Analyse d'impact de la réglementation (AIR) : Révision de l'OSCPT

Michael Altorfer
Dr. Samuel Rutz
Dr. Michael Funk
Noé Arnold
Lukas Grether

Rapport commandé par FONGIT
26.05.2026
ISSN 2235-1868

Meta information

Titre :	Analyse d'impact de la réglementation (AIR) : Révision de l'OSCPT
Version :	V1
Date :	26.05.2026
Auteurs :	Michael Altorfer, Noé Arnold, Michael Funk, Lukas Grether, Samuel Rutz
Contact :	Samuel Rutz, +41 79 204 78 83, samuel.rutz@swiss-economics.ch

Ottikerstrasse 7, 8006 Zürich
www.swiss-economics.ch

Résumé

La Suisse s'est imposée comme un site de premier plan pour les modèles d'affaires fondés sur la confiance numérique. Cela tient à sa neutralité et à sa stabilité politiques, à son approche réglementaire pragmatique et à son accès à des talents qualifiés. Même en l'absence d'une stratégie numérique globale, le cadre existant a fourni une sécurité juridique et une prévisibilité suffisantes pour favoriser l'innovation dans des domaines tels que la cybersécurité, les communications sécurisées et les services cloud.

Le présent rapport examine les implications économiques de la révision proposée de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT). S'appuyant sur des entretiens avec des parties prenantes, des estimations de coûts au niveau des entreprises et des projections quantitatives, il constate que la révision proposée constitue un écart substantiel par rapport aux principes réglementaires établis, avec des effets touchant l'ensemble de l'économie et particulièrement prononcés dans le secteur de la confiance numérique. Bien que formellement présentée comme proportionnée, la révision proposée soumettrait la plupart des fournisseurs de services de communication dérivés à des obligations plus strictes, générant des coûts substantiels et transformant la « swissness » d'un atout en un passif.

La mise en œuvre intégrale de la révision proposée pourrait entraîner des pertes de bien-être économique allant jusqu'à 36 milliards de CHF et des pertes d'emplois allant jusqu'à 219 300 postes dans le secteur de la confiance numérique d'ici 2035. Plus fondamentalement, la révision risque d'éroder la cohérence réglementaire et la réputation de la Suisse en tant que juridiction de confiance – représentant un potentiel point de basculement pour son rôle de plaque tournante internationale de l'innovation en matière de confiance numérique, avec des effets d'entraînement affectant l'ensemble de l'économie suisse.

Résultats principaux

Vue d'ensemble de la situation actuelle

La politique numérique suisse est actuellement caractérisée par une ambiguïté fondamentale qui menace sa position de place économique de confiance.

Alors que la stratégie « Suisse numérique » vise à promouvoir la souveraineté des données et la confiance des citoyens, la révision proposée de l'OSCPT introduit une incertitude réglementaire et engendre finalement une incohérence stratégique.

Une très grande majorité des réponses à la consultation publique s'opposent au projet de révision de l'OSCPT, reflétant une résistance à travers tout le spectre politique et économique.

L'opposition s'étend à l'ensemble du spectre politique et économique, des groupes de la société civile dénonçant une surveillance de masse inconstitutionnelle aux fonds de capital-risque redoutant des effets néfastes pour l'écosystème des start-ups.

La révision de l'OSCPT étendrait sensiblement la portée et le caractère intrusif des obligations de surveillance en Suisse.

La nouvelle structure vise la proportionnalité, mais en pratique, la plupart des FSCD seraient soumis à des obligations de surveillance considérablement renforcées (p. ex. conservation des métadonnées et suppression du chiffrement).

La révision proposée place les entreprises suisses dans une position structurellement désavantageuse par rapport à leurs homologues de l'UE et des États-Unis.

Les comparaisons internationales montrent que tant l'UE que les États-Unis ont soit abandonné, soit jamais introduit d'obligations indiscriminées de conservation des données. En imposant la conservation des métadonnées et la divulgation automatique, la Suisse mettrait en place un régime nettement plus intrusif que ceux des juridictions comparables.

Impacts sur les entreprises concernées

Plusieurs milliers d'entreprises pourraient être touchées, avec des coûts de mise en conformité projetés par entreprise atteignant des millions.

À ce stade, les estimations directes des coûts sont intrinsèquement incertaines et dépendent fortement des détails de mise en œuvre et du modèle d'affaires des entreprises concernées. À long terme, les coûts indirects (p. ex. l'incertitude réglementaire ou les coûts d'opportunité) pourraient dépasser les coûts directs.

Le préjudice est déjà en cours – la « swissness » se transforme aujourd'hui déjà d'un atout concurrentiel premium en un passif stratégique pour les entreprises axées sur la protection des données.

L'incertitude réglementaire est déjà exploitée par des concurrents internationaux dans des appels d'offres B2B pour remettre en question la fiabilité des prestataires suisses. Cette érosion de la réputation est économiquement significative, étant donné que la confiance est l'une des principales raisons pour lesquelles les clients choisissent les services suisses.

Analyse macroéconomique

Le secteur de la confiance numérique est un important moteur de croissance pour la Suisse, mais son élan est très sensible aux chocs réglementaires.

La demande mondiale de services de confiance numérique étant en hausse, le marché suisse de la confiance numérique est bien positionné pour une croissance substantielle au cours de la prochaine décennie. Cependant, un « choc de réputation » résultant de la révision de l'OSCPT pourrait enfermer la Suisse dans un sentier de développement défavorable, entravant la formation de clusters technologiques.

Les effets négatifs d'entraînement pourraient s'étendre bien au-delà du secteur technologique, menaçant la réputation globale de fiabilité de la Suisse.

La confiance est loin d'être un facteur négligeable ; elle affecte la productivité totale des facteurs (PTF), l'accumulation du capital, les incitations à l'innovation et les décisions de localisation des entreprises à mobilité internationale. Si la « prime de confiance suisse » se dissipe, même les services non directement concernés dans d'autres secteurs pourraient voir leur compétitivité internationale diminuer.

Les projections quantitatives suggèrent qu'une mise en œuvre intégrale de la révision pourrait entraîner une perte de bien-être économique (« welfare ») dans le secteur de la confiance numérique allant jusqu'à 36 milliards de CHF en 2035.

La divergence entre le statu quo et la révision proposée révèle un écart saisissant dans la création de valeur économique, représentant 3 à 4 pour cent du PIB suisse. Alors que l'estimation de la borne inférieure indique une perte de bien-être économique de 3 milliards de CHF, la borne supérieure suggère que l'impact de la croissance sacrifiée pourrait être bien plus grave pour l'économie suisse.

Les pertes cumulées de recettes fiscales du secteur de la confiance numérique devraient atteindre jusqu'à 22 milliards de CHF pour la prochaine décennie.

Les pertes cumulées estimées de recettes fiscales de 3 à 22 milliards de CHF sur la période 2025-2035 par rapport au statu quo sont dues aux recettes sacrifiées de taxe sur la valeur ajoutée (TVA), d'impôts sur les bénéfices et d'impôts sur le revenu.

La révision de l'OSCPT risque de provoquer un exode massif de cerveaux, avec des pertes d'emplois estimées allant jusqu'à 219 300 postes au cours de la prochaine décennie.

Si la mise en conformité peut créer quelques emplois spécialisés, l'effet net des entreprises qui réduisent leurs activités ou quittent le marché est clairement négatif. D'ici 2035, la création d'emplois sacrifiée pourrait sévèrement impacter le marché du travail suisse, avec des pertes estimées allant de 22 400 à 219 300 postes.

Table des matières

Résumé 3
Résultats principaux 4
Table des matières 7
1 Introduction 11
1.1 Contexte 11
1.2 Mandat 12
1.3 Méthode et structure 12
2 Vue d'ensemble de la situation actuelle 13
2.1 La réglementation numérique suisse à la croisée des chemins 13
2.2 Résumé de la révision proposée de l'OSCPT 15
2.3 Options réglementaires 17
2.3.1 Brève description des deux options réglementaires 17
2.3.2 Résumé des différences réglementaires 18
2.4 Réactions des parties prenantes à la révision proposée de l'OSCPT 19
2.5 La législation dans l'UE et aux États-Unis 24
2.5.1 Situation juridique dans l'UE et comparaison avec la Suisse 25
2.5.2 Situation juridique aux États-Unis et comparaison avec la Suisse 26
2.6 Résumé 27
3 Impacts sur les entreprises concernées 30
3.1 Impact sur les FST 30
3.2 Impact sur les FSCD 31
3.2.1 Entreprises concernées 32
3.2.2 Nombre d'entreprises concernées 33
3.2.3 Coûts de mise en œuvre 35
3.2.4 Conséquences 37
3.3 Résumé de l'impact sur les entreprises concernées 40
4 Analyse macroéconomique 43
4.1 Importance du secteur de la confiance numérique 43
4.2 Conséquences de la révision proposée de l'OSCPT 49
4.3 Perspectives 52
4.3.1 Hypothèses sous-jacentes des options réglementaires 52
4.3.2 Quantification 54
4.4 Résumé 59

A Catégories et obligations des FST et des FSCD 60
A.1 Maintien du statu quo 60
A.2 Introduction intégrale de la révision de l'OSCPT 62
B Quantification du marché suisse de la confiance numérique 67
B.1 Revenus 67
B.2 Bien-être économique 71
B.3 Emploi 71
B.4 Impôts 72
B.5 Sources de données 73

Tableaux

Tableau 1 : Description de la catégorisation 16
Tableau 2 : Résumé des obligations pour les FSCD....29
Tableau 3 : Catégories de FST et leurs obligations respectives....61
Tableau 4 : Catégories de FSCD et leurs obligations respectives 62
Tableau 5 : Catégories de FST et leurs obligations respectives....64
Tableau 6 : Catégories de FSCD et leurs obligations respectives 66

Figures

Figure 1 : Aperçu des personnes obligées de collaborer visées par la révision proposée 15
Figure 2 : Mesures de surveillance de la correspondance par poste et télécommunication par type, 2020-2024 24
Figure 3 : Heatmap des canaux d'impact sectoriels....51
Figure 4 : Différences de revenus 54
Figure 5 : Différences de bien-être économique cumulées (2025-2035)....55
Figure 6 : Différences d'emploi 57
Figure 7 : Différences cumulées de recettes fiscales (2025-2035)....58
Figure 8 : Taille du marché suisse de la confiance numérique en 2025....68
Figure 9 : Estimations des taux de croissance....70

Abréviations

ACN	Alliance pour la Confiance Numérique
AIR	Analyse d'impact de la réglementation
B2B	Business to Business
CA	Conférence des achats de la Confédération CA
CPP	Code de procédure pénale
CJUE	Cour de justice de l'Union européenne
DACH	Allemagne (D), Autriche (A) et la Suisse (CH)
DBMR	Data Bridge Market Research
DFJP	Département fédéral de justice et police

DSG	Data Protection Act
E-ID	Identité électronique (e-ID)
ETP	Équivalent Temps Plein
FST	Fournisseur de services de télécommunication
FSCD	Fournisseur de services de communication dérivés
IA	Intelligence Artificielle
IP	Internet protocol
IPO	Initial public offering
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
MCN	Marché de la confiance numérique
ONG	Organisation Non Gouvernementale
OSCPT	Ordonnance sur la surveillance de la correspondance par poste et télécommunication
OTT	Over-the-Top
PAT	Personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers
PIB	Produit Intérieur Brut
PME	Petite et Moyenne Entreprise
PTF	Productivité totale des facteurs (PTF
R&D	Research and development
SaaS	Software as a Service
SCPT	Service de Surveillance de la correspondance par poste et télécommunication
SECO	Secrétariat d'État à l'économie
TIC	Technologies de l'Information et de la Communication
TVA	Taxe sur la valeur ajoutée
UE	Union Européenne
US	Etats Unis
VoIP	Services de communication sur Internet équivalents aux services de télécommunication
VPN	virtual private network
WEF	World Economic Forum
WMC	Warrant management component

1 Introduction

1.1 Contexte

Le 29 janvier 2025, le Conseil fédéral a ouvert la consultation sur la révision proposée de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT).[1] La procédure de consultation, qui s'est clôturée le 6 mai 2025, a recueilli de nombreuses réactions, en grande partie négatives, de la part d'un large éventail de parties prenantes. Des entreprises spécialisées dans la fiabilité des données et les communications sécurisées, notamment les leaders du secteur Proton, Threema et Nym, ainsi que des associations professionnelles, des partis politiques, des organisations non gouvernementales (ONG) et des organisations de consommateurs ont exprimé de vives préoccupations concernant la révision proposée.[2]

La révision prévue, sous la direction du Département fédéral de justice et police (DFJP), porte principalement sur l'extension des capacités de surveillance des autorités de poursuite pénale. Il convient notamment de souligner qu'elle élargit les obligations de surveillance pour les fournisseurs de services de communication dérivés (FSCD) et introduit de nouvelles catégories de services, telles que les FSCD à obligations restreintes et les FSCD à obligations complètes, qui seraient toutes deux soumises à des exigences plus strictes. Ces exigences plus strictes comprennent des obligations étendues de conservation des données et d'identification, des obligations de documentation et de rapport. Dans certains cas, les fournisseurs devraient également permettre des réponses automatisées aux demandes des autorités de poursuite pénale.[3] Les critiques font valoir que de telles mesures imposeraient des coûts de mise en conformité disproportionnés et créeraient un risque de sécurité significatif. Ils s'inquiètent que les obstacles à l'innovation et à l'entrée sur le marché pourraient compromettre la position de la Suisse en tant que leader mondial dans le domaine des technologies de confiance numérique et de protection des données.

Plus de 200 réponses ont été soumises lors de la procédure de consultation, la majorité demandant soit une révision fondamentale, soit le retrait complet du projet. Le DFJP a évalué les résultats de la consultation et prépare une analyse d'impact de la réglementation (AIR). Après l'achèvement de cette AIR, le DFJP prévoit d'organiser une deuxième consultation.[4]

---

[1] Surveillance des télécommunications et entreprises obligées de collaborer : ouverture d'une consultation [21.01.2026]. Nous faisons toujours référence au projet de janvier 2025 comme à la révision proposée.

[2] Voir Procédure de consultation 2022/21 [20.01.2026].

[3] Voir Procédure de consultation 2022/21 [20.01.2026].

[4] Fernmeldeüberwachung und mitwirkungspflichtige Unternehmen: Bundesrat nimmt Ergebnis des Vernehmlassungsverfahrens zur Kenntnis [02.03.2026].

1.2 Mandat

Dans ce contexte, FONGIT a commandé une AIR indépendante pour la révision de l'OSCPT. L'évaluation porte à la fois sur les effets au niveau des entreprises et sur les effets macroéconomiques de la révision proposée de l'OSCPT.

L'objectif de cette évaluation est de fournir une analyse fondée sur des éléments concrets qui dépasse le cadre des charges administratives et met en lumière les implications plus larges pour le secteur de la confiance numérique et la Suisse dans son ensemble.

L'AIR compare deux scénarios réglementaires :

- Le statu quo; et
- Le projet de consultation du Conseil fédéral de janvier 2025.

Pour chaque scénario, l'AIR évalue les impacts tant microéconomiques que macroéconomiques. Au niveau microéconomique, cela comprend les coûts de mise en conformité, les effets sur la concurrence et les prix, et les implications plus larges pour les investissements, l'innovation, les clusters technologiques et les recettes publiques. Au niveau macroéconomique, l'AIR estime les impacts potentiels sur le produit intérieur brut (PIB), l'emploi, les recettes fiscales et la réputation internationale de la Suisse en tant que nation de confiance numérique.

1.3 Méthode et structure

Le présent rapport présente l'AIR réalisée pour la révision de l'OSCPT et en résume la méthodologie et les principaux résultats. Il est structuré comme suit :

- Le **chapitre 2** fournit un aperçu de la situation actuelle, couvrant la stratégie numérique de la Suisse, la révision proposée de l'OSCPT, les options réglementaires examinées, les réactions des parties prenantes lors de la procédure de consultation, et une comparaison avec les cadres juridiques de l'Union européenne (UE) et des États-Unis (États-Unis).
- Le **chapitre 3** analyse l'impact sur les entreprises concernées. Le chapitre porte principalement sur les FSCD, car les changements réglementaires proposés affectent le plus ces services. Une section séparée examine également les implications pour les fournisseurs de services de télécommunication (FST).
- Le **chapitre 4** procède à l'analyse macroéconomique. Nous explorons d'abord l'importance du secteur de la confiance numérique, puis les conséquences de la révision proposée de l'OSCPT, y compris les éventuels effets d'entraînement intersectoriels. Enfin, nous conduisons une analyse quantitative pour évaluer l'impact sur le marché de la confiance numérique, le bien-être économique, l'emploi et les recettes fiscales.

The results are based on desk Les résultats reposent sur des recherches documentaires, des informations et analyses fournies par FONGIT et, dans la mesure du possible, étayées par des indicateurs quantitatifs. La recherche est complétée par les enseignements d'entretiens d'experts menés avec des représentants des organisations suivantes : Société Numérique, Proton, SIX, Threema, Trust Valley.

2 Vue d'ensemble de la situation actuelle

Le présent chapitre examine la révision proposée de l'Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) dans le contexte plus large du cadre de la politique numérique de la Suisse. Il commence par souligner l'ambiguïté de la stratégie numérique actuelle de la Suisse, puis expose les éléments clés de la révision proposée de l'OSCPT avant d'introduire et de contraster les options réglementaires analysées dans ce rapport. Le chapitre passe ensuite en revue les positions exprimées par les parties prenantes lors de la procédure de consultation. Ces réponses fournissent des premières indications de l'ambiguïté de la politique et des effets indésirables potentiels sur l'écosystème numérique suisse. Ces premières indications sont étayées par les analyses au niveau des entreprises et macroéconomiques qui suivent. Enfin, la proposition suisse est évaluée dans un contexte international au travers d'une comparaison avec les cadres juridiques de l'Union européenne (UE) et des États-Unis, complétant ainsi la base analytique pour les chapitres suivants.

2.1 La réglementation numérique suisse à la croisée des chemins

L'approche de la Suisse en matière de réglementation numérique se trouve actuellement à la croisée des chemins. D'un côté, la Confédération a à plusieurs reprises signalé son ambition de se positionner comme un hub numérique de confiance, fondée sur une protection solide des données, la confiance des citoyens et la promotion de modèles d'affaires innovants respectueux de la protection des données. De l'autre, un développement réglementaire récent – la révision proposée de l'OSCPT, qui étend de manière indiscriminée les obligations de surveillance pour les fournisseurs de services de communication dérivés (FSCD, p. ex. les services de messagerie, les services de courrier électronique ou les prestataires de stockage cloud) – risque de compromettre cette trajectoire en introduisant une incertitude juridique, une incohérence interne et des ambiguïtés dans le cadre réglementaire.

Une conclusion centrale tirée tant des réponses à la consultation que de nos entretiens est que de nombreuses parties prenantes concernées peinent à identifier une stratégie numérique claire et cohérente en Suisse, même si le Conseil fédéral met à jour et adopte annuellement la stratégie « Suisse numérique ».[5] Plutôt que d'être guidée par une vision réglementaire globale unique, il semble que la politique numérique suisse ait évolué au travers d'une série d'initiatives individuelles et d'actes juridiques. Cela n'a pas été intrinsèquement problématique jusqu'à présent. En dépit de l'absence d'une stratégie directrice clairement articulée, l'environnement réglementaire global est resté praticable et compatible avec les modèles d'affaires numériques fondés sur la confiance. Les partenaires interrogés ont souligné à plusieurs reprises que, d'un point de vue réglementaire, la Suisse n'a jamais été perçue comme un précurseur mondial. Cependant, c'est un lieu d'implantation attractif pour les entreprises grâce à son cadre réglementaire raisonnable et globalement mesuré, combiné à

[5] Le Conseil fédéral adopte la stratégie Suisse numérique 2026 [20.01.2026].

des facteurs tels que la qualité de l'enseignement supérieur (p. ex. l'EPFL, l'ETH), la neutralité, la stabilité, la réputation et les standards de vie.

De plus, plusieurs autres politiques récentes ont directement ou indirectement promu la Suisse comme lieu d'implantation pour les entreprises dans l'espace numérique. Celles-ci comprennent la promotion d'espaces de données fiables et de l'autodétermination numérique[6], les investissements publics dans des organisations telles que FONGIT ou le Trust Valley, et les programmes fédéraux de financement de l'innovation numérique[7] qui visent à favoriser un écosystème propice à l'innovation pour les start-up technologiques, y compris celles opérant dans le domaine de la confiance numérique.

La loi suisse sur la protection des données (LPD) intègre la minimisation des données en tant que principe fondamental, signalant une retenue dans l'utilisation et la conservation des données personnelles. D'autres initiatives étatiques, telles que l'identité électronique (E-ID) ou la souveraineté numérique – deux des thèmes prioritaires de la stratégie numérique Suisse 2026 – reposent explicitement sur la confiance des citoyens et des initiatives basées en Suisse. Pris ensemble, ces éléments désignent un environnement réglementaire qui, bien que fragmenté, a jusqu'ici été globalement cohérent dans sa logique sous-jacente. Cet environnement protège les droits numériques des utilisateurs et favorise les modèles d'affaires fondés sur la confiance numérique.

En résumé, la réglementation numérique suisse a jusqu'à présent été pragmatique. En dépit de l'absence d'une stratégie numérique globale clairement articulée, l'environnement réglementaire est resté globalement compatible avec les modèles d'affaires fondés sur la confiance et a fourni un niveau de prévisibilité suffisant pour que les entreprises puissent opérer. Cependant, la révision de l'OSCPT risque de perturber cet équilibre. Elle introduit des obligations qui entrent en conflit avec les principes réglementaires établis, sans intégration claire dans le cadre juridique et politique plus large. Cela génère une incertitude significative pour les personnes concernées. En tant que telle, elle ne représente pas simplement un autre ajustement réglementaire, mais un point de basculement – ou selon les mots d'un interviewé « une catastrophe". Bien que cette évaluation ne soit peut-être pas encore pleinement évidente au regard des faits présentés jusqu'ici, le reste du rapport démontre pourquoi la Suisse ne serait plus un lieu d'implantation viable pour les entreprises de confiance numérique si la révision proposée était introduite.

---

[6] Promotion of trustworthy data spaces and digital self-determination [20.01.2026].

[7] Innosuisse funds 33 projects as part of the Swiss Accelerator as a transitional measure for Horizon Europe [20.01.2026]. Il a engagé 60,4 millions de CHF, orientant les capitaux vers l'informatique quantique, l'intelligence artificielle et la cybersécurité.

2.2 Résumé de la révision proposée de l'OSCPT

La révision partielle de l'OSCPT vise à aligner le droit suisse de la surveillance sur les technologies modernes de communication numérique. La révision, qui a fait l'objet d'une consultation début 2025, est principalement motivée par le mandat figurant dans la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et par la nécessité judiciaire résultant du « jugement Threema » du Tribunal fédéral en 2021. Ce dernier se réfère à l'arrêt de principe du Tribunal fédéral suisse (arrêt 2C_544/2020), qui a protégé la confidentialité de l'application de messagerie Threema en statuant qu'elle n'est pas un fournisseur de services de télécommunication (FST) au sens du droit suisse de la surveillance.

L'objectif central de la révision proposée est de définir les catégories de personnes obligées de collaborer (POC) avec plus de précision, afin de garantir que l'imposition d'obligations de surveillance soit claire, juridiquement certaine et – chose cruciale – proportionnée (art. 5 al. 2 de la Constitution fédérale).[8] Pour atteindre la proportionnalité requise, le Conseil fédéral a introduit une recatégorisation complète des POC, structurant les obligations en fonction de l'échelle économique et de la portée des utilisateurs d'un prestataire. La figure 1 présente un aperçu des personnes obligées de collaborer visées par la révision proposée.

Figure 1 : Aperçu des personnes obligées de collaborer visées par la révision proposée

FST fournisseur de services de télécommunication	**FSDC** fournisseur de services de communication dérivés	**PAT** Personnes qui mettent à la disposition de tiers leur accès à un réseau de télécommunication public
Un FST fournit une connexion réseau et assure la transmission technique d'informations telles que la voix, les SMS ou l'accès à Internet. Parmi les exemples, on peut citer les opérateurs de réseau Sunrise, Swisscom ou Salt.	Un FSDC propose des services de communication s'appuyant sur les réseaux de télécommunications existants sans gérer l'infrastructure de transmission sous-jacente. Ces services comprennent la messagerie, le courrier électronique, les VPN ou le stockage dans le cloud. On peut citer par exemple Proton, Threema ou Ricardo.	Un PAT peut être une personne physique ou morale qui permet à des tiers d'accéder à un réseau public de télécommunications, par exemple via des points d'accès Wi-Fi publics. Ces entités ne fournissent pas elles-mêmes de services. On peut citer comme exemples les hôtels, les restaurants ou les CFF.
Effets économiques significatifs attendus du fait de la révision proposée ?		
✓	✓	×

Remarque : la base des entretiens et du matériel de consultation, des effets économiques significatifs sur les PAT semblent peu probables.

Source : Illustration de Swiss Economics

[8] Rapport explicatif relatif à l'ouverture de la procédure de consultation : Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT) [21.01.2026].

Nouvelle catégorisation des personnes obligées de collaborer

La nouvelle réglementation prévoit d'établir des niveaux distincts pour les fournisseurs de services de télécommunication (FST) et les fournisseurs de services de communication dérivés (FSCD) ; voir le tableau 1.

Tableau 1 : Description de la catégorisation

Catégorie POC	Sous-catégories	Seuil pour l'upgrade/obligations complètes	Obligations clés des obligations complètes
FST	deux	▪ Par défaut : « obligations complètes ». ▪ Un déclassement vers « obligations restreintes » requiert un chiffre d'affaires inférieur à CHF 100 millions *et* une participation à moins de 10 cibles de surveillance par année.	Conservation des métadonnées (6 mois), service de piquet 24h/24 et 7j/7, suppression du chiffrement, transmission automatisée des données et capacité de surveillance en temps réel.
FSDC	trois	▪ Par défaut : « obligations minimales ». ▪ Le niveau 2 (« obligations restreintes ») est déclenché par plus de 5 000 usagers. ▪ Le niveau 3 (« obligations complètes ») est déclenché par : un chiffre d'affaires consolidé du groupe de plus de CHF 100 millions *ou* plus de 1 million d'usagers.	(Presque) les mêmes obligations étendues que les FST à « obligations complètes ». Les « obligations restreintes » sont exemptes de la conservation des métadonnées, du service de piquet et de la transmission automatisée des données.

Remarque : Voir l'annexe A.2 pour une description détaillée de la catégorisation proposée et des obligations.

Selon le rapport explicatif[9] relatif à l'ouverture de la procédure de consultation, cette approche graduée vise à éviter le saut réglementaire disproportionné qui obligeait auparavant les FSCD en croissance à assumer immédiatement la charge complète et coûteuse des obligations. Cependant, tous les FSCD comptant plus de 5 000 participants font automatiquement partie du niveau 2 des « obligations restreintes » et doivent en notifier le Service de surveillance de la correspondance par poste et télécommunication (Service SCPT) dans un délai de trois mois. Ensuite, ils disposent de six mois pour se conformer aux obligations de collaboration supplémentaires (« Mitwirkungspflichten ») telles que l'identification des utilisateurs. Il convient de noter que la mise en conformité avec les obligations requiert généralement des adaptations techniques et organisationnelles, dont les coûts sont entièrement à la charge des services (voir chapitre 3). Cependant, les services sont indemnisés pour les coûts engagés lors d'opérations de collaboration spécifiques. [10]

[9] Rapport explicatif relatif à l'ouverture de la procédure de consultation : Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT) [21.01.2026].

[10] Voir Ordonnance sur le financement de la surveillance de la correspondance par poste et télécommunication (OF-SCPT) [05.03.2026] et le projet de révision Procédure de consultation 2022/21 [20.01.2026].

Outils d'enquête standardisés

À la demande des autorités de poursuite pénale, trois types de collecte d'informations et deux types de surveillance seront introduits, formalisant ainsi des procédures qui étaient auparavant traitées comme des demandes ad hoc. L'objectif est de standardiser certaines informations et la surveillance rétroactive pour l'identification des utilisateurs (qui étaient auparavant traitées comme des cas particuliers) et de permettre la surveillance en temps réel de certaines données de contenu.[11] Il convient notamment de souligner que la plupart des demandes – aussi bien dans le cadre des nouveaux outils standardisés que d'autres obligations de collaboration – ne nécessitent pas d'autorisation judiciaire préalable.

2.3 Options réglementaires

La présente section expose les différences réglementaires entre le statu quo et une mise en œuvre intégrale de la révision. Avant de détailler les différences réglementaires spécifiques, nous présentons brièvement les options réglementaires.

2.3.1 Brève description des deux options réglementaires

Maintien du statu quo

Le scénario de référence suppose que le cadre réglementaire actuel reste inchangé, y compris l'OSCPT telle qu'appliquée depuis le « jugement Threema » du Tribunal fédéral. Aucune modification ne serait apportée à la définition, à la classification ou aux obligations des entreprises soumises à l'OSCPT. Tant les FSCD que les FST continueraient à opérer selon les règles existantes, et aucune exigence technique, organisationnelle ou procédurale supplémentaire ne serait imposée.[12]

Introduction intégrale de la révision de l'OSCPT

Le scénario de l'intervention réglementaire suppose l'adoption de l'OSCPT révisée telle que proposée début 2025, sans intégrer les retours de la consultation ni les amendements ultérieurs. L'ordonnance révisée introduit plusieurs modifications importantes à la structure et au contenu de la législation, affectant de multiples catégories d'acteurs.

L'impact le plus substantiel concerne les FSCD, dont le cadre réglementaire devient plus large et plus détaillé. En conséquence, la présente étude se concentre principalement sur l'évaluation des implications de l'ordonnance révisée pour les FSCD. D'autres entités, telles que les FST, sont analysées avec moins de détail. Les PAT ne sont pas examinées par la suite, car la révision proposée n'a que des implications très limitées pour elles.

[11] Voir Procédure de consultation 2022/21 [20.01.2026] pour plus de détails.

[12] Une description détaillée des catégories et des obligations des FST et des FSCD se trouve à l'annexe A.1.

2.3.2 Résumé des différences réglementaires

Différences réglementaires pour les FST

Les obligations fondamentales pour les FST restent en grande partie inchangées. Néanmoins, la révision introduit quelques ajustements spécifiques qui pourraient avoir des conséquences pour certains prestataires. La principale nouveauté est l'extension du seuil de chiffre d'affaires pour le statut d'obligations restreintes. Sous le régime précédent, le seuil de CHF 100 millions ne s'appliquait qu'aux revenus générés par les services de télécommunication. En vertu de l'ordonnance révisée, le seuil est calculé sur la base du chiffre d'affaires suisse total de l'entreprise, indépendamment du fait qu'il provienne de services de télécommunication ou d'autres activités. Cet ajustement a deux implications :

- Il durcit le seuil, car les chiffres d'affaires à l'échelle de l'entreprise sont par définition égaux ou supérieurs aux seuls revenus de télécommunication ;
- Il réduit le nombre de FST éligibles au statut d'obligations restreintes, notamment pour les entreprises diversifiées dont les services de télécommunication ne représentent qu'une partie des activités totales.

Différences réglementaires pour les FSCD

La révision proposée introduit plusieurs changements qui durcissent matériellement le régime réglementaire pour les FSCD. Bien que ces prestataires aient déjà été soumis à la réglementation en vertu de l'ordonnance précédente et aient pu être désignés comme prestataires à obligations étendues de surveillance ou de renseignement, le cadre révisé élargit considérablement la portée, les seuils et la profondeur de ces obligations. Alors que le concept de base des FSCD reste inchangé, les exigences réglementaires deviennent substantiellement plus contraignantes.

Le durcissement le plus significatif du cadre réglementaire pour les FSCD résulte de l'introduction de seuils plus bas et plus larges pour sortir de la catégorie de base. Étant donné que 5 000 participants constituent un seuil faible sur les marchés numériques, une proportion substantiellement plus grande de FSCD – en fait, presque tous – entrera dans des catégories à obligations plus élevées par rapport au régime actuel. Cela a été confirmé par tous les partenaires interrogés et a également été souligné lors de la procédure de consultation.

Une deuxième source de durcissement découle de l'ensemble étendu et plus détaillé d'obligations applicables aux niveaux réglementaires supérieurs. Les obligations renforcées en matière de soutien à la surveillance ne s'appliquaient auparavant qu'aux FSCD à obligations étendues, une catégorie dans laquelle aucun prestataire n'avait jamais été classé en raison des seuils élevés.[13] L'ordonnance révisée applique en grande partie les mêmes obligations déjà au niveau des obligations restreintes. Pour les FSCD soumis à des obligations com-

[13] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025]. À noter que les FSCD avec obligations étendues constituent une catégorie dans l'actuelle OSCPT (voir Annexe A.1).

plètes, les exigences s'étendent davantage, comme indiqué dans le tableau 6 de l'annexe A.2. En conséquence, les FSCD dans le niveau des obligations complètes sont réglementés d'une manière substantiellement équivalente au régime appliqué aux FST à obligations complètes. Les FSCD dans le niveau des obligations restreintes font face à des exigences globalement comparables à celles imposées aux FST à obligations restreintes.

Les obligations dans l'OSCPT révisée sont ainsi non seulement plus détaillées, mais s'appliquent également à des seuils beaucoup plus bas, aboutissant à un régime réglementaire plus strict et plus complet pour les FSCD. Les obligations qui ne s'appliquaient auparavant qu'à la catégorie des FSCD à obligations étendues ou aux FST s'étendront désormais à un ensemble bien plus large de services.

2.4 Réactions des parties prenantes à la révision proposée de l'OSCPT

La procédure de consultation de l'OSCPT a révélé des positions fortes et opposées parmi les principaux groupes de parties prenantes. Le soutien à la révision proposée provient principalement des autorités cantonales et des autorités de poursuite pénale. L'opposition la plus forte vient du secteur de la confiance numérique. Cependant, la position de l'industrie est soutenue par des organisations de la société civile, plusieurs organisations non gouvernementales (ONG), tous les partis politiques, et d'autres acteurs tels que des fonds de capital-risque et SIX. Dans l'ensemble, la plupart des parties prenantes s'opposent à la révision proposée de l'OSCPT.[14]

Industrie de la confiance numérique (entreprises et associations)

L'opposition la plus virulente vient du **secteur de la confiance numérique** (voir encadré 1). Certaines de ces entreprises sont qualifiées de FSCD et sont donc directement concernées. D'autres entreprises anticipent des répercussions négatives en raison des atteintes à la réputation des entreprises suisses du secteur. Représentées par des leaders industriels tels que **Proton**[15], **Nym**[16], et **Threema**[17], ces entreprises font valoir que la révision proposée – notamment la conservation des métadonnées et la suppression des obligations de chiffrement appliqué – représente une menace existentielle pour leurs modèles d'affaires. Ces modèles d'affaires sont fondamentalement construits sur la minimisation de la collecte de données et la maximisation de la sécurité. Selon ces entreprises, le stockage de données supplémentaires et l'affaiblissement des protections de chiffrement élargirait la surface d'attaque potentielle et réduirait finalement la sécurité des utilisateurs. Proton a déjà mis en place une

[14] Sauf indication contraire, les informations figurant dans cette section proviennent de Procédure de consultation 2022/21 [20.01.2026].

[15] Proton propose des services numériques axés sur la protection de la vie privée, notamment la messagerie sécurisée, le VPN et le stockage cloud.

[16] Nym propose un VPN basé sur une technologie de noise generating mixnet afin de protéger les métadonnées contre le traçage.

[17] Threema propose un service de messagerie sécurisée avec chiffrement de bout en bout.

infrastructure de serveurs à l'étranger et a publiquement signalé que de nouveaux investissements et une expansion pourraient avoir lieu hors de Suisse, car l'environnement réglementaire national proposé est en conflit avec la proposition de valeur fondamentale de l'entreprise.[18]

Les principaux points de critique et préoccupations soulevés par le secteur lors de la consultation sont :

- **Risque de délocalisation** : Le seuil des « obligations complètes » (1 million d'utilisateurs ou CHF 100 millions de chiffre d'affaires) pénalise la croissance réussie axée sur la protection des données. Proton a publiquement indiqué que la mise en œuvre de la révision nécessiterait une relocalisation, la qualifiant de « suicide économique » pour le secteur. Le seuil des « obligations restreintes » (5 000 usagers) couvre pratiquement tous les FSCD, imposant une charge réglementaire aux PME. Le secteur soutient que ce seuil bas étouffe l'innovation, provoque des délocalisations et réduit l'attractivité de la Suisse.
- **Dépassement de portée** : Les définitions des POC imposées sont inappropriées pour leurs services. Par exemple, imposer des obligations d'identification aux réseaux privés virtuels (VPN) compromet fondamentalement leur service essentiel – l'anonymat – tandis que l'inclusion du stockage cloud personnel (« Online-Speicherdienste ») est considérée comme étendant la définition des FSCD au-delà de sa limite légale centrée sur la communication.
- **Déséquilibre des coûts fixes** : Le système de compensation actuel ne couvre que les coûts variables (par opération). Les entreprises, en particulier les PME, doivent assumer des coûts d'investissement fixes substantiels pour construire et maintenir l'infrastructure de mise en conformité requise, ce qui nuit de manière disproportionnée à leur compétitivité.

L'industrie de la confiance numérique, soutenue par de nombreuses entreprises comme la Poste Suisse, SIX, Redalpine, Founderful, Ronzani Schlauri Anwälte et d'autres, avertit que les conséquences s'étendent bien au-delà des coûts de mise en conformité directs pour les entreprises individuelles. Elle soutient que les mesures proposées compromettent l'image de la Suisse en tant que l'une des principales « nations de confiance numérique » mondiales. Ce signal négatif aurait des conséquences de grande portée car il menacerait la compétitivité de la Suisse dans le secteur technologique et sa réputation.

[18] P.ex.., Proton to Expand Infrastructure Beyond Switzerland Over Surveillance Law Fears [20.01.2026], Aus für Anonymität: Schweizer Online-Nutzer sollen sich identifizieren müssen [20.01.2026], Switzerland's New Surveillance Law: A Privacy Crisis for Encrypted Services [20.01.2026].

Encadré 1 : Le secteur de la confiance numérique

Le secteur de la confiance numérique comprend des entreprises dont l'objectif principal est d'établir la confiance, la sécurité, la protection des données, l'intégrité et l'assurance dans les systèmes, interactions et identités numériques. Il peut être structuré en trois domaines interdépendants :[19]

- **Cybersécurité :** Solutions et services protégeant l'environnement informatique interne des organisations et des individus, y compris la détection des violations et la réponse aux incidents, la criminalistique numérique et l'audit, et la simulation des menaces ou des attaques.
- **Sécurité numérique :** Technologies et services qui établissent la confiance dans les interactions avec le monde extérieur, notamment la gestion des identités et des accès, la biométrie, les transactions sécurisées, les systèmes industriels et les réseaux. Cette catégorie couvre également les services d'interaction et de communication sécurisées tels que les messageries, les fournisseurs de courrier électronique, les VPN et les solutions en cloud.
- **Intelligence artificielle (IA) de confiance :** IA conçue et déployée selon des normes juridiques, éthiques et techniques rigoureuses, mettant l'accent sur la transparence, l'explicabilité, la robustesse, la supervision humaine et la protection des données. Cela comprend à la fois les modèles d'IA générative pour la création de contenu et les applications d'IA spécifiques à un domaine telles que la détection des fraudes, la maintenance prédictive et les outils de cybersécurité.

Ensemble, ces domaines permettent des interactions numériques sécurisées et fiables, protègent les données et les informations personnelles, et contribuent à maintenir la confiance dans les systèmes numériques.

Société civile et ONG

Des groupes de la société civile comme la « Société Numérique » et la « Stiftung für Konsumentenschutz » ont soumis des déclarations critiques, faisant valoir que la révision représente une violation fondamentale du droit suisse et des droits de l'homme.

- **Surveillance de masse inconstitutionnelle** : La révision est considérée comme une « attaque contre les droits fondamentaux » (art. 13 de la Constitution fédérale) et comme l'établissement d'une « expansion massive et généralisée de la surveillance » incompatible avec l'équilibre que la LSCPT[20] est censée maintenir. Dans un cas extrême, la révision pourrait signifier que les autorités de poursuite pénale envoient une demande automatisée toutes les cinq secondes aux entreprises ayant des obligations complètes de surveillance, récupérant ainsi tous les accès enregistrés en temps réel et constituant un historique complet.[21]

---

[19] Voir aussi l'Observatory of Digital Trust Sector 2025 [30.01.2026].

[20] La loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

[21] Die Schweiz ist drauf und dran, autoritäre Überwachungsstaaten zu kopieren [21.01.2026].

- **Violation du principe de légalité** : Les critiques soutiennent que le Conseil fédéral outrepasse ses compétences déléguées en utilisant une ordonnance (OSCPT) pour mettre en œuvre des restrictions profondes aux droits fondamentaux, une question qui devrait constitutionnellement être réservée à une loi du Parlement.
- **Conflit avec la protection des données** : La conservation obligatoire étendue des données est jugée incompatible avec les principes de minimisation des données et de limitation des finalités en vertu de la nouvelle LPD, augmentant les risques de sécurité en créant de vastes silos de données attrayants pour les hackers.
- **Incompatibilité avec le droit de l'UE** : La révision est jugée incompatible avec le droit de l'UE car la Cour de justice de l'Union européenne (CJUE) a établi que, en général, la conservation indiscriminée et durable de données est toujours incompatible avec le droit de l'UE.

Autorités cantonales et autorités de poursuite pénale

Les gouvernements cantonaux (notamment Fribourg, le Valais, Nidwald, Lucerne, Schwytz et les Grisons) ont généralement soutenu la révision comme nécessaire et techniquement solide.

- **Lacunes en matière de sécurité publique et service de piquet 24h/24 et 7j/7** : Le canton d'Argovie s'est vivement opposé à l'exclusion des nouvelles demandes d'identification (p. ex. IR_58_IP_INTERSECT[22]) de l'obligation de service de piquet 24h/24 et 7j/7. Il avertit que le fait de ne pas imposer des capacités de réponse immédiate crée des « lacunes de surveillance significatives » dans des cas d'urgence élevée comme les enlèvements ou les menaces terroristes. De plus, le canton s'oppose à l'exclusion des FSCD à obligations minimales et restreintes de l'obligation de service de piquet.
- **Inflexibilité technique et opérationnelle** : Les cantons de Soleure et de Saint-Gall ont souligné que le Warrant Management Component (WMC), c'est-à-dire l'outil administratif utilisé pour la surveillance, ne peut actuellement pas modifier un ordre existant pour inclure un nouveau dispositif (Multi-Device) ou une nouvelle carte SIM (Extra-SIM), obligeant les enquêteurs à déposer un nouvel ordre.
- **Nécessité d'une réforme législative supérieure** : La « Conférence suisse des Ministères publics » (CMP) ainsi que les cantons de Schwytz et des Grisons ont souligné que – bien que les révisions de l'ordonnance soient des ajustements techniques nécessaires – elles sont insuffisantes pour résoudre le défi systémique à long terme de la collecte de preuves numériques. Ils préconisent des réformes fondamentales des lois supérieures, notamment la LSCPT et le Code de procédure pénale (CPP).

[22] IR_58_IP_INTERSECT est un nouveau type d'information. Il pourrait être utilisé pour l'identification des utilisateurs par formation d'intersection. Voir le rapport explicatif relatif à l'ouverture de la procédure de consultation : Révision partielle de deux ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (OSCPT, OME-SCPT) [21.01.2026] pour plus de détails.

En contraste avec ces préoccupations opérationnelles, les cantons de Vaud et de Genève ont particulièrement mis l'accent sur les implications économiques et constitutionnelles de la révision. Les deux cantons ont mis en garde contre le fait que les obligations proposées risquent d'affaiblir l'économie numérique suisse, notamment les prestataires de services de communication axés sur la protection des données et la sécurité. Genève a explicitement fait référence au droit récemment consacré constitutionnellement à l'intégrité numérique et a averti que certaines obligations de surveillance – notamment celles affectant le chiffrement de bout en bout – pourraient éroder la confiance dans les services numériques suisses. Vaud a également souligné que des obligations trop larges ou insuffisamment différenciées pourraient désavantager les prestataires suisses par rapport aux concurrents étrangers et a demandé un alignement plus étroit sur les normes européennes.

Encadré 2 : Utilisation des mesures de surveillance de la correspondance par poste et télécommunication

En 2024, la Suisse a enregistré une augmentation significative des surveillances de la correspondance par poste et télécommunication. Les autorités de poursuite pénale et le Service de renseignement de la Confédération ont ordonné plus du double des mesures de surveillance via le Service SCPT par rapport à l'année précédente (voir figure 2).[23] Le principal moteur de cette évolution a été la forte augmentation des recherches par champ d'antennes, qui ont été multipliées par cinq par rapport à 2023. La recherche par antenne comprend les relevés de toutes les communications, tentatives de communication et accès réseau qui se sont produits à un endroit spécifique et qui ont eu lieu via des cellules de téléphonie mobile spécifiques. La forte augmentation des chiffres de recherche par antenne est principalement due à un changement récent dans la méthodologie de mesure.[24]

D'autres formes de surveillance ont également notablement augmenté : la surveillance en temps réel a augmenté de 46 pour cent pour atteindre 1 818 cas, tandis que les mesures de surveillance rétroactive ont augmenté d'environ un quart pour atteindre 6 149 cas. Le nombre de recherches d'urgence en 2024 a également crû substantiellement, atteignant 1 223 ordres – environ 20 pour cent de plus que l'année précédente –, tandis que le nombre de recherches de personnes a légèrement diminué à 35.

Les mesures de surveillance ont porté sur plusieurs catégories d'infractions clés. Avec 43 pour cent, la plus grande part concernait les infractions financières, dont le volume de surveillance a

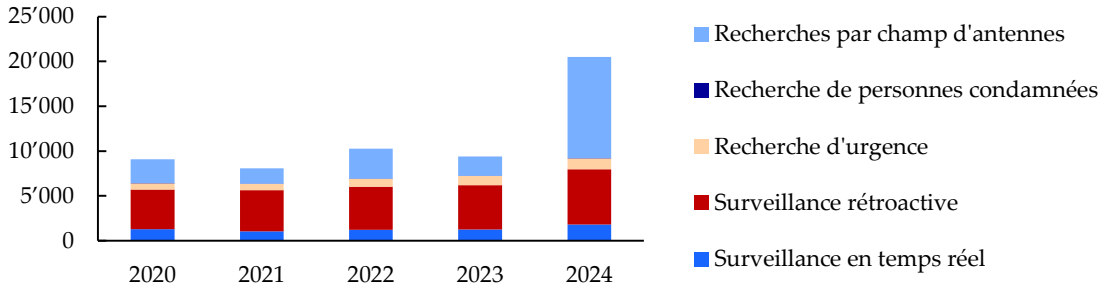
[23] Statistiques | Service Surveillance de la correspondance par poste et télécommunication SCPT [18.11.2025].

[24] Auparavant, le décompte dépendait du nombre de cellules individuelles utilisées lors de la recherche ; désormais, le décompte est simplifié et repose uniquement sur le fournisseur de services et la plage horaire (jusqu'à deux heures), indépendamment du nombre de cellules concernées ; Conférence des achats de la Confédération CA: Statistique de la surveillance des télécommunications : davantage de mesures ordonnées [18.11.2025].

plus que triplé par rapport à 2023. Les mesures liées aux infractions contre la vie et l'intégrité corporelle ont également fortement augmenté, représentant 19 pour cent de tous les ordres et plus que doublé par rapport à l'année précédente. Environ 10 pour cent des mesures concernaient de graves violations de la loi sur les stupéfiants, où une augmentation de plus de 15 pour cent a été enregistrée. D'autres catégories – telles que les recherches d'urgence, les infractions contre la liberté personnelle et les infractions contre l'ordre public – ont également enregistré des augmentations, bien que dans une moindre mesure.

Dans l'ensemble, les chiffres pour 2024 montrent une expansion nette de l'activité de surveillance. Ils indiquent que les instruments respectifs sont utilisés de manière large et avec une intensité croissante par les autorités, en particulier dans les domaines de la criminalité financière, des infractions violentes et de la criminalité liée aux stupéfiants.

Figure 2 : Mesures de surveillance de la correspondance par poste et télécommunication par type, 2020-2024



Source : Illustration Swiss Economics basée sur le Service SCPT[25]

2.5 La législation dans l'UE et aux États-Unis

Compte tenu de l'impact potentiel sur la compétitivité de la Suisse en tant que pôle technologique, il est instructif de comparer le cadre proposé avec ceux de l'UE et des États-Unis – les plus grandes économies et régulateurs du monde. Du point de vue suisse, l'alignement sur ces juridictions est pertinent pour quatre raisons. Premièrement, tant l'UE que les États-Unis définissent les normes réglementaires mondiales dans l'économie numérique. Deuxièmement, pour une petite économie ouverte, la convergence réglementaire minimise les frictions transfrontalières et les coûts de mise en conformité pour les entreprises actives à l'international. Troisièmement, ces régions représentent des alternatives de relocalisation crédibles pour les entreprises technologiques suisses, faisant de leurs cadres juridiques des références de compétitivité et d'innovation. Quatrièmement, les utilisateurs des FSCD suisses ont de faibles coûts de substitution et peuvent facilement remplacer ces services par des prestataires établis dans l'UE ou aux États-Unis.

Les sections suivantes résument et comparent les régimes de surveillance et de conservation des données dans l'UE et aux États-Unis selon quatre dimensions : (i) la portée des presta-

[25] Statistiques | Service Surveillance de la correspondance par poste et télécommunication SCPT [18.11.2025].

taires concernés, (ii) les obligations de conservation des données, (iii) l'accès aux données et les recours juridiques disponibles, et (iv) le traitement du chiffrement de bout en bout. L'analyse montre que le cadre suisse proposé – notamment sa large portée, sa conservation obligatoire et ses exigences d'accès automatisé aux données – ferait de la Suisse un cas à part parmi les démocraties occidentales et placerait son industrie numérique dans une position de désavantage significatif.

2.5.1 Situation juridique dans l'UE et comparaison avec la Suisse

Contexte juridique

Le cadre de conservation des données de l'UE est issu de la directive 2006/24/CE, adoptée pour harmoniser les lois nationales de surveillance pour les fournisseurs de services de télécommunication et d'Internet. Elle exigeait la conservation des métadonnées dans une gamme de services, y compris la téléphonie, les services Internet, le courrier électronique et la téléphonie sur Internet. Cependant, à partir de 2009, la directive a fait l'objet d'importantes contestations constitutionnelles et judiciaires. Dans des arrêts de principe successifs – *Digital Rights Ireland and Others* (2014, C-293/12 et C-594/12), *Tele2 Sverige and Watson and Others* (2016, C-203/15 et C-698/15), et *La Quadrature du Net and Others* (2020, C-511/18, C-512/18 et C-520/18) – la CJUE a statué que la conservation indiscriminée des données viole les droits fondamentaux de l'UE. La Cour a déterminé que de telles obligations générales étaient disproportionnées, sans lien clair entre les données conservées et des menaces de sécurité spécifiques. Elle a établi que, en général, la conservation indiscriminée et durable de données est toujours incompatible avec le droit de l'UE.

En conséquence, la directive de l'UE sur la conservation des données a été invalidée, et les mises en œuvre nationales ont divergé. Certains États membres, notamment l'Allemagne, les Pays-Bas et la Roumanie, ont entièrement abrogé leurs cadres en conformité avec les arrêts. D'autres – la France, l'Italie, l'Espagne et la Pologne – ont maintenu des régimes nationaux limités, bien que ceux-ci restent juridiquement vulnérables et seulement partiellement appliqués. Le résultat est un paysage fragmenté dans lequel la plupart des juridictions de l'UE n'imposent plus d'obligations de conservation systématiques.

Portée et obligations

Même là où la conservation nationale des données existe encore, la portée reste bien plus étroite que ce qui est proposé dans le cadre de la révision suisse de l'OSCPT. Les cadres de l'UE s'appliquent généralement uniquement aux opérateurs de réseau, aux fournisseurs de services Internet et aux prestataires de communication de base (p. ex. la téléphonie ou le courrier électronique). En revanche, la proposition suisse étend les obligations à presque tous les services « Over-the-Top (OTT) » – y compris les plateformes de messagerie, les VPN, les proxies et les fournisseurs de stockage de fichiers. Cela transformerait la Suisse en l'un des rares pays occidentaux imposant des obligations de surveillance à l'ensemble de l'écosystème en ligne.

Accès aux données et garanties juridiques

En vertu de la pratique de l'UE, l'accès aux données conservées est soumis à une autorisation judiciaire dans presque tous les cas impliquant des données de contenu, de trafic ou de localisation. Les prestataires ont qualité pour contester les ordres de divulgation au motif de la proportionnalité, de la nécessité ou de la légalité. Aucune législation de l'UE ne prescrit l'exécution automatisée ou l'accès direct aux systèmes par les autorités. En revanche, la proposition suisse introduirait un mécanisme de divulgation automatisé obligeant certains prestataires à établir des interfaces techniques permettant aux autorités de poursuite pénale d'interroger directement les données des utilisateurs. Une telle obligation est unique parmi les démocraties occidentales et créerait, entre autres, des vulnérabilités systémiques en matière de cybersécurité.

Chiffrement de bout en bout

L'UE n'a pas adopté de mesures portant atteinte au chiffrement de bout en bout. Bien que la Commission européenne ait proposé en 2022 un règlement (« Chat Control 2.0 ») prescrivant la numérisation côté client pour les contenus de type abus sexuels d'enfants, il a rencontré une opposition écrasante de la part des États membres et reste bloqué. Le droit actuel de l'UE, fondé sur la directive e-Privacy, interdit toujours la surveillance générale ou les mandats de déchiffrement. Les autorités suisses, en revanche, n'ont pas explicitement agi contre le chiffrement de bout en bout, mais risquent d'en affaiblir indirectement la protection, car la révision proposée exige que les services soient capables de supprimer le chiffrement qu'ils ont eux-mêmes appliqué.

Comparaison

Par rapport à l'UE, le projet suisse se distingue par sa conservation indiscriminée, l'absence de contrôle judiciaire et l'application automatisée. La plupart des juridictions de l'UE se sont orientées vers une surveillance ciblée et proportionnée soumise au contrôle des tribunaux. Le cadre suisse proposé inverse cette tendance, combinant les éléments les plus intrusifs des États membres de l'UE (p. ex. les obligations françaises de conservation des données[26]) avec des garanties procédurales plus faibles, c'est-à-dire des exigences d'autorisation judiciaire limitées. Son adoption isolerait la Suisse des normes européennes en matière de protection des données et compromettrait sa position de juridiction de confiance pour les données.

2.5.2 Situation juridique aux États-Unis et comparaison avec la Suisse

Contexte juridique

Les États-Unis n'ont jamais mis en place de lois générales sur la conservation des données. Le Patriot Act de 2001 a élargi l'accès aux données existantes, mais sans imposer une conservation préventive. Une tentative ultérieure – le SAFETY Act de 2009 – proposait d'obli-

[26] Telecoms, Media and Internet Laws and Regulations France 2026 [10.03.2026].

ger les prestataires à conserver des données d'identification des utilisateurs pendant deux ans, mais a été rejetée par le Congrès. En conséquence, les prestataires américains ne conservent que les données nécessaires aux opérations commerciales et les produisent sur demande légale. Cette approche de réglementation minimale a notamment favorisé l'essor des États-Unis en tant que leader technologique mondial.

Accès aux données et garanties juridiques

L'accès des autorités de poursuite pénale aux données suit aux États-Unis une hiérarchie claire :

- **Les assignations à comparaître (« subpoenas »)** pour les données hors contenu (p. ex. les coordonnées des abonnés) peuvent être émises mais peuvent être contestées pour excès de portée, pertinence insuffisante ou charge excessive.
- **Les mandats de perquisition (« warrants »)**, requis pour les données de contenu, doivent être émis par un juge sur la base d'une cause probable et peuvent être contestés en vertu du Quatrième amendement.

Le droit américain prévoit ainsi de multiples garanties procédurales et des voies explicites permettant aux prestataires de contester les demandes de données. Contrairement au modèle suisse proposé, il n'existe pas d'obligations d'accès automatisé ou direct aux systèmes. Le cadre juridique met l'accent sur la collecte ciblée et le contrôle judiciaire, maintenant un équilibre entre sécurité et la protection des données.

Chiffrement de bout en bout

Les tentatives d'imposer le déchiffrement ont échoué. Le *Lawful Access to Encrypted Data Act* de 2020 – qui aurait obligé les prestataires à fournir des données non chiffrées sur demande – a été abandonné faute de soutien politique. En conséquence, le chiffrement de bout en bout reste protégé et largement utilisé dans les services numériques américains.

Comparaison

Par rapport aux États-Unis, le cadre proposé par la Suisse implique une surveillance nettement plus indiscriminée. Alors que les États-Unis s'appuient sur un accès post-factum ciblé soumis au contrôle judiciaire, le système suisse imposerait une collecte préventive et indiscriminée de données couplée à des portes dérobées techniques obligatoires (p. ex. la suppression du chiffrement). L'approche américaine offre une protection plus forte pour les prestataires et les utilisateurs, préservant à la fois la protection des données et la compétitivité. La révision suisse, en revanche, éroderait les deux, positionnant le pays parmi les régimes de surveillance les plus intrusifs du monde occidental.

2.6 Résumé

La politique numérique suisse se trouve à la croisée des chemins. D'un côté, le pays s'est positionné comme une place numérique de confiance, mettant l'accent sur une forte protection des données, des conditions-cadres favorables à l'innovation et des initiatives visant la

souveraineté numérique et les espaces de données fiables. De l'autre, la révision proposée de l'OSCPT va dans la direction opposée en étendant considérablement les obligations de surveillance. Plutôt que de renforcer le positionnement de la Suisse en tant que place numérique de confiance, elle risque d'éroder la cohérence réglementaire et de générer une incertitude pour les entreprises dont les modèles d'affaires reposent sur la protection des données et la sécurité. Cette tension se reflète dans la procédure de consultation, qui révèle une large résistance à l'approche proposée. Alors que les autorités cantonales partiellement et les autorités de poursuite pénale généralement soutiennent la révision, une grande majorité des réponses à la consultation s'y oppose. Les critiques les plus vives viennent de l'industrie de la confiance numérique, soutenue par des organisations de la société civile, des partis politiques et des investisseurs. Ces parties prenantes font valoir que les obligations proposées entrent directement en conflit avec les modèles d'affaires fondés sur la minimisation des données, le chiffrement fort et l'anonymat des utilisateurs, créent des coûts de mise en conformité disproportionnés et génèrent de fortes incitations à la délocalisation. Les groupes de la société civile soulignent en outre des préoccupations constitutionnelles, notamment des violations du principe de proportionnalité, du principe de légalité et du droit de la protection des données.

Dans ce contexte, le rapport développe et compare les différences de deux scénarios réglementaires alternatifs : le maintien du statu quo et l'introduction intégrale de la révision de l'OSCPT. Bien que la nouvelle structure soit censée améliorer la proportionnalité, les seuils choisis – notamment le bas seuil d'entrée de 5 000 usagers pour les FSCD à obligations restreintes – signifient qu'en pratique, la plupart des services seraient soumis à des obligations de surveillance. Combinée aux obligations considérablement élargies imposées au niveau des FSCD à obligations restreintes, une introduction intégrale de la révision étendrait sensiblement à la fois la portée et le caractère intrusif de la surveillance en Suisse par rapport au statu quo.

La comparaison internationale renforce encore ces préoccupations. Tant l'UE que les États-Unis se sont éloignés de la conservation indiscriminée des données et des obligations de surveillance larges. Dans l'UE, la conservation généralisée a été jugée en grande partie incompatible avec les droits fondamentaux par la CJUE, et les régimes nationaux restants sont étroits, contestés et faiblement appliqués. En d'autres termes, l'approche envisagée serait incompatible avec la réglementation de l'UE. Les États-Unis n'ont jamais introduit la conservation obligatoire des données et s'appuient sur un accès ciblé ex post soumis au contrôle judiciaire. La proposition suisse introduirait un cadre nettement plus strict que dans les juridictions comparables.

Le tableau 2 illustre cette divergence. Il montre que des obligations clés telles que la conservation des métadonnées, les obligations d'identification, la conservation de la dernière adresse IP et la divulgation automatique s'appliqueraient plus largement dans le cadre suisse proposé que dans la pratique suisse actuelle et dans l'UE ou aux États-Unis. Il convient de noter que les grandes entreprises technologiques internationales opérant en vertu du droit de l'UE ou des États-Unis ne sont pas soumises aux obligations suisses. Le tableau

met ainsi en évidence le risque que la révision place les FSCD établis en Suisse dans un désavantage structurel par rapport aux concurrents étrangers en raison des obligations supplémentaires ne s'appliquant qu'aux entreprises établies en Suisse.

Tableau 2 : Résumé des obligations pour les FSCD

	Statu quo CH	Révision OSCPT « obligations complètes »	Révision OSCPT « obligations restreintes »	UE	États-Unis	Entreprises internationales (Google, Meta)
Obligation de conservation des métadonnées	×	✓	×	×	×	×
Obligation d'identification	×	✓	✓	×	×	×
Obligation de conservation de la dernière adresse IP	×	✓	✓	×	×	×
Divulgation automatique	×	✓	×	×	×	×
Dernière adresse IP sans ordonnance judiciaire	×	✓	✓	×	×	×

Remarque : La divulgation automatique, la conservation des métadonnées et l'obligation d'identification existent dans l'état actuel en Suisse, mais ne sont pas appliquées.

Source : Swiss Economics basé sur Proton

Dans l'ensemble, le chapitre 2 démontre que la révision proposée de l'OSCPT ne se bornerait pas à moderniser le droit suisse de la surveillance, mais durcirait fondamentalement le cadre réglementaire. Ce faisant, elle contrecarrerait les objectifs plus larges de la politique numérique suisse et établirait un régime nettement plus intrusif que ceux de l'UE et des États-Unis. Plusieurs partenaires interrogés ont averti que la révision proposée de l'OSCPT pourrait constituer un point de basculement, affectant négativement la réputation internationale de la Suisse en tant que juridiction numérique de confiance et prévisible, d'autant plus que la réglementation doit être introduite par la petite porte au moyen d'une ordonnance.

3 Impacts sur les entreprises concernées

Le présent chapitre examine l'impact de la révision prévue sur les entreprises qui seraient directement concernées par les mesures proposées. S'appuyant sur le chapitre précédent, il identifie les types d'entreprises pertinents et expose les canaux par lesquels l'OSCPT révisée influencerait leurs opérations et leurs structures de coûts. L'analyse porte sur l'option réglementaire d'une mise en œuvre intégrale de la révision de l'OSCPT.

Le présent chapitre ne couvre pas les effets indirects potentiels, tels que les impacts de second ordre découlant de considérations de réputation ou les implications pour l'attractivité de la Suisse en tant que lieu d'implantation commercial. Ces effets sont traités séparément au chapitre 4. En outre, le présent rapport ne fournit pas d'analyse détaillée des impacts sur les utilisateurs finaux et d'autres parties prenantes. Des exemples illustratifs sont cependant présentés dans l'encadré 3.

3.1 Impact sur les FST

Les fournisseurs de services de télécommunication (FST) constituent un groupe important et hétérogène dans le champ d'application de l'OSCPT. Selon la définition utilisée dans l'ordonnance, il existe actuellement environ 1 000 entités en Suisse qui se qualifient comme FST. Parmi celles-ci, seul un petit sous-ensemble – actuellement six prestataires – est soumis à l'ensemble complet des obligations en vertu du régime existant. La grande majorité des FST peut donc opérer sous une charge réglementaire réduite, souvent parce que leurs services ou leur échelle ne satisfont pas aux seuils déclenchant les exigences complètes de mise en conformité. Des données indiquent cependant que seules 200 des quelque 1 000 entreprises éligibles ont demandé et obtenu un déclassement, indiquant un certain manque de transparence, de compréhension du cadre actuel, ou simplement une non-implication par l'OSCPT jusqu'à présent.[27]

Comme discuté à la section 2.3.2, le principal changement réglementaire introduit par la révision de l'OSCPT pour les FST réside dans l'extension potentielle du groupe soumis aux obligations complètes. Les partenaires interrogés n'ont pas été en mesure de fournir des estimations précises du nombre d'entreprises qui seraient affectées par une telle mise à niveau. Cela reflète la diversité des modèles d'affaires au sein de la catégorie des FST, ainsi que l'incertitude créée par la révision proposée. Cependant, seules les entreprises qui sont reclassées et mises à niveau feraient face à des exigences de mise en conformité matériellement plus élevées.

Pour les prestataires soumis aux obligations complètes, les coûts supplémentaires qui en résultent devraient varier considérablement. Les partenaires interrogés ont souligné que les coûts dépendraient fortement de facteurs propres à l'entreprise, tels que l'infrastructure technique existante, les types de données déjà traitées et stockées, et si des mesures organi-

[27] 800 Schweizer Unternehmen hätten weniger Überwachungspflichten… wenn sie davon wüssten! [28.11.2025].

sationnelles – telles qu'un service de piquet 24h/24 et 7j/7 – sont déjà en place en raison d'autres exigences réglementaires ou de besoins opérationnels. Pour les entreprises qui ne sont pas encore soumises à des obligations comparables, il est plausible de supposer que les coûts supplémentaires seraient similaires à ceux des FSCD qui seraient mis à niveau vers les obligations complètes. Comme le montre la section 3.2.3, des coûts initiaux de CHF 2 à 3 millions et des coûts courants de CHF 1,5 million par année sont attendus pour les FSCD.[28]

Il est important de noter que les partenaires interrogés ne s'attendaient pas à ce que la révision de l'OSCPT crée un désavantage concurrentiel significatif au sein du secteur national des FST. Étant donné que les FST offrent des services comparables, ils seraient tous soumis au même cadre réglementaire et toute augmentation des coûts s'appliquerait de manière symétrique. De plus, contrairement aux FSCD, les FST opèrent principalement sur un marché national fortement réglementé et ne sont pas exposés au même degré de concurrence internationale que les FSCD. En conséquence, il n'est pas attendu que les changements réglementaires perturbent matériellement la dynamique concurrentielle, même s'ils entraînent des coûts de mise en conformité plus élevés pour un sous-ensemble de prestataires. Ces coûts supplémentaires seraient très probablement répercutés sur les clients, de sorte que les services des FST deviendraient plus chers.

En résumé, la révision de l'OSCPT affecterait le secteur des FST principalement par la reclassification et la mise à niveau potentielle de certains prestataires vers les obligations complètes. Bien que cela implique des coûts supplémentaires pour les entreprises concernées, l'ampleur de ces coûts devrait varier considérablement en fonction des structures existantes et de l'exposition réglementaire. Dans le même temps, la révision n'est pas susceptible de modifier significativement la concurrence au sein du marché national des FST, car les exigences réglementaires s'appliqueraient uniformément à tous les prestataires comparables et la pression concurrentielle internationale reste limitée. En conséquence, la présente étude n'approfondit pas davantage les effets sur les FST, les impacts attendus étant limités et les données disponibles ne permettant pas une différenciation significative ou une quantification robuste entre les entreprises. Une analyse de marché plus approfondie et systématique serait nécessaire pour tirer des conclusions définitives sur le nombre de prestataires concernés et l'ampleur des coûts de mise en conformité associés.

3.2 Impact sur les FSCD

Les fournisseurs de services de communication dérivés (FSCD) sont susceptibles d'être les plus touchés par les mesures proposées. La présente section fournit une analyse détaillée en quatre étapes. Premièrement, elle définit les types d'entreprises relevant du champ d'ap-

[28] Ces estimations demeurent incertaines, dans la mesure où les entreprises ne disposent pas encore d'une vision précise de la forme et de la portée des futures exigences. En particulier, les données requises pour se conformer à l'obligation d'identification pourraient considérablement accroître la complexité de mise en œuvre, dès lors que le respect de cette obligation repose sur des normes strictes de sécurité des données devant être mises en place pour protéger celles-ci. Il est par exemple évident qu'une adresse IP nécessiterait une protection moindre que des copies de passeport enregistrées.

plication des FSCD. Deuxièmement, elle estime le nombre d'entreprises directement impactées. Troisièmement, elle présente les coûts directs et indirects associés. Enfin, elle examine les conséquences opérationnelles et stratégiques plus larges pour ces entreprises.

3.2.1 Entreprises concernées

Les FSCD offrent un ensemble hétérogène de services en ligne qui constituent un intermédiaire de la communication entre les utilisateurs sans être des opérateurs de télécommunication traditionnels. Sur la base du rapport explicatif du DFJP, des entretiens et des recherches documentaires, les groupes suivants relèvent clairement du concept de FSCD dans le projet de révision du Conseil fédéral :[29]

- **Services d'accès indirect à Internet (services VPN et proxy)** : Ces services redirigent le trafic Internet indépendamment du service d'accès à Internet de l'utilisateur et modifient généralement l'adresse IP source sous laquelle les utilisateurs apparaissent en ligne. Ils sont couramment utilisés pour le chiffrement, l'anonymisation ou le contournement des restrictions de géoblocage. Les exemples suisses comprennent **ProtonVPN** et **Nym**, qui commercialisent tous deux explicitement la protection des données et la sécurité comme caractéristiques fondamentales.
- **Applications de transmission de données entre utilisateurs (applications et logiciels)** : Cette catégorie comprend les applications et programmes permettant la transmission de texte, de voix, d'images, de vidéos ou d'autres données entre utilisateurs, à condition qu'ils ne soient pas fournis en association avec un accès à Internet. La définition est technologiquement neutre et couvre aussi bien les logiciels mobiles que de bureau. Les exemples suisses incluent **Infomaniak** et **Swissdotnet**, qui permettent tous deux la transmission de données entre utilisateurs via Internet.
- **Services de communication sur Internet équivalents aux services de télécommunication (VoIP)** : Ces services remplacent fonctionnellement les offres de télécommunication traditionnelles, telles que les appels vocaux, mais sont fournis entièrement via Internet et indépendamment des opérateurs de réseau. Des exemples typiques sont la téléphonie et les services de vidéoconférence sur Internet. Des exemples de VoIP suisses sont des services tels que **Chorus Call** ou **Virtual-Call**.
- **Services de courrier électronique pour des tiers** : Les services de courrier électronique comprennent le webmail, l'hébergement de messagerie professionnelle et les solutions de messagerie sécurisée ou chiffrée proposées aux utilisateurs ou aux organisations. Ils représentent l'une des formes les plus établies de services de communication dérivés. Les exemples suisses de prestataires comprennent **Proton Mail** et **Swissmail**, qui offrent tous deux des services de messagerie aux clients privés et professionnels.

[29] Un échantillon des entreprises mentionnées a été contacté afin d'obtenir une évaluation de l'impact de l'OSCPT sur leurs activités. Seules quelques entreprises ont répondu à cette demande.

- **Services de messagerie et de notification sur Internet pour des tiers** : Les services de messagerie permettent une communication en temps réel ou asynchrone entre les utilisateurs via du texte, des images, des messages vocaux ou du contenu multimédia. Cela comprend les applications de messagerie instantanée, les plateformes de chat et les composantes de messagerie intégrées dans des plateformes plus larges. Les exemples suisses comprennent **Threema** et **Session**, ainsi que les fonctionnalités de messagerie au sein de plateformes suisses telles que **Digitec** ou **Ricardo**.
- **Services de stockage en ligne, d'hébergement et de partage de contenu :** Ces services permettent aux utilisateurs de stocker, de partager et de travailler de manière collaborative sur des contenus numériques tels que des documents ou des fichiers. Bien que leur fonction principale soit le stockage de données, la communication s'effectue via le partage de liens, les droits d'accès, les commentaires et l'édition collaborative. Les exemples suisses comprennent **Exoscale**, **Hostpoint**, **nine** et **Tresorit**, qui offrent tous des fonctionnalités d'hébergement ou de stockage en cloud. L'élément communicatif découle de la possibilité d'interaction entre plusieurs utilisateurs autour d'un contenu partagé. À ce titre, ces services sont considérés comme des FSCD même si la communication n'est pas leur fonction principale annoncée.

Cette liste représente des exemples illustratifs basés sur le rapport explicatif et les entretiens menés pour cette étude. La définition des FSCD est large et technologiquement neutre, ce qui signifie que des **types de services supplémentaires et/ou des modèles d'affaires hybrides** peuvent également entrer dans son champ d'application. À ce stade, les partenaires interrogés n'ont pas identifié d'autres exemples concrets au-delà des catégories exposées ci-dessus ; ils ont cependant souligné l'incertitude juridique persistante pour les entreprises potentiellement concernées.

3.2.2 Nombre d'entreprises concernées

Il n'existe pas de chiffres fiables sur le nombre d'entreprises qui relèveraient de la catégorie des FSCD. Les réponses à la consultation, les recherches documentaires et les entretiens d'experts menés en préparation de cette étude n'ont pas permis d'établir une fourchette fiable ou un décompte total de ces entreprises. Néanmoins, les données disponibles indiquent qu'un nombre substantiel d'entreprises opérant en Suisse pourraient potentiellement entrer dans le champ d'application. Plusieurs données illustrent l'ampleur des prestataires de services potentiellement concernés :

- CompanyData.com répertorie 456 entreprises de communication en Suisse, couvrant un large éventail d'offres de services numériques et de télécommunication.[30] Bien que toutes ces entreprises ne se qualifient pas nécessairement comme FSCD, leur offre de communication peut les faire entrer dans la définition des FSCD.

[30] List of Communication Companies in Switzerland [20.01.2026].

- Une étude sur les plateformes de rencontres en ligne dans l'espace DACH trouve environ 400 plateformes de rencontres desservant le marché suisse.[31] Il n'est pas clair combien de ces entreprises sont légalement établies en Suisse et seraient donc directement concernées par la révision de l'OSCPT. Les exemples suisses comprennent DuoLivo et swissfriends. Les plateformes de rencontres s'appuient généralement sur des fonctionnalités de messagerie et de notification entre utilisateurs, ce qui peut les faire entrer dans la définition des FSCD.
- L'enquête annuelle de la FHNW auprès des détaillants en ligne couvre 581 détaillants en ligne suisses. [32] Certaines de ces plateformes fournissent des services de messagerie ou de notification intégrés permettant la communication entre utilisateurs, comme Ricardo ou tutti.ch. Cependant, il n'existe pas de données systématiques sur le nombre de détaillants enquêtés offrant de telles fonctionnalités d'une manière qui les qualifierait comme FSCD.
- PoiData.io répertorie 1 090 entreprises d'hébergement web en Suisse en décembre 2025.[33] Sur la base du rapport explicatif, il semble probable que beaucoup de ces entreprises se qualifient comme FSCD.
- Swiss made software, un label pour les entreprises logicielles suisses, compte plus de 1100 membres. [34] Il n'est pas clair combien de ces membres se qualifient comme FSCD, mais des exemples potentiellement concernés comprennent Threema, Infomaniak et Cloudpartner.
- Selon Tracxn, le secteur suisse des logiciels en tant que service (SaaS) comprend 2 280 entreprises. Certaines de ces entreprises, p. ex. Proton, se qualifient clairement comme FSCD, mais il n'existe pas de données systématiques sur le nombre total de FSCD dans le secteur SaaS. [35]

Ces chiffres suggèrent que le nombre d'entreprises potentiellement concernées est susceptible d'être significatif, même si seul un sous-ensemble d'entreprises dans chaque catégorie se qualifie finalement comme FSCD en vertu du cadre juridique révisé. L'absence d'un décompte précis reflète l'absence de classifications statistiques robustes alignées sur les fournisseurs de services de communication dérivés. Cette incertitude a été soulevée à plusieurs reprises par les partenaires interrogés et lors des consultations, et illustre la nécessité d'une plus grande clarté sur le nombre d'entreprises concernées pour évaluer les effets économiques de manière plus précise.

---

[31] Der Online-Dating-Markt in der Schweiz 2018/2019 [20.01.2026].

[32] Zumstein, Dörner & Schüler (2025). Onlinehändlerbefragung 2025. Onlinehändlerbefragung 2025 [11.03.2026].

[33] List of Web hosting companies in Switzerland? [20.01.2026].

[34] swiss made software – uniting quality and digital sovereignty [20.01.2026].

[35] SaaS Sector in Switzerland [20.01.2026].

3.2.3 Coûts de mise en œuvre

Les directives du SECO pour les analyses d'impact de la réglementation[36] ainsi que les directives d'estimation des coûts réglementaires pour les entreprises[37] indiquent toutes deux explicitement que les coûts directs et indirects doivent être pris en compte dans l'analyse des impacts sur les entreprises.

Coûts directs

Les partenaires interrogés ont souligné que toute estimation des coûts est intrinsèquement incertaine à ce stade en raison de l'affinement réglementaire en cours et des détails de mise en œuvre pas encore finalisés. Ils dépendent également fortement du modèle d'affaires de chaque FSCD, de son échelle, de sa pile technologique et de sa maturité en matière de conformité existante. La révision proposée pourrait nécessiter une refonte complète de l'architecture de sécurité pour certaines entreprises, tandis que pour d'autres, les coûts supplémentaires pourraient être négligeables, leurs systèmes et processus existants satisfaisant déjà largement aux exigences anticipées. D'une manière générale, plus le modèle d'affaires d'une entreprise est axé sur la protection des données, plus les coûts sont élevés.

Néanmoins, les partenaires interrogés ont fourni des ordres de grandeur des coûts qui illustrent l'ampleur de l'impact monétaire direct attendu :

- **FSCD à obligations restreintes** : Les personnes interrogées estiment les coûts annuels de mise en conformité dans la région de CHF 1 million par entreprise, tirés par le besoin de spécialistes en informatique supplémentaires, d'une capacité de serveurs étendue et du développement de systèmes pour soutenir les nouvelles obligations de disponibilité de l'information et de rapport. Si un prestataire doit externaliser l'infrastructure de conservation ou utiliser des services hyperscaler pour répondre aux demandes de conservation des données, ces coûts pourraient s'élever à plusieurs millions de francs, selon les volumes d'utilisateurs et la nature et la durée exactes des obligations de conservation.
- **FSCD à obligations complètes** : Pour les prestataires plus importants soumis à des obligations complètes de surveillance, les coûts de développement estimés sont d'environ CHF 2 à 3 millions, avec des dépenses annuelles courantes d'environ CHF 1,5 million pour couvrir le personnel (ingénieurs en sécurité, personnel de conformité), le stockage de données et le soutien opérationnel pour la disponibilité 24h/24 et 7j/7 et les interfaces automatisées.

Un facteur déterminant des coûts directs est le besoin de personnel qualifié. La mise en œuvre nécessite une analyse détaillée des structures de données internes, l'identification et la mise en correspondance des champs de données juridiquement pertinents avec les formats de sortie requis, et le développement de mécanismes d'interrogation automatisés ou semi-automatisés. En outre, les organisations doivent définir des processus internes de va-

[36] Manuel sur l'analyse d'impact de la réglementation (AIR) [20.01.2026].

[37] Guide pour l'estimation des coûts [20.01.2026]. Ce guide se fonde sur la loi sur l'allégement des coûts de la réglementation pour les entreprises.

lidation et d'approbation, construire une documentation étendue et effectuer des tests rigoureux. Cette phase nécessite une expertise technique spécialisée, soutenue par des ressources juridiques et de conformité – une combinaison qui augmente considérablement la charge de personnel. L'opérationnalisation de ces systèmes peut également nécessiter une formation continue, la rétention de spécialistes et des frais généraux supplémentaires pour les processus de sécurité et d'audit.

Parmi les FSCD, les prestataires de services de stockage en cloud font face à un risque réglementaire particulièrement élevé en vertu de la révision proposée. Bien que la portée précise des obligations potentielles de conservation des métadonnées reste non définie, les évaluations de l'industrie suggèrent que les prestataires pourraient être tenus de mettre en œuvre des capacités de conservation étendues. Un prestataire estime que les coûts supplémentaires pourraient atteindre 10 pour cent des revenus pour les petits prestataires, contre environ 1 pour cent pour les grands prestataires nationaux de stockage cloud.

Le marché du stockage cloud est caractérisé par des marges faibles et une concurrence intense des hyperscalers mondiaux tels qu'AWS et Azure. Les prestataires suisses opèrent généralement avec des marges faibles et ont une portée limitée pour répercuter des coûts de mise en conformité supplémentaires significatifs sans éroder leur position concurrentielle. Si les exigences de conservation s'avèrent étendues, les dépenses d'investissement, de stockage et d'exploitation associées dépasseraient probablement de manière soutenue les marges d'exploitation. Dans ce cas, le modèle d'affaires de l'offre de services de stockage en cloud depuis la Suisse ne serait plus économiquement viable. La sortie du marché ou la délocalisation des activités vers des juridictions à moindres charges réglementaires représenteraient alors des réponses rationnelles et potentiellement inévitables.

Coûts immatériels et indirects

Outre les coûts directs quantifiables, les entreprises concernées peuvent également encourir des coûts moins facilement quantifiables mais potentiellement significatifs :

- **Perturbation stratégique** : Les feuilles de route, les cycles de développement de produits et les efforts d'innovation peuvent être mis en pause, retardés ou réorientés, car les ressources techniques et de conformité sont détournées vers des constructions liées à la surveillance.
- **Incertitude réglementaire** : Le simple processus d'adaptation à un régime réglementaire en évolution crée des coûts – par exemple, dans la planification de scénarios, l'évaluation juridique et les négociations avec les clients ou les investisseurs – car les entreprises se prémunissent contre des obligations futures ambiguës qui pourraient être préjudiciables à leur modèle d'affaires.
- **Coûts d'opportunité** : Le temps et le capital alloués à la mise en conformité, à la planification de scénarios et à d'autres tâches supplémentaires dues à la révision proposée ne peuvent pas être déployés ailleurs, ce qui ralentit potentiellement la croissance du marché ou les améliorations des produits.

Ces impacts indirects apparaissent rarement comme des postes budgétaires explicites, mais ont des effets tangibles sur la capacité organisationnelle, la flexibilité stratégique et le positionnement concurrentiel. À long terme, l'importance de ces coûts indirects peut dépasser celle des coûts directs. Les coûts exposés ci-dessus ne représentent donc qu'une partie de la charge économique globale ; les conséquences plus larges sont examinées dans la section suivante.

3.2.4 Conséquences

L'élargissement proposé des obligations de surveillance pour les FSCD est susceptible de générer des impacts concurrentiels, stratégiques et de marché significatifs, notamment pour les entreprises dont les propositions de valeur sont liées à la confiance, à la protection des données, à la sécurité et à la « swissness ».

Désavantage concurrentiel et effets de réputation

Une préoccupation centrale des FSCD suisses est que les obligations révisées mineraient leur position concurrentielle par rapport aux concurrents étrangers. Contrairement aux FST traditionnels, les FSCD opèrent généralement sur des marchés mondiaux. Les FSCD suisses sont donc en concurrence directe avec des services dont le siège est dans des juridictions où aucune obligation de surveillance comparable ne s'applique, notamment aux États-Unis et dans l'UE. Des exemples prominents comprennent les services de messagerie tels que WhatsApp et Signal, ou les fournisseurs de messagerie électronique tels que Microsoft Outlook et Gmail.

Lorsque les concurrents étrangers font face à des exigences équivalentes moindres ou nulles, les FSCD suisses supporteraient des coûts de mise en conformité plus élevés et des contraintes opérationnelles. Ceux-ci peuvent se traduire par des prix plus élevés, des cycles d'innovation plus lents, une fonctionnalité de produit réduite ou la nécessité de reconcevoir des fonctionnalités essentielles. Plus fondamentalement, les dépenses supplémentaires de mise en conformité, de conservation et d'exploitation peuvent éroder des marges déjà faibles dans des segments concurrentiels internationaux. Dans les marchés caractérisés par une haute transparence des prix et une portée limitée de répercussion des coûts (p. ex. le stockage cloud), des augmentations de coûts soutenues peuvent rendre la prestation basée en Suisse économiquement non viable. Dans de tels cas, la sortie du marché ou la délocalisation vers des juridictions à moindres charges réglementaires devient une réponse économique rationnelle.

Au-delà des pressions purement sur les coûts, la révision constitue une menace directe pour la proposition de valeur unique des prestataires. Ces effets sont particulièrement prononcés pour les entreprises axées sur la protection des données dont les modèles d'affaires sont explicitement construits sur la minimisation des données et de fortes garanties de confidentialité. Pour ces prestataires, les obligations d'identification et de conservation des données

introduites par la révision de l'OSCPT sont structurellement incompatibles avec leur proposition de valeur fondamentale.

Le désavantage concurrentiel est déjà évident aujourd'hui. Selon les partenaires interrogés, l'incertitude réglementaire entourant la révision est de plus en plus exploitée par des concurrents internationaux dans des processus d'appels d'offres, notamment sur les marchés B2B, pour remettre en question l'adéquation des prestataires suisses. Combinée à la visibilité internationale de la révision, [38] cette dynamique contribue à une détérioration de la confiance perçue dans les services suisses axés sur la protection des données, et ce avant même que les règles n'entrent en vigueur. Ce canal réputationnel est économiquement pertinent : selon une enquête clients menée par un partenaire interrogé, la réputation est la deuxième raison la plus importante pour laquelle les clients choisissent son service plutôt que ceux des concurrents.

Plusieurs partenaires interrogés ont en outre souligné que la « swissness », actuellement un atout concurrentiel, risque de se transformer en désavantage – notamment pour les entreprises axées sur la protection des données – dans le cadre révisé. Cette préoccupation n'est pas purement théorique. Proton, la plus grande entreprise suisse de technologie de protection des données, a déjà commencé à délocaliser des parties de son infrastructure en Allemagne et en Norvège, citant explicitement l'incertitude juridique et les préoccupations selon lesquelles les obligations de surveillance révisées seraient en conflit avec ses engagements en matière de protection des données. Proton a également déclaré publiquement que l'adoption de la révision de l'OSCPT dans sa forme proposée nécessiterait de nouvelles délocalisations. [39] Les partenaires interrogés s'attendent à ce que d'autres prestataires axés sur la protection des données emboîtent le pas, car leur proposition de valeur unique ne serait plus compatible avec la réglementation suisse.

Dans la perspective d'avenir, les concurrents internationaux non soumis à des régimes de surveillance équivalents sont susceptibles de capter des parts de marché des prestataires suisses au fur et à mesure que les utilisateurs accordent la priorité à des garanties de protection des données crédibles. D'un point de vue économique, ce résultat affaiblirait non seulement les entreprises nationales, mais aussi l'efficacité de l'objectif réglementaire lui-même : étant donné la haute substituabilité des services de communication numérique entre les frontières, les activités criminelles sont susceptibles de se déplacer vers des plateformes étrangères. Cela annulerait les avantages de surveillance visés tout en réduisant la création de valeur nationale.

---

[38] P. ex., Proton to Expand Infrastructure Beyond Switzerland Over Surveillance Law Fears [20.01.2026], Aus für Anonymität: Schweizer Online-Nutzer sollen sich identifizieren müssen [20.01.2026], Switzerland's New Surveillance Law: A Privacy Crisis for Encrypted Services [20.01.2026].

[39] Proton Says It'll Leave Switzerland if This Controversial Law Is Passed [20.01.2026], Proton-CEO Andy Yen: «Wer Gesetzgebung der Polizei überlässt, sollte sich nicht wundern, wenn er eines Tages in einem Polizeistaat aufwacht» [21.01.2026].

Perturbation stratégique et coûts d'opportunité

L'adaptation à des obligations étendues et incertaines nécessite la réaffectation de ressources rares, éloignées du développement des produits et de l'innovation, vers la mise en conformité et l'atténuation des risques. Pour de nombreuses entreprises, cela peut impliquer des lancements de produits retardés, des investissements reportés et une réorientation stratégique. En conséquence, les entreprises concernées risquent de prendre du retard par rapport aux concurrents étrangers non soumis à des obligations comparables.

L'incertitude réglementaire affecte en outre le positionnement stratégique des entreprises vis-à-vis des investisseurs et des marchés des capitaux. Des obligations peu claires ou en évolution augmentent le risque réglementaire perçu, ce qui peut mettre les valorisations sous presseion, augmenter les coûts de financement et décourager les investissements, en particulier pour les scale-ups et les start-ups en phase avancée. Plusieurs partenaires interrogés ont noté que pour les entreprises envisageant des introductions en bourse (IPO) ou de grands tours de financement de croissance, l'incertitude entourant la révision de l'OSCPT agit comme un signal négatif, contraignant les options stratégiques bien au-delà de la portée immédiate de la mise en conformité en matière de surveillance.

Conséquences sur le marché du travail et l'emploi

Le changement réglementaire peut également affecter l'emploi au niveau de l'entreprise, avec des implications macroéconomiques plus larges pour l'emploi (voir aussi le chapitre 4). D'une part, les obligations de mise en conformité élargies nécessitent du personnel spécialisé supplémentaire, tel que des experts en sécurité informatique, des responsables de la conformité et des ingénieurs de données. Cela peut entraîner la création de certains emplois dans les entreprises. Les données de l'industrie suggèrent cependant qu'une telle demande pourrait coïncider avec des pénuries de compétences et des pressions salariales croissantes, limitant l'ampleur des gains nets d'emplois. [40] En outre, ces postes supplémentaires sont principalement axés sur la conformité et ne contribuent pas directement à la création de valeur ou à l'innovation. D'autre part, si une part significative d'entreprises se délocalise, réduit leurs activités ou quitte le marché suisse, les pertes d'emplois sont susceptibles de l'emporter sur les embauches liées à la conformité. Les entreprises en démarrage avec des ressources limitées sont particulièrement exposées, car ces petites entreprises sont incapables d'absorber des coûts de mise en conformité largement fixes et des exigences de personnel spécialisé. Les partenaires interrogés ont systématiquement évalué l'effet net sur l'emploi comme négatif, en particulier à moyen et long terme.

Impacts sur la création de valeur et les recettes fiscales

Les effets sur la création de valeur et les finances publiques découlent directement des dynamiques concurrentielles et stratégiques décrites ci-dessus. Les entreprises qui réduisent

[40] Switzerland Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026].

leur présence en Suisse – en délocalisant des infrastructures, des entités juridiques, de la propriété intellectuelle ou des sièges sociaux à l'étranger – contribuent moins au PIB national, aux recettes de l'impôt sur les bénéfices des sociétés et aux chaînes d'approvisionnement locales. Si des employés hautement qualifiés se délocalisent en même temps que ces activités, l'impact s'étend aux recettes fiscales sur le revenu et aux cotisations de sécurité sociale, amplifiant les pertes fiscales.

Au-delà des effets fiscaux directs, de telles délocalisations affaiblissent les retombées de connaissances, les effets de clustering et d'agglomération ainsi que les dynamiques d'écosystème qui sont essentiels pour les secteurs portés par l'innovation. Un flux sortant soutenu d'entreprises et de talents risque de déclencher une forme de fuite des cerveaux, réduisant l'attractivité de la Suisse comme lieu d'implantation pour les technologies orientées vers la confiance, la sécurité et la protection des données. Ces effets sectoriels sont analysés plus en détail à la section 4.1.

3.3 Résumé de l'impact sur les entreprises concernées

Le présent chapitre a analysé les effets économiques de la révision proposée de l'OSCPT sur les entreprises **directement** soumises à la réglementation, notamment les fournisseurs de services de télécommunication (FST) traditionnels et les fournisseurs de services de communication dérivés (FSCD).

Pour les **FST**, le principal changement réglementaire découle de la reclassification potentielle de certains prestataires vers les obligations complètes. Bien que cela augmente les coûts de mise en conformité pour les entreprises concernées, l'ampleur de ces coûts devrait varier considérablement selon les infrastructures existantes et l'exposition réglementaire. Il est important de noter que la concurrence au sein du marché suisse des FST ne devrait pas être matériellement affectée, car les prestataires comparables feraient face à des obligations similaires et la pression concurrentielle internationale reste limitée. En conséquence, des coûts plus élevés seraient très probablement répercutés sur les clients.

La situation est fondamentalement différente pour les **FSCD**. La définition des services de communication dérivés est large et technologiquement neutre, couvrant un large éventail de modèles d'affaires numériques, y compris la messagerie, le courrier électronique, l'hébergement, les services cloud et les fonctionnalités de communication intégrées dans des plateformes. Bien que le nombre précis d'entreprises concernées ne puisse pas être quantifié de manière robuste en raison des limitations de données et de l'incertitude juridique, les données disponibles suggèrent qu'un nombre substantiel d'entreprises établies en Suisse pourraient entrer dans le champ d'application.

Pour ces entreprises, notamment celles du secteur du stockage cloud ou dont les modèles d'affaires sont axés sur la protection des données, les **coûts directs de mise en conformité** sont attendus comme significatifs. Selon que les entreprises sont soumises à des obligations restreintes ou complètes, les données d'entretien indiquent des coûts annuels de mise en conformité de l'ordre de CHF 1 million pour les obligations restreintes et des investissements initiaux de CHF 2 à 3 millions plus des coûts récurrents d'environ CHF 1,5 million

par année pour les obligations complètes. Ces coûts sont principalement dictés par les besoins en personnel spécialisé, l'infrastructure de conservation des données, les ajustements de l'architecture de sécurité et la disponibilité opérationnelle 24h/24 et 7j/7. Au-delà de ces dépenses directes, les entreprises font également face à des **coûts indirects** importants liés à l'incertitude réglementaire, aux coûts d'opportunité et à la réaffectation interne des ressources.

La révision a des conséquences particulièrement prononcées au niveau de l'entreprise pour les FSCD aux modèles d'affaires axés sur la protection des données. Premièrement, les FSCD suisses subissent un désavantage concurrentiel et des risques de réputation par rapport aux concurrents étrangers. Deuxièmement, les entreprises doivent détourner des ressources de l'innovation vers la mise en conformité, retardant le développement de produits, contraignant la flexibilité stratégique et réduisant l'attractivité pour les investissements, notamment pour les start-ups. Troisièmement, les effets sur le marché du travail comprennent une demande accrue de rôles de conformité spécialisés, mais des pertes nettes d'emplois sont probables si les entreprises réduisent leurs activités, se délocalisent ou quittent le marché, notamment dans les postes hautement qualifiés. Enfin, la création de valeur nationale et les recettes fiscales peuvent diminuer à mesure que les entreprises déplacent des infrastructures, des entités juridiques ou des employés à l'étranger, réduisant ainsi leurs contributions au PIB, leurs paiements fiscaux et les retombées de connaissances. Les implications macroéconomiques et internationales plus larges sont analysées dans le chapitre suivant.

Encadré 3 : Impact sur d'autres parties prenantes : utilisateurs privés et institutions publiques

Les conséquences ne concernent pas seulement les entreprises, mais aussi d'autres parties prenantes. L'obligation de stocker des métadonnées augmente à la fois la disponibilité et la concentration d'informations sensibles dans les entreprises concernées par la révision de l'OSCPT. La simple présence de telles données sur des serveurs élargit la surface d'attaque potentielle pour les cyberattaques, comme l'ont notamment souligné l'Internet Society[41] et le Konsumentenforum Suisse[42]. Les entreprises qui opéraient précédemment avec des architectures minimisant les données sont tenues de conserver des informations qui, sinon, ne seraient pas stockées, car elles n'ont aucune valeur technique. Cela crée des cibles supplémentaires pour le piratage, puisque la valeur attendue d'une violation réussie augmente.

La révision affecte également les consommateurs en réduisant la sécurité globale de leurs données personnelles. Le préjudice potentiel résultant d'une seule violation de sécurité augmente à mesure que de plus grands volumes de métadonnées sont stockés pendant des périodes plus longues. Ces risques surviennent indépendamment de tout comportement illicite de la part des utilisateurs concernés et s'appliquent à la population générale.

Dans le même temps, l'accumulation de métadonnées affecte également la facilité d'utilisation, la flexibilité et la qualité effective des services que les prestataires peuvent offrir. Une part substantielle de la valeur de ces services est tirée de la minimisation des données et de la confidentialité. Les exigences prescrivant une collecte ou une conservation de données plus large compromettent directement ces attributs essentiels du produit, entraînant une détérioration de la qualité de service perçue du point de vue de l'utilisateur.

La révision de l'OSCPT affecte également les institutions publiques, qui dépendent de plus en plus des services de communication numérique sécurisés. Par exemple, les autorités fédérales suisses, y compris l'armée suisse, ont adopté les services de messagerie chiffrée de Threema comme canal de communication principal, en grande partie en réponse aux préoccupations de confidentialité et de protection des données.

La révision proposée pourrait modifier les propriétés de sécurité de ces services en introduisant la conservation obligatoire des métadonnées. Comme pour les utilisateurs privés, la disponibilité et la concentration accrues des métadonnées pourraient élargir les vulnérabilités de sécurité potentielles pour les institutions fédérales et les fonctionnaires. Ce risque pourrait être encore amplifié si la pression réglementaire pousse les prestataires suisses à délocaliser des infrastructures, telles que des serveurs de données, à l'étranger. Dans de tels cas, des communications sensibles impliquant des fonctionnaires fédéraux ou du personnel militaire pourraient être stockées selon des normes de sécurité différentes ou en dehors du contrôle direct des autorités suisses.

En conséquence, la révision pourrait accroître l'exposition des communications gouvernementales et militaires aux violations de données ou aux accès non autorisés. Bien que cela n'implique pas une perte immédiate de confidentialité, cela augmente les risques attendus associés au traitement d'informations sensibles liées à l'État et peut affecter la résilience numérique à long terme des institutions publiques.

4 Analyse macroéconomique

Le présent chapitre analyse les impacts macroéconomiques d'une mise en œuvre intégrale de l'OSCPT révisée par rapport à une continuation du statu quo. Les FSCD et les FST ne se cantonnent pas à un seul secteur, mais sont intégrés dans un large éventail d'activités économiques – par exemple dans la finance (p. ex. SIX), le commerce électronique (p. ex. Digitec) et le secteur de la confiance numérique (p. ex. Threema). En conséquence, les effets de la révision de l'OSCPT devraient être hétérogènes selon les secteurs. L'impact négatif le plus fort est attendu dans le secteur de la confiance numérique, qui dépend fondamentalement de la crédibilité, de la confidentialité et d'une gestion sécurisée des données (voir section 3.2). Des mesures telles que le chiffrement amovible et les périodes prolongées de conservation des données (voir sections 2.3.2 et annexe A.2) risquent d'éroder cette confiance, d'augmenter les surfaces d'attaque et la probabilité de violations de données, avec des pertes de confiance potentiellement rapides et disproportionnées.

4.1 Importance du secteur de la confiance numérique

La Suisse offre des conditions exceptionnelles pour le développement de la confiance numérique. La neutralité et la stabilité politiques historiques, des institutions fortes et indépendantes, la sécurité juridique et la stabilité politique créent un environnement particulièrement fiable pour les industries à forte intensité de données. Les normes de protection des données du pays – combinées à une réglementation praticable – sont considérées comme des avantages décisifs de localisation. Cela se reflète dans la présence de sociétés internationales telles que Kaspersky, Acronis ou SWIFT, qui exploitent des centres de données en Suisse pour bénéficier de son infrastructure de haute qualité et de son solide régime de protection des données.[43]

Pour institutionnaliser et accélérer cet élan, les cantons de Vaud et de Genève ont fondé le « Trust Valley » en 2020, un centre de compétences dédié à la cybersécurité, à la confiance numérique et aux technologies émergentes. La région accueille actuellement plus de 300 entreprises spécialisées et plus de 500 experts, formant un écosystème de confiance numérique dense et à croissance rapide.[44] Des initiatives complémentaires, telles que la Swiss Digital Initiative et son étiquette « Digital Trust Label » pionnière au niveau mondial, renforcent la position de la Suisse en fournissant des normes internationalement reconnues pour les services numériques dignes de confiance. Ces efforts sont soutenus par une colla-

---

[41] Internet Society Switzerland Chapter. (2025). *Geplante VÜPF-Revision bedroht Grundrechte und kompromittiert Verschlüsselungen.* Geplante VÜPF-Revision bedroht Grundrechte und kompromittiert Verschlüsselung - ISOC Switzerland Chapter [02.03.2026].

[42] Konsumentenforum Switzerland. (2025). *Stellungnahme zur VÜPF-Revision.* https://konsum.ch/wp-content/uploads/2025/05/VL-Stellungnahme-Konsumentenforum.pdf [11.03.2026].

[43] Factsheet: Die Schweiz als Standort für Cybersicherheit [20.01.2026].

[44] Voir le site internet de la Trust Valley.

boration public-privé robuste. Par exemple, plus de 50 partenaires issus du gouvernement et du monde académique (dont l'EPFL) se réunissent annuellement au « Trust Valley Day » pour coordonner leurs priorités stratégiques sectorielles, réseauter et explorer des opportunités illustrant la vivacité du cluster technologique.

Au-delà de ces développements institutionnels, l'importance économique du secteur est de plus en plus mesurable. Selon différentes analyses de marché, le marché mondial de la confiance numérique devrait atteindre entre CHF 92 et 386 milliards en 2025, dont CHF 3,2 à 6,4 milliards peuvent être – sur la base de calculs de Swiss Economics – attribués au secteur suisse de la confiance numérique.[45] Le marché suisse devrait croître à un taux annuel compris entre 10,1 et 21,6 pour cent dans les années à venir. Cela implique une taille de marché projetée entre CHF 5,2 et 17,1 milliards d'ici 2030 et entre CHF 8,5 et 45,5 milliards d'ici 2035. Cette croissance est portée par la numérisation rapide des industries de base (finance, santé, industrie manufacturière), des dépenses élevées de R&D par habitant soutenues par des programmes fédéraux favorables à l'innovation numérique et l'accent de longue date de la Suisse sur la souveraineté des données et la protection des données.[46]

Le secteur suisse de la confiance numérique s'étend au-delà de la région du lac Léman. Le pays accueille également l'un des clusters de blockchain les plus reconnus au monde : la « Crypto Valley » de Zoug.[47] Au cours de la dernière décennie, des politiques fiscales d'entreprise favorables, la clarté juridique et une base d'investisseurs hautement férue de technologie ont permis aux entreprises de blockchain et Web3 de se développer mondialement depuis la Suisse. La région a attiré des centaines de start-ups, de fondations mondiales (p. ex. la Fondation Ethereum) et des capitaux-risque importants, consolidant ainsi la réputation de la Suisse comme environnement neutre, sécurisé et propice à l'innovation pour les technologies décentralisées.

---

[45] Les calculs sont présentés à l'Annexe **Fehler! Verweisquelle konnte nicht gefunden werden.**. L'étendue de la fourchette s'explique par une définition imprécise du marché de la confiance numérique et par la disponibilité limitée des données.

[46] Voi p. ex. Digital Trust Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026], Switzerland Cybersecurity Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031) [20.01.2026].

[47] Voir le site internet de la Crypto Valley.

Encadré 4 : Vers un cluster d'innovation de type Stockholm ?

Un point de référence européen convaincant pour les dynamiques de cluster est Stockholm, qui s'est imposé comme l'un des écosystèmes technologiques les plus réussis du continent.[48] Il produit un nombre élevé d'entreprises à portée mondiale à partir d'un marché national relativement petit. L'écosystème de Stockholm – valorisé à environ USD 250 milliards avec plus de 2 500 start-ups et plus de 30 licornes[49] – s'est développé grâce à une mobilisation soutenue de capitaux, une intégration profonde entre les institutions de recherche, les investisseurs et les partenaires d'entreprises, et une culture d'ambition internationale et de collaboration. La présence d'histoires de succès mondialement reconnues (p. ex. Spotify, Klarna) a généré un recyclage et un réinvestissement significatifs des fondateurs-opérateurs dans de nouvelles entreprises, créant un cycle auto-renforçant d'expérience, de capital et de leadership qui réduit les frictions de croissance pour les générations suivantes d'entreprises.[50]

La Suisse présente plusieurs similitudes structurelles qui pourraient soutenir une trajectoire comparable :

- haute concentration de talents deep-tech et solides ancres académiques (EPFL, ETH Zurich),
- cadres politiques favorisant la sécurité juridique et un faible risque réglementaire,
- un écosystème de capital-risque établi (p. ex. Redalpine, Founderful),
- des clusters émergents et internationalement visibles (Trust Valley, Crypto Valley), et
- une expansion régulière du marché des secteurs pertinents.

Ensemble, ces facteurs positionnent bien la Suisse pour émerger comme un homologue du cluster d'innovation de Stockholm. Pour réaliser ce potentiel, il faudrait répliquer les mécanismes qui ont permis les premiers succès de la Suède, notamment une formation de capital solide, une internationalisation dès la création et une boucle de rétroaction de sorties réussies générant des entrepreneurs et investisseurs expérimentés.

L'expérience de la Suède suggère que le succès engendre le succès : les sorties de licornes et les scale-ups non seulement génèrent du capital, mais produisent également un vivier de fondateurs, de dirigeants et d'investisseurs providentiels expérimentés qui financent et encadrent activement la prochaine génération d'entreprises, renforçant les dynamiques de cluster et réduisant les obstacles à la montée en puissance.

La question de savoir si un tel développement se matérialise finalement en Suisse est, bien entendu, incertaine. Cependant, plusieurs partenaires interrogés ont souligné que le secteur de la confiance numérique se trouve à un point d'inflexion critique, où un nouveau cluster est susceptible d'émerger. À l'heure actuelle, la Suisse semble bien positionnée pour concourir dans cette course. Cependant, une mise en œuvre intégrale de la révision proposée de l'OSCPT mettrait, selon les interviewés, effectivement fin à cette course avant qu'elle n'ait vraiment commencé pour la Suisse.

Rôle de la souveraineté des données, de la protection des données et de la réputation dans le secteur de la confiance numérique

Un corpus de recherche croissant sur la gouvernance des données et l'économie de la protection des données souligne que des régimes solides de protection des données et des arrangements clairs de souveraineté des données sont des facteurs clés dans la localisation des industries de la confiance numérique. L'OCDE montre que les environnements de données fiables et bien gouvernés renforcent à la fois la confiance dans l'ensemble de l'écosystème de données et stimulent les investissements et le partage des données. À l'inverse, une gouvernance faible et la perte de contrôle sur les données compromettent l'innovation et la création de valeur numérique.[51]

De même, la recherche empirique dans le domaine de l'économie de la protection des données a montré que la volonté des utilisateurs et des entreprises d'adopter des services numériques dépend de manière critique de la fourniture de garanties de protection des données crédibles. Lorsque ces garanties sont compromises, l'utilisation, l'innovation et la croissance du marché déclinent.[52] Le rapport sur la confiance numérique du CEBR quantifie cette relation, montrant que des niveaux plus élevés de confiance numérique sont associés à une croissance économique significativement plus forte et que les déficits de confiance se traduisent par un potentiel non réalisé de PIB et de revenus. Le rapport constate qu'une augmentation de 5 points de pourcentage de la confiance numérique est associée à une augmentation moyenne du PIB par habitant de USD 3 000.[53] Si la souveraineté des données et les protections des données sont affaiblies, les entreprises peuvent retenir des données sen-

---

48 Des dynamiques de cluster similaires ont également été observées dans d'autres pôles d'innovation de premier plan, notamment à Tel Aviv. Là-bas, des décennies de soutien public ciblé, une forte mobilisation du capital-risque (p. ex. via l'initiative Yozma) et une intégration étroite entre académie, start-ups et entreprises multinationales ont engendré un écosystème d'envergure mondiale – particulièrement dans les domaines de la cybersécurité, de l'intelligence artificielle et des sciences de la vie. À l'instar de Stockholm, Tel Aviv illustre la manière dont les premières scale-ups, les sorties et l'internationalisation peuvent déclencher des cycles auto-renforçants de formation de capital, de recyclage des talents et d'expérience entrepreneuriale. Voir p. ex. "Start-up Nation": An incomplete history and profile of Israel's rise in Cybersecurity [20.01.2026], Tel Aviv Ranks #4 Global Startup Ecosystem in 2025 Global Startup Ecosystem Report by Startup Genome [20.01.2026].

49 STOCKHOLMS EKOSYSTEM FÖR STARTUPS 2025 [27.02.2026].

50 Stockholm - Europe's Unicorn Factory [27.02.2026].

51 Going Digital to Advance Data Governance for Growth and Well-being [20.01.2026], Data governance | OECD [20.01.2026], Privacy and data protection [20.01.2026].

52 Acquisti, Tayolor & Wagman (2016). The Economics of Privacy.

53 The digital trust index [20.01.2026].

sibles, délocaliser des infrastructures critiques ou réduire les investissements. Cela pourrait conduire à la stagnation ou même à l'érosion des clusters de confiance numérique.[54]

De récentes analyses politiques et industrielles vont encore plus loin en définissant la souveraineté des données comme un « impératif stratégique de conception » pour construire et maintenir la confiance numérique. [55]

Une perte de confiance a ainsi un impact économique direct et significatif. Le World Economic Forum (WEF) avertit qu'une rupture durable de la confiance dans la technologie et la protection des données met en danger l'innovation et la force économique : « *If trust in technology is lost forever, then so too might be the possibility of a future of innovation and opportunity.* » Une enquête de McKinsey[56] montre que plus de la moitié des consommateurs n'achètent qu'auprès d'entreprises connues pour protéger les données des clients. Dès que des rapports sur des violations de données ou un traitement douteux de la protection des données émergent, les clients passent aux concurrents (40 pour cent des répondants ont mis fin à leur relation commerciale en raison d'une violation de la protection des données). [57] L'enquête établit en outre qu'une solide réputation en matière de protection des données attire non seulement les clients, mais aussi les investisseurs et les travailleurs qualifiés. Certaines parties de la littérature considèrent même la confiance numérique comme du capital immatériel : une fois que la confiance a été ébranlée, il est difficile de la regagner. [58]

Cet effet est également observable au niveau de l'entreprise. Selon une enquête Gartner auprès des CIO (« Chief Information Officer ») en Europe occidentale, 61 pour cent signalent des préoccupations accrues concernant la souveraineté numérique et le contrôle des données et de l'infrastructure en raison de développements géopolitiques. Cela a conduit à

---

[54] Des exemples concrets sont la délocalisation de l'infrastructure de Proton (voir section 3.2.4) ou la relocalisation de Session en Suisse (voir Introducing the Session Technology Foundation [20.01.2026]). À noter que Session s'est relocalisé en Suisse avant que le projet de révision de l'OSCPT soit rendu public.

[55] Voir p. ex. Cybersecurity as Switzerland's Strategic Imperative [22.01.2026], Data Sovereignty: The Driving Force Behind Europe's Sovereign Cloud Strategy [20.01.2026], Digital trust: Why it matters for businesses [20.01.2026], SAP's Sovereignty Commitment: "Building a Secure and Sovereign Future, Together" [20.01.2026], Why data sovereignty is now a dealbreaker in cybersecurity [21.01.2026].

[56] Digital trust: Why it matters for businesses [20.01.2026].

[57] Ce phénomène se manifeste actuellement dans le secteur de l'IA à la suite du changement de contrat du Département de la Défense américain (DoD). Après que le DoD a résilié son accord avec Anthropic – selon les informations disponibles, en raison du refus de ce dernier de faciliter la surveillance de masse nationale – et signé un contrat direct avec OpenAI, les données de marché ont enregistré une forte progression d'Anthropic's Claude dans le classement de l'App Store (voir Claude just beat ChatGPT on the App Store, and the reason is surprising [09.03.2026]). L'impact a été suffisamment significatif pour que le PDG d'OpenAI, Sam Altman, précise publiquement sur X [09.03.2026] qu'OpenAI ne s'engagerait pas dans la surveillance de masse, dans le but de restaurer la confiance des consommateurs.

[58] Paliszkiewicz, Chen, Launer (2022). Trust and Digital Business., Digital trust: Why it matters for businesses [20.01.2026], Why data sovereignty is now a dealbreaker in cybersecurity [21.01.2026].

une plus grande dépendance aux solutions de cloud locales ou régionales. [59] Une analyse de Proton a révélé qu'environ 75 pour cent des entreprises cotées en Europe utilisent des services technologiques américains. [60] En conséquence, un passage aux technologies européennes nécessiterait que le marché européen – y compris le secteur de la confiance numérique – croisse significativement. En accord avec ces conclusions, Gartner prévoit une hausse significative des dépenses en infrastructure de cloud souverain et prédit que les dépenses en cloud souverain en Europe augmenteront de plus de 80 pour cent d'une année sur l'autre en 2026. [61] Cela suggère que les préoccupations concernant la souveraineté deviennent un facteur clé dans les décisions d'investissement. Dans ce contexte plus large, il semble que les entreprises accordent une importance croissante à l'environnement juridique et réglementaire dans lequel leurs données sont hébergées.

En outre, les récentes discussions au sein de l'UE concernant une préférence européenne dans les marchés publics suggèrent que non seulement les entreprises, mais aussi les gouvernements adaptent leur comportement. Surtout dans les domaines de la défense et de la souveraineté numérique, des préoccupations concernant une trop grande dépendance aux États-Unis ainsi que des inquiétudes sécuritaires vis-à-vis des prestataires américains sont soulevées en Suisse. [62] Bien que ces développements soient encore à un stade précoce, ils suggèrent que les solutions européennes pourraient avoir des opportunités de croissance significatives dans le secteur public.

Dans ce contexte, les perspectives de croissance pour les prestataires suisses de confiance numérique sont structurellement solides. La demande de souveraineté des données, d'infrastructure en cloud sécurisée et de garanties de protection des données crédibles s'accélère rapidement, augmentant ainsi la taille globale du marché de la confiance numérique. Dans le même temps, les entreprises réévaluent les lieux d'hébergement et les environnements réglementaires, créant une marge pour les juridictions de confiance pour capter une part relative plus grande de ce marché en croissance. La Suisse, avec sa réputation de stabilité juridique, de confiance, de neutralité et de crédibilité institutionnelle, est bien positionnée pour bénéficier de cette double dynamique – un marché en expansion et le potentiel d'augmenter sa part. Cependant, la révision proposée de l'OSCPT introduit un risque de baisse significatif : elle affaiblit le paysage réglementaire suisse et la perception de la marque suisse, compromettant précisément l'avantage de confiance sur lequel repose cette opportunité de croissance, contraignant ainsi ou même inversant la trajectoire d'expansion du secteur.

---

[59] Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers [13.02.2026].

[60] US tech rules the European market [18.02.2026].

[61] Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026 [13.02.2026].

[62] Voir p. ex. Von der Abhängigkeit zur Selbstbestimmung: Die digitale Zukunft der Schweiz [18.02.2026], Können wir uns bei unserer Verteidigung noch auf die USA verlassen? [18.02.2026], How tenaciously Palantir courted Switzerland [24.02.2026].

4.2 Conséquences de la révision proposée de l'OSCPT

En s'appuyant sur l'analyse du secteur de la confiance numérique, la présente section examine les conséquences économiques d'une mise en œuvre intégrale de l'OSCPT révisée. L'analyse procède du secteur le plus directement concerné vers les conséquences macroéconomiques plus larges, reflétant la manière dont les effets réglementaires et de réputation peuvent se propager des décisions prises par des entreprises individuelles à l'économie au sens large.

Effets immédiats sur le secteur de la confiance numérique

Les entretiens menés indiquent systématiquement que la révision de l'OSCPT compromettrait fondamentalement les perspectives de croissance du secteur suisse de la confiance numérique. Bien que seul un sous-ensemble d'entreprises de confiance numérique soit directement soumis aux obligations révisées, les partenaires interrogés ont souligné que les mesures compromettraient la viabilité de tout modèle d'affaires axé sur la protection des données en érodant la confiance perçue, affectant ainsi négativement l'ensemble du secteur suisse de la confiance numérique.

Des ajustements sont déjà observables. Proton a établi une infrastructure de serveurs à l'étranger et a publiquement signalé que de nouveaux investissements et une expansion en Suisse sont en suspens tant que la mise en œuvre de l'OSCPT révisée reste imminente. Selon Proton, l'environnement réglementaire suisse n'est plus compatible avec sa proposition de valeur fondamentale.

Les personnes interrogées ont en outre indiqué que des considérations similaires s'appliquent à un large éventail de start-ups et de scale-ups actifs dans les technologies de renforcement de la protection des données, les communications sécurisées, la cybersécurité et les services en cloud, ainsi qu'à d'autres prestataires à orientation internationale.

Un autre exemple de cette tendance est le prestataire VPN PrivadoVPN. Début 2026, la société a annoncé sa relocalisation en Islande, liant explicitement cette décision à des préoccupations concernant la révision proposée de l'OSCPT.[63]

En conséquence, la croissance dynamique de l'écosystème du Swiss Trust Valley est susceptible d'être freinée. Plutôt que d'évoluer vers un cluster dynamique, l'écosystème risque la stagnation ou la fragmentation, car des entreprises phares se développent à l'étranger et des start-ups se délocalisent tôt dans leur cycle de vie ou sont fondées hors de Suisse dès le départ. Compte tenu de l'influence significative des effets de réseau, du mentorat et de la signalisation dans la formation de clusters, le départ ou l'absence d'expansion de quelques acteurs proéminents peut suffire à empêcher le développement d'un hub international viable.

[63] 'Our users deserve better' – PrivadoVPN set to leave Switzerland on privacy grounds | TechRadar [13.02.2026].

Effets de réputation et perte de confiance comme canal de transmission

Au-delà des effets sectoriels directs, tous les partenaires interrogés ont insisté sur l'importance des retombées de réputation. La réputation internationale de la Suisse en tant que juridiction de confiance, neutre et discrète est largement considérée comme un actif commun pouvant bénéficier à un large éventail d'activités économiques. La confiance est cependant de manière asymétrique fragile : elle est coûteuse et longue à construire, mais peut se perdre rapidement et est difficile à restaurer une fois endommagée.

La confiance affecte la productivité totale des facteurs (PTF), l'accumulation de capital, les incitations à l'innovation et les décisions de localisation des entreprises à mobilité internationale. [64] Les interventions réglementaires qui modifient les perceptions de la fiabilité peuvent donc avoir un effet accablant sur des secteurs au-delà de ceux directement concernés. La révision de l'OSCPT risque de déclencher précisément un tel choc de réputation.

Retombées vers d'autres secteurs fondés sur la confiance

Les conséquences économiques de la révision de l'OSCPT ne resteront probablement pas confinées au secteur de la confiance numérique. Des perceptions négatives peuvent se répandre vers d'autres industries à forte intensité de confiance, notamment la finance, l'assurance, les services de données liés à la santé, les collaborations de recherche avancées et des parties du secteur des services exportables.

Dans ces industries, la Suisse ne concurrence pas internationalement sur le prix ou l'échelle, mais sur la crédibilité, la stabilité et la qualité institutionnelle. Un affaiblissement du récit de la « Suisse de confiance » pourrait réduire la compétitivité même si les produits et services eux-mêmes restent inchangés. Ce mécanisme reflète des développements internationaux récents, où des changements dans la fiabilité perçue des juridictions (notamment les États-Unis) – plutôt que des changements technologiques – ont amené des entreprises et des gouvernements à réévaluer la localisation des données, les choix de fournisseurs et les dépendances stratégiques. [65]

D'un point de vue macroéconomique, de telles retombées amplifient le choc initial. Les décisions de délocalisation des entreprises de confiance numérique peuvent avoir des effets secondaires sur les relations bancaires, les structures de financement, les services professionnels et l'activité des marchés des capitaux. Au fil du temps, cela peut affaiblir l'écosystème d'innovation plus large et réduire l'attractivité de la Suisse comme lieu d'implantation pour les activités à haute valeur ajoutée.

La figure 3 résume les canaux d'impact sectoriels spécifiques de la révision. Elle souligne que les FSCD au sein du secteur de la confiance numérique sont les plus directement et

[64] See e.g. Smith (2020). Trust and Total Factor Productivity: What Do We Know About Effect Size and Causal Pathways?, de Bliek & Burger (2015). Regional Trust, Liabilities of Foreignness and the Location Decision of Multinational Firms in Europe.

[65] P. ex. Should Europe wean itself off US tech? [20.01.2026], Get over your X: A European plan to escape American technology [20.01.2026].

sévèrement concernés, faisant face à des coûts plus élevés et à une détérioration de la confiance. Cependant, la figure illustre également que même les secteurs en dehors de l'économie de la confiance peuvent encore être affectés, reflétant la pertinence large, à l'échelle économique, de la confiance et de la réputation. Ces effets secondaires sur d'autres secteurs peuvent survenir via plusieurs canaux. Par exemple, la baisse du revenu des ménages dans le secteur de la confiance numérique peut réduire la consommation, avec des répercussions négatives pour des secteurs tels que le tourisme ou la construction.

Figure 3 : Heatmap des canaux d'impact sectoriels

	Autres secteurs (par exemple, le tourisme, le bâtiment)	Autres secteurs basés sur la confiance (par exemple, la finance, l'assurance)	Secteur «Digital trust»
Non-FSDC	Effets secondaires	Effets d'entraînement sur la réputation	Confiance perçue
FSDC	Coûts ↑ Effets secondaires	Coûts ↑ Effets d'entraînement sur la réputation	Coûts ↑ Confiance perçue

Source : Illustration de Swiss Economics

Dépendance de sentier et implications agrégées pour la croissance et les investissements

La révision proposée de l'OSCPT pourrait compromettre les avantages concurrentiels de la Suisse fondés sur la confiance et la réputation, qui sont structurels plutôt que cycliques. Si la confiance devait s'éroder sur une période prolongée, cela affaiblirait les incitations à l'investissement, ralentirait l'innovation et freinerait la croissance de la productivité, affectant les trajectoires de croissance à long terme. Une fois que les clusters fondés sur la confiance ne parviennent pas à émerger ou que les activités existantes se délocalisent, il devient difficile de récupérer l'élan et les investissements sacrifiés, même si le cadre réglementaire est ajusté ultérieurement.

Dans ce contexte, la dépendance au sentier (« path dependency ») est une considération clé. Les décisions réglementaires prises aujourd'hui ne façonneront pas seulement l'environnement juridique immédiat, mais aussi les choix de localisation à long terme et le développement de l'écosystème.[66] Une fois que les entreprises ont déplacé des investissements à l'étranger, délocalisé des parties de leurs opérations ou dépriorisé la Suisse dans leurs stratégies de croissance, il est coûteux et long de revenir sur ces décisions. Les partenaires interrogés ont systématiquement souligné que des corrections réglementaires ultérieures ne sont pas suffisantes pour inverser les dommages causés par une période prolongée d'incertitude. Dans cette perspective, la révision de l'OSCPT comporte le risque d'enfermer la Suisse dans un sentier de développement défavorable en affaiblissant précisément les secteurs construits sur ses forces traditionnelles de confiance, de stabilité et de crédibilité institutionnelle.

[66] Voir p. ex. Martin & Sunley (2006). Path dependence and regional economic evolution. Journal of Economic Geography., Dixit & Pindyck (1994). Investment Under Uncertainty. Princeton U. Press.

D'un point de vue de la croissance structurelle, le développement des activités numériques fondées sur la confiance peut être compris comme une dynamique de courbe en S. La Suisse semble être positionnée au début de la phase d'expansion, où les effets de réseau, la formation de clusters et les rendements croissants à l'échelle peuvent générer une croissance accélérée. Dans une telle phase, l'élan précoce est critique : si l'incertitude réglementaire empêche l'écosystème d'atteindre une masse critique, l'économie risque de rester sur le segment inférieur et plat de la courbe au lieu de passer à une expansion soutenue. S'enfermer dans un sentier de non-expansion à ce stade n'impliquerait pas seulement des pertes à court terme, mais la perte d'une trajectoire de croissance élevée entière qui, une fois manquée, est difficile à recréer.[67]

4.3 Perspectives

La présente section développe une évaluation prospective du secteur suisse de la confiance numérique sous les deux options réglementaires décrites (voir section 2.3) : maintien du statu quo et introduction intégrale de la révision de l'OSCPT. L'objectif n'est pas de produire des estimations ponctuelles, mais d'illustrer comment différentes voies réglementaires pourraient façonner le développement du secteur à moyen et long terme. Compte tenu de l'incertitude inhérente entourant à la fois la mise en œuvre réglementaire et la réponse des entreprises, la quantification est intentionnellement présentée comme une fourchette d'estimations.

4.3.1 Hypothèses sous-jacentes des options réglementaires

Maintien du statu quo

En supposant que le cadre réglementaire actuel continue, l'économie suisse et le secteur de la confiance numérique devraient croître globalement en conformité avec les projections existantes. La Suisse conserverait son positionnement établi en tant que juridiction de confiance pour les services numériques à forte intensité de données et critiques en matière de sécurité, et la « prime de confiance suisse » resterait intacte. Les entreprises pourraient continuer à se développer au sein de la Suisse, de nouveaux entrants considéreraient la Suisse comme un lieu d'implantation attractif. En outre, les effets de réseau au sein du Digital Trust Valley soutiendraient la croissance. Dans ce scénario, l'incertitude porte principalement sur le rythme de la croissance, non sur sa direction, c'est pourquoi nous présentons une fourchette relativement large mais strictement positive d'estimations.

Il est crucial que le scénario du statu quo suppose une clarté réglementaire. On suppose que tous les acteurs considèrent une révision des obligations OSCPT pour les FSCD comme étant hors de l'agenda politique et n'anticipent pas de nouvelles tentatives législatives pour

[67] Voir p. ex., Porter, M. E. (1998). Clusters and the New Economics of Competition. Harvard Business Review., Arthur, W. B. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events. The Economic Journal., Rogers, E. M. (2003). Diffusion of Innovations (5th ed.). Free Press.

réintroduire des dispositions comparables dans un avenir prévisible. En d'autres termes, le scénario de base reflète non seulement une continuation du régime actuel, mais aussi l'absence d'une incertitude réglementaire renouvelée qui pourrait autrement retarder les investissements, les décisions de développement ou l'entrée sur le marché.

L'incertitude restante concernant la croissance future est double. [68] Premièrement, la trajectoire du secteur suisse de la confiance numérique est étroitement liée aux dynamiques mondiales et dépendra de la vigueur avec laquelle la demande internationale se développe. Deuxièmement, une incertitude subsiste quant à l'évolution de la part de marché relative de la Suisse. Cependant, les données présentées suggèrent que, étant donné la demande croissante de souveraineté des données et de juridictions de confiance, la Suisse est bien positionnée pour augmenter sa part au sein du marché mondial en croissance.

Introduction intégrale de la révision de l'OSCPT

La deuxième option reflète la mise en œuvre de l'OSCPT révisée. Nous supposons que l'économie suisse croîtra globalement en ligne avec les projections existantes et que le secteur de la confiance numérique continuera d'exister en Suisse. Cependant, nous supposons que sa taille agrégée restera globalement inchangée sur une période de cinq à dix ans, impliquant une croissance nette nulle. Comme nous l'expliquons ci-dessous, ces hypothèses sont conservatrices pour plusieurs raisons.

Premièrement, les FSCD seraient directement et de manière disproportionnée affectés. Des coûts de mise en conformité plus élevés, des contraintes opérationnelles et l'incertitude juridique obligeraient de nombreux prestataires existants à adapter substantiellement leurs modèles d'affaires ou à délocaliser des activités à l'étranger. Deuxièmement, et de manière cruciale, l'impact ne se limiterait pas aux seuls FSCD. Le secteur de la confiance numérique est très intégré. L'attractivité de la Suisse réside dans sa réputation collective en tant que juridiction fiable et prévisible pour les services numériques de confiance. Un changement réglementaire perçu internationalement comme compromettant la confidentialité et la sécurité juridique se répercuterait donc sur des entreprises non formellement soumises à la réglementation. Cela entraînerait une détérioration de leur positionnement sur le marché international, à mesure que la « prime de confiance suisse » s'érode. Cela pourrait potentiellement conduire à des réductions d'activités, à des délocalisations ou à des fermetures d'entreprises dans le secteur suisse de la confiance numérique qui ne se qualifient pas comme FSCD. En outre, les données présentées à la section 4.2 indiquent que d'autres secteurs fondés sur la confiance – et potentiellement l'économie suisse dans son ensemble – pourraient être affectés, impliquant une croissance inférieure à celle actuellement projetée.

Pris ensemble, ces effets résulteraient très probablement en un ralentissement de la croissance économique suisse et un effondrement (partiel) du secteur de la confiance numérique.

---

[68] Si la clarté réglementaire s'accompagnait d'un cadre structurellement amélioré et favorable à l'innovation, la croissance pourrait dépasser la borne supérieure du scénario de référence correspondant au statu quo. Ce scénario optimiste n'est pas intégré dans les projections du présent rapport.

Ils impliquent également la perte du moteur de croissance du secteur. Bien que le secteur de la confiance numérique puisse subsister, son expansion vibrante actuelle et ses dynamiques de clustering se dissiperaient presque certainement. Notre hypothèse selon laquelle la taille agrégée du secteur numérique reste la même est donc conservatrice.

4.3.2 Quantification

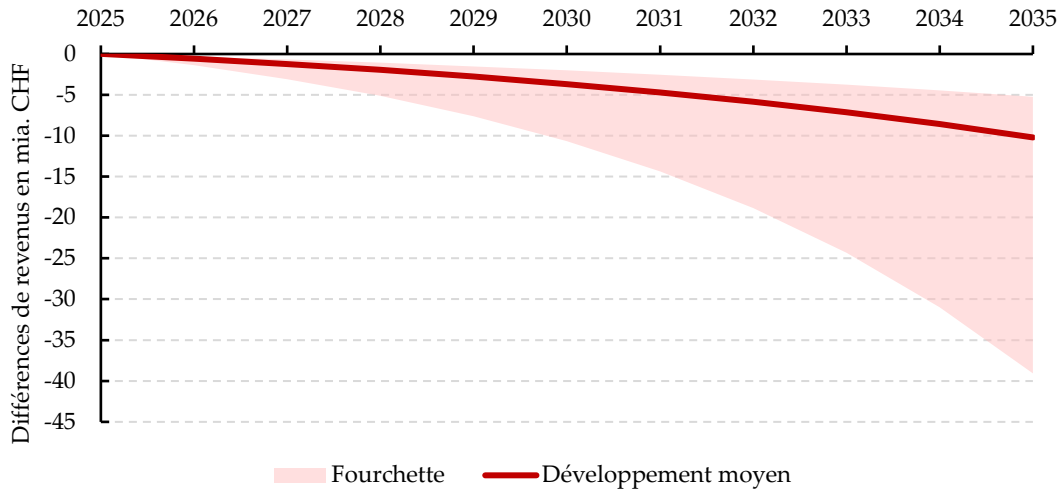
La présente section quantifie les effets économiques, en se concentrant sur les revenus, le bien-être économique, l'emploi et les impacts fiscaux. Elle présente la différence entre une trajectoire basée sur le statu quo et une mise en œuvre intégrale de la révision de l'OSCPT. Les hypothèses sous-jacentes, les calculs détaillés et les sources de données sont documentés à l'annexe B.

Impact sur les revenus

On estime actuellement que le secteur de la confiance numérique en Suisse vaut entre CHF 3,2 et 6,4 milliards. Cependant, la croissance projetée diffère sensiblement selon les trajectoires.

Dans le cas du statu quo, le secteur devrait se développer à un taux annuel moyen de 12 pour cent au cours de la prochaine décennie (avec une fourchette de 10,1 à 21,6 pour cent). Si la révision de l'OSCPT est introduite, on s'attend à ce que le secteur connaisse une croissance nulle sur la même période. L'impact de la révision proposée de l'OSCPT sur le secteur de la confiance numérique est calculé comme la différence entre ces deux trajectoires au cours des dix prochaines années, comme illustré à la Figure 4 4.

Figure 4 : Différences de revenus



Source : Illustration de Swiss Economics

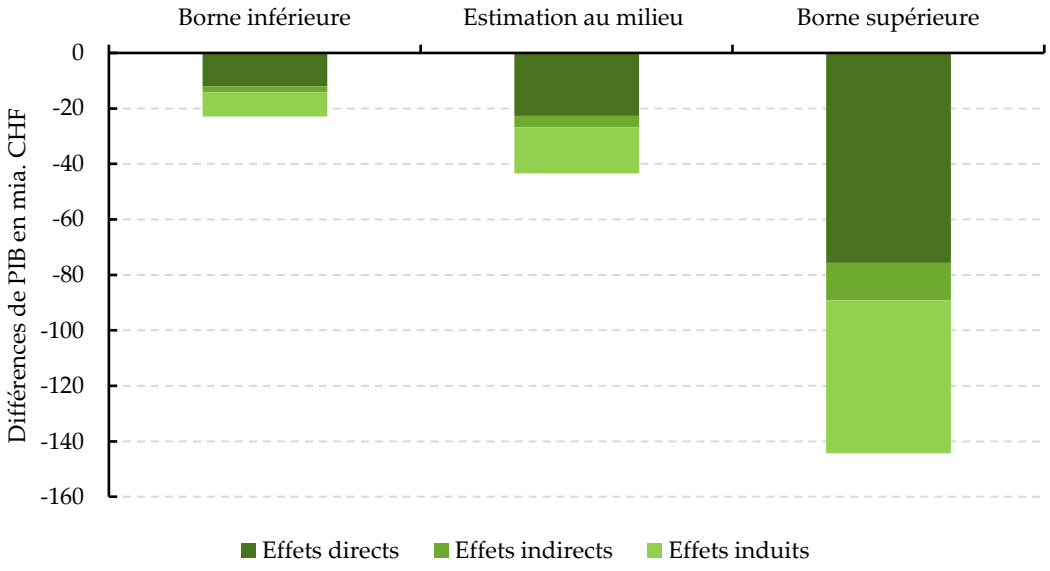
La figure 4 montre l'impact négatif croissant de manière exponentielle des différentiels de croissance persistants dans le temps. La fourchette qui s'élargit illustre que l'incertitude augmente avec l'horizon de projection. D'ici 2030, les pertes annuelles de revenus potentielles se situent dans une fourchette de CHF 2 à 10,7 milliards, augmentant jusqu'à CHF

5,2 à 39,1 milliards d'ici 2035. Si les effets à court terme peuvent sembler modérés, cette trajectoire indique que les conséquences à long terme deviendront de plus en plus significatives en raison du caractère cumulatif de la croissance du secteur. Il convient également de noter que, si la croissance prévue du secteur s'avère plus forte, les effets négatifs seront d'autant plus importants au fil du temps. Notre estimation au milieu de la fourchette suggère des pertes cumulées potentielles d'environ CHF 46,8 milliards d'ici 2035.

Impact sur le bien-être économique

L'analyse du bien-être économique se concentre sur les estimations d'ordre de grandeur des pertes de bien-être économique cumulées sur la période 2025-2035. Les impacts sur le bien-être économique sont dérivés à l'aide de tableaux entrées-sorties, qui permettent la décomposition des effets en composantes directes, indirectes et induites. Les pertes directes de bien-être économique reflètent la valeur ajoutée sacrifiée au sein du secteur de la confiance numérique lui-même ; les effets indirects captent les retombées le long des chaînes d'approvisionnement en amont, tandis que les effets induits découlent de la réduction du revenu des ménages et de la consommation. Ces estimations sont agrégées sur l'horizon de projection complet pour fournir une évaluation cumulative des implications pour le bien-être économique. La figure 5 présente les résultats pour la borne inférieure, l'estimation au milieu de la fourchette et la borne supérieure.

Figure 5 : Différences de bien-être économique cumulées (2025-2035)



Source : Illustration de Swiss Economics

Les résultats indiquent une perte de bien-être économique cumulée de l'ordre de CHF 14 milliards comme borne inférieure lorsque seuls les effets directs et indirects sont pris en compte. Selon les hypothèses relatives à la croissance sectorielle, la borne supérieure de ces pertes directes et indirectes de bien-être économique pourrait atteindre environ CHF 89 milliards. Si les effets induits sont également inclus, l'impact cumulé de la borne supérieure pourrait s'élever jusqu'à CHF 144 milliards. Cependant, étant donné que les effets induits

sont très sensibles aux hypothèses de modélisation, ces chiffres doivent être interprétés comme des fourchettes indicatives plutôt que comme des estimations précises, les bornes supérieures reflétant une incertitude substantielle.

Encadré 5 : Quantification des retombées intersectorielles

Au-delà des effets directs dans le secteur de la confiance numérique, des retombées négatives vers l'économie suisse au sens large sont probables (voir section 4.2). Bien que ces effets soient potentiellement substantiels, ils sont par nature difficiles à quantifier et soumis à une incertitude considérable. Une façon d'illustrer la gravité potentielle de tels effets de débordement est l'indice de confiance numérique du CEBR.[69] La Suisse obtient actuellement 73 points d'indice, reflétant des niveaux élevés de confiance dans les services numériques, la gouvernance et la protection des données. Un déclin de la confiance – par exemple déclenché par la révision proposée de l'OSCPT – devrait abaisser ce score. Si les niveaux de confiance de la Suisse devaient tomber à ceux observés dans des pays comme l'Allemagne ou les États-Unis (environ 20 points d'indice plus bas), le PIB par habitant pourrait diminuer au fil du temps d'environ USD 12 000 – environ 10 pour cent de son niveau actuel.[70] Bien que ces estimations doivent être interprétées avec prudence, elles indiquent qu'une telle évolution impliquerait une perte substantielle de bien-être économique pour la population suisse.

La plupart des partenaires interrogés n'ont pas été en mesure de quantifier l'impact négatif sur l'économie suisse. Néanmoins, ils ont souligné une asymétrie importante : les effets économiques directs sont les plus prononcés pour les entreprises opérant au sein du secteur de la confiance numérique – avec des pertes de bien-être économique incluant les effets induits atteignant jusqu'à CHF 36 milliards ou 3 à 4 pour cent du PIB en 2035. [71] Cependant, les coûts les plus importants résulteront probablement des retombées intersectorielles et des pertes de confiance à l'échelle économique.

---

[69] The digital trust index [20.01.2026]. Nous avons obtenu les chiffres relatifs à la Suisse sur demande auprès du CEBR.

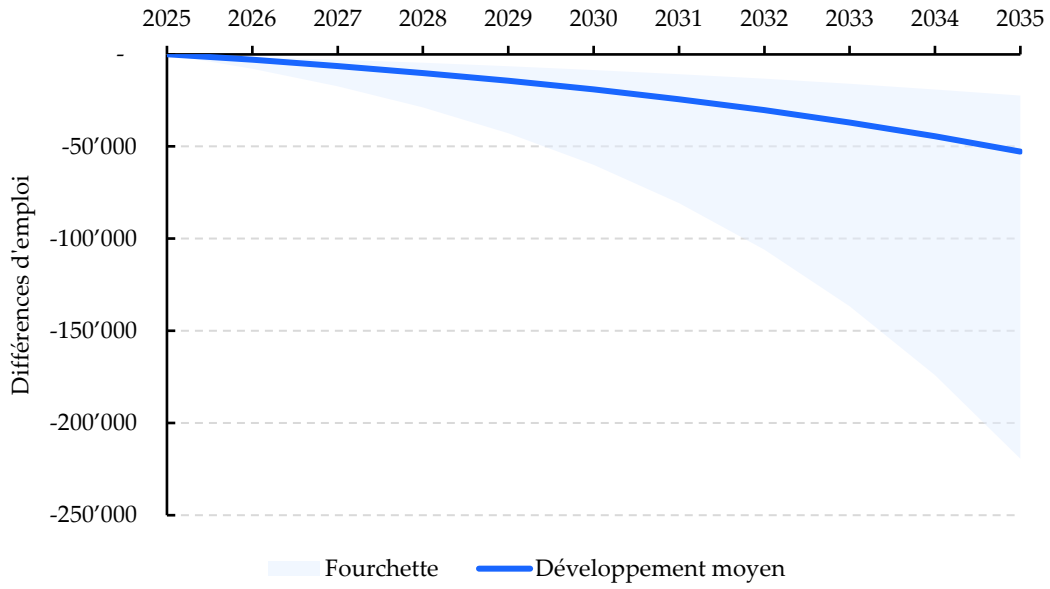
[70] L'analyse du CEBR indique qu'une augmentation d'un point d'indice de confiance numérique est associée en moyenne à une hausse du PIB par habitant de 596 USD (The digital trust index [20.01.2026]). En conséquence, une baisse de 20 points d'indice est associée en moyenne à une diminution du PIB par habitant d'environ 12'000 USD. Par ailleurs, le FMI estime le PIB par habitant de la Suisse en 2025 à 111'050 USD (IMF Switzerland Country Data [06.03.2026]). Dès lors, la baisse d'environ 12'000 USD correspond à environ 10 pour cent du niveau actuel du PIB par habitant.

[71] 36 milliards de CHF correspondent à 3 à 4 pour cent du PIB suisse en 2035 si le taux de croissance nominal du PIB se situe en moyenne entre 0,75 et 3,25 pour cent. Le taux de croissance effectif devrait se situer dans cette fourchette (voir p. ex. Energieperspektiven 2050+ Volkswirtschafltiche Auswirkungen [06.03.2026] publié par le Conseil fédéral

Impact sur l'emploi

L'emploi dans le secteur de la confiance numérique est estimé entre 13 800 et 36 200 postes en 2025. Comme décrit à l'annexe B, l'emploi est projeté en utilisant la même fourchette de taux de croissance que celle appliquée aux revenus, assurant une cohérence entre les indicateurs économiques. L'impact de la révision proposée de l'OSCPT est, comme précédemment, quantifié comme l'écart entre le statu quo et une mise en œuvre intégrale de la révision de l'OSCPT. La figure 6 illustre les trajectoires d'emploi résultantes sur les dix prochaines années.

Figure 6 : Différences d'emploi



Source : Illustration de Swiss Economics

La figure illustre un impact négatif qui s'intensifie rapidement. La dispersion croissante des résultats reflète une incertitude croissante à mesure que l'horizon de projection s'étend. D'ici 2030, les pertes d'emplois estimées dans le secteur de la confiance numérique se situent entre 8 500 et 60 000 postes, augmentant jusqu'entre 22 400 et 219 300 d'ici 2035. Ce schéma suggère que, si l'impact à court terme reste relativement contenu, les effets à plus long terme deviendront de plus en plus sévères. Dans le scénario de développement au milieu de la fourchette, les pertes d'emplois sont estimées à environ 52 700 postes d'ici 2035. Ensemble, ces chiffres suggèrent un risque significatif d'un exode à grande échelle de travailleurs hautement qualifiés du secteur suisse de la confiance numérique, impliquant que la révision de l'OSCPT pourrait déclencher une fuite des cerveaux majeure.

Impact sur les recettes fiscales

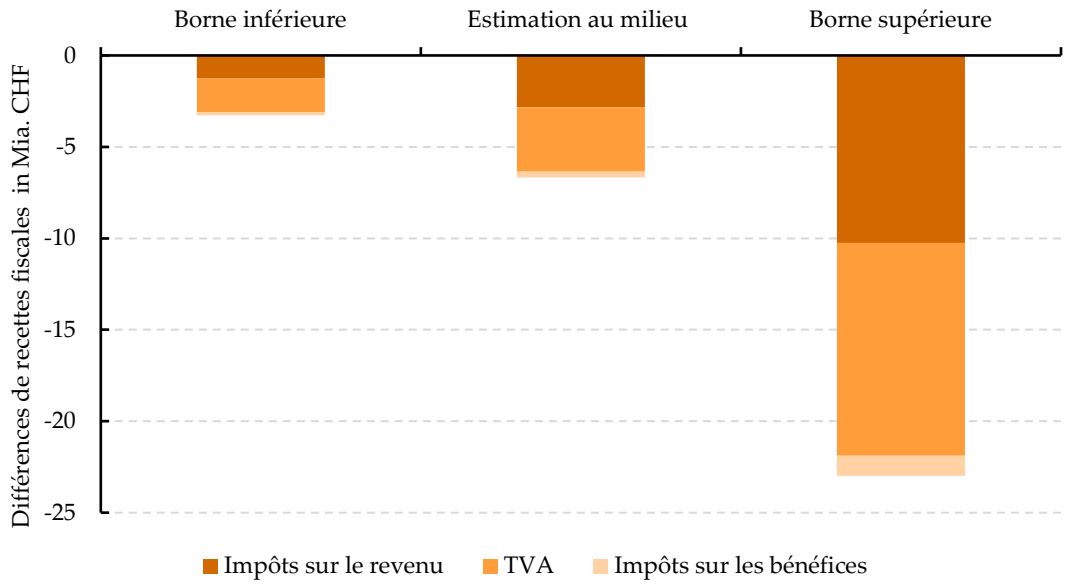
Compte tenu de l'incertitude substantielle entourant l'estimation des recettes fiscales sacrifiées, nous limitons l'analyse à des estimations d'ordre de grandeur des pertes fiscales cumulées sur la période 2025-2035. Le calcul se concentre sur les recettes fiscales provenant de :

- la taxe sur la valeur ajoutée (TVA),
- des impôts sur les bénéfices, et
- des impôts sur le revenu, y compris les impôts communaux, cantonaux et les impôts fédéraux directs.

L'annexe B fournit une description détaillée des hypothèses sous-jacentes et des choix méthodologiques utilisés dans le calcul pour chaque catégorie fiscale.

Les résultats sont présentés à la figure 7. La large fourchette reflète l'incertitude concernant les dynamiques sectorielles futures. Dans ce contexte, les résultats doivent – à nouveau – être interprétés comme indicatifs. Dans l'ensemble, les pertes estimées de recettes fiscales cumulées sur l'horizon de projection se situent entre environ CHF 3 et 22 milliards.

Figure 7 : Différences cumulées de recettes fiscales (2025-2035)



Source : Illustration de Swiss Economics

4.4 Résumé

Le présent chapitre évalue les conséquences macroéconomiques d'une mise en œuvre intégrale de l'OSCPT révisée comparée au maintien du statu quo. Les FSCD et les FST étant intégrés dans un large éventail d'activités économiques, les effets de la révision seront hétérogènes selon les secteurs. Les impacts les plus significatifs sont attendus dans le secteur de la confiance numérique, où les modèles d'affaires reposent fondamentalement sur la crédibilité, la confidentialité et la gestion sécurisée des données. Compte tenu de ce rôle central et de ses fortes dynamiques de croissance, le secteur de la confiance numérique est analysé comme le principal canal de transmission par lequel des effets macroéconomiques plus larges se matérialisent.

L'analyse montre qu'une mise en œuvre intégrale de la révision de l'OSCPT affaiblirait substantiellement les perspectives de croissance du secteur suisse de la confiance numérique. Bien que seul un sous-ensemble d'entreprises soit directement concerné, l'érosion perçue de la fiabilité de la Suisse affecterait l'ensemble de l'écosystème. Les données d'entretiens et le comportement observé des entreprises indiquent un risque élevé d'investissements bloqués, de délocalisation des activités à l'étranger et de dissipation des dynamiques de cluster. Au mieux, le secteur stagnerait à moyen et long terme.

Quantitativement, la divergence entre les deux options réglementaires est substantielle. Par rapport au statu quo, les pertes annuelles de revenus dans le secteur de la confiance numérique sont estimées à CHF 5,2 à 39,1 milliards d'ici 2035. Les pertes cumulées de revenus s'élèvent à environ CHF 47 milliards d'ici 2035 dans l'estimation au milieu de la fourchette, reflétant les effets cumulatifs de la croissance sacrifiée. Les pertes de bien-être économique, mesurées par l'analyse entrées-sorties, sont estimées à CHF 14 à 89 milliards pour les effets directs et indirects sur la période 2025-2035.

Cette dynamique se retrouve également dans les effets sur l'emploi : d'ici 2035, les pertes d'emplois par rapport au statu quo sont estimées entre 22 400 et 219 300 postes, avec une estimation d'environ 53 000 postes sacrifiés au milieu de la fourchette. Les recettes fiscales sacrifiées sur la même période sont estimées à entre CHF 3 milliards et 22 milliards en termes cumulés, incluant la TVA, les impôts sur les bénéfices et les impôts sur le revenu.

Au-delà de ces effets quantifiables, le chapitre met en évidence le risque d'un impact macroéconomique plus large, porté par des facteurs de réputation. Un affaiblissement de la position internationale de la Suisse en tant que juridiction de confiance affecterait probablement d'autres secteurs à forte intensité de confiance, amplifiant le choc initial. Bien que ces retombées soient difficiles à quantifier, elles représentent potentiellement le coût économique le plus important. Dans l'ensemble, les résultats indiquent que la révision de l'OSCPT pose un risque structurel significatif pour la croissance, l'emploi, le bien-être économique et les finances publiques, en raison de la perte d'un moteur de croissance clé fondé sur la confiance de l'économie suisse.

A Catégories et obligations des FST et des FSCD

A.1 Maintien du statu quo

Le tableau 3 résume les catégories et les obligations des FST, et le tableau 4 fournit le même aperçu pour les FSCD. Ces deux résumés sont basés sur la version actuelle de l'OSCPT. Les obligations détaillées sont définies dans l'OSCPT du 26 mars 2024.

Tableau 3 : Catégories de FST et leurs obligations respectives

Catégorie	Critères de classification	Obligations
FST à obligations restreintes (art. 51)	Déclassement sur demande auprès du Service SCPT si les conditions légales sont remplies. Critères principaux : (a) le prestataire fournit des services de télécommunication **exclusivement dans le domaine de l'enseignement et de la recherche**, *ou* (b) au cours des 12 derniers mois, il a reçu au **maximum 10 ordres de surveillance concernant 10 cibles de surveillance différentes**, et (c) le **chiffre d'affaires domestique total du service de transmission et du service de communication dérivé est inférieur à CHF 100 millions** au cours de chacun des deux derniers exercices. L'évaluation est basée sur **le chiffre d'affaires du service de transmission et du service de communication dérivé**, et non sur le chiffre d'affaires total de l'entreprise.	Les obligations fondamentales comprennent : ▪ identifier les utilisateurs par des moyens appropriés[72] ▪ conserver les informations sur les abonnés requises pour les demandes de renseignement ▪ fournir des réponses standardisées aux demandes de renseignements et des renseignements spéciaux ▪ démontrer la disponibilité opérationnelle pour les demandes de renseignements ▪ permettre les mesures de surveillance, accorder l'accès aux systèmes si nécessaire et supprimer le chiffrement appliqué par le prestataire ▪ transmettre les métadonnées de trafic disponibles sur demande, sans obligation de conservation
FST à obligations complètes	Catégorie standard : chaque FST est initialement considéré comme un FST à obligations complètes. Un déclassement ne prend effet qu'une fois approuvé formellement par le Service SCPT. Si les critères de l'art. 51 cessent d'être remplis, le FST doit en informer le Service SCPT, qui procède alors à la remise à niveau vers la catégorie des obligations complètes.	Toutes les obligations de la catégorie à obligations restreintes, plus : ▪ service de piquet 24h/24 et 7j/7 ▪ conservation des métadonnées de trafic nécessaires pour certaines demandes de renseignements et la surveillance rétroactive ▪ fourniture de renseignements via l'interface automatisée du Service SCPT et démonstration de la capacité à l'utiliser ▪ fourniture automatisée de renseignements et utilisation obligatoire de l'interface de demandes de renseignements ▪ capacité technique de fournir à la fois des données de contenu et des métadonnées pour la surveillance en temps réel et rétroactive Les FST nouvellement reclassés bénéficient de délais de transition de 2 ou 12 mois, selon la complexité des obligations

[72] Le rapport explicatif mentionne quelques exemples pouvant constituer des moyens appropriés au sens de l'art. 19. Par exemple, l'identification par carte de crédit et la sauvegarde des données d'autorisation, ou l'identification par carte SIM et la sauvegarde de l'identité internationale de l'abonné mobile (IMSI).

Tableau 4 : Catégories de FSCD et leurs obligations respectives

Catégorie	Critères de classification	Obligations
FSCD sans obligations plus étendues	Catégorie par défaut, applicable tant que ni les critères relatifs aux obligations plus étendues de renseignement (art. 22) ni ceux relatifs aux obligations plus étendues de surveillance (art. 52) ne sont remplis.	Uniquement des obligations fondamentales de collaboration et de renseignement : ▪ fournir des renseignements sous forme non formalisée ▪ permettre les mesures de surveillance et accorder l'accès aux systèmes si nécessaire ▪ fournir tout renseignement nécessaire à la surveillance ▪ transmettre les métadonnées de trafic disponibles sur demande, sans obligation de conservation
FSCD avec obligations plus étendues de renseignement (art. 22)	**Le Service SCPT déclare** un FSCD comme prestataire soumis à des obligations plus étendues lorsque, à la date de référence du 30 juin : **10 cibles de surveillance différentes ou plus** (moyenne sur 12 mois sur l'ensemble des services de communication dérivés), *ou* **chiffre d'affaires domestique supérieur à CHF 100 millions** au cours des deux derniers exercices, à condition qu'une part importante des activités porte sur des services de communication dérivés *et* que le prestataire compte **plus de 5'000 abonnés**.	Obligations similaires à celles des FST à obligations complètes en matière de **renseignement**. Toutefois, certaines exceptions s'appliquent : ▪ au lieu d'un service de piquet 24h/24 et 7j/7, fournir les coordonnées d'un service de piquet interne (le cas échéant) pour les cas urgents ▪ pas d'obligation de fournir des renseignements conformément aux art. 48a à 48c Délais de transition : 2 mois pour les obligations simples, 12 mois pour les obligations techniquement complexes
FSCD avec obligations plus étendues de surveillance (art. 52)	**Le Service SCPT déclare** un FSCD comme prestataire soumis à des obligations plus étendues lorsque, à la date de référence du 30 juin : **plus de 100 demandes de renseignements** (moyenne sur 12 mois sur l'ensemble des services de communication dérivés), *ou* **chiffre d'affaires domestique supérieur à CHF 100 millions** au cours des deux derniers exercices, à condition qu'une part importante des activités porte sur des services de communication dérivés *et* que le prestataire compte **plus de 5'000 abonnés**.	Obligations similaires à celles des FST à obligations complètes en matière de **surveillance**. Toutefois, certaines exceptions s'appliquent : ▪ pas d'obligation d'effectuer les types de surveillance visés aux art. 56a, 56b, 67 let. b et c, et 68 al. 1 let. b et c ▪ pas d'obligation de fournir des renseignements conformément aux art. 48a à 48c Délais de transition : 2 à 12 mois selon la complexité des obligations

A.2 Introduction intégrale de la révision de l'OSCPT

Définition et obligations des FST

Un fournisseur de services de télécommunication (FST) est un prestataire responsable de la transmission technique des informations. Contrairement aux prestataires de services qui opèrent en superposition d'un autre réseau, les FST offrent des services d'accès ou de transport directement aux utilisateurs finaux et assument la responsabilité contractuelle d'assurer la transmission des communications. Cela comprend les prestataires qui exploitent un

réseau de télécommunication public, offrent un accès direct à un tel réseau (p. ex. l'accès à Internet), fournissent des services de communications mobiles publics ou des services de téléphonie publique conjointement avec l'accès au réseau.

Parce que les FST opèrent au niveau de la couche de transmission et peuvent détenir des métadonnées de trafic et des contenus de communication pertinents pour la surveillance, l'ordonnance leur impose un ensemble gradué d'obligations. Celles-ci sont divisées en deux catégories : FST à obligations restreintes et FST à obligations complètes. Cette dernière constitue le cas par défaut en vertu de l'ordonnance révisée. Le tableau 5 résume les deux catégories et leurs obligations respectives.

Tableau 5 : Catégories de FST et leurs obligations respectives

Catégorie	Critères de classification	Obligations
FST à obligations restreintes (art. 16b)	Déclassement sur demande au Service SCPT si les conditions légales sont remplies. Critères principaux : (a) le prestataire fournit des services de télécommunication **exclusivement dans le domaine de l'enseignement et de la recherche**, *ou* (b) au cours des 12 derniers mois, il a reçu a**u maximum 10 ordres de surveillance concernant 10 cibles de surveillance différentes**, *et* (c) **le chiffre d'affaires domestique total de l'entreprise est inférieur à CHF 100 millions** au cours de chacun des deux derniers exercices commerciaux. L'évaluation est basée sur **le chiffre d'affaires total de l'entreprise**, c'est-à-dire pas uniquement le chiffre d'affaires lié aux télécommunications.	Les obligations fondamentales comprennent : ▪ identifier les utilisateurs par des moyens appropriés ▪ conserver les informations sur les abonnés requises pour les demandes de renseignements ▪ fournir des réponses standardisées aux demandes de renseignements et des renseignements spéciaux ▪ démontrer la disponibilité opérationnelle pour les renseignements ▪ permettre les mesures de surveillance, accorder l'accès aux systèmes si nécessaire et supprimer le chiffrement appliqué par le prestataire ▪ transmettre les métadonnées de trafic disponibles sur demande sans obligation de conservation
FST à obligations complètes (art. 16c)	Catégorie standard : chaque FST est initialement considéré comme un FST à obligations complètes. Un déclassement ne prend effet qu'une fois que le Service SCPT l'approuve formellement. Si les critères de l'art. 16b cessent d'être remplis, le FST doit en notifier le Service SCPT, qui déclare alors la remise à niveau vers la catégorie des obligations complètes.	Toutes les obligations de la catégorie des obligations restreintes plus : ▪ service de piquet 24h/24 et 7j/7 ▪ conservation des métadonnées de trafic nécessaires pour certaines demandes de renseignements et la surveillance rétroactive ▪ fourniture de renseignements via l'interface automatisée de demandes de renseignements du Service SCPT et démonstration de la disponibilité à l'utiliser ▪ fourniture automatisée de renseignements et utilisation obligatoire de l'interface de demandes de renseignements ▪ capacité technique de fournir à la fois des données de contenu et des métadonnées pour la surveillance en temps réel et rétroactive. Les FST nouvellement mis à niveau bénéficient de délais de transition de 6 ou 12 mois, selon la complexité des obligations.

Définition et obligations des FSCD

Un fournisseur de services de communication dérivés (FSCD) est un prestataire qui permet la communication interpersonnelle entre utilisateurs, mais le fait sur la base de l'infrastructure de communication d'un autre service de télécommunication. Les FSCD n'exploitent pas leurs propres réseaux d'accès ou de transport ; au lieu de cela, ils offrent des fonctionnalités de communication « over the top » d'un service de communication primaire. Cela comprend, par exemple, les fonctionnalités de messagerie, d'appel ou d'autres fonctions de communication interpersonnelle intégrées dans des plateformes en ligne, des applications ou des services numériques. Les FSCD peuvent être des prestataires indépendants ou offrir

des fonctionnalités de communication dans le cadre d'un écosystème de services numériques plus large.

Ce qui caractérise les FSCD d'un point de vue juridique n'est pas le modèle d'affaires, mais le fait technique qu'ils s'appuient sur l'infrastructure de communication sous-jacente d'un autre prestataire tout en permettant la communication interpersonnelle directe. Parce qu'ils agissent comme intermédiaires dans le processus de communication et peuvent détenir des informations liées aux utilisateurs ou aux messages pertinentes pour la surveillance, l'ordonnance les soumet à des obligations graduées selon leur échelle. Un résultat important de la procédure de consultation est que la définition des FSCD n'est pas entièrement claire même pour les professionnels du domaine, et qu'il existe donc une incertitude considérable sur quelles entreprises – en plus des exemples nommés – pourraient également être des FSCD.

Les obligations des FSCD sont réparties en trois catégories. FSCD à obligations minimales, FSCD à obligations restreintes et FSCD à obligations complètes. Le tableau 6 résume les trois catégories et leurs obligations respectives.

Tableau 6 : Catégories de FSCD et leurs obligations respectives

Catégorie	Critères de classification	Obligations
FSCD à obligations minimales (art. 16e)	**Catégorie par défaut**, applicable tant que ni les critères des obligations restreintes ni ceux des obligations complètes ne sont remplis. Concrètement : **moins de 5 000 participants** (moyenne sur 12 mois) **et moins de CHF 100 millions** de chiffres d'affaires domestiques au cours de chacun des deux derniers exercices commerciaux.	Uniquement des obligations fondamentales de collaboration et de renseignements : ▪ fournir des renseignements sous forme non formalisée ▪ permettre les mesures de surveillance et accorder l'accès aux systèmes si nécessaire ▪ fournir tout renseignement nécessaire à la surveillance ▪ transmettre les métadonnées de trafic disponibles sur demande sans obligation de conservation
FSCD à obligations restreintes (art. 16f)	**Mise à niveau automatique** lorsque, à la date de référence du 30 juin : **plus de 5 000 mais moins de 1 million de participants** (moyenne sur 12 mois sur l'ensemble des services de communication dérivés) *et* **chiffres d'affaires domestiques de moins de CHF 100 millions** au cours des deux derniers exercices commerciaux.	Obligations alignées sur les FST à obligations restreintes : ▪ identifier les utilisateurs par des moyens appropriés ▪ conserver les informations sur les abonnés requises pour les demandes de renseignements ▪ fournir des réponses standardisées aux demandes de renseignements et des renseignements spéciaux ▪ démontrer la disponibilité opérationnelle pour les renseignements ▪ supprimer le chiffrement appliqué par le prestataire Les obligations supplémentaires doivent être mises en œuvre dans les 6 mois suivant le 30 juin.
FSCD à obligations complètes (art. 16g)	**Deuxième mise à niveau** pour les prestataires d'une pertinence économique ou d'une base d'utilisateurs significative. Critères : (a) **au moins 1 million de participants** (moyenne sur 12 mois, date de référence 30 juin), *ou* (b) **des chiffres d'affaires domestiques de plus de CHF 100 millions** au cours des deux derniers exercices commerciaux.	Obligations alignées sur les FST à obligations complètes. Toutes les obligations de la catégorie des obligations restreintes plus : ▪ service de piquet 24h/24 et 7j/7 ▪ conservation des métadonnées de trafic nécessaires pour certaines demandes de renseignements et la surveillance rétroactive (conservation de 6 mois) ▪ fourniture automatisée de renseignements et utilisation obligatoire de l'interface de demandes de renseignements ▪ capacité technique de fournir à la fois des données de contenu et des métadonnées pour la surveillance en temps réel et rétroactive. Délais de transition : 6 mois pour les obligations plus simples, 12 mois pour celles techniquement complexes.

B Quantification du marché suisse de la confiance numérique

La présente annexe détaille la quantification des impacts économiques considérés dans cette étude. L'annexe B.1décrit la méthodologie utilisée pour estimer les revenus, l'annexe B.2 couvre l'évaluation des effets sur le bien-être économique, l'annexe B.3 expose l'approche pour quantifier l'emploi, et l'annexe B4 présente l'estimation des effets fiscaux. Toutes les sources de données et références clés sous-jacentes à ces quantifications sont résumées à l'annexe B.5.

B.1 Revenus

Deux approches complémentaires sont utilisées pour estimer la taille du marché de la confiance numérique (MCN) suisse en 2025 :

- **Allocation « top-down » du MCN mondial** à la Suisse sur la base de la part de la Suisse dans le PIB mondial, ainsi que de sa part dans les marchés mondiaux des technologies de l'information et des communications (TIC) et de la cybersécurité.
- **Extrapolation à partir de la France**, utilisant des données de revenus publiées pour le marché français de la confiance numérique et les adaptant à la Suisse selon les tailles relatives des marchés.

Les deux approches sont d'abord décrites en détail, après quoi les estimations résultantes pour le MCN suisse sont présentées.

Décomposition du MCN mondial 2025

La part suisse du marché mondial de la confiance numérique est calculée à l'aide de la formule suivante :

$$\boldsymbol{MCN_{CH} = MCN_{Global} * Part_{CHF/Global} * FX_{USD/CHF}} \quad (1)$$

où MCN_{Global} désigne le marché mondial estimé de la confiance numérique, $Part_{CHF/Global}$ représente la part de la Suisse dans l'économie mondiale ou les marchés pertinents, et $FX_{USD/CHF}$ est le taux de change USD/CHF.

Les estimations du MCN mondial provenant de six études de marché vont de USD 110 à 482 milliards. La part suisse est approximée en utilisant la part de la Suisse dans le PIB mondial ainsi que sa part dans les marchés mondiaux des TIC et de la cybersécurité. Sur cinq indicateurs différents, les parts résultantes varient de 0,4 à 2,5 pour cent.[73] Le taux de change est basé sur le taux moyen annuel USD/CHF de l'Administration fédérale des contributions pour 2025, fixé à 0,83.

[73] Part du PIB selon le FMI, part des TIC selon Mordor Intelligence et part de la cybersécurité selon Mordor Intelligence, Data Bridge Market Research et Ken Research.

Extrapolation du MCN français 2025

Pour une deuxième approche, un observatoire de marché publié par l'Alliance française pour la confiance numérique (*Alliance pour la Confiance Numérique*, ACN) est utilisé. Dans son observatoire 2025, l'ACN rapporte des revenus de EUR 21,3 milliards pour le secteur français de la confiance numérique en 2024, contre des revenus mondiaux totaux de EUR 33,5 milliards des entreprises françaises.

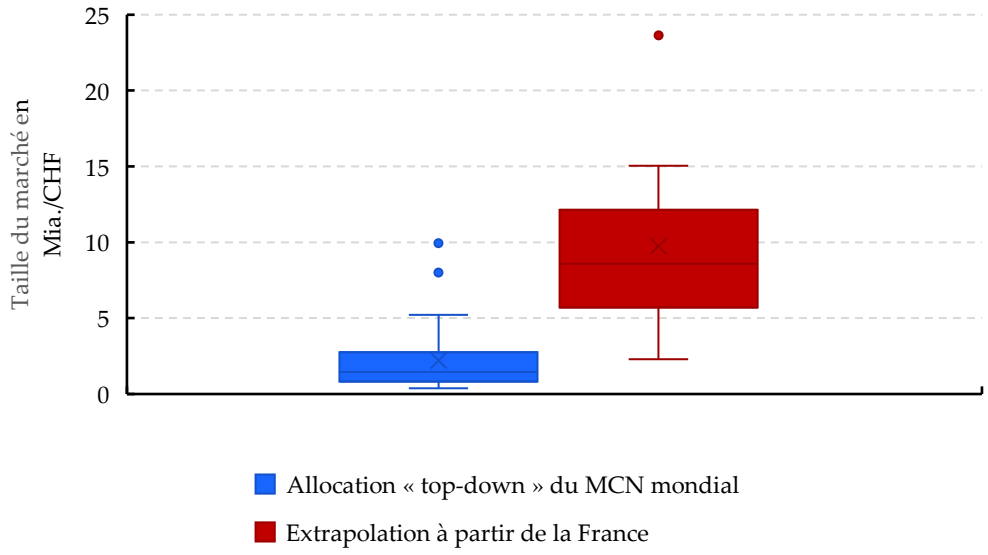
Pour obtenir les chiffres pour 2025, les revenus sont extrapolés en supposant un taux de croissance annuel constant de 7,6 pour cent, correspondant au taux de croissance annuel moyen observé entre 2018 et 2024 en France. Cela donne des revenus français de confiance numérique de EUR 22,9 à 36,0 milliards en 2025.

Le MCN suisse est ensuite dérivé en adaptant l'équation (1) aux données de revenus françaises et en les adaptant selon la part de la Suisse par rapport à la France. Cinq estimations alternatives de cette part sont considérées, allant de 11 à 70 pour cent. [74] Le taux de change EUR/CHF est fixé à 0,94.

MCN suisse en 2025

Compte tenu de la large dispersion des paramètres d'entrée, la taille estimée du marché suisse de la confiance numérique est soumise à une incertitude substantielle (voir figure 8).

Figure 8 : Taille du marché suisse de la confiance numérique en 2025



Source : Illustration de Swiss Economics

Les estimations suggèrent que le MCN suisse en 2025 se situe entre CHF 0,4 et 23,6 milliards. Cette large fourchette est due à trois facteurs principaux : Premièrement, les projections du MCN mondial diffèrent considérablement selon les sources, les estimations de Pre-

[74] Part du PIB selon le FMI, part des TIC selon Mordor Intelligence et part de la cybersécurité selon Mordor Intelligence, Data Bridge Market Research et Ken Research.

cedence Research étant plus de quatre fois inférieures à celles de Mordor Intelligence. Deuxièmement, la décomposition descendante du marché mondial donne généralement des estimations inférieures à l'extrapolation basée sur les données françaises. Troisièmement, les parts de marché suisses supposées varient considérablement selon les indicateurs : les chiffres de cybersécurité de Ken Research impliquent un MCN suisse plus de six fois plus grand que les estimations basées sur les données de cybersécurité de Mordor Intelligence.

Pour dériver une estimation centrale plus plausible, un poids plus important est accordé aux estimations basées sur la France, car elles reposent sur des revenus observés et spécifiques au secteur provenant d'un marché national de confiance numérique clairement défini plutôt que sur des estimations approximatives du marché mondial. L'analyse se concentre donc sur les revenus domestiques français, en excluant les revenus internationaux, pour éliminer la possibilité d'une valeur aberrante clairement à la hausse. Sur cette base, les estimations mondiales les plus basses et les résultats supérieurs impliqués par l'extrapolation des revenus internationaux français sont exclus. De plus, les parts de marché suisses impliquées par Mordor Intelligence et Ken Research semblent incompatibles avec les parts de PIB et de TIC de la Suisse, qui sont bien reflétées dans les estimations rapportées par Data Bridge Market Research. En conséquence, une part suisse de 1 pour cent du MCN mondial et de 30 pour cent du marché domestique français sont supposées comme valeurs les plus probables. Sur la base de ces considérations, le MCN suisse en 2025 est estimé dans une fourchette d'environ CHF 3,2 à 6,4 milliards.

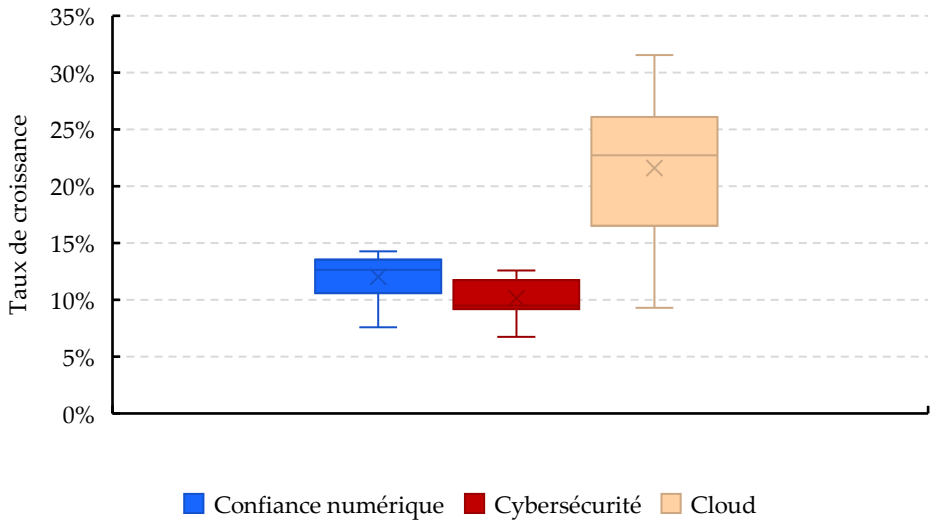
Nous excluons les pertes de revenus indirectes liées aux activités en amont de l'analyse quantitative. Cependant, une évaluation de haut niveau basée sur les tableaux entrées-sorties indique que la prise en compte de ces effets indirects impliquerait des pertes de revenus supplémentaires de l'ordre de 60 pour cent.

Croissance du marché

Plusieurs taux de croissance ont été identifiés qui fournissent une fourchette plausible pour le développement du MCN suisse au cours des 5 à 10 prochaines années.

- **Confiance numérique** : Cette catégorie comprend les estimations de croissance disponibles pour les marchés mondial et français de la confiance numérique. Aucune projection dédiée pour le MCN suisse n'a été identifiée, soulignant l'incertitude entourant sa trajectoire autonome.
- **Cybersécurité** : Cette catégorie comprend les estimations de croissance pour les marchés mondial, français et suisse de la cybersécurité. La cybersécurité constituant un segment central du MCN, ces chiffres fournissent un indicateur pertinent de la dynamique de marché attendue.
- **Cloud** : Cette catégorie contient des estimations pour les marchés mondiaux et suisses du cloud (p. ex. stockage cloud, cloud public). Le cloud fait partie de la sécurité numérique et représente donc un domaine pertinent du MCN.

Figure 9 : Estimations des taux de croissance



Remarque : Bien que les données suggèrent que le marché suisse du cloud a récemment dépassé la croissance mondiale, les benchmarks mondiaux sont maintenus sans ajustement à la hausse pour garantir un cadre d'évaluation conservateur.[75]

Source : Illustration de Swiss Economics

La figure montre que les taux de croissance estimés de tous les domaines varient considérablement. Cependant, en moyenne, la cybersécurité croît le moins à 10,13 pour cent et le cloud le plus à 21,59 pour cent. Cette divergence est cohérente avec les cycles de vie de l'industrie : alors que la cybersécurité représente un marché plus mature et établi, le secteur du cloud est encore dans sa phase d'expansion précoce, caractérisée par une croissance plus dynamique. Cette fourchette fournit une estimation structurée pour la calibration des scénarios. La cybersécurité représente le segment le plus mature du MCN et constitue donc une borne inférieure. Les marchés du cloud, en revanche, captent les composantes les plus dynamiques et portées par l'innovation de l'écosystème de la confiance numérique et définissent ainsi une borne supérieure économiquement plausible. L'estimation moyenne du MCN sert de référence centrale.

S'appuyer sur ces trois moyennes sectorielles assure la cohérence, évite de choisir sélectivement des valeurs aberrantes individuelles et ancre la projection du MCN suisse dans les dynamiques de marché de segments étroitement liés. En conséquence, 10,13 pour cent est appliqué comme borne inférieure conservatrice, 21,59 pour cent comme borne supérieure reflétant les dynamiques de forte croissance, et 12,01 pour cent comme taux de croissance central plausible pour le MCN suisse au cours des 5 à 10 prochaines années.

[75] Cloud Computing 2022 [17.02.2026].

B.2 Bien-être économique

L'impact sur le PIB est estimé à l'aide de tableaux entrées-sorties pour les NOGA 62 et 63 (services informatiques et d'information), qui servent de substitut pour le secteur de la confiance numérique. Ce cadre permet de dériver des effets de valeur ajoutée directs, indirects et induits sur la base des estimations de revenus présentées ci-dessus. La valeur ajoutée directe reflète la contribution générée au sein du secteur de la confiance numérique lui-même. L'estimation résultante pour la Suisse, basée sur les NOGA 62 et 63, est globalement cohérente avec les estimations correspondantes de l'ACN pour le secteur français de la confiance numérique. La valeur ajoutée indirecte capte les effets de retombées en amont le long de la chaîne d'approvisionnement et est dérivée à l'aide de coefficients d'entrée sectoriels établis du cadre entrées-sorties.

Bien que l'estimation des effets directs et indirects soit relativement robuste et bien ancrée dans les données sous-jacentes, la valeur ajoutée induite – principalement portée par la consommation supplémentaire financée par des revenus des ménages plus élevés – est soumise à une incertitude substantiellement plus grande. Comme elle dépend d'hypothèses comportementales et d'effets multiplicateurs, la composante induite doit donc être interprétée comme une borne supérieure des effets sur le bien-être économique plutôt que comme une estimation centrale.

B.3 Emploi

L'emploi dans le MCN suisse en 2025 est estimé à l'aide de deux approches.

- **Extrapolation à partir de la France** : Cette approche s'appuie sur les chiffres d'emploi publiés pour le secteur français de la confiance numérique et les adapte à la Suisse selon les tailles relatives des marchés.
- **Ratio revenus par employé** : Cette méthode s'appuie sur le ratio publié revenus par équivalent temps plein (EPT)[76] dans les tableaux entrées-sorties pour les codes NOGA 62 et 63 en Suisse et l'adapte selon le taux d'emploi moyen. Ce ratio est ensuite appliqué aux revenus estimés à mi-fourchette.

Une allocation top-down du MCN mondial n'est pas réalisable en raison de l'absence de données fiables sur l'emploi mondial. L'extrapolation suit donc la même méthodologie que celle exposée à l'annexe B.1 ; nous excluons également les pertes de revenus indirectes liées aux activités en amont de l'analyse quantitative.

Premièrement, selon l'ACN, le secteur français de la confiance numérique employait environ 107 000 personnes en 2024. L'application de l'approche d'adaptation (voir annexe B.1) donne une fourchette de 12 900 à 84 400 employés pour le secteur suisse de la confiance

[76] De manière intuitive, ce ratio décrit le chiffre d'affaires moyen généré par une entreprise du secteur pour chaque équivalent plein temps (EPT). Si le ratio chiffre d'affaires par EPT est ensuite pondéré par le taux d'emploi moyen, il indique le chiffre d'affaires moyen généré par employé.

numérique en 2025. En utilisant la part de marché plausible de 30 pour cent précédemment identifiée, on obtient une estimation ponctuelle d'environ 36 200 employés.

Deuxièmement, nous appliquons le ratio revenus par employé de CHF 352 000 par employé[77] aux revenus à mi-fourchette de 2025 dans le MCN suisse pour calculer l'emploi dans le MCN suisse. Cela donne une estimation de 13 800 employés. Notre client estime l'emploi actuel à environ 25 000. En conséquence, nous utilisons l'estimation du client comme estimation au milieu de la fourchette, le ratio revenus par employé comme borne inférieure et la figure extrapolée comme borne supérieure pour les projections d'emploi.

Croissance de l'emploi

La croissance de l'emploi est calibrée à l'aide de données historiques pour le secteur français de la confiance numérique. Selon l'ACN, l'emploi est passé de 52 300 employés en 2018 à 107 000 en 2024, correspondant à un taux de croissance annuel moyen de 12,67 pour cent sur la période 2018 à 2024. La croissance a été particulièrement forte entre 2023 et 2024, lorsque l'emploi est passé de 89 000 à 107 000 (une augmentation de 20 pour cent).

Ce taux de croissance le plus récent dépasse considérablement les taux de croissance rapportés pour le marché global en France et est donc traité comme une valeur aberrante exclue de l'analyse de référence. Pour rester conservateurs, nous appliquons la même fourchette de taux de croissance à l'emploi qu'aux revenus, malgré le fait que les données historiques pour la France suggèrent que la croissance de l'emploi a en moyenne dépassé la croissance des revenus d'environ cinq points de pourcentage.

B.4 Impôts

L'estimation des recettes fiscales sacrifiées est soumise à une incertitude croissante, notamment sur des horizons temporels plus longs. Néanmoins, conformément aux directives méthodologiques[78], nous fournissons des estimations d'ordre de grandeur, car la présentation d'une fourchette plausible de résultats offre une valeur analytique plus grande que de s'abstenir de quantifier. L'estimation couvre les effets sur la taxe sur la valeur ajoutée (TVA), les revenus des impôts sur le revenu et les bénéfices.

TVA

L'impact TVA est dérivé des pertes de revenus estimées et applique un taux de TVA constant de 8,1 pour cent.[79] Pour rester conservateurs, la TVA est supposée être déduite des

[77] Calculé sur la base de 420'000 CHF par EPT multiplié par le taux d'emploi de 83,5 pour cent. Par souci de simplification, il est supposé que ce ratio reste constant au cours des dix prochaines années.

[78] Guide pour l'estimation des coûts [20.01.2026]. Ce guide se fonde sur la loi sur l'allégement des coûts de la réglementation pour les entreprises.

[79] Il s'agit également vraisemblablement d'une hypothèse conservatrice, dans la mesure où la TVA a progressivement augmenté au cours des dernières décennies et que deux projets actuellement examinés par le Parlement pourraient conduire à de nouvelles hausses.

chiffres de revenus déclarés plutôt qu'ajoutée, évitant ainsi une surestimation des pertes de recettes fiscales.

Impôts sur le revenu

L'estimation des impôts sur le revenu suppose un revenu brut annuel de CHF 108 000, correspondant au revenu médian le plus bas observé en 2024 dans les secteurs pertinents, c'est-à-dire les télécommunications (NOGA 61), les services informatiques (NOGA 62) et les activités de services d'information (NOGA 63). Prendre la médiane plutôt que la moyenne et supposer un niveau de revenu constant dans le temps reflète une approche conservatrice. Le taux d'imposition effectif moyen est fixé à 13 pour cent, sur la base du calculateur fiscal suisse[80] et correspondant à un individu célibataire de 35 ans résidant à Zurich en 2025. Il convient de noter que le secteur de la confiance numérique est actuellement concentré dans les cantons de Genève et de Vaud, où le taux d'imposition effectif pour le même niveau de revenu se situerait entre 15 et 18 pour cent. L'hypothèse retenue sous-estime donc, plutôt qu'elle ne surestime, les pertes potentielles d'impôts sur le revenu.

Impôts sur les bénéfices

L'impact estimé sur les impôts sur les bénéfices est dérivé des revenus cumulés sur la période 2025 à 2035. Étant donné que le secteur de la confiance numérique est encore dans une phase de forte croissance et est caractérisé par une grande part de start-ups, une marge bénéficiaire conservatrice de 5 pour cent est supposée. Cette hypothèse se situe bien en dessous de la marge bénéficiaire moyenne rapportée du secteur des logiciels de 8,8 pour cent en 2022 telle que documentée dans le Swiss Software Industry Survey 2023. Pour la fiscalité, nous appliquons le taux effectif actuel d'imposition des bénéfices de 14 pour cent pour les bénéfices jusqu'à CHF 10 millions du canton de Vaud.

B.5 Sources de données

Valeur	Signification	Source	Lien
EUR 21.3 Mds	Revenus en FR par les entreprises françaises de confiance numérique 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
EUR 33.5 Mds	Revenus mondiaux par les entreprises françaises de confiance numérique 2024	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
7.6 %	Taux de croissance moyen du secteur de la confiance nu-	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf

[80] Tax calculator [28.01.2026].

	mérique en France 2016-24		
107’000	Employés dans le secteur français de la confiance numérique 2024	ACN	https://www.decision.eu/wp-content/uploads/2024/06/Observatory-of-digital trust-sector-2024.pdf
89’000	Employés dans le secteur français de la confiance numérique 2023	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2025/06/acn-observatory-of-digital trust-2025.pdf
52’300	Employés dans le secteur français de la confiance numérique 2018	ACN	https://www.confiance-numerique.fr/wp-content/uploads/2023/11/Observatoire-ACN-de-la-Confiance-numerique-2019.pdf
USD 3’360 Mds USD 1’000 Mds USD 117’170 Mds	PIB FR PIB CH PIB Mondial	IMF	https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD
0.831 0.937	FX USD/CHF FX EUR/CHF	FTA	https://www.estv.admin.ch/estv/de/home/bundesabgaben/wehrpflichtersatzabgabe/wpe-jahresmittelkurse.html
USD 135 Mds 13.3 %	MCN mondial 2025 TCAC	FMI	https://www.futuremarketinsights.com/reports/digital trust-market
USD 133 Mds 13.3 %	MCN mondial 2025 TCAC	GVR	https://www.grandviewresearch.com/industry-analysis/digital trust-market-report
USD 482 Mds 14.28 %	MCN mondial 2025 TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/digital trust-market
USD 110.47 Mds 11.6 %	MCN mondial 2025 TCAC	Presedence research	https://www.precedenceresearch.com/digital trust-market
USD 388.54 Mds 12 %	MCN mondial 2025 TCAC	Market Research Future	https://www.marketresearchfuture.com/reports/digital trust-market-21989
USD 118 Mds	MCN mondial 2024	Ken Research	https://www.kenresearch.com/global-digital trust-market
USD 44.7 Mds	Marché TIC en Suisse	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/switzerland-ict-market
USD 135 Mds	Marché TIC en France	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/france-ict-market
USD 6’030	Marché TIC mon-	Mordor Intelli-	https://www.mordorintelligence.com/industry-re-

Mds	dial	gence	ports/information-and-communications-technology-market
USD 0.97 Mds 6.75 %	Taille du marché cybersécurité en Suisse 2025 TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/switzerland-cybersecurity-market
USD 2.66 Mds 9.3 %	Taille du marché cybersécurité en Suisse 2024 TCAC	Data Bridge Market Research (DBMR)	https://www.databridgemarketresearch.com/nucleus/switzerland-cybersecurity-market
USD 3.5 Mds	Taille du marché cybersécurité en Suisse 2024	Ken Research	https://www.kenresearch.com/switzerland-cybersecurity-market
USD 3.5 Mds 9.4 %	Taille du marché cybersécurité en Suisse 2024 TCAC	Trend Tracker Analytics	https://www.linkedin.com/pulse/north-america-switzerland-cybersecurity-market-cnwxc/
USD 235.5 Mds 12.28 %	Taille du marché cybersécurité mondial 2025 TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cyber-security-market
USD 301.92 Mds 12.6 %	Taille du marché cybersécurité mondial 2025 TCAC	Presedence Research	https://www.precedenceresearch.com/cyber-security-market
USD 227.59 Mds 9.1 %	Taille du marché cybersécurité mondial 2025 TCAC	Markets & Markets	https://www.marketsandmarkets.com/PressReleases/cyber-security.asp
USD 203.9 Mds 9.5 %	Taille du marché cybersécurité mondial 2024 TCAC	DBMR	https://www.databridgemarketresearch.com/reports/global-cybersecurity-market
USD 141 Mds	Taille du marché cybersécurité mondial 2024	Ken Research	https://www.kenresearch.com/global-cybersecurity-software-market
USD 9.1 Mds 11.08 %	Taille du marché cybersécurité en France 2025 TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/france-cybersecurity-market
USD 8.09 Mds	Taille du marché cybersécurité en France 2024	DBMR	https://www.databridgemarketresearch.com/nucleus/france-cybersecurity-market

11.2 %	TCAC		
USD 5.0 Mds	Taille du marché cybersécurité en France 2024	Ken Research	https://www.kenresearch.com/france-cybersecurity-for-critical-infrastructure-market
8.1 %	TVA	FTA	https://www.estv.admin.ch/de/mwst-steuersaetze-schweiz
CHF par mois 9’380 9’874 9’014	Revenu médian 2024 : Télécommunications, services informatiques, activités de services d'information	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/loehne-erwerbseinkommen-arbeitskosten.html
48.62 % 57.32 % 92.72 % CHF 420’000	Valeur ajoutée directe Valeur ajoutée indirecte Valeur ajoutée induite Revenus par EPT	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/volkswirtschaft/input-output.html
5.362 m 4.480 m	Employés EPT	FSA	https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/erwerbstaetigkeit-arbeitszeit/erwerbsbevoelkerung/arbeitsmarktstatus.html
14 %	Impôts sur les bénéfices Vaud	KPMG	https://kpmg.com/ch/de/medien/medienmitteilungen/2025/05/clarity-swiss-taxes.html
8.8 %	EBIT industrie logicielle 2022	Swiss Software Industry Survey 2023	https://www.swico.ch/media/filer_public/93/d4/93d4ad40-8986-4eb5-9fc6-6e632871faac/ssis_report_2023.pdf
23.45%	Marché stockage cloud Mondial TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-storage-market
24.41%	Marché stockage cloud Mondial TCAC	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-storage-market
31.1%	Marché Cloud IA mondial TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-ai-market
31.53%	Marché Cloud IA mondial TCAC	DBMR	https://www.databridgemarketresearch.com/reports/global-cloud-ai-market
9.31%	Marché services Cloud gérés TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/cloud-managed-services-market
17.69%	Marché Cloud public mondial TCAC	Mordor Intelligence	https://www.mordorintelligence.com/industry-reports/public-cloud-market
22.95%	Marché migration Cloud public mon-	DBMR	https://www.databridgemarketresearch.com/reports/global-public-cloud-migration-market

	dial TCAC		
22.5%	Cloud public en Suisse TCAC	PWC	https://www.pwc.ch/en/insights/fs/how-swiss-banks-and-insurers-can-leverage-the-cloud-for-value-creation.html
12.97%	Marché services Cloud en Suisse TCAC	DBMR	https://www.databridgemarketresearch.com/nucleus/switzerland-cloud-service-market
20%	Taux de croissance IaaS & SaaS en Suisse	Kellerhals Carrard	https://kellerhals-carrard.ch/download/204/2022_cloud_computing_switzerland.pdf