www.jusletter.ch

Sylvain Métille / Marie-Laure Percassi

Les collectivités publiques face à l'externalisation informatique

Analyse sous l'angle de la protection des données personnelles

Les collectivités publiques sont nombreuses à utiliser des outils informatiques fournis par des prestataires externes. Ces solutions utilisent de plus en plus souvent la technologie de l'informatique en nuage (« cloud computing » en anglais) – ce qui pose la question de leur compatibilité avec la législation sur la protection des données. Le présent article montre que les solutions en nuage sont en principe admissibles du point de vue de la protection des données, mais que d'autres obstacles – surtout politiques – peuvent s'opposer à leur utilisation.

Catégories d'articles : Articles scientifiques
Domaines juridiques : Protection des données

Proposition de citation : Sylvain Métille / Marie-Laure Percassi, Les collectivités publiques face à l'externalisation informatique, in : Jusletter 29. September 2025

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Table des matières

1. Introduction
2. Sous-traitance
   2.1. Introduction
   2.2. Règles applicables
      2.2.1. Au niveau fédéral
      2.2.2. Au niveau cantonal
   2.3. Discussion
3. Secret professionnel et secret de fonction
   3.1. Introduction
   3.2. Règles applicables
   3.3. Discussion
4. Transfert de données personnelles à l'étranger
   4.1. Introduction
   4.2. Cas de transferts à l'étranger
   4.3. Règles applicables
      4.3.1. Au niveau fédéral
      4.3.2. Au niveau cantonal
   4.4. Discussion
5. Analyse d'impact
   5.1. Introduction
   5.2. Règles applicables
      5.2.1. Au niveau fédéral
      5.2.2. Au niveau cantonal
   5.3. Discussion
6. Autres considérations
   6.1. Introduction
   6.2. ONum
   6.3. LSI
   6.4. LMeta
   6.5. Règles en matière de marchés publics
   6.6. Indépendance numérique
7. Conclusion

1. Introduction

[1] Les collectivités publiques ont recours à de nombreuses solutions informatiques externes – c'est-à-dire développées et fournies par des prestataires externes – pour mener à bien leurs activités. De plus en plus régulièrement, ces solutions utilisent la technologie de l'informatique en nuage (« *cloud computing* » en anglais). Ce terme général est utilisé pour désigner la fourniture de services informatiques à distance et à la demande. Les plus connus sont la fourniture de logiciels en tant que service (*Software as a service*, SaaS), la fourniture d'une plateforme de développement d'applications en tant que service (*Platform as a service*, PaaS) et la fourniture d'infra-

structures en tant que service (*Infrastructure as a service*, IaaS).[1] La technologie *cloud* a souvent pour caractéristique que l'ordinateur d'un tiers (parfois à l'étranger) est utilisé[2].

[2] L'admissibilité des solutions d'informatique en nuage sous l'angle de la protection des données personnelles – en particulier si elles sont utilisées par une collectivité publique et impliquent un transfert de données à l'étranger – a suscité de nombreuses questions et critiques au cours de ces dernières années. Comme on le verra, certaines évolutions récentes confirment désormais que l'usage de l'informatique en nuage est compatible avec la législation suisse.

[3] Pour parvenir à ce constat, nous examinerons les différentes règles de protection des données personnelles spécifiques qui s'appliquent en cas d'utilisation d'une solution d'informatique en nuage. Nous aborderons d'abord les principes relatifs à la sous-traitance (2) puis les règles sur le secret de fonction, applicables aux membres des autorités et des fonctionnaires (art. 320 CP[3]), et sur le secret professionnel (art. 321 CP) (3). Nous analyserons ensuite les normes concernant le transfert de données personnelles à l'étranger (4). Il sera ensuite question des normes prévoyant l'obligation de réaliser une analyse d'impact à certaines conditions (5). Enfin, après avoir présenté quelques considérations pertinentes, mais étrangères à la protection des données personnelles (6), nous terminerons par une conclusion (7).

[4] Précisons enfin que la présente contribution ne traite pas des données relatives aux personnes morales. Il est toutefois intéressant de souligner que, au niveau fédéral, celles-ci ne sont plus considérées comme des données personnelles depuis l'entrée en vigueur de la nouvelle LPD[4]. Ces données sont désormais soumises à des règles propres lorsqu'elles sont traitées par des organes fédéraux ; pour l'heure, ce régime découle de l'art. 71 LPD (disposition transitoire qui prévoit que les dispositions d'autres actes de droit fédéral qui font référence à des données personnelles continuent de s'appliquer au traitement des données concernant des personnes morales pendant les cinq ans suivant l'entrée en vigueur la LPD) et des art. 57*r* ss LOGA[5]. La LOGA sera toutefois modifiée afin d'y intégrer des bases légales réglementant le traitement de données de personnes morales par les organes fédéraux[6]. Ces nouvelles dispositions devront entrer en vigueur le 1er septembre 2028 au plus tard[7]. L'art. 57*s*bis al. 2 let. a AP-LOGA[8], s'il entre en vigueur, instaurera une divergence notable entre les règles relatives aux données personnelles et les données relatives aux personnes morales en matière de transfert de données à l'étranger : contrairement

1 Chancellerie fédérale, Cadre juridique de l'utilisation de services d'informatique en nuage public dans l'administration fédérale : Rapport en exécution du jalon 5 de la stratégie d'informatique en nuage du Conseil fédéral, mars 2025, pp. 8 s., disponible à l'adresse https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html (dernière consultation le 8 juillet 2025) ; Michael Montavon, Cyberadministration et protection des données, thèse Fribourg, Genève/Zurich/Bâle 2021, pp. 459 ss.

2 C'est cette idée qu'exprime la phrase humoristique bien connue « *There is no cloud, it's just someone else's computer* » (« il n'y a pas de nuage, c'est juste l'ordinateur de quelqu'un d'autre »).

3 Code pénal suisse du 21 décembre 1937 (RS 311.0).

4 Loi fédérale sur la protection des données personnelles du 25 septembre 2020 (RS 235.1). Comp. art. 5 let. a LPD et art. 3 let. b de l'ancienne Loi fédérale sur la protection des données du 19 juin 1992.

5 Loi sur l'organisation du gouvernement et de l'administration du 21 mars 1997 (RS 172.010).

6 Département fédéral de justice et police, Modification de la loi sur l'organisation du gouvernement et de l'administration (protection des données concernant des personnes morales par les organes fédéraux), Rapport explicatif relatif à l'ouverture de la procédure de consultation, 21 mai 2025, p. 2.

7 Département fédéral de justice et police (nbp. 6), p. 17.

8 Avant-projet de modifiant la Loi sur l'organisation du gouvernement et de l'administration du 21 mai 2025. L'avant-projet est disponible à l'adresse https://cms.news.admin.ch/fileservice/sdweb-docs-prod-nsbcch-files/files/2025/05/21/dd684a5e-9577-4dd8-a239-f71b1946b436.pdf (dernière consultation le 26 août 2025).

à ce qui vaut pour les personnes physiques (voir 4 ci-dessous), il ne sera pas exigé que l'État de destination possède une législation assurant un niveau de protection adéquat pour les données des personnes morales[9]. Les normes spéciales posant des conditions plus strictes en matière de communication à l'étranger (et qui ne concernent pas la question du *niveau de protection assuré par la législation de l'État destinataire*; par exemple les dispositions en matière d'entraide judiciaire) s'appliqueront toutefois également aux personnes morales[10].

2. Sous-traitance

2.1. Introduction

[5] Le recours à une solution d'informatique en nuage constitue en principe un cas de sous-traitance du traitement de données personnelles[11]. Nous présenterons les règles prévues en la matière par la législation fédérale (2.2.1) et les législations cantonales (2.2.2) avant de déterminer si celles-ci permettent l'utilisation d'une solution informatique en nuage (2.3).

2.2. Règles applicables

2.2.1. Au niveau fédéral

[6] Selon l'art. 9 al. 1 LPD, le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou la loi le prévoie et que les conditions suivantes soient réunies : seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui-même (let. a) et aucune obligation légale ou contractuelle de garder le secret ne l'interdit (let. b). L'art. 9 al. 2 LPD précise que le responsable du traitement doit en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données.

2.2.2. Au niveau cantonal

[7] Afin d'avoir un aperçu large des règles cantonales en matière de protection des données, nous avons choisi de présenter les législations des cantons romands (Fribourg, Genève, Jura et Neuchâtel, Valais et Vaud), ains que celles des cantons de Berne, du Tessin et de Zurich.

9 Département fédéral de justice et police (nbp. 6), p. 26 s.

10 Département fédéral de justice et police (nbp. 6), p. 27.

11 Chancellerie fédérale (nbp. 1), pp. 12 et 20; Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 p. 6652; Daniel Dzamko-Locher, in : Sylvain Métille (édit.), L'informatique en nuage, Berne 2022, p. 86. L'EDPB souligne qu'il est important d'identifier les rôles de chaque entité intervenant dans le traitement des données pour s'assurer de respecter la législation en matière de protection des données, en particulier s'agissant des données de télémétrie (EDPB, 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, 17 janvier 2023, pp. 12, 19 et 30, disponible à l'adresse https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf [dernière consultation le 8 juillet 2025]).

[8] Les lois cantonales sur la protection des données prévoient des règles identiques ou similaires à celles de la LPD. Mis à part dans les cantons de Berne[12], du Tessin[13] et de Vaud (où la révision de la législation en matière de protection des données se fait attendre)[14], ces lois contiennent toutefois des spécificités. On peut notamment relever les éléments suivants :

- Fribourg : la LPrD/FR[15] contient quatre dispositions spécifiques (art. 18 à 21 LPrD/FR) en matière de sous-traitance impliquant l'utilisation d'une solution d'informatique en nuage, que la loi nomme « externalisation » (cf. art. 4 al. 1 let. g LPrD/FR). Ces dispositions prévoient, entre autres, que les lieux de traitement doivent être situés en tout temps sur le territoire suisse ou sur le territoire d'un État garantissant un niveau de protection des données adéquat (art. 18 al. 2 LPrD/FR ; ce point est développé ci-dessous, 4.4), que le contrat de sous-traitance doit décrire obligatoirement un certain nombre d'éléments (art. 19 al. 1 let. b LPrD/FR) et que le traitement de données personnelles sensibles et le traitement de données qui font l'objet d'une obligation légale ou contractuelle de garder le secret peuvent être externalisés si la confidentialité à l'égard du sous-traitant est assurée de manière que ce dernier ne puisse avoir accès à leur contenu (art. 21 al. 1 LPrD/FR ; cela signifie que les données doivent être chiffrées[16]) ;
- Genève : l'art. 36C al. 2 et 3 nLIPAD/GE[17] donne des précisions sur la forme et le contenu du contrat de sous-traitance (art. 36C al. 2 et 3 nLIPAD/GE) et autorise la sous-traitance impliquant un transfert de données personnelles uniquement si l'État de destination dispose d'une législation assurant un niveau de protection adéquat conformément à la liste établie par le Conseil fédéral (art. 36C al. 6 nLIPAD/GE ; ce point est développé ci-dessous, 4.4) ;
- Jura et Neuchâtel : l'art. 54 al. 1 let. d CPDT/JUNE[18] prévoit qu'en cas de sous-traitance, les données doivent être traitées uniquement en Suisse, excepté si le traitement n'y est possible qu'à un coût disproportionné ou s'il ne peut être effectué qu'à l'étranger (art. 54 al. 1 let. d CPDT/JUNE ; ce point est développé ci-dessous, 4.4). En outre, selon l'art. 23a al. 1 let. c CPDT/JUNE, tout projet de sous-traitance à l'étranger doit être soumis au préposé pour préavis

12 Cf. art. 16 LCPD/BE (Loi bernoise sur la protection des données du 19 février 1986 [RS/BE 152.04]), qui autorise la sous-traitance (nommée « traitement sur mandat ») sans réellement poser de conditions.

13 Cf. art. 23 P-nLPDP/TI (Disegno di Legge sulla protezione dei dati personali). Le canton du Tessin a entamé il y a plusieurs années déjà un processus de révision de sa loi cantonale sur la protection des données (actuellement : Legge sulla protezione dei dati personali du 9 mars 1987, RS/TI 163.100). Pour plus d'informations sur ce processus législatif, voir https://www4.ti.ch/can/sgcds/pd/generalita/revisione-totale-lpdp [dernière consultation le 23 juillet 2025]).

14 Cf. art. 18 LPrD/VD (Loi vaudoise sur la protection des données personnelles du 11 septembre 2007 [RS/VD 172.65]), qui n'ajoute pas de conditions supplémentaires par rapport à l'art. 9 LPD.

15 Loi fribourgeoise sur la protection des données du 12 octobre 2023 (RS/FR 17.1).

16 Message du Conseil d'État fribourgeois 2023-CE-149 accompagnant le projet de loi sur la protection des données (révision totale) du 26 juin 2023, p. 23.

17 Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (RS/GE A 2 08), dans sa nouvelle version adoptée le 3 mai 2024 (mais non encore entrée en vigueur).

18 Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel des 8 et 9 mai 2012 (RS/NE 150.30).

- Valais : l'art. 29 al. 2 LIPDA/VS[19] donne des précisions sur la forme et le contenu du contrat de sous-traitance ;
- Zurich : l'art. 9 P-nIDG/ZH[20] ne prévoit pas d'obligation de conclure un contrat avec le sous-traitant.

2.3. Discussion

[9] La sous-traitance de données personnelles au fournisseur d'une solution d'informatique en nuage est admissible pour autant que les conditions prévues par la législation en matière de protection des données soient respectées[21].

[10] À cet égard, quelques précisions s'imposent.

[11] La sous-traitance n'étant généralement pas prévue par la loi, un contrat (qui peut prendre la forme d'un contrat séparé, mais aussi de conditions générales ou d'une annexe au contrat principal) devra être conclu avec le sous-traitant – condition qui peut aisément être respectée[22]. Lorsqu'une loi cantonale s'applique, il conviendra de vérifier si celle-ci prévoit des exigences particulières pour ce contrat, par exemple la forme écrite ou un contenu minimal[23].

[12] Dans ce contrat, il est recommandé de prévoir une obligation générale d'assister le responsable du traitement (si possible sans frais supplémentaires) pour répondre aux demandes de personnes concernées[24] et d'autorités ainsi que pour démontrer sa conformité aux exigences légales. En outre, des obligations spécifiques pour le sous-traitant devraient figurer dans le contrat, en particulier qu'il agisse uniquement sur instructions du responsable du traitement, qu'il s'engage à respecter la confidentialité, qu'il supprime et renvoie au responsable du traitement, selon le choix de ce dernier, toutes les données personnelles au terme de la prestation de services, qu'il informe immédiatement en cas de cyberincidents (même s'ils ne concernent pas des données personnelles), qu'il informe dès que possible en cas de demande d'accès d'autorités, etc. On s'assurera également d'avoir accès à la liste des sous-traitants ultérieurs[25] et aux mesures de sécurité,[26] et

19 Loi valaisanne sur l'information du public, la protection des données et l'archivage du 9 octobre 2008 (RS/VS 170.2).

20 Vorlage 5923 Gesetz über die Information und den Datenschutz (IDG). Le canton de Zurich a entamé il y a plusieurs années déjà un processus de révision de sa loi cantonale sur la protection des données (actuellement : Gesetz über die Information und den Datenschutz du 12 février 2007, RS/ZH 170.4). Le projet de loi, avec des propositions de la *Kommission für Staat und Gemeinden* a désormais été soumise au *Staatsrat* zurichois pour adoption (cf. https://www.kantonsrat.zh.ch/geschaefte/geschaeft/?id=bbb4248013ca433eb50e68677eaaecd0 pour plus d'informations sur ce processus législatif [dernière consultation le 23 juillet 2025]).

21 PRIVATIM, Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud, 3 février 2022, p. 7, disponible à l'adresse https://www.privatim.ch/wp-content/uploads/2023/10/privatim_Cloud-Merkblatt_v3_01_20220203_def._FR.pdf (dernière consultation le 8 juillet 2025).

22 L'EDPB relève toutefois qu'il est parfois difficile de négocier les termes du contrat (EDPB [nbp. 11], p. 14).

23 Voir art. 36C al. 2 et 3 nLIPAD/GE ; art. 19 al. 1 let. b LPrD/FR ; art. 29 al. 2 LIPDA/VS. À noter que, selon la Directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (Directive 2016/680), le contrat de sous-traitance doit contenir les éléments mentionnés à l'art. 22 par. 3 Directive 2016/680 et être établi en la forme écrite, y compris la forme électronique (art. 22 par. 4 Directive 2016/680) (CR LPD-Métille, art. 9 N 41).

24 PRIVATIM (nbp. 21), p. 3.

25 Sur la difficulté à obtenir des informations spécifiques à cet égard, voir EDPB (nbp. 11), pp. 15 s.

26 PRIVATIM (nbp. 21), p. 7

on prendra garde au for et au droit applicable au contrat[27]. Enfin, il est judicieux de prévoir une clause rappelant que le sous-traitant, en sa qualité d'auxiliaire, est soumis au secret de fonction et qu'il s'engage à le respecter[28].

[13] L'exigence selon laquelle seuls les traitements que le responsable du traitement serait en droit d'effectuer lui-même peuvent faire l'objet d'une sous-traitance ne pose pas de problème non plus. On rappellera qu'une collectivité publique doit en principe se fonder sur une base légale pour traiter des données personnelles[29], mais la base légale ne doit pas envisager spécifiquement la sous-traitance. Soulignons également qu'en cas de sous-traitance, le responsable du traitement reste responsable de la protection des données personnelles[30]. À cela s'ajoute – par analogie avec les art. 55 et 101 CO – qu'il doit choisir avec soin ses sous-traitants, leur donner des instructions adéquates et les surveiller de manière appropriée[31].

[14] La dernière condition exige qu'aucune obligation légale ou contractuelle de garder le secret n'interdise la sous-traitance. S'agissant des obligations légales de garder le secret, en particulier du secret de fonction (art. 320 CP) et du secret professionnel (art. 321 CP), elles sont développées ci-dessous (3). Quant aux engagements contractuels, il est nécessaire de les examiner au cas par cas.

[15] Au surplus, on relèvera que la loi fribourgeoise pose plusieurs exigences supplémentaires par rapport au droit fédéral (cf. art. 18 ss LPrD/FR), auxquelles les collectivités publiques fribourgeoises devront prendre garde en cas de recours à une solution d'informatique en nuage. Il n'y a rien de problématique dans ces règles, étant précisé que la question de la limitation du traitement au territoire suisse ou au territoire d'un État garantissant un niveau de protection des données adéquat est développée ci-dessous (4.4).

3. Secret professionnel et secret de fonction

3.1. Introduction

[16] Comme exposé ci-dessus (2.2), la plupart des règles fédérales et cantonales en matière de protection des données posent, comme condition à la sous-traitance, qu'aucune obligation de garder le secret n'interdise celle-ci. Cette exigence mérite quelques développements, raison pour laquelle elle est traitée ici séparément.

---

27 Préposé cantonal à la protection des données et à la transparence du canton de Genève, Fiche info « Informatique en nuage », 11 décembre 2023, p. 9, disponible à l'adresse www.ge.ch/document/fiche-info-du-ppdt-informatique-nuage-enjeux-risques (dernière consultation le 8 juillet 2025).

28 PRIVATIM (nbp. 21), p. 3 ; Préposé cantonal à la protection des données et à la transparence du canton de Genève (nbp. 28), p. 9 ; voir également ci-dessous, 3.3.

29 Voir art. 34 LPD ; art. 5 LPrD/FR ; art. 36 nLIPAD/GE ; art. 16 CPDT/JUNE ; art. 17 LIPDA/VS ; art. 5 LPrD/VD.

30 Art. 19 al. 1 LPrD/FR ; art. 36C al. 5 nLIPAD/GE ; art. 54 al. 2 CPDT/JUNE. Précisons qu'il s'agit d'un principe général, qui s'applique également en l'absence de disposition en ce sens (notamment dans le cadre de la LPD ; voir CR LPD-Métille, art. 9 N 69).

31 Chancellerie fédérale (nbp. 1), p. 19 ; Sylvain Métille, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019, p. 617 ; CR LPD-Métille, art. 9 N 71 ; Dzamko-Locher (nbp. 11), p. 87 ; Esther Zysset, Der behördliche Gang in die Cloud – Betrachtungen zur Auslagerung im öffentlichen Sektor Datenschutz, Amtsgeheimnis, Steuergeheimnis, Jusletter 23 septembre 2024, Rz. 14. À noter que l'art. 19 al. 1 let. a LPrD/FR prévoit expressément cette règle.

[17] La question de savoir si une obligation de garder le secret s'oppose à la sous-traitance se pose immanquablement dans le domaine public, car les employés travaillant pour des autorités sont soumis au secret de fonction (art. 320 CP). Suivant les circonstances, ils peuvent aussi être soumis au secret professionnel (art. 321 CP ; par exemple les médecins exerçant dans un hôpital public).

3.2. Règles applicables

[18] La disposition topique protégeant le secret de fonction est l'art. 320 CP, qui prévoit que quiconque révèle un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il a eu connaissance à raison de sa charge ou de son emploi ou en tant qu'auxiliaire d'une autorité ou d'un fonctionnaire, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (ch. 1).

[19] Le secret professionnel est quant à lui protégé par l'art. 321 CP, qui dispose que les ecclésiastiques, avocats, défenseurs en justice, notaires, conseils en brevet, contrôleurs astreints au secret professionnel en vertu du code des obligations, médecins, dentistes, chiropraticiens, pharmaciens, sages-femmes, psychologues, infirmiers, physiothérapeutes, ergothérapeutes, diététiciens, optométristes, ostéopathes, ainsi que leurs auxiliaires, qui révèlent un secret à eux confié en vertu de leur profession ou dont ils ont eu connaissance dans l'exercice de celle-ci, sont, sur plainte, punis d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire (ch. 1).

3.3. Discussion

[20] S'agissant du secret professionnel, le Conseil fédéral considère que, lorsque le sous-traitant doit être qualifié d'auxiliaire au sens de l'art. 321 CP, la condition de l'art. 9 al. 1 let. b LPD (aucune obligation légale ou contractuelle de garder le secret n'interdit la sous-traitance) est respectée[32].

[21] La question de savoir si les fournisseurs de services informatiques en nuage doivent être qualifiés d'auxiliaires en matière de secret professionnel a récemment été résolue par le Tribunal fédéral. Ainsi, dans l'ATF 145 II 229, il indique que « [d]oivent aussi être considérées comme auxiliaires les personnes extérieures à l'étude, auxquelles l'avocat confie des tâches, comme par exemple [...] » le professionnel externe chargé de la conservation et de la protection à distance des données informatiques de l'avocat[33].

[22] Pendant longtemps, la situation en matière de secret de fonction était plus incertaine. En effet, jusqu'au 31 décembre 2022, l'art. 320 CP, relatif au secret de fonction, ne soumettait pas les auxiliaires au secret de fonction. De ce fait, le raisonnement exposé ci-dessus en lien avec le secret professionnel ne pouvait pas être repris en matière de secret de fonction, sauf en considérant, par analogie, que le secret de fonction s'appliquait également aux auxiliaires[34].

---

32 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 p. 6651 ; *contra* : Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB) / Externalisation du traitement des données et secret professionnel (art. 321 CPS), Zurich 2016, pp. 53 ss.

33 ATF 145 II 229, consid. 7.3.

34 Métille (nbp. 31), p. 613.

[23] La situation a été clarifiée avec l'entrée en vigueur, le 1er janvier 2023, du nouvel art. 320 CP. Celui-ci prévoit désormais la punissabilité des auxiliaires. Le Message du Conseil fédéral relatif à la modification de l'art. 320 CP souligne que l'ajout des auxiliaires dans le cercle des personnes soumises au secret de fonction a pour but de permettre à l'administration de recourir à des auxiliaires externes du domaine des technologies de l'information et de la communication[35].

[24] Dès lors qu'un sous-traitant doit être qualifié d'auxiliaire au sens de l'art. 320 CP, il est également soumis à l'obligation de respecter le secret de fonction[36] (ce qui implique aussi que celui qui partage un secret avec cet auxiliaire n'est pas punissable[37]).

[25] Selon la Conseillère fédérale Karin Keller Sutter, c'est aussi le cas si le sous-traitant se trouve dans un État tiers ; elle considère que l'art. 320 CP s'applique également à un prestataire de services à l'étranger. Dans sa réponse à la Question Porchet 22.7249, elle a expliqué le 14 mars 2022 que « selon [l'ancien droit], les fournisseurs de services TIC externes à l'administration n'[étaient] en principe pas considérés comme des fonctionnaires de fait, ceci selon l'art. 110 ch. 3 CP. Dès lors, ils [n'étaient] pas tenus de garder les secrets de fonction qu'ils dét[enaient] dans l'exercice de leur activité, selon l'art. 320 ch 1 CP. Considérant que le droit [...] était lacunaire sur ce point, le Parlement a modifié l'art. 320 CP. [...] Les auxiliaires [peuvent maintenant] également répondre de violation du secret de fonction. Cette révision [...] s'appliqu[e] également à un prestataire de services TIC à l'étranger. Le Conseil fédéral est conscient du fait que la mise en œuvre du droit pénal suisse contre un prestataire à l'étranger peut se heurter à des difficultés pratiques. Cela étant dit, dans le cadre du droit futur comme du droit actuel, il appartiendra aux tribunaux de juger au cas par cas s'il y a ou non infraction à l'art. 320 CP »[38].

[26] Vu ce qui précède, en particulier la modification récente de l'art. 320 CPet la clarification du Conseil fédéral, on ne saurait désormais soutenir que le secret de fonction ou le secret professionnel s'oppose à ce que les collectivités publiques suisses fassent appel à des sous-traitants fournissant des solutions d'informatique en nuage, même s'ils se situent à l'étranger[39].

[27] Le Délégué à la transformation numérique et à la gouvernance de l'informatique va également dans ce sens : il indique que des données couvertes par une obligation de garder le secret peuvent être stockées dans un nuage public à condition que des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissant le respect du droit applicable soient prises[40]. La mention de la qualité d'auxiliaire devrait être une mesure contractuelle suffisante, qui peut être éventuellement complétée par une pénalité contractuelle en cas de violation de la confidentialité. Quant aux mesures techniques et organisationnelles, ce sont celles qui sont déjà exigées sous l'angle du principe et de l'obligation de sécurité.

[28] Au niveau fédéral, la Chancellerie fédérale souligne cependant que « [l]'accès du fournisseur de services en nuage à des données soumises au secret de fonction doit, dans le cadre d'une

35 Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 pp. 2886 ss.

36 Préposé cantonal à la protection des données et à la transparence du canton de Genève (nbp. 27), p. 2.

37 Chancellerie fédérale (nbp. 1), p. 28.

38 BO 2022 N 353 s.

39 La Chancellerie fédérale souligne les risques en cas d'auxiliaire situé à l'étranger, sans toutefois en tirer de conclusion juridique (Chancellerie fédérale [nbp. 1], p. 29).

40 Délégué à la transformation numérique et à la gouvernance de l'informatique, AR010 – Principes relatifs à l'informatique en nuage de l'administration fédérale, 13 mars 2025, p. 14, disponible à l'adresse https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html (dernière consultation le 8 juillet 2025), pp. 16, 18 et 20.

externalisation dans le nuage, être limité de manière appropriée, voire rendu aussi étroit que possible par des mesures contractuelles, organisationnelles et techniques »[41]. Cette règle semble toutefois plutôt résulter de l'art. 12 let. a ONum[42] et du principe de proportionnalité ancré à l'art. 6 al. 2 LPD que de la règlementation en matière de secret de fonction.

[29] Les sous-traitants ne sont toutefois pas toujours conscients de leur obligation de respecter le secret de fonction. Pour cette raison, il est opportun de prévoir une clause à ce sujet dans le contrat de sous-traitance, indiquant que le sous-traitant est soumis au secret de fonction et qu'il s'engage à le respecter[43]. L'absence d'une telle clause pourrait constituer une violation de l'obligation d'instruire du responsable du traitement, mais pas une violation du secret de fonction car la qualité d'auxiliaire n'en dépend pas[44].

[30] Enfin, on soulignera que les auxiliaires des auxiliaires doivent aussi être qualifiés d'auxiliaires au sens de l'art. 321 CP[45].

4. Transfert de données personnelles à l'étranger

4.1. Introduction

[31] Le recours à un logiciel en nuage entraîne régulièrement un transfert de données personnelles à l'étranger[46]. Après quelques explications sur les situations impliquant un transfert à l'étranger (4.2), nous exposerons les règles fédérales (4.3) et cantonales (4.3.2) en la matière et examinerons si celles-ci autorisent le recours à l'informatique en nuage (4.4).

4.2. Cas de transferts à l'étranger

[32] En cas d'utilisation d'une solution d'informatique en nuage, un transfert à l'étranger a lieu si le sous-traitant a son siège dans un État tiers[47]. Dans ce cas, si le sous-traitant a accès aux données, il y accédera depuis l'État où il se situe (p. ex. pour des prestations d'assistance[48]). Il peut en particulier arriver que les données personnelles soient hébergées en Suisse, mais que le distributeur de la solution informatique – avec qui le contrat est conclu – se trouve à l'étranger. En outre, il y a également transfert à l'étranger si les données sont stockées dans des serveurs situés

41 Chancellerie fédérale (nbp. 1), p. 28.

42 Cf. 6.2 ci-dessous.

43 Préposé cantonal à la protection des données et à la transparence du canton de Genève (nbp. 27), p. 9 ; voir également ci-dessus, 2.3.

44 Voir Métille (nbp. 31), p. 614.

45 Frédéric Erard, Le secret médical : Étude des obligations de confidentialité des soignants en droit suisse, Thèse Neuchâtel, Zurich 2021, N 398

46 Dzamko-Locher (nbp. 11), pp. 86 s. Sur les situations impliquant un transfert de données personnelles à l'étranger, voir également, s'agissant du RGPD, EDPB, Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD, Version 2.0, 14 février 2023, disponible à l'adresse https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_fr.pdf (dernière consultation le 8 juillet 2025). Ces lignes directrices mettent en évidence le fait qu'un transfert de données personnelles à l'étranger ne peut avoir lieu que si les données sont communiquées à une entité distincte (N 20).

47 Téo Genecand, in : Yaniv Benhamou/Bertil Cottier (édit.), Petit commentaire LPD, Bâle 2023, art. 16 N 15.

48 PRIVATIM (nbp. 21), nbp. 7.

dans un État tiers[49] (qui peuvent être des serveurs fournis par des sous-traitants ultérieurs), car les données sont communiquées à une autre personne dans un État tiers[50].

[33] À lire la prise de position du Préposé fédéral à la protection des données et à la transparence (PFPDT) du 13 mai 2022 concernant l'utilisation de M365 par la SUVA,[51] qu'il faudrait également considérer que, lorsque la maison mère du sous-traitant se trouve aux États-Unis, il y a un transfert de données personnelles vers les États-Unis. Cette situation, qui concerne spécifiquement les États-Unis, découlerait du fait qu'une loi américaine – le U.S. CLOUD ACT[52] – permet d'obliger les fournisseurs de services informatiques ayant un lien avec les États-Unis à transmettre des données aux autorités américaines dans le contexte de procédures pénales relatives à des crimes graves[53]. Le simple fait qu'un accès aux données – via la société mère de Microsoft – soit théoriquement possible dans des cas très limités suffirait à considérer qu'un transfert de données personnelles vers les États-Unis a lieu. Le PFPDT n'a aucunement développé son raisonnement et on ne discerne pas s'il s'agit d'un raccourci erroné, d'une situation particulière au cas traité ou d'une généralisation du PFPDT. Cet avis ne fait d'ailleurs pas l'unanimité et de nombreux auteurs de doctrine considèrent qu'une telle situation n'entraîne pas de communication de données personnelles aux États-Unis[54]. À notre sens, la doctrine doit être suivie. Le seul fait que les autorités américaines puissent éventuellement, dans des circonstances spécifiques, avoir accès à des données personnelles stockées hors des États-Unis n'est qu'une situation théorique et on ne saurait considérer qu'il s'agit d'un transfert de données personnelles à l'étranger. Nous n'avons d'ailleurs pas connaissance d'une application du U.S. CLOUD ACT a une société européenne du seul fait qu'elle serait économiquement détenue par une société américaine qui n'a aucun accès aux données concernées dans le cadre de son activité. En outre, avec l'entrée en vigueur du Swiss-U.S. DPF[55] (cf. 4.4 ci-dessous), ce débat a perdu toute portée.

---

49 Philipp Fischer, in : Meier Philippe/Métille Sylvain (édit.), Commentaire romand LPD, Bâle 2023, art. 16 N 129 ; Genecand (nbp. 47), art. 16 N 15.

50 Voir notamment EDPB (nbp. 46), N 15 ss.

51 PFPDT, Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace « M365 », 13 mai 2022, disponible à l'adresse https ://www.edoeb.admin.ch/de/13062022-auslagerung-von-personendaten-durch-die-suva-in-eine-microsoft-cloud (dernière consultation le 8 juillet 2025).

52 Clarifying Lawful Overseas Use of Data Act, disponible à l'adresse https://www.congress.gov/bill/115th-congress/senate-bill/2383/text (dernière consultation le 8 juillet 2025). Le U.S. CLOUD Act est une modification d'une autre loi, le Stored Communications Act (SCA).

53 Sur la portée concrète du Cloud Act, voir notamment OFJ, Rapport sur le US CLOUD Act (loi Cloud), 17 septembre 2021, p. 6 ss, disponible à l'adresse https ://www.bj.admin.ch/dam/bj/fr/data/publiservice/publikationen/berichte-gutachten/gutachten/2021-09-17-us-cloud-act.pdf.download.pdf/2021-09-17-us-cloud-act.pdf (dernière consultation le 22 juillet 2025) ; Justin Hemmings/Sreenidhi Srinivasan/Peter Swire, Defining the Scope of « Possession, Custody, or Control » for Privacy Issues and the CLOUD Act, Journal of National Security Law and Policy 10/2020, p. 631 ss, pp. 631–675.

54 Fischer (nbp. 49), art. 16 N 157 ; Genecand (nbp. 47), art. 16 N 17 ; Sylvain Métille, L'utilisation de Microsoft 365, illégale en Suisse ? Blog smetille.ch, 17 juin 2022, disponible à l'adresse https://smetille.ch/2022/06/17/lutilisation-de-microsoft-365-illegale-en-suisse/ (dernière consultation le 8 juillet 2025).

55 Swiss-U.S. Data Privacy Framework Principles, qui constitue un cadre garantissant la sécurité des échanges de données personnelles entre la Suisse et les entreprises certifiées aux États-Unis.

4.3. Règles applicables

4.3.1. Au niveau fédéral

[34] L'art. 16 al. 1 LPD autorise le transfert de données personnelles à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat.

[35] La liste établie par le Conseil fédéral figure à l'Annexe 1 de l'OPDo[56] et contient les États suivants : Allemagne, Andorre, Argentine, Autriche, Belgique, Bulgarie, Canada, Chypre, Croatie, Danemark, Espagne, Estonie, États-Unis (pour les données personnelles traitées par les organisations certifiées conformément aux principes du Swiss-U.S. Data Privacy Framework ; nous y reviendrons ci-dessous), Finlande, France, Gibraltar, Grèce, Guernesey, Hongrie, Île de Man, Îles Féroé, Irlande, Islande, Israël, Italie, Jersey, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monaco, Norvège, Nouvelle-Zélande, Pays-Bas, Pologne, Portugal, Tchéquie, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Uruguay.

[36] S'agissant en particulier des États-Unis, ils sont reconnus depuis le 15 septembre 2024 comme offrant un niveau de protection adéquat pour les données personnelles traitées par les organisations certifiées[57] conformément aux principes du cadre de protection des données entre la Suisse et les États-Unis (Swiss-U.S. Data Privacy Framework)[58].

[37] Il est néanmoins souvent fait mention des risques liés à l'U.S. CLOUD Act ainsi qu'au FISA[59].[60] À ce sujet, l'Office fédéral de la justice a procédé à une analyse approfondie des accès aux données personnelles transférées depuis la Suisse par les autorités publiques aux États-Unis[61]. Il est arrivé à la conclusion que « lorsque les autorités d'application du droit pénal ou les autorités de sécurité nationale des États-Unis accèdent à des données personnelles transférées depuis la Suisse vers des organisations certifiées [dans le cadre du Swiss-U.S. DPF], un cadre juridique est en place, définissant les conditions dans lesquelles l'accès peut avoir lieu et garantissant que cet accès et l'utilisation ultérieure des données sont limités à ce qui est nécessaire et proportionné à l'objectif d'intérêt public poursuivi. Ces garanties peuvent être invoquées par les personnes concernées grâce aux voies de droit offertes et sont ainsi effectives »[62]. Ces garanties ressortent notamment du Swiss-U.S. DPF, du Décret exécutif 14086 du 7 octobre 2022[63], du Règlement sur

---

56 Ordonnance sur la protection des données du 31 août 2022 (RS 235.11).

57 La liste est disponible à l'adresse https://www.dataprivacyframework.gov/list.

58 Ce niveau de protection adéquat a été reconnu en vertu des garanties octroyées par le décret exécutif 14086 du 7 octobre 2022, par le Règlement du 7 octobre 2022 sur la cour d'examen en matière de protection des données du procureur général des États-Unis, par la Directive 126 de la communauté du renseignement (procédures de mise en œuvre pour le mécanisme de recours en matière de renseignement selon le décret exécutif 14086) établie par le bureau de la directrice du renseignement national le 6 décembre 2022 et par la désignation de la Suisse le 7 juin 2024 en tant qu'État bénéficiant du mécanisme de recours à deux niveaux comprenant l'accès à la cour d'examen en matière de protection des données.

59 Foreign Intelligence Surveillance Act, disponible à l'adresse https://www.law.cornell.edu/uscode/text/50/chapter-36 (dernière consultation le 8 juillet 2025). La section 702 du FISA autorise l'*Attorney General* et le *Director of National Intelligence* à collecter des renseignements concernant des personnes situées hors des États-Unis.

60 Chancellerie fédérale (nbp. 1), p. 23.

61 OFJ, Évaluation de l'adéquation – États-Unis, 30 avril 2024, disponible à l'adresse https://www.newsd.admin.ch/newsd/message/attachments/89020.pdf (dernière consultation le 8 juillet 2025).

62 OFJ (nbp. 61), pp. 31 s. Voir également Zysset (nbp. 31), N 36, qui mentionne que le U.S. CLOUD Act ne joue plus de rôle s'agissant des entreprises américaines certifiées selon le Swiss-U.S. Data Privacy Framework.

63 https://www.state.gov/executive-order-14086-policy-and-procedures (dernière consultation le 8 juillet 2025).

la cour d'examen en matière de protection des données du procureur général des États-Unis (U.S. Attorney General) publié le 7 octobre 2022[64] , de la Directive 126 de la communauté du renseignement établie par l'ODNI le 6 décembre 2022[65], ainsi que de la Désignation de la Suisse le 7 juin 2024 en tant qu'État bénéficiant du mécanisme de recours à deux niveaux comprenant l'accès à la cour d'examen en matière de protection des données (« *Qualifying State* »)[66]. Il n'y a donc plus besoin de mettre en place des clauses contractuelles types et de réaliser une « Analyse d'impact des transferts des données » (AITD)[67] avant un transfert aux États-Unis[68].

[38] Si l'État de destination ne figure pas dans cette liste, un transfert reste possible si l'une des garanties listées à l'art. 16 al. 2 LPD permet d'assurer un niveau de protection adéquat (notamment des clauses contractuelles type) ou si l'une des dérogations mentionnées à l'art. 17 al. 1 LPD s'applique.

4.3.2. Au niveau cantonal

[39] Certains cantons ont prévu des exigences identiques ou très similaires à la LPD pour le transfert de données personnelles à l'étranger (transfert autorisé si l'État figure dans la liste des États reconnus par le Conseil fédéral comme disposant d'une législation assurant un niveau de protection adéquat, si une garantie permet d'assurer un niveau de protection adéquat ou si une dérogation s'applique). C'est le cas des cantons de Berne[69], du Tessin[70], du Valais[71], de Vaud[72] et de Zurich[73].

[40] D'autres cantons sont plus restrictifs. Ainsi, dans les cantons de Fribourg et de Genève, un transfert à l'étranger n'est possible que si l'État de destination dispose d'une législation assurant un niveau de protection adéquat (art. 18 al. 2 LPrD/FR et art. 36C al. 6 nLIPAD). Dans les cantons du Jura et de Neuchâtel, la sous-traitance impliquant un transfert à l'étranger n'est admissible que si le coût d'un traitement en Suisse est disproportionné ou si le traitement ne peut être effectué qu'à l'étranger[74]. En outre, dans ces deux cantons, le responsable du traitement a l'obligation de

64 https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court (dernière consultation le 8 juillet 2025).

65 https ://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf (dernière consultation le 8 juillet 2025).

66 https://www.justice.gov/opcl/media/1355326/dl?inline (dernière consultation le 8 juillet 2025) et https://www.justice.gov/opcl/executive-order-14086 (dernière consultation le 8 juillet 2025).

67 L'AITD, appelée *Transfer Impact Assessment* (« TIA ») en anglais, vise à déterminer si un transfert de données personnelles vers un pays non adéquat se basant sur des clauses contractuelles types est autorisé, le cas échéant avec des mesures supplémentaires. Le PFPDT a publié un guide permettant de procéder à cette analyse (https ://backend.edoeb.admin.ch/fileservice/sdweb-docs-prod-edoebch-files/files/2024/11/29/ffb21a6a-7be0-4b34-b65a-10cea151985f.pdf [dernière consultation le 24 juillet 2025]). Le guide de la Commission Nationale de l'Informatique et des Libertés (CNIL), qui est l'autorité de contrôle française en matière de données personnelles, est toutefois plus détaillé. Il est disponible à l'adresse https ://www.cnil.fr/fr/analyse-dimpact-des-transferts-des-donnees-la-cnil-publie-la-version-finale-de-son-guide-aitd (dernière consultation le 24 juillet 2025).

68 Katharina Martin/Philipp Fischer, Swiss-US Data Privacy Framework : un premier pas vers une approche plus pragmatique ? 17 janvier 2025, disponible à l'adresse www.swissprivacy.law/332 (dernière consultation le 8 juillet 2025).

69 Art. 14a LCPD/BE.

70 Art. 20 P-nLPDP/TI.

71 Art. 25 LIPDA/VS.

72 Art. 17 LPrD/VD.

73 Art. 36 P-nIDG/ZH.

74 Art. 54 al. 1 let. c CPDT/JUNE.

soumettre les projets de sous-traitance à l'étranger au préposé à la protection des données et à la transparence (art. 23a al. 1 let. c CPDT/JUNE). On peut se demander si ces règles, qui restreignent le transfert vers des pays adéquats, sont compatibles avec le droit supérieur, en particulier la Convention 108, qui est en vigueur pour la Suisse depuis 1998[75]. Cette question est examinée ci-dessous.

4.4. Discussion

[41] Au niveau fédéral, ainsi que dans les cantons de Berne, du Tessin, du Valais, de Vaud et de Zurich, un traitement de données personnelles effectué à l'aide d'une solution d'informatique en nuage impliquant une communication de données personnelles à l'étranger ne répond pas à des conditions spécifiques : les règles sur le transfert à l'étranger s'appliquent. Pour autant que celles-ci soient respectées, le recours à un outil informatique impliquant une communication de données personnelles hors de Suisse est admissible.

[42] Par ailleurs, depuis que la Suisse a été reconnue par les États-Unis comme un *Qualifying State* et que le Swiss-U.S. DPF s'applique, il n'est plus nécessaire de recourir à des garanties contractuelles comme les clauses contractuelles types en cas de transfert de données personnelles vers une entreprise certifiée établie aux États-Unis[76]. La Chancellerie fédérale estime tout de même que des mesures de sécurité additionnelles devraient être mises en place en raison du risque d'accès par les autorités américaines[77]. Cette conception ne peut toutefois plus être soutenue, car elle ne repose pas sur des exigences légales et reviendrait à priver le Swiss-U.S. DPF de sa portée.

[43] Soulignons que la question du transfert à l'étranger se pose en pratique pour des outils dont l'utilisation implique le plus souvent un transfert de données personnelles vers un pays de l'Espace économique européen ou vers une entreprise américaine certifiée selon le Swiss-U.S. DPF[78]. Dans ces cas-là, le transfert est admissible, car il s'agit d'États disposant d'une législation assurant un niveau de protection adéquat. Lorsque le pays de destination ne dispose pas d'une telle législation, déterminer si un transfert est autorisé – par exemple sur la base de clauses contractuelles types – est moins évident et les autorités de protection des données ne fournissent aucune liste de pays pour lesquels des garanties contractuelles sont ou pas suffisantes. De telles garanties ne suffisent pas toujours, notamment lorsque l'État est caractérisé par une forte surveillance étatique (l'Inde ou la Chine par exemple)[79]. Un examen au cas par cas à l'aide d'une AITD[80] est donc nécessaire[81]. On relèvera néanmoins que des clauses contractuelles types de-

75 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (RS 0.235.1).

76 Chancellerie fédérale (nbp. 1), p. 25 ; Martin/Fischer (nbp. 68).

77 Chancellerie fédérale (nbp. 1), p. 25. La *Kantonale Fachstelle für Datenschutz* du canton de Saint-Gall estime également que M365 ne peut être utilisé pour traiter des données personnelles que si celles-ci sont chiffrées, en raison du risque d'accès aux informations par les autorités américaines (Bericht der kantonalen Fachstelle für Datenschutz, 4 mars 2025, p. 7). Le *Datenschutzbeauftragte des Kantons Zurich* partage cet avis s'agissant des données soumises au secret professionnel ou au secret de fonction (Datenschutzbeauftragte des Kantons Zurich, Leitfaden : Microsoft 365 in Gemeinden, p. 49

78 Microsoft Corporation fait notamment partie des entreprises certifiées.

79 PRIVATIM (nbp. 21), p. 4.

80 Sur la notion d'AITD, voir nbp. 67 ci-dessus.

81 Voir PFPDT, Guide pour l'examen de la licéité de la communication transfrontière de données (art. 16, al. 2, let. b et d, LPD), publié en juin 2021 et adapté en mai 2023 ; voir également EDPB (nbp. 11), pp. 17 ss ; Zysset

vraient être suffisantes pour un transfert vers une entreprise américaine non certifiée, et ce grâce au cadre juridique désormais en place entre la Suisse et les États-Unis[82].

[44] Comme exposé ci-dessus (4.3.2), les cantons de Fribourg, Genève, Jura et Neuchâtel ont prévu des règles plus strictes en matière de transfert à l'étranger. La question de leur conformité au droit supérieur – à savoir la Convention 108 – se pose donc.

[45] Selon l'art. 4 par. 1 Convention 108, les parties à la Convention 108 doivent prendre, dans leur droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données figurant dans la Convention 108. Cet instrument concerne tant le secteur privé que le secteur public[83] et s'applique aux cantons.

[46] En matière de transferts à l'étranger, l'art. 12 par. 2 Convention 108 prévoit qu'une partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre partie. Une partie à la Convention 108 peut toutefois déroger à cette règle dans deux cas :

- si sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre partie apporte une protection équivalente (art. 12 par. 3 let. a Convention 108) ; ou
- lorsque le transfert est effectué à partir de son territoire vers le territoire d'un État non contractant par l'intermédiaire du territoire d'une autre partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la partie visée au début du présent paragraphe (art. 12 par. 3 let. b Convention 108).

[47] Précisons que la Convention 108+, récemment ratifiée par la Suisse mais pas encore entrée en vigueur, prévoit une règle similaire[84]. En outre, elle autorise (mais n'oblige pas) les parties à permettre, à certaines conditions, un transfert de données personnelles vers des États qui ne sont pas parties à la Convention 108+ (art. 12 par. 2 à 4 Convention 108+).

[48] Il en résulte que l'art. 18 al. 2 LPrD/FR et l'art. 36C al. 6 nLIPAD – qui autorisent le transfert de données personnelles uniquement si l'État de destination est jugé adéquat – sont admissibles au regard de la Convention 108. Il convient toutefois de relever que la liste des États établie par le Conseil fédéral à l'Annexe 1 de l'OPDo – à laquelle se réfèrent les législations fribourgeoise[85]

(nbp. 31), N 24 ss. Notons que le Contrôleur européen de la protection des données (CEPD) a rendu une décision le 8 mars 2024 dans laquelle il a retenu – entre autres – que les institutions européennes, en utilisant Microsoft 365, ne respectaient pas les règles sur le transfert à l'étranger vers des États ne disposant d'une législation assurant un niveau de protection adéquat (EDPS investigation into use of Microsoft 365 by the European commission [case 2021–0518], Decision, 8 March 2024, https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf [dernière consultation le 8 juillet 2025]). Cette décision très exigeante et quasi impossible à respecter en pratique fait actuellement l'objet de deux actions en annulation différentes devant la Cour de justice de l'Union européenne (CJUE), l'une de la Commission européenne (Affaire T-262/24) et l'autre de Microsoft Ireland Operations (Affaire T-265/24).

82 Martin/Fischer (nbp. 68) (qui considèrent toutefois qu'un TIA est nécessaire).

83 Art. 3 par. 1 Convention 108.

84 Art. 4 par. 1 Convention 108+ ; voir également Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 p. 6617.

85 Art. 15 al. 1 LPrD/FR.

et genevoise[86] – ne se recoupe pas entièrement avec la liste des États ayant ratifié la Convention 108[87].

[49] Quant à la règle posée par l'art. 54 al. 1 let. d CPDT/JUNE, elle n'est pas conforme à la Convention 108, car elle n'autorise le transfert à l'étranger – que l'État de destination soit partie à la Convention 108 ou non – que de manière très restrictive, à savoir uniquement si le coût d'un traitement en Suisse est disproportionné ou si le traitement ne peut être effectué qu'à l'étranger. Il s'agit donc d'une forte limitation au transfert de données vers des États parties à la Convention 108.

[50] Soulignons également que, dans un tableau comparatif annexé au rapport explicatif relatif à CPDT/JUNE révisée[88] , il est indiqué au sujet de l'art. 54 al. 1 let. d CPDT/JUNE que « [s]elon la doctrine, un traitement de données personnelles soumises au secret de fonction est susceptible de constituer une infraction pénale. Il n'est possible d'imposer le respect de ce secret qu'aux sous-traitants déployant leur activité en Suisse ». L'art. 54 al. 1 let. d CPDT/JUNE a été adopté en 2022[89] – soit avant la modification de l'art. 320 CP relatif au secret de fonction – et la situation a depuis lors changé (la sous-traitance à l'étranger est désormais considérée comme respectant le secret de fonction ; voir ci-dessus,3.3). De ce fait, la raison ayant conduit à l'adoption de l'art. 54 al. 1 let. d CPDT/JUNE n'est plus actuelle et plus justifiée. Le législateur devrait donc corriger la CPDT/JUNE rapidement.

[51] La Convention 108 est contraignante pour les États qui y sont parties[90], qui doivent donc incorporer dans leur législation les règles qu'elle contient[91]. Toutefois, elle n'est pas « *self executing* » : aucun droit individuel n'en découle[92], de sorte qu'un citoyen ne peut l'invoquer. Par analogie avec la jurisprudence rendue par le Tribunal fédéral en matière de contrôle abstrait des lois[93], on pourrait toutefois considérer qu'une règle de droit cantonal incompatible avec une norme hiérarchiquement plus élevée doit être interprétée de manière conforme au droit supérieur. Dans le cas présent, on pourrait considérer qu'un traitement en Suisse a un coût disproportionné au sens de l'art. 54 al. 1 let. d CPDT/JUNE dès le moment où une solution informatique adaptée est proposée par un fournisseur se trouvant à l'étranger dans un pays considéré comme adéquat. La

86 Art. 36C al. 6 nLIPAD.

87 Cette liste figure sur la page https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (dernière consultation le 8 juillet 2025). D'une part, quelques pays reconnus dans l'OPDo comme offrant un niveau de protection adéquat n'ont pas ratifié la Convention 108, par exemple le Canada, Israël ou la Nouvelle-Zélande. D'autre part, plusieurs États ayant ratifié la Convention 108, comme le Mexique, le Maroc, le Sénégal, la Tunisie ou la Russie, ne sont pas reconnus comme offrant un niveau de protection adéquat (ni par le Conseil fédéral, ni par la Commission européenne). À noter que, même si la Russie ne fait plus partie du Conseil de l'Europe et n'est plus partie à la Convention européenne des droits de l'Homme depuis 2022, elle reste partie à la Convention 108 en qualité d'État non-membre du Conseil de l'Europe.

88 Rapport explicatif à l'appui du projet de révision partielle de la convention intercantonale relative à la protection des données et à la transparence dans les cantons du jura et de Neuchâtel [CPDT-JUNE], annexe : tableau comparatif avec commentaires, p. 35, disponible à l'adresse (dernière consultation le 8 juillet 2025).

89 BGC NE 2021-2022 Tome 7, p. 367.

90 Voir la page https://www.edoeb.admin.ch/fr/08092023-la-suisse-ratifie-la-convention-108 (dernière consultation le 8 juillet 2025).

91 Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, p. 9.

92 Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, p. 9 ; voir également Sylvain Métille, Swiss Information Privacy Law and the Transborder Flow of Personal Data, JICLT, Vol. 8, No. 1, 2013, pp. 71 ss, p. 74.

93 Voir ATF 149 I 248 consid. 3.3 et les références citées.

notion de coût disproportionné ne doit pas seulement prendre en compte les coûts de licence, mais également les coûts humains engendrés par la migration vers une autre solution ou l'utilisation d'une solution moins performante.

5. Analyse d'impact

5.1. Introduction

[52] Le recours à une solution d'informatique en nuage peut parfois entraîner l'obligation de procéder à une analyse d'impact relative à la protection des données personnelles (« AIPD »). Après une présentation des règles fédérales (5.2.1) et cantonales (5.2.2) relatives à cette obligation, nous exposerons comment celles-ci impactent les outils d'informatique en nuage (5.3).

5.2. Règles applicables

5.2.1. Au niveau fédéral

[53] L'art. 22 al. 1 LPD prévoit que, lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune. Quelques exceptions existent (art. 22 al. 4 et 5 LPD).

[54] L'art. 22 al. 2 LPD précise que l'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants : traitement de données sensibles à grande échelle (let. a) et surveillance systématique de grandes parties du domaine public (let. b).

[55] L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux (art. 22 al. 3 LPD).

[56] Si l'analyse d'impact révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit consulter le PFPDT avant de procéder au traitement des données personnelles (art. 23 al. 1 LPD). Le PFPDT peut alors formuler des objections et proposer au responsable du traitement des mesures appropriées (art. 23 al. 3 LPD).

[57] Lorsque le responsable du traitement est un organe fédéral, il devra respecter les Directives AIPD[94] édictées par le Conseil fédéral[95] . En outre, l'Office de la justice a élaboré un « instrument d'examen préalable des risques » permettant de déterminer si un risque élevé (entraînant l'obli-

[94] Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale du 28 juin 2023, FF 2023 1882.

[95] Chancellerie fédérale (nbp. 1), p. 18.

gation de procéder à une analyse d'impact) existe[96] , ainsi qu'un guide de mise en œuvre pour les analyses d'impact[97].

5.2.2. Au niveau cantonal

[58] Les lois des cantons de Fribourg[98], de Genève[99], du Jura et de Neuchâtel[100], du Tessin[101], du Valais[102] et Zurich[103] (mais non celle de Berne) prévoient l'obligation de procéder à une analyse d'impact. Les règles cantonales en matière d'analyse d'impact sont pratiquement identiques à celles prévues par la LPD.

[59] Ainsi, dans les cantons précités, une analyse d'impact est obligatoire lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée[104]. Comme en droit fédéral, certaines des lois cantonales précitées prévoient que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement[105]. Elles précisent parfois qu'un risque élevé existe en cas de traitements de données sensibles à grande échelle[106] et de surveillance systématique de grandes parties du domaine public[107], mais également en cas de profilage[108] et de traitements d'une ampleur ou d'une intensité particulière recourant à des technologies, à des mécanismes ou à des procédures accentuant le risque d'atteinte aux droits fondamentaux des personnes concernées[109].

[60] L'analyse d'impact doit contenir une description du traitement envisagé, une évaluation des risques ainsi qu'une description des mesures prévues pour protéger les droits fondamentaux des personnes concernées[110].

[61] Les règles cantonales divergent quant à la suite à donner à l'analyse d'impact. À Genève, si l'analyse n'est pas liée à un projet d'acte législatif, elle est dans tous les cas soumise à la pré-

---

96 Cet instrument est disponible à l'adresse https://www.bj.admin.ch/dam/bj/fr/data/staat/datenschutz/instrument-risikovorpruefung.xlsx.download.xlsx/instrument-risikovorpruefung-f.xlsx (dernière consultation le 8 juillet 2025).

97 Le guide est disponible à l'adresse https://www.bj.admin.ch/dam/bj/fr/data/staat/datenschutz/dsfa-leitfaden.pdf.download.pdf/dsfa-leitfaden-f.pdf (dernière consultation le 8 juillet 2025).

98 Art. 41 s. LPrD/FR.

99 Art. 37B nLIPAD/GE.

100 Art. 23b CPDT/JUNE.

101 Art. 13 P-nLPDP/TI.

102 Art. 30b LIPDA/VS.

103 Art. 32 P-nIDG/ZH.

104 Art. 41 al. 1 LPrD/FR (qui mentionne toutefois uniquement le risque pour les droits fondamentaux) ; art. 37B al. 1 nLIPAD ; art. 23b al. 1 CPDT/JUNE ; art. 13 P-nLPDP/TI (qui mentionne toutefois uniquement le risque d'une violation de la protection des données) ; art. 30b al. 1 LIPDA/VS. Dans le canton de Zurich, les organes publics ont toujours l'obligation d'évaluer les risques pour les droits fondamentaux de la personne concernée (art. 32 P-nIDG/ZH).

105 Art. 41 al. 2 LPrD/FR ; art. 37B al. 2 nLIPAD ; art. 23b al. 2 CPDT/JUNE ; art. 30b al. 2 LIPDA/VS.

106 Art. 41 al. 2 let. a LPrD/FR ; art. 37B al. 2 let. a nLIPAD ; art. 23b al. 2 let. a CPDT/JUNE ; art. 30b al. 2 let. a LIPDA/VS.

107 Art. 41 al. 2 let. c LPrD/FR ; art. 37B al. 2 let. c nLIPAD ; art. 23b al. 2 let. c CPDT/JUNE ; art. 30b al. 2 let. c LIPDA/VS.

108 Art. 41 al. 2 let. b LPrD/FR ; art. 37B al. 2 let. b nLIPAD ; art. 23b al. 2 let. b CPDT/JUNE ; art. 30b al. 2 let. b LIPDA/VS.

109 Art. 41 al. 2 let. d LPrD/FR.

110 Art. 41 al. 3 LPrD/FR ; art. 37B al. 3 nLIPAD ; art. 23b al. 3 CPDT/JUNE ; art. 13 P-nLPDP/TI ; art. 30b al. 3 LIPDA/VS.

posée cantonale ou au préposé cantonal pour avis avant le début du traitement[111]. Dans le Jura et à Neuchâtel, le préposé se prononce également de toute manière sur l'analyse d'impact et les mesures de sécurité envisagées[112]. En revanche, à Fribourg, en Valais, et à Zurich, l'autorité de surveillance (Fribourg), respectivement le préposé (Valais et Zurich) ne sont consultés que si l'analyse d'impact confirme ou révèle l'existence d'un risque élevé[113] ; ces autorités communiquent ensuite leurs éventuelles objections[114]. Quant à la loi tessinoise, elle ne prévoit pas de suite à l'analyse d'impact.

5.3. Discussion

[62] Vu les règles exposées ci-dessus, une analyse d'impact ne doit pas systématiquement être réalisée lorsque l'utilisation d'une solution d'informatique en nuage est envisagée[115]. Seul un examen des caractéristiques du traitement de données personnelles permet de déterminer si cette obligation s'applique ou pas.

[63] Lorsque la réalisation de l'analyse d'impact est obligatoire, la collectivité publique responsable du traitement devra examiner en détail les risques que présente l'usage de la solution d'informatique en nuage envisagée et les mesures qui peuvent être prises. Cette analyse poussée – et l'éventuelle consultation de l'autorité compétente en matière de protection des données – permettra à l'autorité de déterminer en connaissance de cause les mesures à prendre dans un cas spécifique d'utilisation d'informatique en nuage.

[64] Précisons néanmoins que l'analyse d'impact ne vise pas à vérifier le respect des conditions légales (ce qui doit être fait avant le stade de l'analyse d'impact) et qu'elle ne peut pas remettre en cause le principe même de la légalité de la sous-traitance, ni de celle du transfert à l'étranger.

6. Autres considérations

6.1. Introduction

[65] En plus des règles contenues dans la protection des données, soulignons que certaines lois applicables en matière de technologie de l'information et de la communication peuvent contenir des dispositions pertinentes en matière de solutions d'informatique en nuage.

111 Art. 37B al. 5 nLIPAD.

112 Art. 23b al. 4 CPDT/JUNE.

113 Art. 42 al. 1 LPrD/FR ; art. 30b al. 4 LIPDA/VS ; art. 32 al. 2 P-nIDG/ZH.

114 Art. 42 al. 2 LPrD/FR (soulignons que l'autorité de surveillance peut également formuler des recommandations selon cette disposition) ; art. 30b al. 4 LIPDA/VS.

115 Voir Délégué à la transformation numérique et à la gouvernance de l'informatique (nbp. 42), pp. 16, 18 et 20 ; Chancellerie fédérale (nbp. 1), p. 19. Au niveau européen, l'EDPB considère que, dans le secteur public, de nombreuses opérations de traitement de données personnelles recourant à un *cloud* remplissent les critères imposant la réalisation d'une analyse d'impact (EDPB [nbp. 12], p. 10).

6.2. ONum

[66] Au niveau fédéral, c'est le cas de l'art. 12 de l'ONum[116], qui autorise les autorités fédérales à donner accès à des données non accessibles au public aux fournisseurs externes de prestations à trois conditions : l'accès doit être nécessaire pour fournir une prestation (let. a), l'autorité responsable des données doit avoir donné son accord, qui doit être documenté de manière traçable (let. b) et des mesures contractuelles, organisationnelles et techniques doivent être prises pour éviter que les données soient transmises plus loin (let. c).

6.3. LSI

[67] En outre, la LSI[117] – qui s'applique à de nombreuses autorités fédérales[118], mais également aux cantons dans certaines situations[119] – contient des dispositions sur la sécurité des moyens informatiques (art. 16 ss LSI). Ces dispositions imposent en particulier l'élaboration d'une procédure de sécurité[120] et le respect de mesures de sécurité minimales[121], en tenant compte de la catégorie de sécurité des moyens informatiques[122]. Les applications recourant à un nuage sont considérées comme des moyens informatiques au sens de ces dispositions[123].

[68] L'art. 17 LSI prévoit trois catégories de sécurité : (i) la catégorie « protection de base », qui comprend les informations classifiées « interne » (cf. art. 13 al. 1 LSI), (ii) la catégorie « protection élevée », qui comprend les informations classifiées « confidentiel » (cf. art. 13 al. 2 LSI) et (iii) la catégorie « protection très élevée », qui comprend les informations classifiées « secret » (cf. art. 13 al. 3 LSI).

[69] Sur la base de ces dispositions de la LSI, le Délégué à la transformation numérique et à la gouvernance de l'informatique[124] et la Chancellerie fédérale[125] considèrent que les données classifiées « secret » peuvent uniquement être stockées dans le nuage privé sécurisé de la Confédération, tandis que les données classifiées « interne » ou « confidentiel » peuvent être stockées dans un nuage public si des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissant le respect du droit applicable sont mises en place.

[70] Dans le canton de Fribourg, les art. 27 ss de la LCyb/FR[126] traitent de l'externalisation (ce par quoi il faut entendre, aux termes de l'art. 3 let. g LCyb/FR, « une forme qualifiée de sous-traitance impliquant l'utilisation de ressources informatiques accessibles à distance, via un réseau

116 Ordonnance sur les services numériques et la transformation numérique dans l'administration fédérale du 2 avril 2025 (RS 172.019.1). L'ONum est entrée en vigueur le 1er mai 2025 et a remplacé l'OTNI (Ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale 25 novembre 2020).

117 Loi fédérale sur la sécurité de l'information du 18 décembre 2020 (RS 128).

118 Art. 2 LSI.

119 Art. 3 LSI.

120 Art. 16 LSI.

121 Art. 18 al. 2 LSI.

122 Art. 17 LSI.

123 Chancellerie fédérale (nbp. 1), p. 31.

124 Délégué à la transformation numérique et à la gouvernance de l'informatique (nbp. 40), pp. 19 s.

125 Chancellerie fédérale (nbp. 1), p. 31.

126 Loi sur la cyberadministration fribourgeoise du 18 décembre 2020 (RS/FR 184.1).

de communication, pour stocker, traiter et partager des données »). À première vue, les conditions posées par ces dispositions ne vont toutefois pas plus loin que les art. 18 ss LPrD/FR.

6.4. LMeta

[71] La LMeta[127], entrée en vigueur le 1er janvier 2024, prévoit des règles en matière d'utilisation de moyens électronique par les autorités fédérales.

[72] L'art. 9 LMETA prévoit que les autorités fédérales soumises à la LMETA publient le code source des logiciels qu'elles développent ou font développer pour l'exécution de leurs tâches, sous réserve que les droits de tiers ou des raisons importantes en matière de sécurité excluent ou limitent cette possibilité.

[73] Cela a pour conséquence que, si une autorité fait développer un logiciel spécifique par un fournisseur externe, elle devra tenir compte de cette exigence. En particulier, elle devra vérifier suffisamment tôt qu'elle détient bien les droits nécessaires sur le logiciel pour publier son code source[128].

6.5. Règles en matière de marchés publics

[74] Avant de choisir une solution informatique externe, les autorités fédérales devront également prendre garde aux règles applicables en matière de marchés publics.

[75] En particulier, au niveau fédéral, les services en nuage sous forme de plateforme de développement d'applications en tant que service (*Platform as a service*, PaaS) ou de fourniture d'infrastructures en tant que service (*Infrastructure as a service*, IaaS) doivent être commandés sur la base de l'appel d'offres OMC 20007[129].

[76] L'art. 6 al. 1 et 2 LMP[130] et l'art. 6 al. 1 et 2 AIMP[131] prévoient tous deux que les soumissionnaires des États envers lesquels la Suisse s'est engagée contractuellement à donner accès à son marché et qui ont contracté le même engagement à son égard sont autorisés à présenter une offre. En outre, lorsque le marché n'est pas soumis aux accords internationaux, les soumissionnaires étrangers sont autorisés à présenter une offre à condition qu'ils proviennent d'États accordant la réciprocité ou que l'adjudicateur les y autorise. Ainsi, un appel d'offres portant sur une solution informatique qui exclut d'emblée les soumissionnaires étrangers afin de privilégier une solution entièrement suisse pourrait être contraire à ces dispositions.

127 Loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités du 17 mars 2023 (RS 172.019).

128 Message concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités du 4 mars 2022, FF 2022 804 p. 39.

129 Délégué à la transformation numérique et à la gouvernance de l'informatique (nbp. 42), p. 17.

130 Loi fédérale sur les marchés publics du 21 juin 2019 (RS 172.056.1).

131 Accord intercantonal sur les marchés publics du 15 novembre 2019.

6.6. Indépendance numérique

[77] La problématique de la « souveraineté numérique » est en outre souvent évoquée en lien avec le transfert de données personnelles à l'étranger : il existe une crainte que la Suisse devienne dépendante de solutions informatiques américaines et risque de ce fait de perdre la maîtrise sur ses données personnelles[132]. Il s'agit donc d'une question d'indépendance, notamment commerciale.

[78] Les « Principes relatifs à l'informatique en nuage de la confédération » contiennent une directive – contraignante – intitulée « stratégie de sortie en cas d'utilisation de services en nuage public », qui oblige les unités administratives fédérales à définir une stratégie de sortie pour chaque projet (ou groupe d'applications)[133]. Cette directive a pour but de sensibiliser à la problématique de la dépendance et de l'anticiper[134]. Toutefois, elle ne s'appuie sur aucune disposition légale, de sorte qu'il semble s'agir d'une thématique plus politique que juridique.

[79] Relevons que la problématique de l'indépendance de l'État va bien au-delà de la thématique de l'utilisation de solutions informatiques externes. D'une part, elle concerne également le matériel, de même que des services qui ne sont pas directement liés au numérique. D'autre part, la question de l'indépendance se pose également si des services sont fournis par un seul prestataire situé en Suisse. Enfin, la question de la dépendance à un sous-traitant doit être distinguée de celle du lieu d'hébergement des données, ces deux problématiques n'étant pas nécessairement liées.

7. Conclusion

[80] Suite à certains changements au niveau légal, les doutes qui existaient – en matière de protection des données et de secret de fonction – sur la légalité de l'utilisation des solutions d'informatique en nuage par les collectivités publiques ont désormais été levés.

[81] D'une part, les États-Unis ont été ajoutés à la liste des pays disposant d'une législation assurant un niveau de protection adéquat, de sorte qu'un outil dont l'utilisation implique un transfert de données personnelles vers une entreprise certifiée aux États-Unis peut être employé sans mettre en place des garanties ou des mesures supplémentaires. Ainsi, le CLOUD Act n'est plus un obstacle à l'utilisation d'outils fournis par des prestataires américains certifiés ou liés par des clauses contractuelles types. En l'état, et contrairement à ce qui prévalait sous l'ancienne LPD, l'exportateur peut se fier à la liste du Conseil Fédéral pour décider si un État offre ou non des garanties suffisantes.

[82] D'autre part, l'art. 320 CP a été modifié pour inclure les auxiliaires parmi les personnes soumises au secret de fonction. Une autorité peut par conséquent communiquer des données personnelles à des sous-traitants – qui sont des auxiliaires au sens de la disposition précitée – sans violer le secret de fonction.

[83] Malgré ces changements, on observe toutefois encore une certaine réticence, de la part des autorités, à recourir à des solutions d'informatique en nuage, y compris par quelques législateurs

132 Voir Chancellerie fédérale (nbp. 1), p. 26.

133 Délégué à la transformation numérique (nbp. 42), p. 14, disponible à l'adresse https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html (dernière consultation le 8 juillet 2025). La *Kantonale Fachstelle für Datenschutz* du canton de Saint-Gall mentionne aussi qu'une stratégie de sortie est nécessaire s'agissant de M365 (Bericht der kantonalen Fachstelle für Datenschutz, 4 mars 2025, p. 15).

134 Délégué à la transformation numérique et à la gouvernance de l'informatique (nbp. 40), p. 14.

cantonaux qui ont adopté des restrictions en violation du droit supérieur. Les arguments avancés pour expliquer pourquoi de telles solutions doivent être considérées avec circonspection ne résultent toutefois pas expressément de la législation en matière de protection des données personnelles ou de secret (de fonction ou professionnel). Il s'agit plutôt de considérations politiques, liées notamment à la souveraineté de l'État, ou de choix internes à l'administration. Cela ne signifie pas que ces réflexions ne sont pas pertinentes, mais il s'agit de critères politiques, éthiques ou de gouvernance, qui doivent être débattus dans ce contexte pour permettre un choix éclairé. Il ne s'agit pas d'interdictions légales.

Sylvain Métille est avocat associé à l'étude HDC à Lausanne, professeur associé à l'Université de Lausanne (où il enseigne notamment la protection des données et le droit pénal informatique) ainsi que responsable scientifique et chargé de cours dans le CAS en Protection des données dispensé par UniDistance.

Marie-Laure Percassi est avocate collaboratrice à l'étude HDC à Lausanne, docteure en droit, chargée de cours dans le CAS en Protection des données dispensé par UniDistance, et chargée de cours et collaboratrice scientifique à l'Université de Neuchâtel.