en implémentant les principes d'anonymisation et d'utilisation primaire de manière similaire.

6.2 Limites du cadre légal existant

6.2.1 État de l'art des attaques d'extraction de données identifiantes : l'anonymisation mise en échec

La pertinence du cadre légal précédemment évoqué doit être mise en perspective avec les récents progrès dans le domaine des techniques d'extraction de données identifiantes à partir d'un produit de données. En effet, ce qui était autrefois considéré comme un simple risque théorique, à savoir une atteinte à la sphère privée engendrée par une divulgation d'attributs tels que l'appartenance à un groupe sensible de la population ou la réidentification directe d'une personne identifiable, est aujourd'hui une réalité. De plus, leur mise en œuvre technique n'est plus une simple vue de l'esprit, mais bel et bien possible à large échelle, donnant lieu à trois catégories d'attaques sur la confidentialité.

En premier lieu, les attaques par appariement consistent à combiner un jeu de micro-données avec une ou plusieurs sources d'informations auxiliaires dans le but d'associer les informations relatives à une même unité identifiable en vue de sa réidentification. Ces micro-données peuvent être obtenues soit illégalement suite à l'exploitation d'une faille de sécurité, soit par des moyens légaux comme une livraison de données pseudonymisées, une reconstruction ou encore une extraction de données à partir d'une publication. Ainsi, ce type d'attaques concerne principalement ce que l'on désigne communément comme micro-données, c'est-à-dire des données directement liées à des personnes identifiables. Avec la démocratisation de la collecte systématique de ce type de données, tout moyen de protection nécessitant d'anticiper la nature et l'étendue des informations auxiliaires disponibles à l'attaquant est voué à être contourné. La réidentification de l'historique de visionnage de film de la plateforme Netflix dans le cadre d'une compétition en science des données par des chercheurs de l'université du Texas à Austin²³ montre à quel point ce type d'attaque est facile à mettre en œuvre et souligne l'impossibilité d'anticiper comment les attaquants utilisent les données auxiliaires à leur disposition.

Les attaques par appariement concernent presque exclusivement les micro-données. Pour les produits de données comprenant une forme d'agrégation ou de généralisation, ils sont quant à eux sujets à un autre type d'attaques, nommées attaques de reconstruction. Ces dernières ont pour objectif d'extraire les micro-données utilisées dans la création d'un produit de données. Ce type d'attaque, autrefois perçu comme un risque potentiel, se révèle aujourd'hui être une vulnérabilité, comme le démontre l'expérience du US Census Bureau²⁴. En effet, ce dernier a réussi à reconstruire et à réidentifier avec succès une part significative de la population américaine à partir des tables du recensement de 2010, malgré l'utilisation de techniques conventionnelles de contrôle de la divulgation telles que l'agrégation et l'établissement de seuils visant à garantir un nombre minimum d'individus dans chaque groupe.

Enfin, le troisième et dernier type d'attaque, connu sous le nom d'attaque par appartenance, ne vise pas à réidentifier un individu, mais simplement à déterminer l'appartenance de celui-ci à un groupe, potentiellement sensible, au sein du jeu de données. Ces attaques sont particulièrement attrayantes pour les attaquants, car les conditions nécessaires à leur succès sont bien plus simples à mettre en place que pour les deux autres types. Le risque associé est particulièrement élevé dans le domaine de la santé publique, où simplement appartenir à un groupe d'individus souffrant d'une maladie ou d'une pathologie rare peut divulguer une information extrêmement sensible.

²³ https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

²⁴ www2.census.gov/library/working-papers/2023/adrm/ces/CES-WP-23-63.pdf

Ces trois catégories d'attaques exposent la vulnérabilité de l'ensemble des produits de données en contournant les méthodes de contrôle du risque de divulgation. En effet, aucune solution technique ne peut offrir une garantie absolue quant à l'échec à 100 % de ces attaques. Par conséquent, il en découle que l'anonymisation, telle que décrite dans la LPD et le RGPD est techniquement impossible à garantir, puisqu'elle requiert une modification irréversible des données identifiantes, ce qui est techniquement impossible. Cela reste toutefois possible d'un point de vue juridique si, en fonction du contexte dans lequel ce traitement a lieu, le risque de succès de ces attaques est jugé suffisamment bas.

La mise à disposition de tout produit de données, qu'il s'agisse de micro-données ou de toute autre forme agrégée, expose les individus à un risque non négligeable de divulgation de données identifiantes. Ce risque résiduel ne peut être réduit à néant qu'en s'abstenant de créer et transmettre le produit. Par conséquent, ce risque de divulgation représente le prix à payer pour bénéficier des avantages offerts par le produit de données : il s'agit d'un compromis entre confidentialité et utilité, soulignant que l'accomplissement de l'un ne peut se faire qu'au détriment de l'autre. Ainsi, lors de la création de tout produit de données, une mise en balance du risque de divulgation par rapport aux bénéfices (en termes d'utilité) doit être effectuée afin de quantifier formellement ce compromis, en recourant à des technologies d'amélioration de la confidentialité des outputs telles que la confidentialité différentielle.

6.2.2 Conséquences pour la législation encadrant la valorisation des données détenues par l'État

L'impossibilité technique de garantir le caractère irréversible de l'anonymisation montre le caractère obsolète de ce principe face aux avancées techniques. Ce constat rend le cadre légal actuel limitant dans l'optique de réaliser le plein potentiel de valorisation des données détenues par l'administration fédérale, et appelle à un cadre légal plus nuancé basé sur la quantification explicite du risque résiduel de divulgation, rendu techniquement possible par l'utilisation de technologies d'amélioration de la confidentialité telles que la confidentialité différentielle.

D'autre part, la création de valeur à partir des données détenues par l'administration fédérale est aussi grandement restreinte par le principe de finalité. Le cadre légal actuel n'offre ainsi que peu de marge de manœuvre pour la réutilisation de ces données à l'aide d'une science des données respectueuse du code de bonnes pratiques de la Confédération pour une science des données centrée sur l'être humain et digne de confiance (point 3 de la décision du CF du 2 Décembre 2022 ; EXE 2022.2746²⁵) ou encore pour leur traitement collaboratif comme décrit dans le cas pratique 2 de ce rapport ou l'exemple « Tableaux globaux de la situation en cas de crise », page 17 du rapport « Science des données pour le bien commun - cas d'application dans l'élaboration des politiques » (point 2 de la décision du CF du 2 Décembre 2022 ; EXE 2022.2746²⁶).

Un élargissement du cadre légal existant autour de la finalité peut être envisagé grâce aux technologies d'amélioration de la confidentialité (PETs) : en effet, les PETs constituent une solution technique pour faciliter une utilisation commune sans partage de données et dont le risque de divulgation lors de la réutilisation de données est formellement contrôlé. Elles assurent ainsi que le risque de souffrir de conséquences néfastes au niveau individuel qui découleraient d'une atteinte à la sphère privée pour les unités identifiables lors de la réutilisation de leurs données est limité. Ainsi, les PETs permettent une réutilisation des données respectueuse de la sphère privée à des fins ne se rapportant pas à des personnes et limité aux organes fédéraux dans les limites prévues par l'article 39 de la LPD.

²⁵ <https://www.bfs.admin.ch/bfs/fr/home/statistiques/catalogues-banques-donnees.assetdetail.29325685.html>

²⁶ <https://www.news.admin.ch/newsd/message/attachments/87132.pdf>

Les PETs ne peuvent en revanche pas assurer à elles seules que l'utilisation de ces données ne soit pas abusive, c'est-à-dire que leur traitement respecte l'ensemble des droits fondamentaux. En outre, elles ne garantissent pas qu'un projet de réutilisation de données soit éthique et bénéfique au bien commun. La production de ce produit de données doit donc s'inscrire dans un cadre plus large prenant en compte sa nature, les données nécessaires et son destinataire en plus de la protection de la sphère privée. Un cadre de gouvernance permettant de couvrir l'ensemble de ces aspects, et leurs risques associés, est nécessaire afin d'assurer la réutilisation de ces données dans le respect de l'État de droit.

6.3 Les « Five Safes » : un cadre de gouvernance pour une science des données respectueuse de la vie privée

L'impossibilité technique de l'anonymisation et les restrictions imposées par le principe de finalité à la création de valeur à partir des données appellent aujourd'hui à un cadre plus nuancé tenant compte de l'ensemble du spectre des risques d'atteinte aux droits fondamentaux et à la confidentialité des individus. En effet, la binarité de ces principes basés sur la notion de conformité échoue à capturer la complexité du risque de divulgation tel qu'il est aujourd'hui connu et ne permet pas à l'administration fédérale de valoriser au mieux ses données afin de faire face aux défis actuels. Il semble donc nécessaire de proposer un cadre permettant de faire l'état des lieux du **continuum** des risques et mesures techniques, organisationnelles et juridiques mises en place pour les contrôler. Il s'agit de proposer des outils donnant une **vision interdisciplinaire et globale** de tout projet de réutilisation de données et permettant une décision éclairée vis-à-vis du compromis risque-utilité, en particulier vis-à-vis du risque de divulgation de données identifiantes.

Formulé il y a plus de 20 ans, le cadre de gouvernance des « Five safes » est largement utilisé par des offices nationaux de statistiques et les services d'archives de données publiques pour la recherche. Ce cadre de gouvernance évalue un projet de réutilisation de données autour de cinq dimensions, à savoir sa nature, les données utilisées, son(ses) destinataire(s), son environnement, et enfin son résultat. Il permet ainsi de couvrir l'ensemble des risques liés à la production et au partage de produits de données dérivés de données identifiantes. Parmi ses utilisateurs, on peut citer les offices nationaux de statistique du Royaume Uni (ONS UK), d'Australie (Australian Bureau of Statistics) et de Nouvelle-Zélande (Stats New Zealand), ou encore le UK Data Service²⁷, Research Data Scotland²⁸ et le Data Innovation Program de la province de Colombie britannique au Canada²⁹.

Largement éprouvé pour encadrer le traitement de données identifiantes sensibles, la formulation de ces « Fives safes » pré-date l'apparition des PETs, mais son exhaustivité et sa flexibilité permet de couvrir également des projets reposant sur l'utilisation des PETs. La figure 7 présente en détail comment ce cadre pourrait se positionner dans le cadre de l'application d'une science des données centrée sur l'être humain et digne de confiance.

²⁷ <https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/>

²⁸ <https://www.researchdata.scot/our-work/data-explainers/what-is-the-five-safes-framework/>

²⁹ <https://www2.gov.bc.ca/gov/content/data/about-data-management/data-innovation-program/privacy-security>

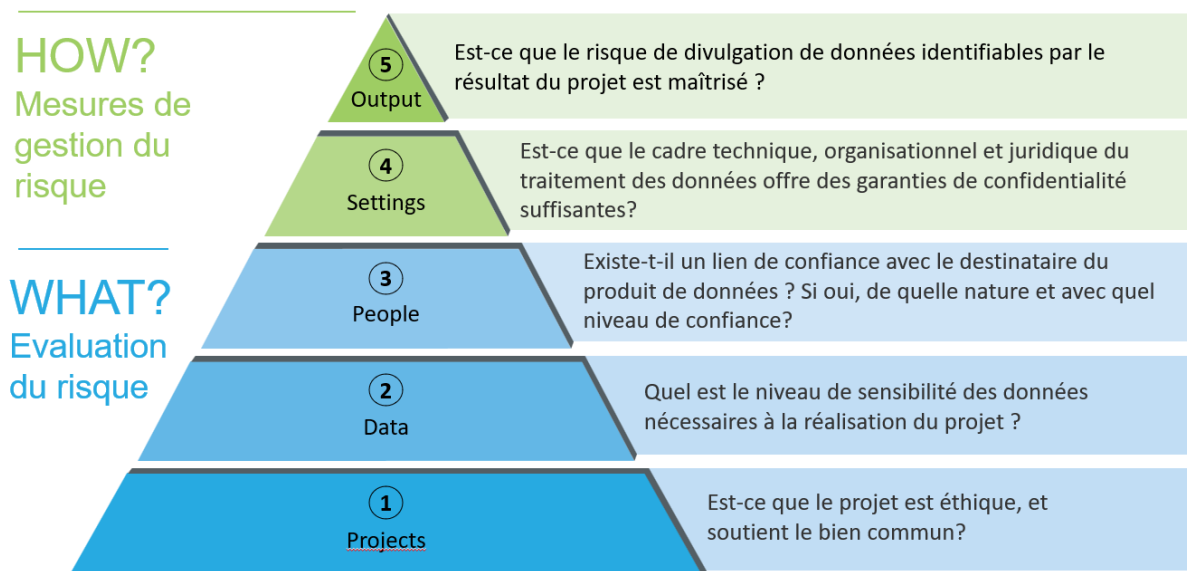


Figure 7 : Les “Five Safes” – Un cadre de gouvernance pour une réutilisation des données détenues par l’Administration fédérale respectueuse des droits fondamentaux et, en particulier, de la vie privée.

Ce cadre de gouvernance permet donc de faire l’état des lieux du contexte de production d’un produit de données autour des dimensions suivantes :

- 1) « **Safe project** » : Est-ce que le projet est éthique, et soutient le bien commun ? Est-ce que le projet est conforme à une science des données centrée sur l’être humain et digne de confiance, qui soutient les politiques publiques ?³⁰ Il est donc nécessaire d’édicter une classification des produits de données en fonction de leur sensibilité et de leurs bénéfices ou risques pour la société. Un exercice similaire a été effectué pour les applications d’intelligence artificielle par l’Union Européenne dans le cadre de législation sur l’IA³¹. Ce type de classification peut être mis en place afin d’encadrer la réutilisation de données au sein de l’administration fédérale et est comparable au volet d’évaluation des risques lors d’une analyse d’impact relative à la protection des données personnelles (AIPD, Art. 22 LPD).
- 2) « **Safe data** » : quel est le niveau de sensibilité des données nécessaires à la réalisation du projet ? Il s’agit ici du degré de **sensibilité** des données originales utilisées pour créer un produit de données et non du produit de données lui-même dont la sensibilité est évaluée par le « Safe Project ». Le niveau de sensibilité d’une information doit faire l’objet d’une évaluation et d’une classification à l’image de l’article 5 de la LPD³².
- 3) « **Safe people** » : Existe-t-il un lien de confiance avec le destinataire du produit de données ? Si oui, de quelle nature et avec quel niveau de confiance ? La confiance est ici à interpréter comme la propension du destinataire du produit de données à « tenter d’en extraire des données identifiantes ». Ce lien de confiance peut prendre différentes formes notamment celle du secret professionnel, d’un contrat, d’une autorisation légale ou d’une accréditation. Par exemple, les différentes entités de l’administration fédérale sont soumises au secret de fonction limitant le risque de divulgation de données identifiantes. Dans le cas de collaborations à l’extérieur de

³⁰ <https://www.bfs.admin.ch/bfs/fr/home/dscc/dscc.assetdetail.29325685.html>

³¹ <https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai>

³² https://www.fedlex.admin.ch/eli/cc/2022/491/fr#art_5

l'administration fédérale, un certain niveau de confiance peut être établi par des mesures contractuelles. A l'inverse, tout produit de données de type Open Government Data n'impose aucune restriction sur le destinataire qui n'est donc lié par aucune relation de confiance.

- 4) « **Safe settings** » : est-ce que le cadre technique, organisationnel et juridique du traitement des données offre des garanties de confidentialité suffisantes ? La dimension « Safe people » permet l'établissement d'un schéma de confiance formalisant ainsi le recours à des PETs permettant de compenser les risques établis dans les points 1 à 3 et se concrétisant par un potentiel déficit de confiance entre les parties impliquées dans le processus de création du produit de données.
- 5) « **Safe outputs** » : est-ce que le risque de divulgation de données identifiantes par le produit de données est maîtrisé ? Le recours à des technologies d'amélioration de la confidentialité des outputs permet ici d'adapter la garantie de limite du risque de divulgation de données identifiantes vis-à-vis du niveau de la sensibilité des données, de la confiance envers le destinataire et de la nature du projet.

Ces cinq dimensions peuvent être regroupée en deux catégories, cf. figure 7 :

- Les dimensions correspondant à l'évaluation du risque d'un projet, répondant à la question « what ? », incluant les dimensions 1 à 3 sont comparables aux volets « description du traitement envisagé » et « évaluation des risques » d'une AIPD (Art. 22 LPD). L'évaluation de cette catégorie est avant tout **subjective** car il s'agit de vérifier l'acceptabilité du projet vis-à-vis des normes sociales, culturelles et politiques. Un risque jugé trop élevé dans une de ces dimensions peut être rédhibitoire et justifier l'interdiction de la réalisation du projet.
- Les mesures de gestion du risque, répondant à la question « how ? » comprenant les dimensions « settings » et « output » : dans cette catégorie, couvrant le dernier volet d'une AIPD, le risque d'accès non-autorisé, de limites d'utilisation et de divulgation peuvent être **objectivement** évalués et mitigés par le biais de mesures organisationnelles, légales et/ou techniques. C'est dans cette catégorie que les PETs offrent une **solution technique** permettant de contrebalancer un risque possiblement élevé dans la première catégorie.

Ce type d'**approche basée sur les risques** s'apparente à des règlements et exigences qui existent déjà dans le contexte de l'application de bases légales existantes, comme par exemple les analyses d'impact relatives à la protection des données personnelles exigées par la LPD³³, ou encore les formulaires de demandes d'appariement des données à l'OFS³⁴. Ce chapitre illustre ainsi comment les PETs présentées dans ce rapport peuvent faciliter l'application de ce type de cadre de gouvernance. Elles permettent un contrôle du risque de divulgation de données identifiantes quelle que soit leur nature (personnes physiques ou morales, entreprises, ménages ou groupes de personnes), et quel que soit le contexte de la réutilisation de données. Elles apparaissent donc comme un élément essentiel à l'application d'une science des données non seulement respectueuse de la vie privée mais aussi centrée sur l'humain et digne de confiance.

³³ <https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html>

³⁴ <https://www.bfs.admin.ch/bfs/fr/home/services/appariement-donnees/pour-compte-tiers.htm>

7 Recommandation pour l'administration fédérale

Afin de garantir la disponibilité des données, il est impératif de maintenir les efforts de catalogage et, surtout, d'harmonisation des données. Ces initiatives permettent non seulement de standardiser les informations collectées, mais également d'assurer une meilleure interopérabilité entre les différents systèmes et bases de données, facilitant ainsi leur accès, leur réutilisation par les divers services et départements ainsi que l'application de techniques de contrôle de la confidentialité.

Il est également crucial de disposer à l'interne de l'administration fédérale de compétences en science des données ainsi qu'en technologies d'amélioration de la confidentialité. Les professionnels qualifiés dans ce domaine sont essentiels pour analyser et interpréter les vastes quantités de données collectées, tandis que les experts en technologies de confidentialité garantissent que les données sensibles sont protégées contre les accès non autorisés et les violations de la confidentialité. En parallèle, une infrastructure informatique adéquate doit être mise en place pour permettre le prototypage et le déploiement de ces technologies. Cela inclut des serveurs performants, des puces de calcul permettant le déploiement d'environnements d'exécution fiables ainsi que les outils logiciels nécessaires au test et à l'implémentation de services permettant l'application de la science des données respectueuse de la vie privée.

Les services de science des données confidentiels tels que décrits dans les deux cas pratiques de ce rapport répondent directement à un des défis auquel fait face aujourd'hui l'administration fédérale : face à la demande croissante de ces services, qui sont appelés à être fournis à large échelle, notamment dans le cadre du projet Digisanté, le potentiel d'utilisation des technologies d'amélioration de la confidentialité permet de simplifier et d'accélérer leur mise à disposition ainsi que de limiter les ressources nécessaires pour les fournir, tout en garantissant les plus hauts standards en termes de protection de la vie privée. La pertinence de ces services dépasse le seul cadre du DFI et concerne l'ensemble de l'administration fédérale, ce qui justifierait qu'ils soient mis à disposition de l'ensemble de l'administration.

En complément, l'adoption d'un cadre de gouvernance pour la réutilisation des données, tel que le modèle des « Five Safes », est nécessaire pour encadrer la réutilisation des données détenues par l'administration fédérale. Ce cadre a pour vocation de fournir une approche structurée basée sur l'évaluation des risques de violation des droits fondamentaux, en particulier le respect de la sphère privée par la confidentialité des données, ainsi que de décrire les mesures organisationnelles, juridiques et techniques mises en place pour les limiter. Il est ainsi essentiel de formuler une base légale régissant la réutilisation des données encadrée par ce cadre de gouvernance. Une législation claire et précise permettra de définir les responsabilités et les obligations des différentes parties prenantes, tout en fournissant un cadre juridique solide pour l'accomplissement des tâches de l'administration fédérale.

Enfin, une communication transparente sur les mesures techniques et organisationnelles mises en place lors de l'utilisation des données détenues par l'administration fédérale dans des projets de science des données est indispensable pour assurer la confiance et la coopération de la société suisse dans son ensemble. Cette transparence doit détailler l'ensemble des mesures permettant d'implémenter au mieux le principe de "Privacy by design" afin de démontrer l'engagement de l'administration envers le respect de la sphère privée.