www.jusletter.ch

Joël Pahud / Sébastien Pittet

Les infractions pénales de la loi sur la protection des données

En adoptant la nouvelle loi sur la protection des données (LPD), le législateur a considérablement renforcé les sanctions pénales en cas de violation des règles de protection des données. Cette contribution passe en revue les différentes infractions pénales de la LPD et approfondit certaines questions en lien avec le devoir de discrétion, la communication de données à l'étranger et la détermination de la personne responsable de la violation.

Catégories d'articles : Contributions
Domaines juridiques : Protection des données

Proposition de citation : Joël Pahud / Sébastien Pittet, Les infractions pénales de la loi sur la protection des données, in : Jusletter 25 septembre 2023

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

Table des matières

1. Introduction

[1] Avec la nouvelle LPD[1], le législateur a considérablement renforcé les sanctions pénales en cas de violation des règles de protection des données. Le champ d'application des art. 60 à 65 LPD a été étendu par rapport au droit en vigueur jusqu'au 31 août 2023 et des comportements qui ne pouvaient donner lieu qu'à des actions civiles ont été érigés en infractions pénales. Contrairement au système européen, les personnes physiques peuvent être sanctionnées en première ligne et risquent une amende jusqu'à CHF 250'000.– en cas de violation.

[2] Dans son avant-projet, le Conseil fédéral envisageait de réprimer plus sévèrement la violation des règles de protection des données. Toutefois, face aux nombreuses critiques formulées en procédure de consultation, le Conseil fédéral a revu sa copie. Le plafond de l'amende a ainsi été réduit de CHF 500'000.– à CHF 250'000.–, la violation du devoir de discrétion est réprimée par une amende en lieu et place d'une peine privative de liberté ou d'une peine pécuniaire, la négligence n'a pas été rendue punissable et, enfin, plusieurs obligations incombant au responsable du traitement n'ont pas été érigées en infractions pénales. On pense en particulier à l'obligation d'annoncer des violations de la sécurité des données (« *data breach notification* »)[2], dont la violation n'est pas sanctionnée pénalement.[3]

[3] Il n'en demeure pas moins que, selon l'objectif exprimé par le Conseil fédéral[4], le volet pénal de la LPD devait être suffisamment renforcé pour « *compenser* » l'absence de pouvoir du Préposé

1 Dans le cadre de cette contribution, l'abréviation LPD fait référence à la nouvelle loi sur la protection des données, en vigueur depuis le 1er septembre 2023 et l'abréviation aLPD fait référence à l'ancienne loi sur la protection des données en vigueur jusqu'au 31 août 2023.

2 Art. 24 LPD ; à ce sujet, voir Célian Hirsch, Le devoir d'informer lors d'une violation de la sécurité des données – avec un regard particulier sur les données bancaires (à paraître).

3 Comparer avec l'art. 50 al. 1 let. b ch. 1 et al. 2 let. d de l'avant-projet.

4 FF 2017 6596 ; cf. déjà Rapport explicatif du 21 décembre 2016 sur l'avant-projet, no de réf. COO.2180.109.7.185665, ch. 1.4.2.5, p. 21.

fédéral à la protection des données et à la transparence (le « **PFPDT** ») d'infliger des sanctions administratives, contrairement à ses homologues européens. Les dispositions pénales proposées par le Conseil fédéral et adoptées sans changement par le parlement (hormis leur numérotation) se veulent « *dissuasives* », sans quoi l'Union européenne pourrait juger que la réglementation suisse en matière de protection des données n'est pas suffisante.[5]

[4] Nous débuterons cette contribution par une comparaison entre le modèle suisse et le modèle européen (*infra* 2) avant d'examiner les différentes infractions de la LPD (*infra* 3) ainsi que les traits communs à ces dernières (*infra* 4). Nous aborderons ensuite quelques questions spécifiques en lien avec le devoir de discrétion (*infra* 5.1), le transfert de données à l'étranger (*infra* 5.2) et l'identification de la personne responsable (*infra* 5.3), avant de conclure (*infra* 6).

[5] En revanche, cette contribution ne traitera pas de l'art. 179^{novies} CP (soustraction de données personnelles), dont la teneur a été modifiée avec effet au 1er septembre 2023, ni de l'art. 179^{decies} CP (usurpation d'identité), qui a été adopté à l'occasion de la révision de la LPD.

2. Le modèle suisse par rapport au modèle européen

[6] Selon le Conseil fédéral, la nouvelle LPD poursuit plusieurs objectifs. Il s'agit d'adapter la législation suisse aux évolutions technologiques, de mieux responsabiliser les responsables du traitement mais aussi de rapprocher la législation suisse de la législation européenne.[6] Cette harmonisation du droit suisse avec le droit européen doit en particulier permettre à la Suisse de continuer à bénéficier de la décision de la Commission européenne reconnaissant la Suisse comme un État offrant un niveau de protection des données adéquat – décision indispensable au bon fonctionnement des relations économiques entre l'Union européenne et la Suisse[7], et permettant le transfert sans exigences supplémentaires de données personnelles depuis les organismes soumis au RGPD[8] vers la Suisse.

[7] En raison de ce dernier objectif, le législateur suisse s'est largement inspiré du RGPD pour réviser la LPD. Une grande partie des obligations du RGPD ont ainsi été reprises par la Suisse. Toutefois, s'agissant des sanctions en cas de violation d'obligations de protection des données, la Suisse s'est passablement écartée du système mis en place au sein de l'Union européenne. Les principales différences développées brièvement ci-dessous concernent (i) l'autorité compétente pour sanctionner des violations (ii) le champ d'application matériel des sanctions (iii) leur champ d'application personnel (iv) leur montant et (v) certaines conditions à la poursuite des infractions.

[8] Tout d'abord, le législateur suisse a érigé certains comportements violant les règles de protection des données en infractions pénales, dont la poursuite incombe aux autorités pénales des cantons, qui appliquent le droit de procédure pénale. L'approche européenne est différente puisque les violations en question font l'objet de sanctions pécuniaires administratives prononcées selon le RGPD par des autorités de contrôle indépendantes nationales chargées de surveiller l'application du RGPD (art. 51 et 83 RGPD).

5 FF 2017 6714 s.

6 FF 2017 6592 s.

7 FF 2017 6593. La décision d'adéquation est attendue dans les prochains mois.

8 L'abréviation RGPD, ou *GDPR* en anglais, fait référence au Règlement général sur la protection des données (Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016).

[9] Ensuite, s'agissant du champ d'application matériel, les sanctions pénales de la LPD renforcent certaines obligations de comportement considérées comme essentielles par le législateur.[9] Si la révision de la LPD a largement étendu le champ des dispositions pénales de la loi, le non-respect de plusieurs obligations de la LPD échappe aux sanctions pénales.[10] Cette approche est différente du droit européen, lequel assortit de sanctions administratives la quasi-totalité des violations du RGPD (art. 83 RGPD).

[10] S'agissant du champ d'application personnel, même lorsque le responsable du traitement est une personne morale, les dispositions pénales de la LPD visent en premier lieu les personnes physiques, alors que les sanctions administratives du RGPD sont dirigées contre les entreprises. La stratégie du Conseil fédéral consistant à diriger les dispositions pénales avant tout contre des personnes physiques a certes été critiquée lors de la procédure de consultation mais s'est néanmoins imposée. Dans son Message, le Conseil fédéral estimait que les sanctions administratives pécuniaires à caractère punitif devaient conserver un caractère exceptionnel en Suisse.[11] En particulier, le Conseil fédéral relevait que « *[l]e fait qu'il n'existe aucun droit de procédure codifié pour les sanctions administratives à caractère pénal implique entre autres le risque de saper les droits procéduraux des personnes physiques* ».[12] Cette approche a tacitement été suivie par le parlement.

[11] Le montant des sanctions diverge également de manière frappante. En droit suisse, les dispositions pénales de la LPD prévoient une amende pouvant atteindre un montant maximum de CHF 250'000.–.[13] En droit européen, l'amende infligée à l'entreprise peut être nettement plus élevée. En fonction des violations, l'art. 83 RGPD prévoit que les amendes peuvent atteindre EUR 20'000'000.– ou jusqu'à 4 % du chiffre d'affaires annuel mondial.[14] Toutefois, dans la mesure où l'amende de la LPD est susceptible d'être infligée en premier lieu à des personnes physiques, son montant maximal devrait selon nous s'avérer dissuasif[15] – à l'exception peut-être des derniers pourcents de fortune et revenus les plus élevés.[16]

[12] Enfin, les infractions pénales de la LPD sont poursuivies uniquement sur plainte et requièrent l'intention de l'auteur. En droit européen, les autorités nationales de protection des données sanctionnent d'office les entreprises qui violent le RGPD, y compris par négligence (art. 83 RGPD).

---

9 FF 2017 6715.

10 Outre l'obligation de notifier les violations de sécurité des données (art. 24 LPD) évoquée plus haut, on ajoutera la tenue d'un registre des activités de traitement (art. 12 LPD) ou la réalisation d'une analyse d'impact sur la protection des données (art. 22 LPD).

11 FF 2017 6713.

12 FF 2017 6714.

13 Les art. 34 et 35 aLPD étaient en revanche alignés avec le plafond ordinaire de l'art. 106 al. 1 CP (CHF 10'000.–).

14 Cf. par exemple la décision du 13 mai 2023 de la Commission irlandaise de protection des données, laquelle a infligé une amende de EUR 1.2 milliard au groupe Meta (décision qui fait actuellement l'objet d'un appel). La décision est disponible à l'adresse : https ://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en (consultée le 17 août 2023).

15 Du même avis : David Rosenthal/Seraina Gubler, Die Strafbestimmungen des neuen DSG, RSDA 1/2021, p. 52 ss, p. 53.

16 En 2020, selon l'Office fédéral de la statistique, 99.4% des femmes salariées et 96.5% des hommes salariés en Suisse avaient un salaire mensuel net inférieur à CHF 12'001 (secteur privé et secteur public ensemble).

3. Survol des infractions

[13] Les infractions pénales de la LPD sont réparties en quatre catégories : la violation des obligations d'informer, de renseigner et de collaborer (*infra* 3.1), la violation des devoirs de diligence (*infra* 3.2), l'insoumission à une décision (*infra* 3.3) et la violation du devoir de discrétion (qui sera traitée séparément au chapitre 5.1).

3.1. Violation des obligations d'informer, de renseigner et de collaborer

[14] Selon l'art. 60 al. 1 let. a LPD, la personne privée s'expose à une amende pouvant aller jusqu'à CHF 250'000 si elle fournit intentionnellement des renseignements inexacts ou incomplets (i) à la personne concernée par une collecte de données personnelles (art. 19 LPD), (ii) à la personne concernée par une décision individuelle automatisée (art. 21 LPD) ou (iii) à la personne qui exerce son droit d'accès (art. 25–27 LPD).

[15] L'art. 60 al. 1 let. b LPD réprime également l'omission intentionnelle d'informer la personne concernée par une décision individuelle automatisée (art. 21 al. 1 LPD) ou par une collecte de données (art. 19 al. 1 LPD) ainsi que l'omission intentionnelle de lui transmettre les informations nécessaires à faire valoir ses droits (art. 19 al. 2 LPD).[17]

[16] Si le responsable du traitement était déjà menacé par une sanction pénale sous le régime de l'aLPD en cas de violation de son obligation d'informer lors d'une collecte de données (art. 14 et 34 al. 1 let. a aLPD), la modification du champ d'application de la norme amplifie largement le risque d'une infraction pénale pour le responsable du traitement. En effet, sous l'aLPD, le responsable du traitement était tenu d'informer la personne concernée uniquement en cas de collecte de données sensibles et de profil de la personnalité (art. 14 aLPD). Aujourd'hui, cette obligation s'étend à tous les traitements de données personnelles (art. 19 LPD).

[17] Concrètement, on peut distinguer deux types d'obligations qui découlent de l'art. 60 al. 1 LPD : (i) le respect des obligations du responsable du traitement à la suite d'une demande d'accès et (ii) le respect des obligations d'informer spontanément la personne concernée. En pratique, les informations destinées à la personne concernée sont généralement intégrées dans une politique de confidentialité (ou déclaration en matière de protection des données), appelée plus communément une *privacy notice*. C'est à travers ce document adressé à la personne concernée que le responsable du traitement remplit en principe ses obligations d'information générale. Comme mentionné ci-dessus, la généralisation de l'obligation d'informer la personne concernée – obligation qui s'adresse dorénavant à tous les responsables du traitement indépendamment du type de données personnelles traitées[18] – constitue une nouveauté importante de la récente révision de la LPD. Selon nous, la rédaction d'une *privacy notice* complète devrait ainsi constituer une priorité pour les responsables du traitement.[19]

---

17 L'omission de répondre à une requête d'accès n'est en revanche pas réprimée.

18 Sous réserve d'exceptions au devoir d'informer (art. 20 LPD), lesquelles devraient cependant rarement s'appliquer en pratique dans un traitement de données personnelles « classique ».

19 Pour le surplus, nous constatons en pratique que la rédaction d'une *privacy notice* et la constitution d'un registre des activités de traitement (art. 12 LPD) poussent le responsable du traitement à déterminer avec précision les données personnelles qu'il traite, première étape primordiale au respect des différentes obligations de la LPD.

[18] Finalement, l'art. 60 al. 2 LPD sanctionne les responsables privés qui, dans le cadre d'une enquête, fournissent intentionnellement au PFPDT des renseignements inexacts ou refusent de collaborer conformément à l'art. 49 al. 3 LPD.[20] En pratique, on peut s'attendre à ce que les responsables du traitement collaborent avec diligence avec le PFPDT de sorte que cette disposition devrait *a priori* jouer un rôle dissuasif plutôt que punitif.[21]

3.2. Violation des devoirs de diligence

[19] L'art. 61 LPD prévoit une sanction dans trois situations spécifiques : (i) la communication sans droit de données personnelles à l'étranger (art. 16–17 LPD), (ii) la transmission sans droit de données personnelles à un sous-traitant (art. 9 LPD) et (iii) le non-respect des exigences minimales en matière de sécurité des données (art. 8 al. 3 LPD). Comme pour les autres dispositions pénales de la LPD, l'intention de l'auteur est requise.

[20] En matière de communication de données personnelles à l'étranger, l'art. 16 LPD prévoit que si des données personnelles sont communiquées dans un État ne garantissant pas un niveau de protection adéquat[22], la protection des données doit être garantie autrement, par exemple à travers des clauses types de protection des données telles que les clauses modèles de l'Union européenne.[23] L'art. 17 LPD précise certaines situations dans lesquelles, malgré un niveau de protection adéquat non-garanti, une communication peut tout de même être effectuée (par exemple avec le consentement de la personne concernée). Comme analysé ci-après[24], le responsable du traitement qui ne respecte pas ces obligations s'expose à une sanction pénale.

[21] La LPD sanctionne également le recours à un sous-traitant qui ne respecterait pas les conditions de l'art. 9 LPD. Selon cette disposition, le traitement par un sous-traitant doit (i) être régi par un contrat garantissant la protection des données, (ii) ne pas dépasser les traitements que le responsable du traitement pourrait lui-même effectuer et (iii) ne pas être interdit par une obligation contractuelle ou légale de garder le secret.[25] Contrairement au régime européen et en particulier à l'art. 28 al. 3 RGPD, l'art. 9 LPD ne définit pas les éléments spécifiques que doit contenir le contrat entre le responsable du traitement et le sous-traitant.[26] En principe, le contrat entre le responsable du traitement et le sous-traitant doit notamment prévoir des mesures techniques et organisationnelles pour garantir la sécurité des données. Il doit également contenir des clauses qui assurent la confidentialité, la disponibilité et l'intégrité des données.[27] Selon nous, le respon-

20 Sur le déroulement d'une enquête du PFPDT, cf. l'Aide-mémoire du PFPDT de mai 2023 relatif aux enquêtes concernant des violations des prescriptions de protection des données ouvertes par le PFPDT.

21 Sous le régime de l'aLPD, une sanction similaire existait déjà et aurait, selon Rosenthal/Gubler (nbp. 15), p. 52, très rarement donné lieu à des amendes (art. 34 al. 2 let. b aLPD).

22 La liste des États garantissant un niveau de protection adéquat figure à l'Annexe 1 de l'OPDo.

23 Le recours aux clauses modèles de l'Union européenne ne garantit pas toujours un niveau de protection approprié. Sur ce point : Philipp Fischer/Sébastien Pittet, L'utilisation des services *cloud* par les responsables de traitement privés, in *:* L'informatique en nuage, Sylvain Métille (éd.), Berne 2022, p. 35 ss (cité : Fischer/Pittet, L'utilisation des services *cloud*), p. 50 ss.

24 *Infra* 5.2.

25 Le non-respect des nouvelles modalités en cas de recours à un sous-sous-traitant (art. 9 al. 3 et 4 LPD et art. 7 OPDo) n'entre pas dans le champ d'application de l'art. 61 LPD.

26 Voir notamment : David Rosenthal/Samira Studer/Alexandre Lombard, La nouvelle loi sur la protection des données, in : Jusletter du 16 novembre 2020, N. 59.

27 Fischer/Pittet, L'utilisation des services *cloud* (nbp. 23), p. 42 s.

sable du traitement devrait pouvoir utiliser les exigences européennes pour se guider dans sa relation contractuelle avec un sous-traitant, étant précisé que le non-respect des exigences européennes en la matière ne devrait toutefois pas pouvoir être directement reproché au responsable du traitement suisse (pour autant qu'il ne soit pas lui-même soumis au RGPD).

[22] Finalement, l'art. 61 let. c LPD sanctionne encore le non-respect des exigences minimales en matière de sécurité des données. Les exigences en matière de sécurité des données ont été définies aux art. 1 à 6 de l'ordonnance du 31 août 2022 sur la protection des données (« OPDo »).[28] Formulées de manière relativement larges, les exigences en matière de sécurité des données comprennent notamment la mise en place de mesures techniques et organisationnelles et visent à assurer la confidentialité, la disponibilité, l'intégrité et la traçabilité des données personnelles.[29]

3.3. Insoumission à une décision

[23] Dernière infraction du volet pénal de la LPD, l'art. 63 LPD vise l'insoumission à une décision du PFPDT ou d'une autorité de recours. L'infraction suppose que la décision en question contienne une clause indiquant expressément que son non-respect expose le contrevenant à une amende de CHF 250'000.– au plus au sens de l'art. 63 LPD. En l'absence de cette clause, l'application de l'art. 63 LPD est exclue. Sur le fond, la norme est ainsi clairement inspirée de l'art. 292 CP.[30]

[24] L'art. 63 LPD complète l'art. 60 al. 2 LPD qui vise à garantir le bon déroulement d'une enquête. Il permet de sanctionner la violation d'une décision prise par le PFPDT en cours, ou à l'issue, d'une enquête.[31] Le PFPDT peut ainsi assortir une décision prise en vertu de l'art. 51 LPD de la menace de l'amende jusqu'à CHF 250'000.–. Le Conseil fédéral conçoit ce mécanisme comme une compensation au fait que le PFPDT ne s'est pas vu attribuer la compétence de prononcer directement des sanctions en cas de violation des règles de la LPD.[32]

[25] Il nous paraît en revanche exclu que le PFPDT assortisse une décision prise en vertu de l'art. 50 LPD (*accès aux renseignements, documents, registres et données ; accès aux locaux et installations ; auditions de témoins ; expertises*) de la menace de la peine de l'art. 63 LPD. Le Message indique clairement que l'art. 63 LPD a été conçu pour renforcer le respect des *obligations* de la LPD et se réfère en outre à l'art. 45 al. 3 du projet qui est devenu l'art. 51 al. 3 LPD.[33] On ne voit toutefois pas ce qui s'opposerait à ce que le PFPDT assortisse également de la menace de la peine de l'art. 63 LPD une décision prise en vertu de l'art. 51 al. 1 (*modification, suspension ou cessation de tout ou partie du traitement, ainsi que l'effacement ou la destruction de tout ou partie des données personnelles)*, al. 2 (*suspendre ou interdire la communication de données personnelles à l'étranger*) ou

28 Sur l'interprétation des exigences minimales qui découlent de l'OPDo : Baeriswyl in : Bruno Baeriswyl/Kurt Pärli/Dominika Blonski, Datenschutzgesetz (DSG), Berne 2023, Art. 8, N. 42 ss.

29 Wohlers remet même en question la compatibilité de la sanction pénale avec l'art. 1 CP (*nullum crimen sine lege*) en raison des exigences trop larges et floues de l'OPDo (Wohlers in : Baeriswyl/Pärli/Blonski (nbp. 28), Art. 61 N. 13 ss).

30 Wohlers, in : Baeriswyl/Pärli/Blonski (nbp. 28), Art. 63 N. 1 ; FF 2017 6715.

31 *Contra* : Rosenthal/Gubler (nbp. 15), p. 55, qui limitent son application aux décisions prises *après* enquête. Il nous semble toutefois que le PFPDT doit pouvoir prendre des mesures provisoires urgentes, sans attendre le terme de son enquête, et les assortir de la menace de la peine de l'art. 63 LPD.

32 FF 2017 6715 et 6717 s.

33 FF 2017 6718.

al. 4 LPD *(ordonner au responsable du traitement privé ayant son siège ou son domicile à l'étranger de désigner un représentant*).[34]

4. Traits communs

[26] Les dispositions pénales de la LPD présentent certaines caractéristiques communes.

[27] D'une part, ces infractions sont des contraventions (art. 333 al. 3 CP). Le législateur les considère donc comme des infractions moins graves que d'autres, érigées en crimes ou en délits.[35] La nature contraventionnelle des art. 60 à 63 LPD a pour conséquence que :

- La tentative n'est pas punissable.[36]
- La complicité n'est pas punissable.[37] En revanche, l'instigation est punissable.[38]
- L'appel[39] peut uniquement être formé pour le grief que le jugement est juridiquement erroné ou que l'état de fait a été établi de manière manifestement inexacte ou en violation du droit, c'est-à-dire de manière arbitraire.[40] Dans la procédure d'appel, aucune nouvelle allégation ou preuve ne peut être produite.[41] La juridiction d'appel peut décider de traiter l'appel en procédure écrite, même sans accord des parties.[42]
- Une condamnation n'est inscrite au casier judiciaire que lorsque l'amende est supérieure à CHF 5'000.–.[43] L'inscription n'apparaît que sur les extraits 1, 2 et 3 destinés aux autorités[44], mais non sur l'extrait 4 destiné aux autorités, ni sur l'extrait destiné aux particuliers.[45]

[28] D'autre part, les infractions de la LPD sont :

- Punies de l'amende de CHF 250'000.– au plus, laquelle ne peut pas être assortie du sursis ou du sursis partiel.[46]
- Poursuivies uniquement sur plainte, à l'exception des art. 60 al. 2 LPD (*fourniture de renseignements inexacts ou refus de collaborer avec le PFPDT*) et 63 LPD (*insoumission à une décision*).

---

34 Dans ce sens : Jonas D. Gassmann, Kommentierung zu Art. 63 DSG, in : Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (éd.), Onlinekommentar zum Bundesgesetz über den Datenschutz, N. 9.

35 Yvan Jeanneret, in : Commentaire romand du Code pénal I, 2e éd., Bâle 2021 (cité : CR CP I-Auteur), Art. 103 N. 1.

36 Art. 105 al. 2 CP.

37 Art. 105 al. 2 CP.

38 CR CP I-Yvan Jeanneret, Art. 105 N. 3 et les références.

39 Au sens des art. 398 ss CPP.

40 TF 6B_362/2012 du 29 octobre 2012, consid. 5.2.

41 Art. 398 al. 4 CPP.

42 Art. 406 al. 1 let. c CPP ; Sven Zimmerlin, in : Andreas Donatsch/Viktor Lieber/Sarah Summers/Wolfgang Wohlers (éd.), Kommentar zur Schweizerischen Strafprozessordnung StPO, 3e éd., Zurich 2020, Art. 406 N. 2.

43 Art. 18 al. 1 let. c ch. 3 LCJ.

44 Le jugement cesse de figurer après 15 ans (extrait 1 ; cf. art. 37 al. 3 en lien avec art. 30 al. 2 let. d LCJ), respectivement après 10 ans (extraits 2 et 3 ; cf. art. 38 al. 3 let. d et 39 LCJ).

45 Art. 40 al. 1 let. b ch. 1 (*a contrario*) et art. 41 LCJ.

46 Art. 105 al. 1 CP.

- Intentionnelles, ce qui comprend le dol direct (ou simple) et le dol éventuel.[47]
- Sujettes à une prescription de l'action pénale de 5 ans (art. 66 LPD). La prescription est donc plus longue que le régime ordinaire applicable aux contraventions (3 ans[48]), mais plus courte que la prescription des délits du Code pénal (7 ans ou 10 ans[49]).

[29] Le choix du législateur de maintenir la poursuite sur plainte pour la plupart des infractions de la LPD va à contre-courant de l'approche observée dans d'autres domaines.

[30] Ainsi, le 1er juillet 2016, après une décennie de poursuite sur plainte, le législateur a érigé la corruption privée en infraction poursuivie d'office (sauf cas de peu de gravité).[50] Le GRECO[51], comme plusieurs auteurs[52], avaient en effet critiqué l'exigence d'une plainte, y voyant une explication à l'absence quasi complète[53] de condamnations pour corruption privée en Suisse depuis 2006.

[31] Aujourd'hui, sept ans après l'adoption de la poursuite d'office, il est vrai que la situation ne semble pas s'être modifiée radicalement. Cela dit, en termes de prévention générale, l'exigence d'une plainte contribue probablement à une forme de « *bagatellisation* », soit « *l'impression fallacieuse que l'infraction [n'est] pas suffisamment sérieuse pour mériter la poursuite pénale, sauf si une entreprise ou un individu s'en plai[nt]* ».[54] Ce qui était valable pour la corruption privée hier l'est également pour la violation des règles de protection des données aujourd'hui et il nous paraît ainsi légitime de s'interroger sur l'efficacité des nouvelles dispositions pénales de la LPD.

[32] La plainte doit être déposée auprès de la police, du ministère public ou de l'autorité pénale compétente en matière de contraventions, par écrit ou oralement, dans les trois mois à compter du jour de la connaissance de l'infraction et de son auteur.[55]

[33] La qualité pour porter plainte appartient au lésé, c'est-à-dire la personne dont le bien juridique protégé par la disposition pénale en cause est directement atteint par l'infraction.[56] Selon la terminologie adoptée par la LPD, il s'agit de la « *personne concernée* »[57], soit la personne physique[58] dont les données personnelles font l'objet d'un traitement qui enfreint les dispositions pénales de la LPD.

---

47 Art. 12 al. 2, seconde phrase, CP : l'auteur agit déjà intentionnellement lorsqu'il tient pour possible la réalisation de l'infraction et l'accepte au cas où celle-ci se produirait (dol éventuel).

48 Art. 109 CP.

49 Art. 97 al. 1 let. c et d CP.

50 Art. 322octies et 322novies CP ; comparer avec les art. 4a et 23 LCD dans leur teneur jusqu'au 30 juin 2016.

51 GRECO, Troisième cycle d'évaluation : Rapport de Conformité sur la Suisse du 18 octobre 2013, publié le 21 novembre 2013 (voir notamment par. 17 à 20). Voir également : FF 2014 3433.

52 Notamment : Nicolas Queloz/Marco Borghi/Maria Lusia Cesoni, Processus de corruption en Suisse, Résultats de recherche – Analyse critique du cadre légal et de sa mise en œuvre – Stratégie de prévention et de riposte, Bâle/Genève/Munich, Collection latine, Vol. 1, 2000, p. 373 ; Daniel Jositsch, Das Schweizerische Korruptionsstrafrecht : Art. 322ter bis 322octies StGB, Zurich 2004, p. 370 ss ; Alain Macaluso, Infractions de corruption dans l'entreprise : aperçu critique du droit positif suisse et perspectives, in : RPS 2012 p. 23, 30 ; Jean-Pierre Méan, Le droit anticorruption et les organisations sportives internationales, in : L'Expert-Comptable Suisse 4/2013 p. 206, 208.

53 Pour un rare exemple de condamnation : OGer ZH SB170091 du 22 août 2018.

54 Ursula Cassani, Droit pénal économique, Bâle 2020, par. 9.142.

55 Art. 304 al. 1 CPP et art. 31 CP ; CR CP I-Katia Villard, Art. 31 N. 7.

56 CR CP I-Daniel Stoll, Art. 30 N. 19.

57 Art. 5 let. b LPD.

58 Contrairement à l'aLPD, la LPD ne protège plus les données des personnes morales.

[34] Le PFPDT n'a pas qualité pour déposer plainte. Il peut en revanche dénoncer des infractions aux autorités de poursuite pénale compétentes et se constituer partie plaignante (au pénal).[59]

[35] À notre sens, le ministère public ou l'autorité cantonale compétente en matière de contraventions qui reçoit une dénonciation du PFPDT pour l'une ou l'autre des infractions à la LPD poursuivies sur plainte peut, voire doit[60], informer la ou les personne(s) concernée(s) de leur droit de déposer plainte. Durant le délai de trois mois et dans l'attente d'une éventuelle plainte, le ministère public ou l'autorité compétente en matière de contraventions peut prendre les mesures conservatoires qui ne souffrent aucun retard.[61]

[36] Pour les infractions qui ne requièrent pas de plainte (art. 60 al. 2 LPD – fourniture de renseignements inexacts ou refus de collaborer pendant une enquête – et art. 63 LPD – insoumission à une décision du PFPDT), le ministère public ou l'autorité cantonale compétente en matière de contraventions saisis d'une dénonciation du PFPDT doit ouvrir une instruction pénale s'il ressort de la dénonciation ou de ses propres constatations des soupçons suffisants laissant présumer qu'une infraction a été commise.[62]

[37] La poursuite et le jugement des infractions à la LPD est du ressort des cantons. En la matière, il n'y a pas de compétence primaire ou subsidiaire du Ministère public de la Confédération.[63] Cela dit, il est concevable que le Ministère public de la Confédération ordonne, le cas échéant, la jonction auprès des autorités fédérales au sens de l'art. 26 al. 2 CPP. On peut penser à l'hypothèse de transferts de données vers l'étranger qui conduiraient à l'ouverture d'une instruction par le Ministère public de la Confédération pour soupçon de violation des art. 271 et 273 CP et qui feraient en parallèle l'objet d'une plainte d'une personne concernée pour soupçon de violation de l'art. 61 let. a LPD.

[38] Les cantons peuvent déléguer la compétence de poursuivre et juger ces contraventions à des autorités administratives (art. 17 al. 1 CPP). Le ministère public et les tribunaux sont toutefois toujours compétents si une contravention à la LPD est en rapport avec des crimes ou des délits (art. 17 al. 2 CPP).

[39] À Zurich par exemple, les *Statthalterämter* sont en principe compétents pour poursuivre et juger toutes les contraventions[64], dont les contraventions à la LPD.[65]

[40] De même, dans le canton de Vaud, cette compétence a été attribuée aux préfets.[66]

---

59 Art. 65 al. 2 LPD ; voir également : Nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT du 9 février 2021.

60 Un tel devoir pourrait se déduire de l'art. 7 CPP ainsi que, par analogie, de l'art. 118 al. 4 CPP.

61 Art. 303 al. 2 CPP.

62 Art. 309 al. 1 let. a CPP (applicable par renvoi de l'art. 357 CPP s'agissant de l'autorité cantonale compétente en matière de contraventions). La notion de soupçons suffisants s'interprète de manière large, conférant ainsi une marge de manœuvre importante au ministère public (respectivement à l'autorité cantonale compétente en matière de contraventions). L'ouverture n'est exclue que lorsque le dossier ne contient aucun élément concret et où l'enquête s'apparenterait à une « *fishing expedition* » ou lorsqu'il existe uniquement des rumeurs floues ou des hypothèses (Grodecki/Cornu in : Commentaire romand du Code de procédure pénale, 2e éd., Bâle 2019 (cité : CR CPP-Auteur), Art. 309 N. 8).

63 Art. 65 LPD ; art. 23 et 24 CPP *a contrario*.

64 §89 Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess (GOG), RS ZH 211.1.

65 Cf. par exemple OGer ZH UE160087 du 22 juillet 2016.

66 Art. 18 al. 1 let. a de la loi sur les préfets et les préfectures (LPréf ; RSV 172.165). Cf. par exemple TC VD Décision / 2014 / 684 du 8 juillet 2014.

[41] À Genève en revanche, si le Service des contraventions dispose d'une compétence générale en matière de contraventions[67], le Procureur général avait toutefois réservé la compétence du ministère public s'agissant de la poursuite des infractions aux art. 34 et 35 aLPD.[68] Il faudra attendre la révision de la directive en question pour connaître la répartition des compétences de poursuite et de jugement sous l'égide des art. 60 ss LPD.

5. Questions choisies

[42] Dans ce chapitre, nous aborderons quelques questions choisies en lien avec les dispositions pénales de la LPD, à savoir le devoir de discrétion (*infra* 5.1), le transfert de données à l'étranger (*infra* 5.2) et l'identification de la personne responsable (*infra* 5.3).

5.1. Le devoir de discrétion

[43] Jusqu'au 31 août 2023, l'art. 35 al. 1 aLPD (*violation du devoir de discrétion*) prévoyait ce qui suit : « *La personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans l'exercice d'une profession qui requiert la connaissance de telles données, est, sur plainte, punie de l'amende.* »

[44] L'ancienne disposition exigeait tout d'abord l'illicéité de la révélation. L'auteur de la révélation pouvait ainsi se prévaloir d'un motif justificatif (consentement, intérêts prépondérants, loi) pour révéler des données personnelles sans violer l'art. 35 al. 1 aLPD.

[45] Ensuite, la révélation devait porter sur des données personnelles secrètes et sensibles ou sur des profils de la personnalité. Les « données personnelles secrètes et sensibles » et les « profils de la personnalité » étaient définis à l'art. 3 let. c et d aLPD. Les premières étaient définies comme des données personnelles sur (i) les opinions ou activités religieuses, philosophiques, politiques ou syndicales, (ii) la santé, la sphère intime ou l'appartenance à une race, (iii) des mesures d'aide sociale, ou (iv) des poursuites ou sanctions pénales et administratives. Les profils de la personnalité étaient définis comme un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

[46] Le champ d'application de l'art. 35 aLPD était donc restreint. En 30 ans d'application, la norme a donné lieu à quelques procédures[69], mais aucune condamnation n'a été prononcée à notre connaissance (du moins selon la jurisprudence accessible en ligne).

[47] Avec la révision de la LPD, le législateur a procédé à un véritable changement de paradigme. L'art. 62 LPD rend désormais punissable d'une amende de CHF 250'000.– au plus la révélation intentionnelle de *toute donnée personnelle secrète* portée à la connaissance de l'auteur dans l'exercice d'une profession qui requiert la connaissance de telles données.

---

67 Art. 11 al. 1 de la loi d'application du code pénal suisse et d'autres lois fédérales en matière pénale (LaCP ; RS GE E 4 10).

68 Art. 7 de la Directive du Procureur général sur les contraventions (D7), état au 10 novembre 2021.

69 Voir p. ex. Kreisgericht SG du 1 décembre 2005, in : RSJ 102/2006, p. 522 ; OGer BE du 18 janvier 2007, in : RJ 2008, n° 1603 ; TC NE du 17 mars 2011, in : RJN 2011, p. 248 ; TC FR du 15 mai 2018 n° 502 2018 30 ; TC VD du 10 septembre 2021, in : CREP 2021/837.

[48] La norme consacre donc une forme de « secret professionnel général ».[70] Au contraire du secret de fonction de l'art. 320 CP et du secret professionnel de l'art. 321 CP, qui constituent des délits propres purs[71], l'art. 62 LPD ne se limite pas à certaines catégories professionnelles comme les membres d'une autorité, les fonctionnaires, les avocats, les notaires ou les médecins.

[49] Le Conseil fédéral a expliqué à ce propos que l'art. 62 LPD « *permet de combler les lacunes qui résultent du cercle restreint des auteurs touchés par les art. 320 et 321 CP* ».[72] Y avait-il réellement des lacunes à combler ? Cette interrogation explique peut-être l'accueil très froid réservé à la disposition correspondante de l'avant-projet lors de la procédure de consultation.[73] Malgré cela, le Conseil fédéral a maintenu l'art. 62 LPD dans le projet de loi[74] et la disposition a été adoptée sans discussion par le parlement.

[50] Le texte légal permet d'identifier les éléments constitutifs suivants :

- Des **données personnelles :** notion centrale de la LPD définie à son art. 5 let. a (« *toutes les informations concernant une personne physique identifiée ou identifiable* »), nous renvoyons aux contributions sur le sujet[75], étant précisé que la notion de données personnelles d'une personne physique est la même que sous l'ancien droit de la protection des données.
- Le caractère **secret** des données personnelles : la protection pénale de l'art. 62 LPD ne s'étend pas à toutes les données personnelles mais aux seules données secrètes. Le Message établit expressément un parallèle entre l'art. 62 LPD et les art. 320 et 321 CP : « *C'est ainsi la notion matérielle de secret du droit pénal qui est pertinente* ».[76] On se référera donc à la jurisprudence y relative, selon laquelle, de façon générale, est secret le fait qui n'est connu que d'un cercle restreint de personnes. Il ne peut s'agir d'un fait ayant déjà été rendu public ou qui est accessible sans difficulté à toute personne souhaitant en prendre connaissance. Il faut en outre qu'il existe un intérêt légitime à ce que le fait soumis au secret ne soit connu que d'un cercle déterminé de personnes, et que le bénéficiaire du secret veuille maintenir celui-ci.[77]
- Des données personnelles secrètes qui ont été **portées à la connaissance de l'auteur dans l'exercice d'une profession qui requiert la connaissance de telles données :** cet élément constitutif figurait déjà à l'art. 35 aLPD. Il faut que les données révélées soient nécessaires à l'exercice de la profession.[78] Le salaire et la fortune d'un potentiel emprunteur sont des

70 Le « *kleine Berufsgeheimnis* » ou le « *Berufsgeheimnis für jedermann* » pour reprendre les expressions de Rosenthal/Gubler (nbp. 15), p. 59.

71 Jean-Marc Verniory, in : Commentaire romand du Code pénal II, Bâle 2017 (cité : CR CP II-Auteur), Art. 320 N. 8.

72 FF 2017 6717.

73 Cf. OFJ, Synthèse des résultats de la procédure de consultation, 10 août 2017, *ad* art. 52, p. 49.

74 Entre l'avant-projet et le projet, l'hypothèse des « *données personnelles secrètes traitées par [l'auteur] à des fins commerciales* » a été supprimée.

75 Rainer J. Schweizer/Severin Bischof, Der Begriff der Personendaten, in : digma – Zeitschrift für Datenrecht und Informationssicherheit, Bruno Baeriswyl/Beat Rudin/Bernhard M. Hämmerli/Rainer J. Schweizer/Günter Karjoth/David Vasella (éd.), 2011, p. 152 ss ; Philippe Meier/Nicolas Tschumy, L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !, in : Jusletter du 23 janvier 2017 ; Philippe Meier, Protection des données, Fondements, principes généraux et droit privé, Berne 2010, N. 418 ss ; Rudin, in : Baeriswyl/Pärli/Blonski (nbp. 28), Art. 5 N. 2 ss.

76 FF 2017 6717.

77 Sur le tout : TF 6B_105/2020 du 3 avril 2020, consid. 1.1 et les références citées.

78 GE Cour de justice, ACPR/369/2020 du 4 juin 2020, consid. 4.3.2.

données personnelles secrètes dont les employés de banque chargés d'apprécier la solvabilité dudit client potentiel prennent connaissance dans l'exercice d'une profession qui requiert la connaissance de ces données. Tel n'est en revanche pas le cas du coiffeur dont le client se confie sur ces mêmes sujets, puisque ces données ne lui sont pas nécessaires pour exercer sa profession.[79]

- Le comportement punissable consiste en la **révélation** de ces données personnelles secrètes : ici aussi, ce sont les art. 320 et 321 CP qui ont servi d'inspiration directe au Conseil fédéral[80], ce qui devra conduire à appliquer la jurisprudence y relative.[81]
- La disposition s'applique à **quiconque** adopte le comportement punissable en question. L'art. 62 al. 2 LPD étend l'infraction aux personnes qui exercent des activités pour le compte d'une personne soumise à l'obligation de garder le secret ou qui sont en formation chez cette dernière. La norme ne se limite pas aux employés de la personne soumise au secret, mais elle vise également les mandataires qui exercent des activités « *pour le compte* » de cette personne.[82] En outre, la révélation demeure punissable alors même que l'exercice de la profession ou la formation ont pris fin (art. 62 al. 3 LPD).
- Sous l'angle subjectif, l'infraction est **intentionnelle**, ce qui inclut le dol éventuel.

[51] Ainsi définis, les contours de l'infraction paraissent extraordinairement flous, au point que sa comptabilité avec l'art. 1 CP (*nullum crimen sine lege*) puisse être remise en question.[83] À notre sens, il serait souhaitable que la jurisprudence interprète restrictivement l'art. 62 LPD. Le champ d'application de la disposition devrait être réduit à plusieurs égards.

[52] D'abord, selon le Message du Conseil fédéral, « *[l]a révélation des données peut être justifiée par l'autorisation de la personne concernée. Les règles générales, ainsi que les principes développés par la jurisprudence et la doctrine dans le cadre de l'art. 321, ch. 2, CP, s'appliquent par analogie* ».[84] Ainsi, lorsque la personne concernée a donné son consentement à une révélation, la révélation ne saurait être pénalement répréhensible sous l'angle de l'art. 62 LPD.

[53] À l'instar de ce qui prévaut sous l'égide de l'art. 321 ch. 2 CP, le consentement n'est soumis à aucune forme : il peut être exprès, tacite ou résulter d'actes concluants.[85] À notre sens, il n'est pas d'emblée exclu de soumettre à la personne concernée une clause de renonciation *anticipée* au secret. Toutefois, la portée de la clause doit être suffisamment claire pour que la personne concernée sache à quoi elle consent.[86] Dans tous les cas, elle ne saurait emporter ni renonciation au secret pour *toutes* les données personnelles confiées par la personne concernée, ni renonciation *irrévocable*.

---

79 GE Cour de justice, ACPR/369/2020 du 4 juin 2020, consid. 4.3.2 en référence au Message du 23 mars 1988, FF 1988 II 491.

80 FF 2017 6717.

81 ATF 142 IV 65, c. 5.1 ; TF 6B_105/2020 du 3 avril 2020, consid. 1.1 et les références citées ; Voir également l'approche différente adoptée dans l'arrêt TF, 6B_1403/2017 du 8 août 2018, consid. 1.2.

82 Wohlers, in : Baeriswyl/Pärli/Blonski (nbp. 28), Art. 62, N. 27.

83 Rosenthal/Gubler (nbp. 15), p. 60–61.

84 FF 2017 6717.

85 ATF 98 IV 218, consid. 2 ; Bernard Corboz, Les infractions en droit suisse, Volume II, 3e éd., Berne 2010, Art. 321 N. 48 ; François Bohnet/Luca Melcarne, La levée du secret professionnel de l'avocat en vue du recouvrement de ses créances d'honoraires, in : SJ 2020 II p. 29 ss, p. 33.

86 Nous rejoignons ici l'avis de Bohnet/Melcarne (nbp. 85), p. 33 s. exprimé dans le contexte de la relation avocat-client et du recouvrement des honoraires.

[54] Ensuite, il faut à notre sens admettre, en application de l'art. 14 CP, que la personne qui révèle des données personnelles secrètes *conformément* à la LPD ne saurait se voir reprocher une violation de l'art. 62 LPD. En d'autres termes, même si l'art. 62 LPD n'exige plus expressément – contrairement à l'art. 35 aLPD – l'illicéité de la révélation, le respect des exigences posées par le LPD exclut selon nous la punissabilité d'une révélation de données personnelles secrètes. Dès lors, les motifs justificatifs de l'art. 31 LPD doivent pouvoir être invoqués par l'auteur de la révélation pour exclure sa punissabilité. La révélation pourrait également être licite au regard d'autres normes, par exemple du droit de procédure[87] ou du droit de la fonction publique fédérale[88], qui permettent ou imposent ladite révélation.

[55] Nous rejoignons en outre l'avis de Rosenthal/Gubler qui estiment que le champ d'application de l'art. 62 LPD ne saurait s'étendre à toutes les données personnelles non publiques ou non accessibles dont une personne a connaissance dans l'exercice de sa profession, mais qu'il devrait être limité à celles qui remplissent deux critères cumulatifs : (i) la personne concernée pouvait objectivement attendre de l'auteur qu'il garde les données en question secrètes et (ii) les données en question ont été portées à la connaissance de l'auteur avec cette attente et non dans un autre contexte.[89]

[56] Enfin, au sein d'une même entreprise, il faut selon nous privilégier une approche relativement libérale : il ne nous semble pas que l'art. 62 LPD ait été adopté pour punir pénalement l'employé qui discute avec son voisin de bureau à la pause de midi.[90] Sous l'angle de l'art. 62 LPD, le cercle des personnes qui sont légitimées à savoir (« *need to know* ») doit à notre sens être défini de manière large, de sorte à incriminer essentiellement les révélations à des tiers.[91]

[57] On précisera par ailleurs que, à notre sens, l'art. 62 LPD ne peut pas être invoqué au titre des « *autres secrets protégés par la loi* » pour refuser de répondre comme témoin ou partie, ou pour refuser de produire des pièces, au pénal[92] comme au civil.[93] En particulier, l'art. 62 LPD ne constitue pas une restriction au séquestre[94] ni, par ricochet, un motif de mise sous scellés.[95] En effet, l'art. 2 al. 3 LPD prévoit que « *les droits des personnes concernées [dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par des dispositions fédérales de procédure] obéissent au droit de procédure applicable* ». À notre sens, l'exclusion de l'art. 2 al. 3 LPD est complète : le droit de procédure applicable règle toutes les questions liées aux droits de toutes les personnes concernées par la procédure, y compris donc par exemple les tiers sommés de comparaître ou de

87 P. ex. art. 163 al. 2 CPP et art. 160 CPC.

88 Art. 22a LPers. On rappellera que la LPD s'applique aux organes fédéraux, mais non aux cantons et aux communes.

89 Rosenthal/Gubler (nbp. 15), p. 61 ; voir également : Jonas D. Gassmann, in : Steiner/Morand/Hürlimann (nbp. 34), Art. 62 N. 16. Cette interprétation restrictive nous paraît s'inscrire dans le prolongement de la jurisprudence précitée du Tribunal fédéral sur la notion de secret, qui exige, dans le contexte des art. 320 et 321 CP, un intérêt légitime au secret et une volonté du bénéficiaire du secret de maintenir celui-ci.

90 Exemple tiré de Rosenthal/Gubler (nbp. 15), p. 62.

91 Rosenthal/Gubler (nbp. 15), p. 62 ; *contra* Niklaus Oberholzer, in : Basler Kommentar zum Strafrecht, 4e éd., Bâle 2018, Art. 321 N. 20.

92 Art. 173 al. 2 CPP.

93 Art. 163 al. 2 et 166 al. 2 CPC.

94 Art. 264 CPP.

95 Art. 248 CPP.

produire des pièces, sans que ceux-ci ne puissent invoquer la LPD.[96] Le Message évoque en effet que l'exclusion de l'application de la LPD concerne « toutes les personnes impliquées » dans la procédure.[97] En revanche, l'art. 2 al. 3 LPD prévoit que la LPD s'applique aux procédures administratives de première instance. Dès lors, le tiers qui serait invité par l'administration à produire des pièces ou à témoigner pourrait invoquer l'art. 62 LPD pour refuser de répondre. Le droit (cantonal ou fédéral) applicable à la procédure administrative de première instance règle ensuite la question de l'admissibilité du refus.[98]

5.2. Transfert de données à l'étranger

[58] Une grande nouveauté parmi les modifications des dispositions pénales de la LPD consiste en la répression de la violation des dispositions relatives au transfert de données personnelles à l'étranger.

[59] En matière de communication de données personnelles à l'étranger, l'art. 16 LPD prévoit que si des données personnelles sont communiquées dans un État ne garantissant pas un niveau de protection adéquat[99], la protection des données doit être garantie autrement, par exemple à travers des clauses types de protection des données telles que les clauses modèles de l'Union européenne.[100] L'art. 17 LPD précise certaines situations dans lesquelles, malgré l'absence d'un niveau de protection adéquat, une communication peut tout de même être effectuée (par exemple avec le consentement de la personne concernée).

[60] L'analyse de la licéité des communications de données personnelles à l'étranger a fait l'objet de nombreux débats, en particulier lorsque les États-Unis ont été considérés comme un État ne garantissant plus un niveau de protection adéquat, d'abord dans l'Union européenne, puis en Suisse.[101]

[61] En raison de la récente décision de la Commission européenne selon laquelle une communication de données aux États-Unis peut être effectuée si les entreprises américaines ont adhéré au *EU-U.S. Data Privacy Framework*, les projets entrainant une communication de données aux États-Unis devraient cependant être à nouveau licites d'un point de vue européen.[102] En Suisse, le PFPDT a annoncé qu'une décision similaire serait prise dans les prochains mois.[103] Cette dé-

96 A l'inverse, sous l'égide de l'art. 2 al. 2 let. c aLPD, qui ne contenait pas la précision sur les « *droits des personnes concernées* » de l'art. 2 al. 3 LPD, la Cour de justice du canton de Genève avait jugé que la LPD restait applicable aux tiers non impliqués dans la procédure civile pendante (ACPR/369/2020 du 4 juin 2020, consid. 4.3.1).

97 FF 2017 6633.

98 Voir par exemple à Genève : art. 32 al. 2 LPA (RS GE E 5 10).

99 La liste des Etats garantissant un niveau de protection adéquat figure à l'Annexe 1 de l'OPDo.

100 Le recours aux clauses modèles de l'Union européenne ne garantit pas toujours un niveau de protection approprié. Sur ce point : Fischer/Pittet, L'utilisation des services *cloud* (nbp. 23), p. 50 ss.

101 Dans l'Union européenne, à la suite de la décision n° C311/18 du 16 juillet 2020 de la Cour de justice de l'Union européenne dans le cadre de l'affaire dite Schrems II ; en Suisse, selon le communiqué du PFPDT du 8 septembre 2020 qui estime que le bouclier de protection des données Suisse – États-Unis n'offre pas un niveau de protection des données adéquat. Sur ces décisions : Philipp Fischer, Schrems II ou la quadrature du cercle, 18 octobre 2020 in : www.swissprivacy.law/17.

102 Pour accéder à la décision d'adéquation : https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_3721. Pour une analyse de la décision : Philipp Fischer, Le EUU.S. Data Privacy Framework déploie (enfin !) ses effets, 11 juillet 2023 in : www.swissprivacy.law/238.

103 https://www.edoeb.admin.ch/edoeb/fr/home/kurzmeldungen/20230410_eu_us_dpf.html (consulté le 17 août 2023).

cision est particulièrement rassurante pour les responsables du traitement souhaitant mettre en place des projets de type *cloud*, prestations qui requièrent souvent le transfert de données aux États-Unis.[104]

[62] Il paraît néanmoins utile d'analyser la situation juridique antérieure au *EU-U.S. Data Privacy Framework* et au potentiel « *CH-U.S. Data Privacy Framework* » (infra 5.2.1) et celle qui va s'en suivre (infra 5.2.2).

5.2.1. Avant le Data Privacy Framework

[63] En pratique, pour déterminer la licéité d'un transfert à l'étranger dans un État ne garantissant pas un niveau de protection adéquat, notamment les États-Unis, et en particulier en cas de recours à des services *cloud*, les responsables du traitement ont développé une approche basée sur le risque (*risk based approach*).[105] Cette approche évalue par exemple le risque qu'une autorité étrangère accède aux données. En fonction des résultats obtenus lors de cette analyse des risques, le recours aux services *cloud* est considéré comme licite ou non, étant précisé qu'un risque résiduel d'un accès par des autorités d'États non-adéquats est souvent considéré comme acceptable et donc le recours aux services *cloud* licite.[106]

[64] Lorsque le responsable du traitement est également soumis au RGPD, cette analyse des risques est souvent obligatoire. En effet, le responsable du traitement européen est en principe obligé d'effectuer une analyse d'impact du transfert (*Transfert impact assessment* ou TIA) en cas de communication de données personnelles aux États-Unis.[107] D'un point de vue suisse, cette analyse de risque est actuellement également recommandée. En effet, dans son Guide pour l'examen de la licéité de la communication transfrontière de données, le PFPDT estime qu'une analyse de transfert de données doit être effectuée dans chaque cas lorsque des données sont communiquées dans des États ne garantissant pas un niveau de protection adéquat.[108]

[65] En contradiction avec cette pratique selon laquelle l'existence d'un risque résiduel est acceptable, le PFPDT a considéré qu'en cas de communication transfrontalière, les mesures de protection prises par le responsable du traitement doivent réduire *à zéro* le risque d'accès aux données

104 Pour une analyse détaillée des enjeux liés au recours à des services *cloud* par des responsables du traitement privés : Fischer/Pittet, L'utilisation des services *cloud* (nbp. 23).

105 Voir notamment la décision du Conseil d'État du canton de Zurich du 30 mars 2022 (« *542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung* »), la pratique de la SUVA publiée dans le prise de position du PFPDT du 13 juin 2022 (« *Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Project Digital Workplace* ») ainsi que la prise de position de la Confédération du 31 août 2022 (« *Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung* »).

106 Cf. notamment : David Rosenthal, Frequently asked questions (faq) on the risk of foreign lawful access and the statistical « rosenthal » method for assessing it du 12 octobre 2022 ; David Vasella, Zurich government council : green light for M365 – Rosenthal risk assessment model canonicalized – risk threshold at 10% over 5 years ; Fischer/Pittet, L'utilisation des services *cloud* (nbp. 23), p. 66 s. ; Gassmann, in : Steiner/Morand/Hürlimann (nbp. 34), Art. 61 N.10.

107 Cette obligation été mise en place à la suite de la décision n° C311/18 du 16 juillet 2020 de la Cour de justice de l'Union européenne dans le cadre de l'affaire dite Schrems II. Avec l'implémentation du Data Privacy Framework, un TIA ne sera vraisemblablement plus obligatoire en cas de communication des données aux États-Unis.

108 Guide du PFPDT pour l'examen de la licéité de la communication transfrontière de données, p. 6. Une fois le *CH-US Data Privacy Framework* mis en place, cette obligation ne devrait probablement plus être exigée en cas de transfert de données personnelles aux Etats-Unis.

personnelles par une autorité étrangère, faute de quoi le transfert est jugé incompatible avec la LPD (nonobstant la mise en place des clauses contractuelles types).[109]

[66] Cette position du PFPDT révèle la complexité de la question et les divergences d'opinions entre les différentes autorités de protection des données suisses. En effet, dans une décision[110] du 30 mars 2022, le Conseil d'État du canton de Zurich avait estimé – après avoir consulté notamment le Préposé cantonal zurichois à la protection des données ainsi que les autorités de poursuite pénale – qu'une approche fondée sur les risques pouvait être appliquée pour analyser la licéité du recours à des services *cloud* par l'administration cantonale zurichoise et que l'existence d'un risque résiduel ne violait pas la LPD.

[67] Les développements ci-dessus mettent en évidence le conflit de devoirs auquel est confronté le responsable du traitement suisse, en particulier si ce dernier est également soumis au RGPD. D'une part, il est dans l'obligation d'effectuer un TIA qui conclura vraisemblablement à l'existence de certains risques, même résiduels. D'autre part, en ayant connaissance du résultat de ce TIA et du risque résiduel, il s'expose à une violation de la LPD en allant de l'avant dans son projet si les autorités pénales se rallient à la position du PFPDT selon laquelle aucun risque résiduel n'est accepté (risque zéro).[111]

[68] Selon nous, une interprétation euro-compatible de l'art. 61 let. a LPD doit prévaloir, conformément au but poursuivi par le législateur lors de la révision de la loi.[112] Le responsable du traitement qui a effectué une analyse de risques conformément aux exigences du RGPD ne saurait se voir reprocher d'avoir violé l'art. 61 let. a LPD par dol éventuel s'il transfère des données personnelles à l'étranger malgré un risque *résiduel* d'accès par une autorité mis en évidence par l'analyse. Une violation par dol éventuel de l'art. 61 let. a LPD pourra en revanche être retenue si le responsable du traitement procède au transfert alors que son analyse de risques révélait des risques importants d'accès à ces données par une autorité étrangère.

5.2.2. Après le Data Privacy Framework

[69] Avec la mise en place du *Data Privacy Framework* dans l'Union européenne, et en Suisse dans un futur proche, les États-Unis garantiront un niveau de protection adéquat pour les données personnelles transférées vers des entreprises américaines qui adhèrent au *Data Privacy Framework*. Il en découle que le transfert de données aux États-Unis ne devra probablement plus s'accompagner automatiquement d'une analyse de risques. Les responsables du traitement n'auront pas non plus l'obligation de mettre en place des clauses-modèles pour assurer la sécurité des données personnelles transférées.

---

109 Guide du PFPDT pour l'examen de la licéité de la communication transfrontière de données ; Prise de position du PFPDT du 13 juin 2022 relative à un projet de la Caisse nationale suisse d'assurance en cas d'accidents (SUVA) ; Pour une analyse de cette prise de position : Sylvain Métille, L'utilisation de Microsoft 365, illégale en Suisse ?, 17 juin 2022, in : https ://smetille.ch/2022/06/17/lutilisation-de-microsoft-365-illegale-en-suisse/ ; Philipp Fischer/Sébastien Pittet, Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?, 16 août 2022 in : www.swissprivacy.law/165.

110 Décision du 30 mars 2022 du Conseil d'État du canton de Zurich « *542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung* ».

111 Dans le cadre de l'analyse de l'utilisation des services *cloud* du Conseil d'État du canton de Zurich du 30 mars 2022, les autorités de poursuite pénale cantonales s'étaient montrées favorables au projet.

112 Cf. *supra* 2.

[70] Néanmoins, si le projet du responsable du traitement implique une communication dans d'autres États ne garantissant pas un niveau de protection adéquat – à travers le recours direct à un sous-traitant ou le recours indirect à des « sous-sous-traitants » (ou sous-traitants ultérieurs) – le responsable du traitement devra respecter ses obligations qui découlent de l'art. 16 al. 2 LPD ou se prévaloir d'une dérogation (art. 17 LPD).

[71] En outre, si les mesures mises en place pour assurer la sécurité des données (art. 16 al. 2 LPD) ne peuvent pas être implémentées en raison du droit interne de l'État récipiendaire, les questions en lien avec l'analyse de la licéité d'un transfert de données personnelles aux États-Unis soulevées avant l'entrée en vigueur du *Data Privacy Framework* pourraient rester d'actualité.

5.3. Responsabilité

[72] La révision de la LPD a généré une certaine inquiétude dans les milieux intéressés[113] : le « simple » employé sera-t-il amendé à hauteur de plusieurs dizaines de milliers de francs, sans que sa hiérarchie ne soit inquiétée, ni que l'entreprise qui l'emploie ne soit sanctionnée ?

[73] Pour rappel, la LPD régit le traitement de données concernant des personnes physiques effectué par des personnes privées ou des organes fédéraux (art. 2 al. 1 LPD). Si la notion de personne privée n'est pas spécifiquement définie dans la loi, il est établi que cette notion couvre aussi bien une personne physique qu'une personne morale[114] qui traite des données dans le cadre d'une relation de droit privé.[115]

[74] Selon le texte de la loi, les infractions pénales de la LPD ne peuvent être commises que par les personnes privées, à l'exclusion des organes fédéraux.[116] Une interprétation littérale de ces dispositions pourrait conduire à admettre qu'une personne morale, responsable du traitement, pourrait engager sa responsabilité en première ligne. Cette interprétation doit néanmoins être écartée, le Conseil fédéral ayant précisé que les sanctions pénales de la LPD ne visent pas l'entreprise, comme en droit européen, mais bien la personne physique responsable de la violation.[117] Cela ressort également de l'art. 6 DPA (applicable par renvoi de l'art. 64 al. 1 LPD) qui fixe le principe de la personnalité des peines, à savoir la responsabilité pénale primaire de la personne physique qui a commis l'infraction.[118]

[75] Le système de responsabilité pénale de la LPD est donc fondé sur une responsabilité de la personne physique (*infra* 5.3.1), la personne morale pouvant néanmoins être tenue pour responsable à titre subsidiaire (*infra* 5.3.2).

---

113 Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales – Synthèse des résultats de la procédure de consultation du 10 août 2017, p. 47.

114 Le projet de loi de 1992 indiquait d'ailleurs expressément qu'une personne privée était une « *personne physique ou morale soumise au droit privé* », mais le Parlement a jugé cette mention superflue, car évidente, et a finalement supprimé cette précision dans l'aLPD (BO 1991 E 1020) ; Meier (nbp. 75), N. 360.

115 Meier (nbp. 75), N. 361.

116 Selon l'art. 5 let. i LPD, un organe fédéral comprend « *l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération* ».

117 FF 2017 6713 ss.

118 Selon l'art. 6 al. 1 DPA, « *[l]orsqu'une infraction est commise dans la gestion d'une personne morale (…), les dispositions pénales sont applicables* ***aux personnes physiques qui ont commis l'acte*** » (mise en évidence ajoutée).

5.3.1. Responsabilité primaire de la personne physique

[76] Lorsque le responsable du traitement est une ou plusieurs personnes physiques, il est *a priori* aisé de déterminer le responsable de la violation de la LPD. La situation se complique en revanche lorsque le responsable du traitement est une personne morale, auquel cas la responsabilité doit être rattachée à une ou plusieurs personnes physiques en particulier.

[77] La responsabilité des infractions LPD commises dans une entreprise est régie par l'art. 64 LPD, qui renvoie aux art. 6 et 7 DPA. Selon l'art. 6 al. 1 DPA, « *[l]orsqu'une infraction est commise dans la gestion d'une personne morale, d'une société en nom collectif ou en commandite, d'une entreprise individuelle ou d'une collectivité sans personnalité juridique ou de quelque autre manière dans l'exercice d'une activité pour un tiers, les dispositions pénales sont applicables aux personnes physiques qui ont commis l'acte* ». L'art. 6 al. 1 DPA rattache ainsi dans un premier temps la responsabilité pénale à l'auteur (*i.e.*, la personne physique) qui a commis l'infraction.[119]

[78] Concrètement, la personne physique en charge de la décision de l'entreprise de communiquer des données à l'étranger ou de recourir à un sous-traitant s'expose à une responsabilité pénale. Il devrait en être de même de celle qui signe (i) la réponse à une demande d'accès ou (ii) la communication de renseignements en lien avec une collecte de données ou de décision individuelle automatisée. Selon les circonstances, un conseiller externe de l'entreprise tel qu'un avocat pourrait également encourir une responsabilité pénale.[120]

[79] S'agissant du conseiller à la protection des données que le responsable du traitement a la possibilité de nommer (art. 10 LPD), on rappellera que son rôle est de former et de conseiller le responsable du traitement. Comme sous le régime de l'aLPD, le conseiller à la protection des données ne doit pas endosser la responsabilité du traitement.[121] Par conséquent, le conseiller à la protection des données qui se limite dans son activité à son rôle de conseiller ne devrait pas pouvoir être exposé à une responsabilité pénale.

[80] Parallèlement à la responsabilité de l'auteur direct de l'infraction, l'art. 6 al. 2 DPA crée également une responsabilité du chef d'entreprise, de l'employeur, du mandant ou du représenté qui, intentionnellement ou par négligence et en violation d'une obligation juridique, omet de prévenir une infraction commise par le subordonné, le mandataire ou le représentant. La violation d'une obligation au sens de l'art. 6 al. 2 DPA suppose une position de garant, soit l'existence d'une obligation juridique spécifique d'empêcher le comportement en cause en exerçant une surveillance, en donnant des instructions et en intervenant au besoin.[122] Selon le Message, les obligations de la LPD, comme toutes normes de droit administratif en principe[123], incombent aux dirigeants de l'entreprise lesquels sont chargés de veiller au respect de la loi.[124] Dès lors, la violation des obligations de la LPD peut être imputée aux dirigeants de l'entreprise.[125]

---

119 Nora Markwalder, Droit pénal de l'entreprise : Évolutions et perspectives en droit pénal administratif, in *:* Alain Macaluso/Laurent Moreillon/Carlo Lombardini/Andrew M. Garbarski (éd.), Développements récents en droit pénal de l'entreprise III, Berne 2022, p. 143 ss, p. 147.

120 Rosenthal/Gubler (nbp. 15), p. 58.

121 Voir notamment : FF 2017 6652.

122 ATF 142 IV 315, consid. 2.2.2.

123 ATF 142 IV 315, consid. 2.2.2.

124 FF 2017 6715.

125 FF 2017 6715.

[81] Le Message va même plus loin : les dirigeants de l'entreprise étant en général responsables des obligations de la LPD, ce sont eux qui devraient être sanctionnés pénalement le cas échéant, « *et non [les] simples exécutants* ».[126] Il n'est toutefois pas certain que cette vision se concrétise en pratique. D'abord, elle se réconcilie mal avec le fait que les art. 6 al. 1 DPA et 6 al. 2 DPA peuvent s'appliquer en parallèle et sanctionner potentiellement à la fois le dirigeant et le « simple exécutant ». Ensuite, le chef d'entreprise ne répond de sa négligence en vertu de l'art. 6 al. 2 DPA que si l'infraction qu'il a omise de prévenir est punissable par négligence également.[127] En présence d'infractions intentionnelles – comme les art. 60 ss LPD – il est nécessaire que le chef d'entreprise ait agi intentionnellement.

5.3.2. Responsabilité subsidiaire de la personne morale

[82] En matière de droit pénal de la protection des données, l'application de l'art. 102 al. 1 CP sur la responsabilité de l'entreprise est exclue dès lors qu'elle suppose un crime ou un délit. De même, les art. 60 ss LPD ne figurent pas au catalogue des infractions visées par l'art. 102 al. 2 CP.

[83] L'art. 64 al. 1 LPD prévoit en revanche l'application de l'art. 7 al. 1 DPA. Selon cette disposition, il est possible de renoncer à poursuivre les personnes physiques et de condamner l'entreprise au paiement de l'amende lorsque (i) l'amende envisagée ne dépasse pas CHF 5'000.– et (i) que l'enquête rendrait nécessaires à l'égard des personnes physiques des mesures d'instruction hors de proportion avec la peine encourue. L'art. 64 al. 2 LPD porte le seuil précité à CHF 50'000.– s'agissant des contraventions de la LPD.

[84] L'art. 7 DPA intervient ainsi comme une exception au principe de la personnalité des peines en permettant de sanctionner une entreprise en lieu et place de la personne physique. Contrairement à l'art. 102 CP, la *ratio legis* de l'art. 7 DPA est l'économie de procédure et non le défaut d'organisation (qui n'est dès lors pas une condition d'application de l'art. 7 DPA).[128] L'entreprise n'est pas condamnée pour l'infraction sous-jacente mais seulement contrainte à payer l'amende.[129] Initialement, l'art. 7 DPA avait été introduit pour remédier aux difficultés rencontrées par les autorités administratives à identifier les personnes physiques auteurs d'infractions, en particulier dans le domaine fiscal.[130]

[85] Une responsabilité subsidiaire de l'entreprise en cas de violation de la LPD est donc envisageable aux conditions suivantes : (i) une infraction est commise au sein de l'entreprise, (ii) l'amende ne doit pas dépasser les CHF 50'000.– et (iii) une enquête pour déterminer la responsabilité des individus selon l'art. 6 DPA engendrerait des mesures d'instruction disproportionnées au regard de l'amende encourue.

126 FF 2017 6715.

127 Fabio Burgener, La responsabilité pénale du chef d'entreprise, in *:* RPS 2015 p. 368 ss, p. 388 et les références ; Andrew M. Garbarski/Alain Macaluso, La responsabilité de l'entreprise et de ses organes dirigeants à l'épreuve du droit pénal administratif, in : PJA 2008 p. 833 ss, p. 842.

128 Markwalder (nbp. 119), p. 147.

129 La doctrine est partagée sur la question de déterminer si l'art. 7 DPA crée une responsabilité à caractère pénal et non uniquement une obligation de payer. Sur la question : Markwalder (nbp. 119), p. 148 et les références citées.

130 Allison Beretta, Sanctionner en vertu des art. 6 et 7 DPA, in *:* Jusletter du 8 juillet 2019, p. 3.

i. Infraction commise au sein de l'entreprise

[86] La responsabilité de l'entreprise fondée sur l'art. 7 DPA est possible uniquement si tous les éléments constitutifs d'une infraction sont réalisés.[131] La norme présente le même paradoxe que l'art. 102 al. 1 CP : son application suppose qu'une personne physique au moins remplisse (à elle seule) tous les éléments constitutifs objectifs et subjectifs d'une infraction alors même que l'autorité pénale ne poursuit pas une personne déterminée.[132] Dans un arrêt de 2006 rendu en matière de TVA, le Tribunal fédéral avait toutefois jugé, à raison, que l'on ne peut pas savoir si une infraction est commise intentionnellement ou par négligence lorsque les personnes physiques ne sont pas identifiées et que l'application de l'art. 7 DPA est envisagée.[133] Seules des considérations objectives devraient ainsi guider l'examen des éléments constitutifs et la fixation de la peine.[134]

ii. Amende maximale de CHF 50'000.–

[87] La responsabilité subsidiaire de l'entreprise conformément à l'art. 7 al. 1 DPA vise en principe des infractions d'importance mineure, conduisant à une amende n'excédant pas CHF 5'000.–. Par l'effet de l'art. 64 al. 2 LPD, ce montant est toutefois porté à CHF 50'000.– dans le cadre des infractions à la LPD.

[88] Le plafond de CHF 50'000.– est une condition d'application de l'art. 7 al. 1 DPA : si la peine concrètement encourue dans le cas d'espèce (par une personne physique) dépasse CHF 50'000, l'entreprise ne peut pas être sanctionnée.[135]

[89] Comme mentionné ci-dessus, l'entreprise est condamnée à payer une amende en lieu et place de la personne physique. La peine est ainsi fixée en fonction de la gravité de l'infraction de la personne physique, conformément à l'art. 47 al. 2 CP, et non en fonction de certains éléments liés à l'entreprise tels que son chiffre d'affaires ou la mauvaise organisation de l'entreprise.[136]

iii. Mesures d'instruction disproportionnées

[90] Pour qu'une responsabilité subsidiaire de l'entreprise puisse être envisagée, l'art. 7 al. 1 DPA exige encore que l'enquête rende nécessaires à l'égard des personnes physiques punissables des mesures d'instruction hors de proportion avec la peine encourue.

[91] L'interprétation de cette notion est difficile en raison du faible nombre de jugements fondés sur l'art. 7 al. 1 DPA. Si des sanctions en application de cette disposition sont certainement courantes en pratique, la condamnation n'est que rarement portée devant les tribunaux.

[92] Dans un arrêt du 13 août 2019, une entreprise a été condamnée à une amende de CHF 800.– par l'Office fédéral de l'énergie en raison d'une infraction à l'art. 56 de la loi fédérale concernant les installations électriques à faible et à fort courant.[137] Dans cet arrêt, le Tribunal fédéral

131 Markwalder (nbp. 119), p. 149.

132 Cf. l'arrêt « La Poste Suisse SA » (ATF 142 IV 333). Voir à ce sujet Katia Villard, La compétence du juge pénal suisse à l'égard de l'infraction reprochée à l'entreprise, 2017, N. 550.

133 TF 6S.488/2005 du 31 octobre 2006, consid. 3 ; Markwalder (nbp. 119), p. 149 ss.

134 Markwalder (nbp. 119), p. 149 ss.

135 TF 6S.488/2005 du 31 octobre 2006, consid. 2 ; Markwalder (nbp. 119), p. 149.

136 Markwalder (nbp. 119), p. 152.

137 TF 6B_596/2019 du 13 août 2019.

a confirmé l'application de l'art. 7 DPA en estimant, tout comme l'autorité cantonale, que l'audition des deux administrateurs de la société pour déterminer la personne physique responsable de l'infraction aurait pris du temps, aurait engendré des frais et que les administrateurs auraient de toute façon invoqué leur droit à garder le silence. Comme le relèvent Garbarski/Markwalder, même si cet arrêt semble favoriser une application extensive de l'art. 7 DPA, cette décision ne doit pas conduire à une utilisation abusive de la disposition qui doit s'analyser uniquement à titre subsidiaire.[138]

[93] L'autorité doit en principe toujours procéder à un minimum d'actes d'investigation destinés à identifier les responsables de l'infraction, l'ampleur de ces investigations devant être analysée en fonction de la peine envisagée. Dans l'arrêt précité, le montant relativement bas de l'amende (CHF 800.–) semble avoir joué un rôle important.[139]

[94] Une autre méthode pour analyser le caractère proportionnel des mesures d'instruction est proposée par Berretta[140] : elle consiste à octroyer un « crédit » aux autorités d'instruction du montant maximal de l'amende imputable (*i.e.*, en matière de LPD, fixé à CHF 50'000.–). Ce n'est qu'une fois le crédit épuisé sans avoir pu identifier l'auteur de l'infraction que l'autorité pourrait utiliser le mécanisme de l'art. 7 DPA. Cette méthode laisserait probablement l'art. 64 LPD lettre morte, le « crédit » paraissant assez élevé pour identifier une personne responsable d'une violation de la LPD dans la plupart des situations.[141]

[95] La notion de mesures d'instruction disproportionnées est indéfinie : l'autorité pénale dispose donc d'un pouvoir d'appréciation important à cet égard. Il n'en demeure pas moins qu'elle doit respecter le caractère subsidiaire et non alternatif de la responsabilité de l'entreprise fondée sur l'art. 7 al. 1 DPA : si la personne physique responsable de l'infraction peut être directement retrouvée et sanctionnée, l'autorité ne dispose en principe pas d'un choix entre une application de l'art. 6 DPA (responsabilité de la personne physique) et de l'art. 7 DPA (responsabilité de l'entreprise).[142]

[96] Il ressort toutefois de certaines décisions administratives que des entreprises ont été condamnées en application de l'art. 7 DPA alors que l'auteur de l'infraction sous-jacente était connu.[143] Dans ces constellations, il semblerait que l'administration ait considéré qu'il était disproportionné de punir personnellement l'employé ayant exécuté des instructions, s'écartant ainsi probablement du but initial de l'art. 7 DPA.[144]

---

138 Andrew Garbarski/Nora Markwalder, Responsabilité pénale de l'entreprise (art. 7 DPA) – caractère disproportionné des mesures d'instruction requises pour identifier l'auteur physique, in : www.verwaltungsstrafrecht.ch du 4 septembre 2019.

139 Garbarski/Markwalder (nbp. 138). Dans le cadre de l'application de l'art. 49 LFINMA, disposition similaire à l'art. 7 DPA, le Tribunal pénal fédéral a également considéré qu'une tentative réelle d'identification des personnes responsables était nécessaire avant de pouvoir déclencher une responsabilité subsidiaire de l'entreprise (SK.2018.47 du 26 avril 2019, consid. 5.11.4 s.).

140 Berretta (nbp. 130), p. 11 s.

141 Les autorités administratives qui appliquent déjà l'art. 7 DPA semblent également écarter cette méthode. En effet, des amendes en application de l'art. 7 DPA ont été prononcées pour des infractions fiscales malgré un plafond fixé à CHF 100'000.–, soit le double de l'art. 64 LPD (voir notamment : Markwalder (nbp. 119), p. 159 ss et Berretta (nbp. 130), p. 10).

142 Andrew Garbarski, L'entreprise dans le viseur du droit pénal administratif : éléments de droit matériel et de procédure, ZSTrR 120/2012, p. 409 ss, p. 419 ; Markwalder (nbp. 119), p. 150.

143 Markwalder (nbp. 119), p. 159.

144 Markwalder (nbp. 119), p. 159 qui effectue une analyse empirique détaillée de l'application de l'art. 7 DPA sur des données collectées auprès de la Direction générale des douanes.

6. Conclusion

[97] Le volet pénal est-il destiné à rester le « maillon faible » de la loi sur la protection des données ?[145]

[98] Si la nouvelle loi entrée en vigueur le 1er septembre 2023 marque une extension de l'appréhension par le droit pénal de certains comportements laissés jusqu'alors impunis, certains choix du législateur réduisent, du moins sur le papier, la probabilité d'une augmentation drastique des procédures pénales pour violation de la LPD. On pense notamment à la poursuite uniquement sur plainte et sans que le PFPDT ne puisse porter plainte directement[146], à l'absence de punissabilité de la négligence et à la compétence attribuée à des ministères publics, voire à des autorités administratives chargées de poursuivre les contraventions, qui n'ont probablement aucune expérience en la matière et certainement d'autres priorités.

[99] Cela dit, il convient d'être prudent au jeu des pronostics lorsque de nouvelles dispositions pénales entrent en vigueur. Les prochains mois et années montreront si le scepticisme affiché par plusieurs auteurs était justifié ou non.

[100] À notre sens, si certaines infractions de la loi révisée devraient continuer à jouer probablement un rôle de « garde-fous » (ainsi les art. 60 al. 1 let. a, 60 al. 2, 61 let. b et c ou encore 63 LPD)[147] et sanctionner en pratique des violations crasses des règles générales de la LPD, d'autres dispositions présentent en revanche un facteur de risque concret et non négligeable pour toute personne qui communique des données personnelles à l'étranger (art. 61 let. a LPD) ou pour toute personne qui se voit confier des données personnelles secrètes nécessaires à sa profession (art. 62 LPD). C'est dire que le cercle des personnes concernées est particulièrement vaste.

[101] En ce sens, ces dispositions pénales constituent des incitatifs supplémentaires à respecter la loi, incitatifs d'autant plus aigus que c'est en principe le porte-monnaie des personnes physiques, et non des entreprises, qui est menacé.

Me Joël Pahud, docteur en droit, est *Counsel* au sein du groupe Contentieux de l'étude d'avocats OBERSON ABELS SA. Il a débuté sa carrière auprès de l'une des principales études d'avocats suisses (2010–2014), avant d'exercer au sein du Ministère public de la Confédération comme procureur assistant, puis comme procureur (2014–2021).

Sébastien Pittet, titulaire du brevet d'avocat, est assistant-doctorant au sein du Centre de droit bancaire et financier de l'Université de Genève.

145 Contrairement au droit européen où les sanctions administratives jouent probablement un rôle prépondérant dans le respect des dispositions du RGPD.

146 *Supra* 4.

147 Dans ce sens : Wohlers, in : Baeriswyl/Pärli/Blonski (nbp. 28), Vorbem. Zu Art. 60 ff., N. 6 ss.