Protection des données personnelles dans la recherche menée par des organes publics

Cadre juridique et pratique actuelle

Astrid Epiney*

Flaminia Dahinden**

La présente contribution s'intéresse non seulement à la protection des données personnelles dans le cadre de recherches scientifiques menées par des organes publics, mais aussi aux conditions dans lesquelles des organes publics peuvent, voire doivent, communiquer des données personnelles à d'autres organes publics (notamment à des hautes écoles) à des fins de recherche. Elle analyse en particulier – sur la base de quelques considérations générales quant à l'application du droit de la protection des données – la portée du « privilège » de la recherche ainsi que la communication de données personnelles en lien avec la recherche.

Der vorliegende Beitrag befasst sich nicht nur mit dem Schutz personenbezogener Daten im Rahmen wissenschaftlicher Forschung durch öffentliche Stellen, sondern auch mit den Bedingungen, unter denen öffentliche Stellen personenbezogene Daten zu Forschungszwecken an andere öffentliche Stellen (insbesondere Hochschulen) weitergeben dürfen oder müssen. Auf der Grundlage einiger allgemeiner Überlegungen zur Anwendung des Datenschutzrechts werden insbesondere die Tragweite des Forschungsprivilegs sowie die Weitergabe personenbezogener Daten im Rahmen der Forschung analysiert.

Plan

I. Introduction et problématique

La recherche scientifique – définie dans la loi fédérale sur l'encouragement de la recherche et de l'innovation (LERI)[1] comme étant la « recherche méthodique de connaissances nouvelles » (art. 2 LERI) – repose largement sur la collecte, le traitement et l'analyse de données. Lorsqu'il s'agit de données à caractère personnel, ces activités soulèvent des questions spécifiques en matière de protection des données, notamment en ce qui concerne la conciliation entre les intérêts de la recherche et le respect des droits fondamentaux des personnes dont les données sont utilisées.

* Astrid Epiney est professeure de droit européen et international ainsi que de droit public à l'Université de Fribourg et directrice de l'Institut de droit européen.

** Flaminia Dahinden, MLaw, est collaboratrice scientifique à l'Institut de droit européen.

1 Loi fédérale du 14 décembre 2012 sur l'encouragement de la recherche et de l'innovation (LERI ; RS 420.1).

Si la majeure partie des activités de recherche (et leur financement) est assurée par des entreprises privées, les établissements de droit public y jouent également un rôle déterminant, notamment les écoles polytechniques fédérales (EPF), les universités cantonales, les hautes écoles spécialisées (HES) ainsi que les hautes écoles pédagogiques (HEP).[2] L'administration fédérale ou cantonale peut également être impliquée dans des activités de recherche afin d'accomplir les tâches publiques qui lui ont été attribuées. Ces projets de recherche peuvent être réalisés par l'administration elle-même, via ses unités administratives, ou être confiés à des hautes écoles, des entreprises privées ou d'autres institutions de recherche.[3] Par ailleurs, les organes publics peuvent être sollicités par des chercheurs et chercheuses qui demandent l'accès à des données personnelles en possession d'un organe public afin de mener une recherche scientifique. Se pose alors la question de savoir dans quelle mesure et à quelles conditions l'organe public peut communiquer des données personnelles qui seront utilisées dans le cadre d'une recherche scientifique.

La présente contribution s'intéresse à la protection des données personnelles lors de recherches menées par des organes publics, plus particulièrement des organes cantonaux, étant donné que les universités cantonales, les HES et les HEP relèvent de la compétence des cantons. Ces établissements de droit public sont confrontés à de nombreuses questions juridiques lorsque, dans le cadre de leurs activités de recherche, ils doivent collecter, conserver ou encore transmettre des données. Dans le contexte des recherches menées au sein des hautes écoles, il sied de rappeler qu'une recherche est aussi considérée comme une recherche entreprise par la haute école si le chercheur ou la chercheuse n'est pas employé-e mais étudiant-e et que la recherche est menée dans le cadre de la haute école en question sous la supervision d'une personne employée à la haute école (comme c'est le cas, par exemple, pour les travaux de Bachelor ou de Master). La personne qui supervise ces travaux devra être considérée comme responsable du traitement des données.

Ainsi, cette contribution vise à déterminer le cadre légal applicable au traitement de données personnelles dans le contexte de la recherche en Suisse – principalement hors domaine de la santé. Pour ce faire, il s'agira, dans un premier temps, de répondre à la question de l'applicabilité du droit de la protection des données au domaine de la recherche et d'esquisser les principes généraux applicables dans ce contexte (II.), avant de se pencher sur les règles de protection des données personnelles au niveau fédéral (III.), puis cantonal, en prenant pour exemple le canton de Fribourg (IV.). Dans un second temps, nous traiterons de la question spécifique de la communication de données (personnelles) à des tiers en vue d'un projet de recherche (V.), avant de formuler une brève conclusion (VI.). Dans une annexe, nous résumerons les quelques arrêts en la matière tirés de la jurisprudence cantonale et fédérale (VII.).

II. Applicabilité du droit de la protection des données

Dans ce chapitre, il sera fait référence à la loi fédérale sur la protection des données (LPD)[4] qui s'applique au traitement de données personnelles concernant des personnes physiques effectué par des personnes privées ou par des organes fédéraux (art. 2 al. 1 LPD). Les considérations développées ci-dessous sont toutefois applicables *mutatis mutandis* aux législations cantonales sur la protection des données, ces dernières étant largement similaires au droit fédéral.

A. Champ d'application de la LPD

1. Traitement de données personnelles

La définition des notions de « traitement » et de « données personnelles » joue un rôle central dans la mesure où elle délimite le champ d'application matériel de la LPD (art. 2 al. 1 LPD).[5] Pour ce qui est du « traitement », ce dernier est à comprendre de façon très large. En effet, selon la définition légale de l'art. 5 let. d LPD, il s'agit de « toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés […] ».[6] à

---

2 Secrétariat d'état à la formation, à la recherche et à l'innovation (SEFRI), Recherche et innovation en Suisse – Rapport intermédiaire 2022, Berne 2022, 26 ss.

3 Secrétariat d'état à la formation, à la recherche et à l'innovation (SEFRI), La recherche et l'innovation en Suisse, Internet : https://www.ressortforschung.admin.ch/rsf/fr/home.html (consulté le 16.7.2025).

4 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD ; RS 235.1).

5 CR LPD-Meier/Tschumy, art. 5 N 18, in : Commentaire romand sur la loi fédérale sur la protection des données, Bâle 2023 (cit. CR LPD-auteur) ; Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2011 (cit. Protection des données), N 418 ss.

6 Le fait que l'opération se fasse de manière automatisée ou manuelle n'a pas d'influence sur la qualification de cette opération en tant que traitement au sens de la LPD, cf. CR LPD-Meier/Tschumy (n. 5), art. 5 N 74.

titre exemplatif, la disposition cite la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données personnelles.

Il peut être noté que les opérations citées ci-dessus se retrouvent généralement dans les activités de recherche, bien qu'à des stades différents. Par exemple, la « collecte » des données peut inclure les enquêtes, les entretiens ou les prélèvements ; l'« utilisation » couvre notamment l'analyse, l'évaluation ou la modélisation ; la « communication » comprend le partage avec des partenaires de recherche ou la publication des résultats. Par ailleurs, la liste de l'art. 5 let. d LPD n'étant pas exhaustive,[7] d'autres opérations typiques de la recherche peuvent tomber sous la notion de traitement, telles que l'anonymisation,[8] la pseudonymisation,[9] la réutilisation[10] ou encore le croisement de données.

Tout comme la notion de traitement, celle de « données personnelles » doit être comprise de façon très large.[11] En effet, elle couvre « toutes les informations concernant une personne physique identifiée ou identifiable » (art. 5 let. a LPD). En soi, une donnée constitue n'importe quelle information, peu importe sa forme, son contenu ou son support.[12] Toutefois, pour qu'elle soit qualifiée de donnée personnelle, il faut qu'elle se rattache à une personne physique identifiée ou identifiable.[13] Une personne est réputée identifiée lorsqu'il ressort directement de l'information qu'il s'agit précisément de cette personne (telle que la pièce d'identité), alors qu'elle est considérée comme identifiable si la corrélation d'informations tirées des circonstances ou du contexte permet son identification (comme le numéro de téléphone, le numéro AVS, l'adresse postale ou encore des éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de la personne).[14]

À noter que la LPD prévoit une sous-catégorie de données personnelles, à savoir les données personnelles sensibles (dites données sensibles) qui bénéficient d'une protection spécifique en raison du risque accru que leur traitement peut entraîner pour la personnalité et les droits fondamentaux de la personne concernée.[15] Listées de manière exhaustive à l'art. 5 let. c LPD, il s'agit (1) des données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, (2) des données sur la santé, la sphère intime ou l'origine raciale ou ethnique, (3) des données génétiques, (4) des données biométriques identifiant une personne physique de manière univoque, (5) des données sur des poursuites ou sanctions pénales et administratives ainsi que (6) des données sur des mesures d'aide sociale. La qualification de données comme étant des données sensibles entraîne plusieurs conséquences.[16] Par exemple, elle influence la forme du consentement qui, lorsqu'il est requis, doit être exprès pour le traitement de données sensibles (art. 6 al. 7 let. a LPD)[17] ou impose des obligations au responsale du traitement qui doit procéder à une analyse d'impact relative à la protection des données personnelles lors d'un traitement de données sensibles à grande échelle (art. 22 al. 1 et 2 let. a LPD).

Ainsi, le traitement de données constitue un élément central des projets de recherche, impliquant fréquemment des données personnelles, voire sensibles, comme les données de santé en médecine ou les opinions politiques en sciences sociales.

---

7 CR LPD-Meier/Tschumy (n. 5), art. 5 N 74.

8 TF, 4A_365/2017, 26.2.2018, c. 5.2.2 ; CR LPD-Meier/Tschumy (n. 5), art. 5 N 27.

9 HGer ZH, HG190107-O, 4.5.2021, c. 3.2.3a ; BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, art. 5 N 34, in : Gabor P. Blechta/David Vasella (éds), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 4e éd., Bâle 2023 (cit. BSK DSG-auteur).

10 Dans le cadre de la recherche, il est question de « traitements primaires » lorsqu'il s'agit de collecter les données (« collecte »), tandis que les « traitements secondaires » désignent les traitements effectués par ceux et celles qui réutilisent les données à des fins de recherche (« réutilisation »), cf. Hélène Bruderer, La réutilisation des données personnelles liées à la santé à des fins de recherche scientifique – étude de droit suisse avec des perspectives de droit comparé, Genève/Zurich 2023, 9 s.

11 CR LPD-Meier/Tschumy (n. 5), art. 5 N 19 ; Sylvain Métille, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations, in : Astrid Epiney/Sophie Moser/Sophia Rovelli (éds), La révision de la Loi fédérale sur la protection des données, Zurich/Bâle/Genève 2022, 1 ss, 4.

12 CR LPD-Meier/Tschumy (n. 5), art. 5 N 20.

13 CR LPD-Meier/Tschumy (n. 5), art. 5 N 21 s.

14 Message du Conseil fédéral du 15 septembre 2017 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 6565 (cit. Message LPD 2017), 6639 ; Rachel Christinat, Protection des données et recherche – Le droit des personnes concernées, in : Sylvain Métille (éds), Protection des données personnelles et recherche, Berne 2024, 31 ss. 36 ; Meier (n. 5), N 431 ss. Cf. en détail par rapport à la notion de données personnelles : Aurélien Pasquier, Die Anwendbarkeit der DSGVO ausserhalb des EWR, Zurich 2025, N 38 ss.

15 CR LPD-Meier/Tschumy (n. 5), art. 5 N 49.

16 CR LPD-Meier/Tschumy (n. 5), art. 5 N 53 pour la liste des dispositions spécifiques applicables aux données sensibles.

17 Le consentement doit être exprimé d'une manière apparente, p. ex. par le biais d'une signature ou d'une déclaration verbale non équivoque. Il n'est toutefois pas nécessaire que le consentement soit donné sous la forme écrite, cf. CR LPD-Meier/Tschumy (n. 5), art. 6 N 96.

2. Données anonymisées ou codées

Étant donné que la LPD s'applique uniquement aux traitements de données se rapportant à une personne identifiée ou identifiable, les données anonymisées peuvent échapper à son champ d'application lorsqu'il n'est plus possible de procéder à la réidentification.[18] En effet, l'anonymisation vise précisément à empêcher l'identification de la personne concernée, à savoir la personne physique dont les données sont traitées. Bien que la LPD ne définisse pas la notion de données anonymisées, il est possible de s'appuyer sur la loi relative à la recherche sur l'être humain[19],[20]qui définit, en son art. 3 let. i LRH, les données anonymisées (liées à la santé), comme étant les données « qui ne peuvent être mis[ses] en relation avec une personne déterminée ou ne peuvent l'être sans engager des efforts démesurés ».

L'anonymisation peut ainsi s'analyser de deux manières. Selon une approche absolue, il y a anonymisation lorsque cette dernière empêche, définitivement et irrémédiablement, le rattachement de la donnée à la personne, même pour la personne responsable de l'anonymisation.[21] Cette anonymisation complète, généralement obtenue par cryptage à sens unique, exclut toute possibilité (même théorique) de réidentification.[22] Selon l'approche relative, l'anonymisation factuelle est suffisante. Cette dernière est admise lorsque la réidentification par un tiers ne paraît possible qu'au prix d'efforts disproportionnés et que, selon le cours ordinaire des choses, il peut être admis qu'aucune personne intéressée ne mettra en œuvre les moyens nécessaires.[23] Dans son message sur la LPD, le Conseil fédéral adopte les deux approches en reconnaissant que la « loi ne s'applique pas aux données qui ont été anonymisées si une réidentification par un tiers est impossible […] ou ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attèlera ».[24] Ainsi, si la réidentification est possible sans efforts disproportionnés – par exemple, au moyen d'informations supplémentaires raisonnablement accessibles ou en croisant les données avec d'autres sources –, les données ne doivent pas être qualifiées d'anonymisées et la LPD reste applicable. L'appréciation du caractère raisonnable des moyens se fait à la lumière des circonstances concrètes du cas d'espèce – telles que le coût et le temps nécessaires à la réidentification, ou encore le type de données –, en prenant en compte les technologies disponibles au moment du traitement.[25] Cette approche (relative) implique aussi que le « caractère anonyme » d'une donnée peut changer au fil du temps, notamment en fonction des développements techniques. Cette conséquence n'est pas sans importance pour les responsables du traitement qui doivent à tout moment s'assurer qu'une réidentification des données n'est pas possible sans efforts démesurés.

Les données anonymisées doivent être distinguées des données dites codées (ou pseudonymisées). Le codage consiste à substituer les données permettant l'identification d'une personne (généralement le nom) par un identifiant ou un code neutre afin d'empêcher l'identification.[26] Contrairement à l'anonymisation, cette opération est réversible, dans la mesure où il demeure possible de rétablir l'identité de la personne concernée à l'aide d'informations supplémentaires, comme une liste de correspondance ou une clé de cryptage.[27] Par conséquent, les données pseudonymisées sont des données personnelles.[28] Dans ces circonstances, il est primordial que les informations supplémentaires, permettant de faire le lien entre le code et la personne concernée, soient conservées séparément et soumises à des mesures techniques et organisationnelles qui garantissent que seules les personnes autorisées y aient accès.[29] Cette question relève de la sécurité des données et sera analysée plus en détail ci-dessous (II.B.6.).

---

18 Meier, Protection des données (n. 5), N 436 ss.

19 Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH ; RS 810.30).

20 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (n. 9), art. 5 N 35.

21 Meier (n. 5), N 437.

22 Meier (n. 5), N 437 ss et 445. À noter qu'il devient de plus en plus difficile de garantir une anonymisation véritablement irréversible, notamment en raison de l'augmentation massive de données disponibles, de leur accessibilité de plus en plus aisée, des progrès des algorithmes de réidentification et des évolutions en cryptographie qui fragilisent les techniques d'anonymisation existantes, cf. Préposé fédéral à la protection des données et à la transparence (PFPDT), Guide relatif aux mesures techniques et organisationnelles de la protection des données, 15 janvier 2024, 28.

23 Message LPD 2017 (n. 14), 6640 ; Meier (n. 5), N 440 ss.

24 Message LPD 2017 (n. 14), 6692.

25 Message LPD 2017 (n. 14), 6640 ; Frédéric Erard, Les données codées dans le contexte de la recherche : personnelles ou anonymes ?, PJA 2021, 606 ss, 609 ; PFPDT (n. 22), 28. En principe, il convient d'appliquer les mêmes critères que ceux utilisés pour la question du caractère « identifiable » d'une personne, à savoir si, selon l'expérience générale de la vie, il faut s'attendre à ce qu'une personne intéressée prenne en charge les efforts nécessaires à la réidentification, cf. BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (n. 9), art. 5 N 35.

26 Bruderer (n. 10), 89 ; CR LPD-Meier/Tschumy (n. 5), art. 5 N 29.

27 Bruderer (n. 10), 90 ; BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (n. 9), art. 5 N 36 ; PFPDT (n. 22), 26.

28 Il convient de relever que les données codées relatives à la santé sont soumises à une réglementation spécifique dans le cadre de la LRH et bénéficient d'un statut particulier, cf. Bruderer (n. 10), 90 ; Erard (n. 25), 608 ss.

29 Cf. également la définition de la notion de « pseudonymisation » retenue par le RGPD (art. 4 par. 5 RGPD) qui souligne cet aspect. À

La distinction entre données anonymisées et données codées est essentielle, dans la mesure où les premières échappent au champ d'application de la LPD, tandis que les secondes doivent être qualifiées de données personnelles.[30] Dans une logique fondée sur l'approche relative des données anonymisées, il pourrait être soutenu que les données codées doivent être considérées comme anonymisées – et donc non personnelles – pour les tiers ne disposant pas de la clé d'identification, dès lors que l'identification de la personne concernée ne serait possible qu'au prix d'efforts disproportionnés – vraisemblablement pas entrepris.[31] Dans ces cas-là, le codage (ou la pseudonymisation) pourrait s'apparenter dans les faits à une anonymisation. Cependant, une telle interprétation aboutirait à exclure ces données de la protection juridique dès leur transmission sous forme codée aux chercheurs et chercheuses, les autorisant ainsi à les traiter librement, sans contrainte.[32] À l'inverse, une approche stricte considère qu'il suffit qu'un seul des acteurs impliqués dans la communication de données codées soit en mesure de réidentifier la personne concernée pour que ces données conservent leur caractère personnel, et soient donc soumises à la réglementation en matière de protection des données.[33] Cette dernière approche offre non seulement une meilleure garantie du droit à l'autodétermination des personnes concernées, mais s'avère également la plus conforme à une interprétation littérale et systémique du texte légal. Celui-ci opère en effet une distinction en recourant tantôt au concept d'anonymisation, tantôt à celui de mise en forme ne permettant pas l'identification des personnes concernées (cf. art. 39 al. 1 let. a, en comparaison avec les let. b et d). À ce titre, l'approche stricte doit être privilégiée, la distinction entre donnée codée et donnée anonymisée devant être maintenue.[34]

Le codage des données présente l'avantage d'une mise en œuvre plus aisée, en ce qu'il évite les incertitudes juridiques liées à l'appréciation du caractère suffisant de l'anonymisation et offre la possibilité de réidentifier la personne concernée, lorsque cela s'avère nécessaire, par exemple, dans le cadre du suivi de la recherche ou de l'exercice de droits individuels.[35]

Il convient de souligner qu'avant même qu'une donnée puisse être considérée comme anonymisée ou codée, les opérations d'anonymisation et de codage constituent, en elles-mêmes, des traitements de données personnelles au sens de la LPD,[36] et relèvent donc de son champ d'application.

B. Principes généraux de la protection des données

Comme tout traitement de données personnelles, celui réalisé à des fins de recherche doit respecter les principes généraux de la protection des données (art. 6 et 8 LPD), à savoir les principes de licéité, de bonne foi, de proportionnalité, de finalité, de reconnaissabilité, d'exactitude et de sécurité. L'idée n'est pas de détailler ici le contenu de ces principes généraux, mais plutôt de les envisager dans le contexte spécifique de la recherche.

1. Principe de licéité

Énoncé à l'art. 6 al. 1 LPD, le principe de licéité exige que tout traitement de données soit licite dans son principe, ses modalités et son étendue.[37] Sa portée diffère selon si l'auteur du traitement est une personne privée ou un organe fédéral : la première doit s'abstenir de violer la personnalité des personnes dont les données sont traitées, alors que le second doit respecter le principe de légalité (art. 5 al. 1 Cst.).[38] Dans le contexte de la protection des données, le principe de la légalité de l'activité étatique est précisé à l'art. 34 LPD : les organes fédéraux ne peuvent traiter ou communiquer des données personnelles que si ce traitement est expressément prévu par une base légale « suffisante », c'est-à-dire une base légale qui remplit les conditions requises au niveau de la formalité (loi au sens

cet égard, il peut être fait mention d'un arrêt dans lequel le Tribunal de commerce du canton de Zurich a estimé que les données personnelles des requérants qu'une banque suisse projetait de transmettre au Department of Justice (DoJ) dans le cadre d'un accord de non-poursuite signé avec les autorités américaines restaient identifiables bien que pseudonymisées. En effet, le tribunal a considéré que les autorités américaines pouvaient raisonnablement, avec les moyens dont elles disposent, réidentifier les personnes concernées, cf. HGer ZH, HG190107-O, 4.5.2021.

30 Erard (n. 25), 609.

31 Dans ce sens, voir : Message LPD 2017 (n. 14), 6640 ; CR LPD-Meier/Tschumy (n. 5), art. 5 N 29.

32 Christinat (n. 14), 38 ; Erard (n. 25), 609.

33 Erard (n. 25), 609.

34 Par ailleurs, une approche trop large priverait de leur portée effective certaines dispositions de la LRH, qui distingue clairement le régime applicable aux données codées de celui applicable aux données anonymisées, indépendamment de la capacité du destinataire à réidentifier les personnes concernées, cf. Erard (n. 25), 613 ss.

35 Alexandre Jotterand/Frédéric Erard, Recherche sur l'être humain et données personnelles, in : Jusletter 30 août 2021, N 41.

36 TF, 4A_365/2017, 26.2.2018, c. 5.2.2 ; HGer ZH, HG190107-O, 4.5.2021, c. 3.2.3a ; CR LPD-Meier/Tschumy (n. 5), art. 5 N 27 ; BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (n. 9), art. 5 N 34.

37 Meier (n. 5), N 639.

38 CR LPD-Meier/Tschumy (n. 5), art. 6 N 22.

matériel, voire au sens formel)[39] ainsi que de la densité normative (précision et clarté).[40] Des atténuations sont prévues à l'art. 34 al. 4 LPD.

Dans le contexte de la recherche scientifique, il nous paraît important de souligner que l'exigence d'une base légale s'applique généralement à toutes les phases du traitement concerné.[41] Ainsi, le principe de légalité doit être respecté non seulement lors de la collecte des données, mais également lors de leur utilisation, de leur conservation ou encore lors de leur publication. À noter toutefois que le traitement de données à des fins de recherche bénéficie d'une atténuation du principe de la légalité (cf. art. 39 al. 2 LPD). De plus amples considérations à ce sujet seront développées ci-dessous (III.B.3.).

2. Principe de bonne foi

Le principe de bonne foi (art. 6 al. 2 LPD), quant à lui, commande d'agir de manière loyale et digne de confiance.[42] Ainsi, les données personnelles ne doivent pas être collectées d'une manière à laquelle la personne concernée ne pouvait s'y attendre.[43] Par exemple, un traitement de données effectué à l'insu ou contre la volonté de la personne concernée serait contraire à la bonne foi.[44] Dans le domaine de la recherche, ce principe se traduit notamment par une information adéquate des participants et participantes, une collecte conforme aux attentes légitimes, et le respect des consentements donnés ou non.

Par ailleurs, le principe de bonne foi constitue un principe général de l'ordre juridique suisse (art. 5 al. 3 et 9 Cst.) qui, en droit de la protection des données, s'applique de façon subsidiaire si aucun autre principe plus spécifique ne peut être invoqué.[45] De cette façon, le principe de bonne foi peut également faire office d'indicateur « éthique »[46] dans le traitement de données à des fins de recherche scientifique.

3. Principe de proportionnalité

Tout traitement de données doit également respecter le principe de proportionnalité (art. 6 al. 2 LPD et art. 5 al. 2 Cst.), c'est-à-dire qu'il doit être apte et nécessaire à atteindre le but poursuivi, tout en s'inscrivant dans un rapport raisonnable entre les moyens utilisés et la finalité visée.[47] Ainsi, le principe de proportionnalité s'applique non seulement au choix du mode de traitement, à son étendue ainsi qu'à la nature des données traitées (proportionnalité matérielle),[48] mais également à la durée de conservation des données (proportionnalité temporelle).[49] L'art. 6 al. 4 LPD prévoit d'ailleurs que les données personnelles doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.

Du principe de proportionnalité découlent également deux autres principes spécifiques au droit de la protection des données, à savoir les principes d'évitement et de minimisation.[50] Le premier privilégie le recours aux données existantes et le second impose de limiter la collecte aux seules données absolument nécessaires au but poursuivi.[51] Ces deux principes doivent être pris en compte dès la phase de conception et appliqués par défaut, conformément à l'article 7 LPD.

Par conséquent, le principe de proportionnalité impose que seules les données strictement nécessaires pour atteindre les objectifs du projet de recherche soient collectées et traitées. Ces exigences doivent être intégrées dès la conception du projet de recherche, notamment dans le choix du type de données, des modalités de traitement et de conservation, ainsi que des conditions d'accès.

---

39 En principe, une base légale au sens formel est requise pour le traitement et la communication de données sensibles, en cas de profilage, ou lorsque la finalité ou les modalités du traitement sont de nature à porter gravement atteinte aux droits fondamentaux de la personne concernée (cf. art. 34 al. 2 LPD en relation avec art. 36 al. 1 Cst.).

40 Dans son message de 1988, le Conseil fédéral indique que « [l]e degré de précision de la base juridique s'appréciera d'après les principes généraux en la matière. Différents critères peuvent ainsi entrer en considération ; parmi ceux-ci, on relèvera la gravité de l'atteinte aux libertés de l'administré, la nature des données traitées, le cercle des personnes concernées, la structure du système informatique ou, le cas échéant, la participation de services cantonaux ou de personnes privées au traitement. A tout le moins, la base juridique doit définir le but du traitement, décrire, dans les grandes lignes, son importance, et désigner les organes qui y participent », cf. Message du Conseil fédéral du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421 (cit. Message LPD 1988), 473.

41 Samah Posse, Le traitement de données personnelles à des fins statistiques, in : Sylvain Métille (éds), Protection des données personnelles et recherche, Berne 2024, 123 ss, 147.

42 Sandra Husi-Stämpfli et al., Protection des données, Zurich/Genève 2024, 86.

43 Husi-Stämpfli et al., (n. 42), 86.

44 Meier (n. 5), N 644 ss ; CR LPD-Meier/Tschumy (n. 5), art. 6 N 25.

45 CR LPD-Meier/Tschumy (n. 5), art. 6 N 25.

46 Meier (n. 5), N 646.

47 Message LPD 2017 (n. 14), 6644.

48 Meier (n. 5), N 723.

49 CR LPD-Meier/Tschumy (n. 5), art. 6 N 33 ss.

50 Message LPD 2017 (n. 14), 6644 ; Métille (n. 11), 9.

51 Message LPD 2017 (n. 14), 6644 ; Meier (n. 5), N 673.

4. Principe de finalité et de reconnaissabilité

Selon le principe de finalité et de reconnaissabilité (art. 6 al. 3 LPD), les données personnelles ne peuvent être collectées que dans le but indiqué et reconnaissable lors de leur collecte pour la personne concernée.[52] Le caractère déterminé des finalités s'apprécie selon les circonstances, l'objectif étant de concilier les intérêts des personnes concernées et ceux de la personne responsable du traitement.[53] Par ailleurs, si les données devaient être réutilisées ultérieurement, le traitement devrait se faire de manière à être compatible avec ces finalités (art. 6 al. 3 LPD *in fine*), sauf si une base légale ou un motif justificatif légitime permet un changement de finalité.[54]

Dans le cadre de la recherche scientifique, il convient de distinguer la recherche primaire (ou prospective) de la recherche secondaire (ou rétrospective) : la recherche primaire implique la collecte et l'utilisation des données spécifiquement pour la recherche énoncée, alors que la recherche secondaire se base sur des données qui ont été collectées dans un but autre que celui de la recherche pour laquelle elles sont désormais utilisées.[55] Cette distinction est pertinente lors de l'évaluation du principe de finalité et de reconnaissabilité dans le cadre de la recherche. En effet, pour une recherche primaire, le principe de finalité s'applique de manière classique, dans la mesure où les personnes participantes doivent être informées clairement de l'objectif de la recherche au moment de la collecte. Pour la recherche secondaire, qui repose sur la réutilisation de données préexistantes, le principe de la finalité est appliqué de manière plus souple. En effet, il n'est pas toujours possible de déterminer, au moment de la collecte des données personnelles, si ces dernières seront d'intérêt pour d'éventuelles recherches scientifiques. Tant que la réutilisation est compatible avec le but initial ou qu'un motif justificatif (notamment l'intérêt public en matière de recherche) peut être invoqué, cette pratique reste licite.[56] Cet assouplissement du principe de finalité est d'ailleurs concrétisé aux art. 31 al. 2 let. e et 39 LPD. De plus amples considérations à ce sujet seront développées ci-dessous (III.B.3.).

5. Principe d'exactitude

Selon l'art. 6 al. 5 LPD, toute personne traitant des données personnelles doit veiller à leur exactitude, c'est-à-dire à ce qu'elles soient correctes, actuelles et objectives.[57] Cette obligation n'est toutefois pas absolue : elle doit être proportionnée à la finalité du traitement (cf. par exemple, art. 32 LPD).[58]

Dans le domaine de la recherche scientifique, cette exigence d'exactitude revêt une certaine importance. Outre le fait qu'il puisse y avoir atteinte aux droits des personnes concernées, des données inexactes peuvent également fausser les résultats. Ce facteur doit être pris en compte et intégré dès la phase méthodologique d'un projet de recherche avec, par exemple, la mise en place de mesures adaptées pour vérifier, corriger ou, si nécessaire, supprimer les données personnelles erronées ou incomplètes. Le choix de ces mesures dépendra du type de recherche, de l'ampleur du traitement et du risque qu'il représente pour les personnes concernées (cf. art. 6 al. 5 *in fine* LPD).

6. Principe de sécurité

Selon le principe de sécurité des données (art. 8 LPD), les responsables du traitement et leurs sous-traitants doivent prendre des mesures techniques et organisationnelles appropriées[59] pour garantir une sécurité adéquate des données personnelles par rapport au risque encouru. Ainsi, plus le risque d'atteinte à la sécurité des données est important, plus les mesures de protection à mettre en place doivent être rigoureuses (cf. art. 1 OPDo).[60] Il y a violation de la sécurité des données lorsque ces dernières sont perdues, modifiées, effacées, détruites, divulguées ou ren-

---

52 En ce sens, des buts vagues ou non déterminés ne suffisent pas, cf. Meier, Protection des données (n. 5), N 676 ss.

53 Message LPD 2017 (n. 14), 6644 ; Métille (n. 11), 9 s.

54 Lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif, le traitement ultérieur est aussi considéré comme compatible avec le but initial, cf. Message LPD 2017 (n. 14), 6645.

55 Bruderer (n. 10), 11 s.

56 Message LPD 2017 (n. 14), 6645. Voir également : Conseil de l'Europe, Brochure Convention 108+ – Rapport explicatif de la Convention 108+, Strasbourg 2018, 22.

57 Meier (n. 5), N 745.

58 En effet, le principe d'exactitude et les devoirs qui y sont liés sont aménagés de manière différenciée, p. ex. pour les archives, les musées, les bibliothèques et les autres institutions patrimoniales publiques dont les tâches visent justement à répertorier et conserver des documents – indépendamment de leur exactitude. Cf. Message LPD 2017 (n. 14), 6646 ; Métille (n. 11), 11.

59 À titre d'exemple, les mesures techniques peuvent comprendre la scission de données, les sauvegardes supplémentaires, l'anonymisation, l'authentification multi-facteurs ou, du côté des mesures organisationnelles, prendre la forme de séparation des fonctions, de conscientisation et de formation au niveau de la gestion des données personnelles, cf. CR LPD-Fanti/Staeger (n. 5), art. 8 N 88.

60 Ordonnance du 31 août 2022 sur la protection des données (OPDo ; RS 235.11). Voir également : CR LPD-Fanti/Staeger (n. 5), art. 8 N 74 ss.

dues accessibles de façon non autorisée, indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 5 let. h LPD et art. 2 OPDo).

Dans le cadre de la recherche scientifique, il est important que la réflexion sur les mesures techniques et organisationnelles ait lieu avant la mise en œuvre du traitement, afin d'anticiper et d'éviter toute violation de la sécurité des données (perte, modification, accès non autorisé, etc.). Ces mesures doivent inclure tant les activités en amont que les activités en aval de la recherche. Le principe de sécurité des données peut se traduire de diverses manières, par exemple, en s'assurant que les données soient codées et que la clé d'identification soit seulement accessible à un nombre restreint de personnes. Si un projet de recherche implique un traitement de données sensibles à large échelle, comme des données personnelles liées à la santé, le risque pour la personnalité ou les droits fondamentaux de la personne concernée est élevé, ce qui justifie des exigences renforcées en matière de sécurité.

C. Autres législations applicables

1. Lois spéciales suisses

En vertu du principe de la *lex specialis*, selon lequel la loi spéciale l'emporte sur la loi générale, il se peut que des dispositions particulières ancrées dans des lois spéciales dérogent au régime général de la LPD.[61] La personne responsable du traitement doit ainsi se renseigner sur les lois spéciales potentiellement applicables au domaine de recherche en question.

À titre d'illustration, pour un traitement de données personnelles liées à la santé dans le domaine de la recherche sur l'être humain, c'est la loi fédérale relative à la recherche sur l'être humain (LRH)[62] qui s'applique, notamment en ce qui concerne la réutilisation desdites données. Par conséquent, les art. 32 ss LRH priment sur les règles générales de la LPD – qui continuent toutefois de s'appliquer pour tous les éléments non couverts par la loi spéciale.[63] De la même manière, si une recherche porte sur l'analyse génétique humaine, ce sera à la LAGH[64] de s'appliquer. Cette dernière renvoie par ailleurs à la LRH en ce qui concerne les analyses génétiques et prénatales humaines ainsi que des données qui en sont issues (art. 2 al. 4 LAGH).

D'autres domaines dans lesquels des dispositions spéciales s'appliquent ou peuvent s'appliquer sont, par exemple, les procédures judiciaires ou les dossiers archivés.

2. La Convention 108+ et le RGPD

Au sein du Conseil de l'Europe, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) a été conclue en 1981 et ratifiée en 1997 par la Suisse.[65] Cette dernière a également ratifié le protocole d'amendement (Conventions 108+)[66] qui entrera en vigueur lorsque 38 états parties l'auront ratifié.[67] La version modernisée de cette Convention prévoit notamment que « le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est compatible avec ces fins moyennant l'application de garanties complémentaires » (art. 5 al. 4 let. b Convention 108+).

Le Règlement général sur la protection des données (RGPD),[68] bien qu'il s'agisse d'un instrument de l'Union européenne, déploie dans certaines situations des effets extraterritoriaux en Suisse, notamment dans le contexte de la recherche.[69] En effet, le RGPD s'applique aux traitements de données effectués « dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union » (art. 3 par. 1 RGPD) et couvre ainsi des projets de recherche qui sont, entre autres, réalisés en Suisse, mais associés à des activités menées dans l'UE à travers un représentant local.[70]

---

61 En effet, la LPD et les législations cantonales en matière de protection des données sont considérées comme des lois générales auxquelles des législations spéciales peuvent déroger.

62 Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH ; RS 810.30).

63 Jotterand/Erard (n. 35), N 18 ss.

64 Loi fédérale du 15 juin 2018 sur l'analyse génétique humaine (LAGH ; RS 810.12).

65 Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 ; RS 0.235.1).

66 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE nº 223).

67 Pour l'heure, 33 États parties ont ratifié la Convention 108+ (état le 30 juin 2025), cf. Conseil de l'Europe, Etat des signatures et ratifications du traité 223, Internet : https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (consulté le 30.6.2025).

68 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD ; JO L 119 du 4.5.2016, 1–88).

69 Pour plus de détails concernant les situations dans lesquelles le RGPD peut trouver application en Suisse dans le contexte de la recherche, voir : Jotterand/Erard (n. 35), N 18 ss.

70 Jotterand/Erard (n. 63), N 13.

Outre le critère du lieu d'établissement, l'art. 3 par. 2 RGPD prévoit l'application des dispositions du RGPD lorsque la personne responsable du traitement (ou sous-traitante) utilise des données personnelles relatives à des personnes qui se trouvent sur le territoire de l'Union européenne et que ce traitement est lié à l'offre de biens ou de services dans l'Union européenne ou au suivi du comportement de personnes dans l'Union européenne. À titre exemplatif, le RGPD pourrait produire des effets extraterritoriaux en Suisse si, dans le cadre d'un projet de recherche, des comportements de personnes situées dans l'Union européenne étaient mesurés en temps réel au moyen de dispositifs connectés.[71]

Plus généralement, le RGPD s'impose fréquemment comme norme de référence lors de collaborations avec des institutions de recherche européennes. Ainsi, lorsqu'un projet mené en Suisse associe des partenaires européens, les chercheurs et chercheuses suisses sont souvent tenus, par le biais de clauses contractuelles, de se conformer aux exigences du RGPD.[72]

Le RGPD prévoit des assouplissements concernant le traitement de données à des fins de recherche scientifique ou historique, également en dérogation au principe de finalité, sous réserve de « garanties appropriées pour les droits et les libertés des personnes concernées » (cf. art. 89 RGPD).[73]

III. Traitement de données par des organes fédéraux : l'art. 39 LPD

A. Généralités

Comme déjà mentionné précédemment, la LPD régit le traitement de données personnelles concernant des personnes physiques effectué par des personnes privées ainsi que par des organes fédéraux (art. 2 al. 1 LPD). Un organe fédéral est défini par la LPD comme « l'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération » (art. 5 let. i LPD).

Afin de déterminer si une personne, physique ou morale, agit en qualité d'organe fédéral, il convient d'examiner la nature juridique de la relation qui la lie à la personne concernée.[74] Lorsque cette relation relève du droit public – par exemple, si l'auteur du traitement agit sur la base d'un mandat légal ou est reconnu comme une institution de droit public –, la personne responsable du traitement est qualifiée d'organe public.[75] Dans le contexte de la recherche, sont ainsi considérés comme organes fédéraux non seulement l'administration fédérale qui entreprend elle-même des recherches scientifiques, mais également les chercheurs et chercheuses privées œuvrant pour le compte d'un organe fédéral (cf. art. 9 LPD), ou encore les EPF qui sont des établissements autonomes de droit public de la Confédération.[76]

En plus des dispositions générales applicables à tout auteur du traitement, la LPD prévoit des dispositions particulières pour le traitement de données effectué par des personnes privées (art. 30 ss LPD) ou par des organes fédéraux (art. 33 ss LPD). Il existe ainsi deux réglementations spécifiques concernant le traitement de données personnelles à des fins de recherche : l'une pour le secteur privé (art. 31 al. 2 let. e LPD) et l'autre pour les organes fédéraux (art. 39 LPD). Cette seconde disposition fait l'objet des prochaines considérations.

B. Traitement à des fins de recherche

En vertu de l'art. 39 al. 1 LPD, les organes fédéraux sont autorisés à traiter des données personnelles à des fins « ne se rapportant pas à des personnes » – telles que la recherche, la planification ou la statistique[77] – pour autant que certaines conditions concernant l'anonymisation, la communication et la publication soient remplies.[78] L'art. 39 al. 2 LPD assouplit quelque peu certaines exigences relatives à la base légale, dans la mesure où l'art. 6 al. 3 LPD (principe de finalité et de reconnaissabilité), l'art. 34 al. 2 LPD (exigence d'une loi au sens formel) ainsi que l'art. 36 al. 1 LPD (communication des données) ne sont pas applicables[79].

---

71 Frédéric Erard, La protection des données dans la recherche, in : Sylvain Métille (éds), Protection des données personnelles et recherche, Berne 2024, 1 ss, 5.

72 Jotterand/Erard (n. 63), N 17.

73 CR LPD-Epiney/Posse (n. 5), art. 39 N 11.

74 CR LPD-Meier/Tschumy (n. 5), art. 5 N 103. Voir également : TAF, A-3548/2018, 19.3.2019, c. 4.5.5. pour une analyse du rapport juridique entre Helsana et les personnes concernées.

75 CR LPD-Meier/Tschumy (n. 5), art. 5 N 103.

76 Cf. art. 5 al. 1 et art. 36c Loi sur les EPF (Loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales; RS 414.110).

77 Il s'agit d'exemples cités par la LPD (« notamment »), d'autres utilisations à des fins ne se rapportant pas à des personnes sont envisageables, cf. BSK DSG-Roos/Keller (n. 9), art. 39 N 9.

78 CR LPD-Epiney/Posse (n. 5), art. 39 N 21.

79 Le régime dérogatoire, aménagé au profit de la recherche scientifique au sens large, est communément désigné comme le «privilège de la recherche», cf. CR LPD-Epiney/Posse (n. 5), art. 39 N 1.

1. Recherche scientifique ne se rapportant pas à des personnes

Pour que le traitement des données personnelles ne soit pas considéré comme se rapportant à des personnes, l'objectif de la recherche scientifique doit être indépendant des individus dont les données sont traitées.[80] Autrement dit, un traitement de données impliquant des données personnelles, mais dont le but est détaché de toute individualité, constitue un traitement à des fins non personnelles au sens de l'art. 39 LPD. Les caractéristiques ou les circonstances des personnes sont pertinentes, et non leur identité.[81]

De cette manière, les recherches axées directement sur des individus – telles que les recherches sur des personnes politiciennes ou sur la généalogie – ne sont pas détachées de l'identité des personnes concernées et ne peuvent bénéficier du régime prévu à l'art. 39 LPD.[82] En d'autres termes, il faut que l'objectif du traitement puisse être atteint de manière équivalente par l'utilisation de données anonymisées ou pseudonymisées.[83]

2. Conditions cumulatives (let. a à d)

La première condition requiert que les données soient anonymisées dès que la finalité du traitement le permet (art. 39 al. 1 let. a LPD). La loi ne précise pas davantage le moment auquel l'anonymisation doit intervenir, celui-ci devant être déterminé au cas par cas, en tenant compte des circonstances particulières et des éléments pertinents.[84] À la lumière du principe de sécurité, une anonymisation devrait toutefois intervenir dans les plus brefs délais, afin de limiter les éventuels impacts négatifs sur la personnalité et les droits fondamentaux de la personne concernée en cas de divulgation des données. Comme indiqué précédemment (II.A.2.), l'anonymisation des données n'est pas chose aisée et présente de réels défis pour la recherche en raison des capacités technologiques, de plus en plus performantes, de réidentification.[85] De cette manière, il est d'autant plus important que le moment d'anonymisation ainsi que les méthodes pour y parvenir soient déterminés à l'avance – par exemple, lors de la planification du projet.[86]

La deuxième condition concerne la communication des données sensibles à des personnes privées par un organe fédéral, cette dernière ne pouvant être effectuée que sous « une forme ne permettant pas d'identifier les personnes concernées » (art. 39 al. 1 let. b LPD). Dans son message, le Conseil fédéral estime que cette condition est réalisée lorsque les données sont communiquées sous une forme pseudonymisée et que la clé de réidentification est détenue auprès de l'organe fédéral en question (anonymisation factuelle).[87] Par conséquent, dans le contexte de la recherche scientifique, les organes publics peuvent transmettre des données, même sensibles, tant que ces dernières sont codées.[88] Étant donné que l'art. 39 al. 1 let. b LPD ne s'applique qu'aux données personnelles particulièrement sensibles et uniquement en cas de communication à des personnes privées, la transmission d'autres catégories de données personnelles à des privés ou à des organes fédéraux, de même que la transmission de données particulièrement sensibles à des organes fédéraux, reste autorisée sans nécessité de codage ou d'anonymisation.[89] Cet aspect facilite ainsi la communication de données à des fins de recherche entre les organes publics.

Toujours en lien avec la communication des données, la LPD impose au destinataire de ne communiquer les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises (art. 39 al. 1 let. c LPD). De ce fait, les organes fédéraux peuvent transmettre des données traitées à des fins non personnelles à des tiers – que ce soient des organes publics ou des personnes privées – à condition que ces derniers les utilisent également exclusivement à des fins non personnelles.[90] Toute transmission ultérieure par ces destinataires à d'autres tiers nécessite l'accord préalable de l'organe fédéral, ce qui permet de garantir le respect de la finalité non personnelle du traitement. Cette exigence de consentement est généralement formalisée par contrat ou par une décision.[91]

Finalement, la quatrième et dernière condition concerne la publication des résultats du traitement, qui ne peut être faite que sous « une forme ne permettant pas d'identifier les personnes concernées » (art. 39 al. 1 let. d LPD). Une donnée est considérée comme publiée dès qu'elle est communiquée à des personnes qui ne sont pas soumises à une obligation de confidentialité (et au respect de la protection

---

80 CR LPD-Epiney/Posse (n. 5), art. 39 N 17.
81 BSK DSG-Roos/Keller (n. 9), art. 39 N 9.
82 Message LPD 1988 (n. 40), 469.
83 BSK DSG-Roos/Keller (n. 9), art. 39 N 9.
84 CR LPD-Epiney/Posse (n. 5), art. 39 N 22 s.
85 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (n. 9), art. 5 N 35.
86 BSK DSG-Roos/Keller (n. 9), art. 39 N 15.
87 Message LPD 2017 (n. 14), 6699.
88 À noter que lorsqu'il s'agit de données médicales, c'est la LRH qui s'applique.
89 BSK DSG-Roos/Keller (n. 9), art. 39 N 16.
90 Message LPD 1988 (n. 40), 480.
91 Message LPD 1988 (n. 40), 480 ; CR LPD-Epiney/Posse (n. 5), art. 39 N 31 s.

des données) concernant les données personnelles.[92] Par conséquent, lorsque les résultats sont réservés à un usage interne, cette disposition ne trouve pas application. En revanche, si une publication – même partielle ou intermédiaire – est envisagée, les données doivent être entièrement codées, voire anonymisées, de manière à ne pas permettre l'identification des personnes concernées.[93]

3. L'art. 39 al. 1 LPD comme « base légale limitée » et assouplissement des exigences relatives à la base légale

Si toutes les conditions énumérées à l'art. 39 al. 1 LPD sont remplies, l'art. 39 al. 2 LPD institue une exception au principe de finalité et de la reconnaissabilité ainsi qu'un assouplissement des exigences en matière de base légale nécessaire au traitement et à la communication des données. Ces dérogations sont énumérées de manière exhaustive.[94]

Ainsi, dans le cadre de la recherche (secondaire), l'utilisation de données collectées à d'autres fins est admise, justifiée entre autres par l'intérêt public en matière de recherche. Selon l'art. 5 al. 4 let. b Convention 108+, si les données doivent en principe être collectées pour des finalités explicites, déterminées et légitimes, le traitement ultérieur à des fins de recherche scientifique ou historique, est compatible avec ces fins moyennant l'application de garanties complémentaires. Ces garanties comprennent, par exemple, « l'anonymisation ou la pseudonymisation des données sauf s'il est indispensable de conserver la forme identifiable, des règles en matière de secret professionnel, des dispositions régissant l'accès restreint et la diffusion restreinte de données aux fins précitées, notamment celles liées aux statistiques et à l'archivage public, ainsi que d'autres mesures d'ordre technique et organisationnel visant la sécurité des données ».[95] La LPD présente ces garanties, non seulement grâce aux conditions listées à l'art. 39 al. 1 LPD, mais également par le biais des principes généraux (art. 6 et 8 LPD).

Une autre conséquence de l'application de l'art. 39 LPD concerne les exigences liées à la base légale. Ces dernières sont assouplies pour les traitements à des fins de recherche, même lorsqu'ils impliquent des données sensibles, du profilage ou un risque grave pour les droits fondamentaux (art. 34 al. 2 LPD). Toutefois, l'assouplissement ne porte que sur les exigences plus restrictives en matière de base légale et n'implique pas une dérogation au principe de légalité : une base légale au sens matériel demeure nécessaire pour les organes fédéraux.[96]

À noter que l'art. 39 LPD ne constitue pas une base légale matérielle « générale » pour tout traitement de données personnelles à des fins non personnelles ; sa portée matérielle comme base légale – toujours à condition qu'il s'agisse d'un traitement à des fins ne se rapportant pas à des personnes, comme dans le cadre de recherches scientifiques – se limite aux traitements de données qui sont déjà en possession de l'organe public en question. Si ce dernier souhaite les traiter à des fins ne se rapportant pas à des personnes (comme dans le cadre de la recherche), l'art. 39 LPD constitue une base légale suffisante. En revanche, la disposition ne permet pas aux organes fédéraux de collecter des données personnelles à des fins de traitement ne se rapportant pas à des personnes.[97] L'approche selon laquelle tout traitement de données personnelles à des fins ne se rapportant pas à des personnes devrait non seulement respecter les conditions de l'article 39 al. 1 LPD, mais également s'appuyer sur une base légale spécifique (et distincte) autorisant un tel traitement (à des fins de recherche),[98] ne saurait convaincre.[99]

En effet, limiter la portée de l'art. 39 LPD à un simple assouplissement de l'exigence de base légale reviendrait à priver cette disposition de sa substance propre. Une interprétation téléologique et systématique plaide en faveur d'une approche plus nuancée. Si l'art. 34 al. 1 LPD (principe de légalité) demeure applicable dans le cadre du traitement de données personnelles à des fins de recherche, l'art. 36 al. 1 LPD – qui impose en principe une base légale pour la communication de données personnelles – est expressément écarté dans le cadre de l'art. 39 LPD. Comme aucune base légale distincte n'est requise pour la communication à des fins de recherche et que le principe de finalité n'est pas applicable, l'art. 39 LPD doit être interprété comme une base légale spécifique autorisant l'organe public à traiter les données personnelles – qu'il

---

92 BSK DSG-Roos/Keller (n. 9), art. 39 N 21. Voir également l'art. 5 let. e LPD qui définit la communication comme « le fait de transmettre des données personnelles ou de les rendre accessibles ».

93 CR LPD-Epiney/Posse (n. 5), art. 39 N 35.

94 CR LPD-Epiney/Posse (n. 5), art. 39 N 38.

95 Conseil de l'Europe, Brochure Convention 108+ – Rapport explicatif de la Convention 108+, Strasbourg 2018, 23.

96 CR LPD-Epiney/Posse (n. 5), art. 39 N 38.

97 Toutefois encore peu clair à ce sujet, CR LPD-Epiney/Posse (n. 5), art. 39 N 3 et 38.

98 P. ex. l'art. 36c Loi sur les EPF.

99 D'un autre avis : Erard (n. 71), 11 ; Préposé fédéral à la protection des données et à la transparence (PFPDT), Recherche (hors domaine de la santé) et protection des données, Internet : https://www.edoeb.admin.ch/fr/recherche-et-protection-des-donnees (consulté le 30.6.2025) ; du même avis qu'ici : BSK DSG-Roos/Keller (n. 9), art. 39 N 4 ; Bruno Baeriswyl, in : Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (éds), Datenschutzgesetz, Berne 2023, art. 39, N 3.

a collectées et qui sont déjà en sa possession – à des fins de recherche ne se rapportant pas à des personnes. Toutefois, l'art. 39 al. 1 LPD ne saurait constituer une base légale suffisante pour un organe public ayant reçu les données personnelles d'un autre organe public à des fins de recherche scientifique (ou d'autres fins ne se rapportant pas à des personnes), car elle permettrait à des organes publics le traitement de données personnelles sans que cet organe dispose lui-même d'une base légale pour la collecte. Ainsi, lorsque l'organe public procède lui-même à la collecte des données personnelles en vertu d'une base légale au sens de l'art. 34 al. 1 LPD, l'art. 39 LPD constitue une disposition spéciale suffisante pour fonder la licéité des traitements ultérieurs nécessaires à la recherche. Cette interprétation ne saurait toutefois s'étendre aux situations dans lesquelles l'organe public concerné n'a pas procédé à la collecte – une base légale spécifique autorisant le traitement des données à des fins de recherche étant dans ce cas-ci requise. À noter que cette question n'a probablement que peu d'importance pratique pour les organes publics menant des activités de recherche, en particulier les hautes écoles, car ils disposent généralement d'une base légale propre régissant également le traitement de données personnelles. Reste à savoir si ces bases légales sont toujours suffisamment claires et précises.

Finalement, et comme déjà évoqué, la dernière dérogation concerne les règles générales de communication de données (art. 36 al. 1 LPD). Dans le contexte du traitement de données à des fins de recherche, les organes fédéraux peuvent communiquer des données personnelles sans qu'une base légale supplémentaire au sens de l'art. 34 al. 1 à 3 LPD ne le prévoit. Ainsi, si les conditions de l'art. 39 al. 1 LPD sont remplies, une base légale explicite en sus de l'art. 39 al. 1 LPD n'est pas nécessaire pour la communication des données personnelles.[100] En revanche, lorsque des données personnelles sont effectivement communiquées, l'organe fédéral est tenu de respecter les exigences de l'art. 39 al. 1 LPD, en particulier concernant la communication de données sensibles à des personnes privées sous forme codée (let. b) et la limitation pour le destinataire de transmettre les données, sauf accord de l'organe fédéral.[101]

[100] BSK DSG-Roos/Keller (n. 9), art. 39 N 29.

[101] BSK DSG-Roos/Keller (n. 9), art. 39 N 30 ; CR LPD-Epiney/Posse (n. 5), art. 39 N 38.

IV. Traitement de données par des organes cantonaux : l'exemple fribourgeois

A. Généralités

Les lois cantonales sur la protection des données sont des lois générales qui s'appliquent habituellement aux traitements de données personnelles effectués par les organes publics cantonaux ou par des personnes privées accomplissant des tâches de droit public.[102] Par conséquent, les traitements de données effectués par les universités cantonales, les HES, les HEP, les hôpitaux cantonaux et universitaires, régionaux et communaux relèvent en principe du droit cantonal applicable.

Le canton de Fribourg compte plusieurs institutions contribuant à la recherche scientifique, notamment l'Université de Fribourg (à laquelle la Haute école pédagogique sera intégrée à partir de l'automne 2025), les Hautes écoles spécialisées ainsi que l'Hôpital cantonal fribourgeois. De ce fait, les projets de recherche menés par ces établissements publics et impliquant un traitement de données personnelles doivent, en plus des législations spéciales applicables, respecter la loi fribourgeoise sur la protection des données (LPrD) du 12 octobre 2023.[103]

Le contenu des dispositions de la LPrD s'inspire en grande partie de la loi fédérale, mais comporte tout de même des particularités. Par exemple, la LPrD couvre non seulement les données personnelles des personnes physiques, mais également celles des personnes morales (cf. art. 1 et 4 LPrD).[104] En ce qui concerne le traitement de données à des fins de recherches par des organes publics, la LPrD contient une disposition analogue à l'art. 39 de la LPD, à savoir l'art. 26 LPrD.

B. Traitement à des fins de recherche

1. Généralités concernant l'art. 26 al. 1 LPrD

Selon l'art. 26 al. 1 LPrD, les organes publics peuvent traiter et communiquer des données personnelles à des fins ne se rapportant pas à la personne – notamment dans le cadre de la recherche – si quatre conditions cumulatives sont remplies. Il est exigé que les données soient détruites ou rendues anonymes dès que la finalité du traitement le

[102] Cf. p. ex. l'art. 2 al. 1 LPrD.

[103] Cette loi a fait l'objet d'une révision totale en 2023 afin de se mettre en conformité avec les nouveaux standards en matière de protection des données, cf. Message 2023-CE-149 du Conseil d'Etat du 26 juin 2023 (cit. Message LPrD), 3.

[104] Message LPrD (n. 103), 3.

permet (let. a) ; qu'une communication des données à des tiers ne se fasse qu'avec le consentement de la personne ou de l'organe qui les lui a transmises (let. b) ; que les données sensibles ne soient transmises à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées (let. c), cela également lors de la publication des résultats du traitement (let. d). Si ces exigences sont réunies, l'art. 26 al. 2 LPrD prévoit des dérogations au principe de finalité (art. 7 LPrD) ainsi qu'un assouplissement des exigences en matière de base légale nécessaire au traitement (art. 5 al. 2 et 3 LPrD) et à la communication des données (14 al. 1 LPrD). Le Conseil d'état fribourgeois justifie cet allégement des exigences en matière de protection des données du fait que « ces traitements présentent des risques moindres dans la mesure […] où ils ne se rapportent pas à des personnes et où certaines prescriptions spécifiques sont respectées ».[105] Il est ainsi tenu compte de l'intérêt public que représente la recherche.

Au vu des précédentes considérations (III.B.2.), il y a lieu de constater que l'art. 26 al. 1 LPrD s'est très largement inspiré de l'art. 39 al. 1 LPD, tant pour les conditions que pour les conséquences de l'application de la disposition. En effet, les deux dispositions exigent que les données soient rendues anonymes dès que la finalité du traitement le permet, que la communication de données sensibles à des personnes privées se fasse sous une forme ne permettant pas l'identification des personnes concernées et que les résultats du traitement soient publiés de manière à garantir l'anonymat des personnes concernées. L'expression « sous une forme ne permettant pas d'identifier les personnes concernées », utilisée aux let. c et d. de l'art. 26 al. 1 LPrD, laisse une certaine marge de manœuvre aux organes publics. En effet, une anonymisation stricte n'est pas requise et la pseudonymisation des données peut se révéler suffisante si la clé de réidentification reste détenue auprès de l'organe en question. Cette approche rejoindrait celle adoptée au niveau fédéral.

Outre l'ordre et la formulation des conditions, de petites différences peuvent toutefois être constatées entre la loi fédérale et la loi cantonale. En effet, la LPrD mentionne également la destruction des données (et pas seulement leur anonymisation) en tant que mesure à prendre « dès que la finalité du traitement le permet », afin de s'assurer de la sécurité des données. En ce sens, cette disposition se révèle plus stricte que la LPD, la destruction des données devant expressément être envisagée. Cette affirmation doit toutefois être relativisée, car le principe de proportionnalité – applicable tant aux organes publics cantonaux que fédéraux – requiert d'évaluer l'opportunité de supprimer des données si ces dernières ne sont plus nécessaires aux finalités du traitement.

Par ailleurs, la législation fribourgeoise prévoit un troisième alinéa selon lequel « les personnes privées qui reçoivent des données personnelles de la part d'un organe public en vue d'un traitement à des fins ne se rapportant pas à la personne s'engagent par écrit à prendre toutes les précautions nécessaires pour protéger la personnalité des personnes concernées ». Cette disposition, qui ne connaît pas d'équivalent explicite en droit fédéral, permet d'imposer contractuellement certaines obligations spécifiques aux destinataires des données. Outre l'exigence de consentement préalable de l'organe public avant toute communication des données à des tiers, d'autres éléments peuvent être compris dans la notion de « précautions nécessaires », tels que la mise en place de mesures techniques et organisationnelles afin de garantir la sécurité des données en évitant tout traitement ou accès non autorisé.

Pour le surplus, et au vu de l'inspiration manifeste de l'art. 26 LPrD par l'art. 39 LPD, nous pouvons renvoyer aux considérations ci-dessus (III.). Ceci vaut notamment pour la question de savoir dans quelle mesure l'art. 26 al. 1 LPrD peut lui-même être considéré comme base légale pour le traitement de données à des fins ne se rapportant pas à des personnes – dont fait notamment partie la recherche scientifique. Nous estimons ainsi que l'art. 26 al. 1 LPrD constitue également une « base légale spécifique limitée », en ce sens qu'il permet (seulement) le traitement de données personnelles par l'organe public qui les a collectées et qui veut désormais les utiliser à des fins ne se rapportant pas à des personnes.

L'autorité cantonale fribourgeoise de la transparence, de la protection des données et de la médiation (ci-après : ATPrDM) a publié un aide-mémoire concernant la communication de données personnelles à des fins de recherche non médicale.[106] Destinés aux directeurs et directrices de projets de recherche, il indique les différentes informations et garanties qui sont nécessaires aux organes publics avant que ces derniers puissent communiquer des informations. Ainsi, pour chaque opération prévue (collecte, traitement, communication, publication des résul-

[105] Message LPrD (n. 103), 25.

[106] Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM), Aide-mémoire concernant la communication de données personnelles à des fins de recherche non médicale (mis à jour le 24 janvier 2025), Internet : https://www.fr.ch/sites/default/files/2025-02/fi1bis--aidememoire-concernant-la-communication-de-donnees-personnelles-a-des-fins-de-recherche-non-medicale--pdf.pdf (consulté le 30.6.2025).

tats, conservation, etc.), des mesures de sécurité et de contrôle appropriées doivent être indiquées.

2. Conservation et archivage

En vertu de l'art. 10 al. 2 LPrD – qui renvoie à l'art. 26 LPrD –, le délai de conservation peut être plus long lorsque les données sont traitées à des fins ne se rapportant pas à la personne. Ainsi, les données personnelles « qui présentent une valeur particulière dans le cadre de recherches, de planifications ou de statistiques n'ont pas besoin d'être supprimées de la même manière »[107] et peuvent être conservées pour des durées plus longues, à condition que des mesures de protection appropriées (des droits des personnes concernées) soient mises en place. Les données personnelles sont par ailleurs soumises à la législation sur l'archivage[108] (cf. art. 23 LPrD).

Il est intéressant de souligner que, selon l'art. 17 LArch, l'organe public qui a versé des documents aux archives peut les consulter à tout moment, sauf s'il s'agit de documents classés selon des noms de personnes et contenant des données personnelles sensibles (art. 17 al. 1 LArch). Dans ce cas, pendant la durée du délai de protection, l'organe public ne peut accéder à ces documents que dans certaines situations précises, à savoir lorsque la consultation vise à constituer un moyen de preuve, à servir des objectifs législatifs ou jurisprudentiels, à permettre des évaluations à des fins statistiques, ou encore à rendre une décision concernant une demande de consultation. De prime abord, cela signifierait qu'un organe public ne peut pas consulter – pendant le délai de protection – des données sensibles à des fins de recherche lorsque ces données ont été archivées.

V. En particulier : la communication de données par des organes public en lien avec la recherche

Si un organe public (fédéral ou cantonal) ne mène pas lui-même des recherches mais est sollicité par un chercheur ou une chercheuse qui a besoin (ou estime avoir besoin) de certaines données pour mener à bien un projet de recherche, la question se pose de savoir dans quelle mesure et à quelles conditions l'organe public en question peut, ou éventuellement doit, communiquer des données personnelles.

De manière générale, les grands principes développés sous III. et IV. s'appliquent aussi pour la question de savoir si un organe public peut communiquer des données personnelles à des chercheurs et chercheuses. Toutefois, il s'agit d'une thématique spécifique, qui soulève des questions distinctes de celles en lien avec la conduite même de la recherche. Sans prétendre à une quelconque exhaustivité (nous tenons notamment à rappeler ici – en sus des aspects traités ci-dessus – que les secrets de fonction et de profession prévus par la loi sont toujours à respecter), nous pouvons distinguer cinq aspects dans ce contexte : le lien avec le principe de la transparence (V.A.), la relation avec les principes généraux régissant la communication de données personnelles par des organes publics (V.B.), la question de savoir si l'organe public est obligé, le cas échéant à quelles conditions, de communiquer des données personnelles (V.C.), le droit des particuliers dont les données ont été communiquées d'être informés et de s'opposer à la communication (V.D.) ainsi que la transmission ultérieure par le destinataire de la communication (V.E.).

A. Portée du principe de la transparence

Selon la loi fédérale sur le principe de la transparence dans l'administration (LTrans)[109] et – au niveau cantonal, à Fribourg – la loi sur l'information et l'accès aux documents (LInf),[110] les organes publics sont tenus à une information (active) adéquate au public. De plus, toute personne a un droit d'accès à des documents officiels détenus par l'organe public. Il existe toutefois des réserves, dont fait notamment partie la protection de la personnalité. Au fond, il s'agit toujours d'opérer une mise en balance des intérêts en présence. Il ne s'agit pas ici d'entrer dans une analyse détaillée ni du principe de transparence consacré par ces actes législatifs de manière générale, ni de son articulation avec le droit de la protection des données en particulier.[111] Pour les questions qui nous occupent, il suffit de relever que la législation sur la transparence vise certes, en principe, à garantir en premier lieu l'accès du public – à savoir des personnes privées (physiques ou morales) – à des informations et documents détenus par des organes publics.

---

107 Message LPrD (n. 103), 18.

108 Loi du 10.09.2015 sur l'archivage et les Archives de l'Etat (LArch ; RSF 17.6).

109 Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans ; RS 152.3).

110 Loi cantonale fribourgeoise du 9 septembre 2009 sur l'information et l'accès aux documents (LInf ; RSF 17.5).

111 Cf. à ce propos, avec d'autres références, p. ex. Bertil Cottier, Transparence et protection des données, in : Bernhard Waldmann/Florian Bergamin (éds), 10 ans LInf Fribourg, Berne 2021, 159 ss ; cf. aussi les commentaires de l'art. 36 LPD.

Toutefois, comme le prévoient notamment l'art. 36 al. 3 LPD, l'art. 39 al. 3 LPD ainsi que l'art. 26 al. 4 LPrD, dès lors qu'un organe public est autorisé (dans le cadre de l'information active) ou tenu (dans le cadre de l'information passive) de rendre publiques des données personnelles ou d'en permettre l'accès, il est *a fortiori* autorisé de les communiquer à un autre organe public à des fins de recherches.

B. Articulation entre, d'une part, l'art. 39 LPD et l'art. 26 LPrD et, d'autre part, l'art. 36 al. 2 LPD et l'art. 14 al. 2 et 3 LPrD

Tant l'art. 39 al. 2 LPD que l'art. 26 al. 2 LPrD déclarent inapplicables – en ce qui concerne les dispositions spécifiques régissant la communication de données personnelles par un organe public – uniquement l'art. 36 al. 1 LPD respectivement l'art. 14 al. 1 LPrD. L'art. 36 al. 2 LPD et l'art. 14 al. 2 LPrD – qui prévoient des conditions particulières pour la communication de données personnelles dans un cas d'espèce – ne sont pas mentionnés. Il se pose alors la question de savoir si un organe public – lorsqu'il est confronté à une demande de communication de données personnelles à des fins de recherches doit – en sus des conditions de l'art. 39 al. 1 LPD respectivement de l'art. 26 al. 1 LPrD – examiner si les conditions des art. 36 al. 2 LPD respectivement de l'art. 14 al. 2 LPrD sont remplies.

Dans la mesure où, selon notre analyse, l'art. 39 al. 1 LPD ainsi que l'art. 26 al. 1 LPrD constituent des bases légales pour la communication de données à des fins de recherche, il n'est pas nécessaire de recourir aux bases légales spécifiques des art. 36 al. 2 LPD et 14 al. 2 LPrD. Le fait que l'art. 36 al. 2 LPD et l'art. 14 al. 2 LPrD restent applicables n'a alors que très peu d'impact pratique dans notre contexte, dans la mesure où l'art. 39 al. 1 LPD et l'art. 26 al. 1 LPrD permettent – aux conditions énoncées par ces dispositions – la communication de données personnelles détenues par l'organe public. Il convient toutefois de rappeler, dans ce contexte, que le traitement de ces données personnelles par le destinataire nécessite une base légale (III.B.3.).

Par ailleurs, et pour autant qu'il y ait un cas d'espèce, la communication de données personnelles à des fins de recherche peut être couverte par l'art. 36 al. 2 lit. a LPD et l'art. 14 al. 2 lit. a LPrD, dans la mesure où elle est indispensable à l'accomplissement des tâches légales du destinataire (la recherche scientifique d'une haute école étant, par exemple, à considérer comme une tâche légale). Il reste à préciser que cette condition doit être démontrée dans chaque cas d'espèce, d'où l'importance de la base légale spécifique de l'art. 39 al. 1 LPD ainsi que de l'art. 26 al. 1 LPrD.

C. Caractère discrétionnaire de la communication des données ?

Selon l'art. 36 al. 6 LPD et l'art. 16 LPrD – qui restent applicables dans le cadre de la communication de données personnelles sur la base de l'art. 39 al. 1 LPD et de l'art. 26 al. 1 LPrD –, la communication des données personnelles est refusée ou restreinte si (entre autres) un intérêt digne de protection de la personne concernée (ou d'un tiers) l'exige. De plus, l'art. 39 al. 1 et l'art. 26 al. 1 LPrD ne prévoient pas d'obligation de l'organe public de communiquer des données personnelles à un autre organe public à des fins de recherches. Dès lors, l'organe public doit opérer une pesée d'intérêts en tenant compte de tous les intérêts en jeu. En font partie notamment le sérieux de la demande, l'importance des données personnelles pour la recherche à mener, la nature des données personnelles à transmettre, les différents traitements des données prévus dans le cadre de la recherche, les personnes ayant accès aux données personnelles ainsi que la durée de la recherche.

Une attention particulière doit être accordée à la liberté de la science (art. 20 Cst.). Si les chercheurs et chercheuses ne peuvent en principe pas déduire de cette disposition (conformément à ce qui prévaut pour la plupart des droits fondamentaux) de droit subjectif à une prestation étatique,[112] il n'en demeure pas moins que la décision de communiquer ou non des données personnelles à des fins de recherche, sur la base de l'art. 39 al. 1 LPD et de l'art. 26 al. 1 LPrD, doit être prise en tenant compte de tous les intérêts en présence, parmi lesquels figure la liberté de la science. Celle-ci, en tant que droit fondamental, revêt également une portée objective, à l'instar d'autres droits fondamentaux.[113] De plus, la jurisprudence du Tribunal fédéral semble admettre que dans certains

---

[112] Cf. p. ex. Véronique Boillet, in : Vincent Martenet/Jacques Dubey (éds), Commentaire romand sur la Constitution fédérale, art. 20 N 7 (avec autres références) ; cf. aussi SG BV-Schweizer, art. 20 N 14, in : Bernhard Ehrenzeller et al. (éds), St. Galler Kommentar – Die Schweizerische Bundesverfassung., 4e éd., Zurich 2023, qui rend toutefois – à juste titre – attentif au fait que dans certaines constellations du moins, un droit subjectif à l'accès à des informations est garantie (n. 19).

[113] Cf. p. ex. Jacques Dubey, Droits fondamentaux, Vol. I, Bâle 2017, § 3 N 109 ss ; Pierre Tschannen, Staatsrecht der Schweizerischen Eidgenossenschaft, Berne 2021, N 280 s. Voir également : art. 35 al. 1 Cst.

cas du moins, un droit à l'information peut être déduit de l'art. 20 Cst.[114] En ce sens, l'importance des données personnelles en question pour le projet de recherche doit être pleinement prise en considération lors de la décision de communiquer les données ou non. Dès lors, il est imaginable qu'il y ait des situations dans lesquelles l'organe public est – malgré le caractère en principe discrétionnaire de la communication des données respectivement le fait qu'il n'existe pas de droit subjectif du chercheur ou de la chercheuse à avoir accès à des données personnelles sur la base de l'art 39 al. 1 ou de l'art. 26 al. 1 LPrD – obligé de communiquer les données personnelles, notamment si la pesée des intérêts mène au résultat clair que l'intérêt (public) de mener à bien la recherche l'emporte sur l'intérêt privé des personnes concernées.

En résumé, si la décision de communiquer des données personnelles sur la base de ces dispositions repose certes sur une pesée d'intérêts, et qu'aucun droit subjectif du demandeur ne découle de l'art. 39 al. 1 LPD ou 26 al. 1 LPrD, il n'en demeure pas moins que l'organe public doit exercer son pouvoir de discrétion à la lumière de tous les intérêts et principes juridiques pertinents, parmi lesquels la liberté de la science revêt une importance particulière. Bien que l'étendue d'un droit individuel à l'accès à des informations détenues par un organe public à des fins de recherche sur la base de l'art. 20 Cst. reste encore à clarifier, un tel droit (aussi sujet, bien entendu, à des restrictions aux conditions de l'art. 36 Cst.) peut, à notre avis, être déduit de l'art. 20 Cst., du moins dans certaines constellations. L'organe public peut alors être tenu de communiquer des données personnelles à des fins de recherche, et il serait en outre possible de faire valoir en justice que le refus de communiquer certaines données personnelles ne prend pas suffisamment en considération des éléments susmentionnés.

D. Relation avec d'autres obligations du responsable de traitement et les droits des personnes concernées

L'art. 39 al. 2 LPD et l'art. 26 al. 2 LPrD énumèrent exhaustivement les dispositions de la LPD et de la LPrD qui ne sont pas applicables au traitement de données ne se rapportant pas à des personnes. Dès lors, les autres dispositions de la LPD et de la LPrD sont pleinement applicables. Ceci vaut non seulement pour les principes énoncés sous II., mais aussi pour les autres obligations du responsable ainsi que les droits de la personne concernée.

En lien avec la recherche scientifique, deux thématiques sont *a priori* particulièrement importantes :

– Premièrement, selon l'art. 19 al. 1 à 3 LPD et l'art. 12 LPrD, le responsable du traitement informe de manière adéquate la personne concernée de la collecte de ses données personnelles, que celle-ci soit effectuée auprès d'elle ou non. Ces dispositions quant au devoir d'informer la personne concernée lors de la collecte de données sont aussi à respecter en lien avec la recherche scientifique. Toutefois, l'art. 20 LPD et l'art. 13 LPrD connaissent des exceptions au devoir d'informer. Il est notamment prévu à l'art. 20 al. 2 LPD – lorsque les données ne sont pas collectées auprès de la personne concernée –, et à l'art. 13 al. 1 let. b LPrD, que le devoir d'information ne s'applique pas si l'information est impossible à donner ou si elle nécessite des efforts disproportionnés. Ces conditions seront fréquemment réunies dans les cas où le chercheur ou la chercheuse a obtenu des données personnelles auprès d'un autre organe public.
– Secondement, la personne concernée a le droit de s'opposer à une communication de données personnelles (art. 37 al. 1 LPD et art. 31 LPrD). Dans le contexte d'une possible opposition de la personne concernée par rapport à la communication de ses données à des chercheurs et chercheuses, il faut prendre en considération qu'elle sera souvent confrontée à la difficulté de ne pas avoir connaissance de cette communication (le devoir d'information ne s'appliquant pas), ce qui l'empêche, *de facto*, d'exercer son droit d'opposition. Par ailleurs, ce point pouvant d'ailleurs revêtir une certaine importance, surtout si la personne concernée a préalablement exprimé son opposition à la communication de ses données, l'organe public peut rejeter l'opposition si les conditions de l'art. 37 al. 2 LPD respectivement de l'art. 31 al. 2 LPrD sont remplies, ou s'il y a un intérêt public prépondérant en faveur de la communication selon l'art. 36 al. 3 LPD respectivement l'art. 11 al. 1 let. c LInf (art. 39 al. 3 LPD et art. 26 al. 4 LPrD). Ce dernier cas de figure est pertinent dans notre contexte : une pesée des intérêts devra être opérée, lors de laquelle l'intérêt public pourra être considéré – tel que démontré plus haut – comme prépondérant lorsque la communication de données se fait à des fins de recherche scientifique (puisque celle-ci est aussi à considérer comme un intérêt public).

[114] ATF 127 I 145 c. 4 ; 148 II 273 c. 6 concernant une pesée d'intérêts lacunaire en lien avec l'accès à des informations archivées en vue d'un projet de recherche. Cf. aussi Jacques Dubey, Droits fondamentaux, Vol. II, Bâle 2017, § 25 N 2439.

E. Transmission ultérieure par le destinataire

Dans le cadre de recherches scientifiques, des données sont souvent transmises à d'autres personnes ou même rendues publiques afin que les résultats des recherches puissent être reproduits. À noter dans ce contexte que le principe des *open research data* gagne en importance. Dans la mesure où les données personnelles ne sont, ou ne peuvent, pas être anonymisées, l'art. 39 al. 1 let. c LPD et l'art. 26 al. 1 let. b LPrD prévoient qu'une communication à des tiers ne peut se faire qu'avec le consentement de l'organe public qui les a transmises. Ce dernier doit alors opérer une nouvelle pesée des intérêts.

Par ailleurs, l'art. 39 al. 1 let. d LPD et l'art. 26 al. 1 let. d LPrD – qui prévoient qu'une publication des résultats de la recherche ne peut se faire que sous une forme ne permettant pas l'identification des personnes concernées – implique que le principe des *open research data* ne peut être appliqué pour les données personnelles. En d'autres termes : du moment que les données « primaires » ne peuvent pas être codées, elles ne peuvent être publiées. Restent réservées, bien entendu, les dispositions de la législation sur le principe de la transparence, à savoir la LTrans et la LInf (cf. V.A.).

VI. Synthèse et conclusion

En conclusion, la protection des données personnelles constitue un enjeu fondamental dans le cadre des recherches conduites par des organes publics. Il est impératif de prendre en compte, dès la phase préparatoire et tout au long du déroulement de la recherche, les principes applicables au traitement des données, en particulier celui de la sécurité des données. En ce qui concerne des données personnelles qui n'ont pas été collectées par l'organe public qui conduit la recherche, les organes publics doivent pouvoir se baser sur une base légale pour le traitement de données dans le cadre de leur recherche. Il convient, dès lors, de veiller à ce que les bases légales pour les hautes écoles soient suffisamment claires et précises. Dans le contexte du traitement de données à des fins de recherches, les exigences concernant ces bases légales peuvent être assouplies en ce qui concerne le niveau de formalité et de densité normative. Que ce soit au niveau fédéral ou cantonal, une loi au sens matériel peut être suffisante et, pour les cas de communication de données à des fins de recherche, également moins précise étant donné qu'une communication est acceptée même si elle n'est pas expressément prévue. Ces assouplissements permettent de trouver un équilibre entre l'intérêt public de la recherche, la liberté de la science, la protection de la personnalité ainsi que les droits fondamentaux des personnes dont les données sont traitées.

Par ailleurs, la protection des données en lien avec la recherche scientifique peut aussi concerner des organes publics qui ne conduisent pas eux-mêmes des recherches, ceci notamment en lien avec des demandes d'accès à des données formulées par des chercheurs et chercheuses. Il s'agit alors essentiellement d'une problématique relative à la communication de données. Dans ce contexte, la pesée des intérêts – en tenant compte de tous les intérêts en jeu, y compris la liberté de la science ancrée à l'art. 20 Cst. – relève d'une importance particulière. Il est alors important que les organes publics s'organisent afin de pouvoir disposer de toutes les informations nécessaires pour pouvoir procéder à cette pesée d'intérêts. Dans cette optique, ils peuvent aussi demander aux chercheurs et chercheuses de fournir des indications à cette fin. Dans certains cas spécifiques, et en tenant compte de l'art. 20 Cst., il est possible que la pesée d'intérêts mène à la conclusion que l'organe public est tenu de communiquer les données personnelles aux chercheurs et chercheuses qui en requièrent l'accès.

La présente contribution a aussi illustré la complexité de la thématique du droit de la protection des données et de la recherche :

- Tout d'abord, il ne sera pas toujours aisé de déterminer exactement les dispositions légales applicables dans la mesure où il ne convient pas seulement de considérer le droit de la protection des données et de l'appliquer à la recherche, mais aussi de déterminer quelles législations spéciales sont – le cas échéant – pertinentes et dans quelle mesure des secrets de fonction ou de profession sont à respecter.
- Ensuite, et sans que cette thématique ait été analysée dans cette contribution, la question se pose de savoir dans quelle mesure les bases légales permettant le traitement de données personnelles à des fins de recherche scientifique existent et sont suffisamment précises. Ceci vaut en particulier pour les hautes écoles cantonales.
- De manière générale, la question de savoir si un traitement poursuit des fins ne se rapportant pas à des personnes peut, dans certains cas, prêter à controverse.
- Les chercheurs et chercheuses eux/elles-mêmes sont confronté-es à un certain nombre d'exigences en matière de protection des données personnelles, ce qui peut constituer un défi important.
- Finalement, en ce qui concerne la communication de données personnelles par un organe public à un

autre organe public, la pesée d'intérêts à opérer peut se révéler très difficile, dans la mesure où l'intérêt de la recherche scientifique et la nécessité de disposer des données personnelles requises pour la mener à bien doivent être pris en compte et qu'il se peut que l'organe public ne soit pas en mesure d'évaluer ces éléments. S'y ajoute le fait – non négligeable – qu'il semble problématique qu'un organe public doive juger de l'intérêt de la recherche scientifique en question, responsabilité qui ne lui est pas attribuée.

En Suisse, ces questions et défis se posent de plus aux niveaux cantonal et fédéral, ce qui ne réduit pas leur complexité. Une coordination accrue entre les différents organes publics confrontés à ces questions pourrait alors s'avérer utile.

VII. Annexe : jurisprudence

A. Concernant le codage et l'anonymisation

Dans son arrêt du 25 mai 2021,[115] le Tribunal cantonal vaudois s'est prononcé sur la question des données codées. Il a rejeté le recours formé par une fondation contre la décision de la Commission cantonale d'éthique (CER-VD), laquelle avait refusé d'autoriser un projet de recherche portant sur une application de suivi du cycle menstruel féminin. La fondation soutenait que le projet ne relevait pas du champ d'application de la loi sur la recherche sur l'être humain (LRH) dans la mesure où il reposait exclusivement sur des données anonymisées. Le Tribunal cantonal a toutefois estimé que les données utilisées ne pouvaient être considérées comme correctement codées au sens de l'art. 26 ORH,[116] dès lors que le lien entre les données de santé et l'identité des utilisatrices n'avait pas été suffisamment rendu méconnaissable. En particulier, la clé d'identification n'était pas conservée par une personne indépendante (cf. art. 5 al. 1 et 26 ORH) et la séparation entre données et identifiants n'était pas techniquement garantie. Par ailleurs, les exigences en matière d'information préalable des personnes concernées (art. 32 ORH), n'avaient pas été respectées, rendant inapplicable le mécanisme de réutilisation avec droit d'opposition prévu à l'art. 33 LRH. Les conditions d'exception de l'art. 34 LRH permettant une réutilisation sans consentement ni information n'étant pas non plus réunies, le Tribunal a confirmé que le projet ne pouvait bénéficier d'une exemption à l'obligation d'autorisation, et que le refus de la CER-VD était conforme au droit applicable.

Cet arrêt met en évidence le principe de sécurité et les mesures techniques qui en découlent, telles que le codage ou l'anonymisation des données. En particulier, lorsqu'il s'agit de données sensibles comme celles de santé en l'espèce, les autorités sont responsables de garantir que les projets respectent pleinement les exigences légales avant de délivrer une autorisation.

Dans le contexte du codage ou de l'anonymisation avant la publication de résultats de recherche, il est possible de mentionner l'ATF 133 IV 107, bien qu'il s'agisse en premier lieu d'une contestation du classement d'une plainte pénale qui touche à la violation du secret professionnel. En effet, en 2004, la « Commission d'experts du secret professionnel en matière de recherche médicale » avait déposé une plainte pénale contre un médecin (chercheur) accusé d'avoir violé le secret de la recherche (art. 321*bis* CP). Ce dernier avait publié en 2002 un rapport contenant des données de patients et patientes (provenant d'archives 1932-1953) sans codage ou anonymisation suffisante, cela dans le cadre d'une recherche mandatée par la Ville de Zurich. Le Ministère public du canton de Zurich avait classé la procédure, estimant que la Commission n'était pas habilitée à porter plainte. En 2007, le TF a confirmé cette position, l'art. 321*bis* CP ne protégeant que la sphère privée des personnes concernées, à l'instar du secret médical (art. 321 CP). En cas de violation, seules les personnes lésées ou, après leur décès, leurs proches peuvent porter plainte. Le TF souligne que la Commission n'est pas « lésée » au sens du droit pénal et ne peut donc pas déposer de plainte pénale, même si elle a autorisé l'accès aux données via une procédure d'autorisation.

En plus de rappeler l'importance d'une anonymisation suffisante, cet arrêt illustre quelque peu la relation entre le respect du secret professionnel et la recherche scientifique.

B. Concernant la consultation de documents d'archives à des fins de recherche

L'importance des archives dans le contexte de la recherche scientifique a pu être rappelée par le Tribunal fédéral dans son ATF 148 I 233. En effet, à la suite de la transmission de dossiers personnels et de dossiers médicaux – émanant tant du Ministère public des mineurs du

[115] TC VD, GE.2020.0095, 11.5.2021.

[116] Ordonnance du 20 septembre 2013 relative à la recherche sur l'être humain à l'exception des essais cliniques (ORH ; RS 810.301).

canton de Bâle-Ville que des Cliniques psychiatriques universitaires de Bâle – aux Archives cantonales, le Tribunal fédéral a procédé à la traditionnelle analyse des conditions des restrictions des droits fondamentaux selon l'art. 36 Cst. Il a d'abord reconnu que cette transmission de données – données qui de plus sont sensibles si elles ont trait à la santé – impliquait une atteinte au droit au respect de la vie privée et à l'autodétermination informationnelle. Toutefois, le TF a ensuite admis la légitimité de cette restriction. Il a relevé que celle-ci reposait sur une base légale formelle suffisante, à savoir la loi cantonale sur l'archivage, et que l'intérêt public à la conservation des documents – notamment en vue de la recherche scientifique – était prépondérant. En outre, le Tribunal fédéral a relevé que l'atteinte respectait le principe de proportionnalité, en particulier grâce aux mécanismes de protection instaurés par la législation cantonale, tels que les délais de protection, l'obligation de procéder à une pesée des intérêts avant toute consultation, ainsi que les conditions spécifiques encadrant l'accès aux documents.

En ce qui concerne la consultation de documents d'archives, un arrêt du Tribunal cantonal tessinois permet de mettre en lumière certains aspects développés dans la présente contribution. En 2003, dans le cadre d'une recherche scientifique portant sur les communes tessinoises, un professeur avait sollicité l'accès à des documents d'archives datant du 19e siècle, conservés dans les archives communales d'un village du canton du Tessin. Sa demande ayant été refusée par les autorités communales, l'affaire est montée jusqu'au Tribunal cantonal tessinois. Dans son arrêt du 10 mars 2006,[117] le Tribunal cantonal a rappelé que certains documents devaient être rendus accessibles en vertu de dispositions légales spécifiques, notamment les données cadastrales, pour autant qu'elles ne portent pas atteinte à la personnalité (art. 970 CC). En revanche, les documents qui n'étaient régis par aucune législation spéciale relevaient de la loi cantonale sur la protection des données personnelles. Dans ce cas, l'accès ne pouvait être accordé que si la demande était suffisamment motivée et permettait de procéder à une mise en balance entre l'intérêt public à la recherche et la protection des droits des personnes concernées. En l'espèce, le chercheur n'avait pas présenté de projet écrit détaillé : il n'avait pas précisé les objectifs de sa recherche, ni identifié les documents qu'il souhaitait consulter. Il n'avait pas non plus indiqué la méthode employée, ni les modalités de publication envisagées. En l'absence de ces éléments, le Tribunal cantonal a considéré que les autorités publiques n'avaient pas excédé leur pouvoir d'appréciation en refusant l'accès général aux archives communales.

Les autorités publiques ont ainsi la responsabilité de veiller à ce que toute décision d'accès aux données à des fins de recherche tienne compte des exigences légales en matière de protection des données personnelles.

Toujours en lien avec la question de consultation d'archives, le Tribunal fédéral s'est prononcé sur l'accès à des archives judiciaires à des fins de recherche dans ATF 127 I 145. Il s'agissait d'un chercheur ayant demandé à consulter des dossiers pénaux archivés relatifs à Martin Schippert, fondateur du groupe de motards « Hell's Angels Switzerland » et décédé en 1981, afin de rédiger une biographie. Selon l'ordonnance zurichoise sur les archives des tribunaux, il était prévu que les dossiers judiciaires ne soient en principe pas accessibles pendant 70 ans, sauf exception accordée par les présidents et présidentes des juridictions concernées. Cette exception était notamment possible si les parties y consentaient ou si un intérêt scientifique prépondérant le justifiait. Sur cette base, le président du tribunal cantonal zurichois a rejeté la demande du chercheur, non pas en raison d'un manque d'intérêt scientifique, mais en raison d'intérêts légitimes opposés. Le Tribunal fédéral a confirmé cette décision. Bien que le chercheur poursuive un but scientifique, cette motivation ne l'emportait pas sur les intérêts légitimes opposables, notamment le droit à la protection de la personnalité des tiers concernés dans les dossiers et des proches de Martin Schippert. Le TF a toutefois laissé la porte ouverte à une nouvelle demande d'accès, pour autant que le chercheur s'engage à anonymiser les données et à obtenir le consentement des proches – ce qui pourrait amener à une appréciation différente du besoin de protection des personnes concernées.

Ainsi, la liberté d'information et la liberté de la science, garanties expressément par la Constitution fédérale, ne fondent pas un droit de portée générale à l'obtention d'informations provenant de sources non généralement accessibles (notamment des dossiers judiciaires archivés, pendant le délai de protection). Cet arrêt aborde également la question de la pesée des intérêts, dont la jurisprudence résumée ci-dessous dessine également les contours (VII.C.).

C. Concernant la pesée des intérêts

Dans l'ATF 148 II 273, le Tribunal fédéral a annulé une décision du Tribunal administratif fédéral (TAF) et lui a renvoyé la cause, en estimant que ce dernier avait insuffisamment motivé le refus d'accès à des dossiers de

[117] TC TI, 52.2004.238, 10.3.2006.

procédure d'asile sollicités dans le cadre d'une thèse de doctorat sur la politique suisse de l'asile dans les années 1980 et 1990. L'affaire concernait un chercheur universitaire souhaitant consulter les dossiers administratifs de X et de sa famille – X ayant tenté, sans succès, d'obtenir l'asile en Suisse avant d'être expulsé. Son parcours avait suscité une certaine attention médiatique et politique. Le Secrétariat d'État aux migrations (SEM) ayant refusé cet accès – décision confirmée par le TAF – l'affaire a été portée devant le Tribunal fédéral. Celui-ci a alors rappelé que, même en l'absence de consentement, l'accès anticipé à des archives contenant des données personnelles pouvait être accordé si un intérêt scientifique prépondérant le justifiait. Il a par ailleurs relevé que X pouvait être qualifié de « personnalité relativement connue », ce qui impliquait une protection moindre de sa sphère privée que celle d'une personne inconnue. Dans ce contexte, le TF a reproché au TAF de ne pas avoir procédé à une pesée complète et individualisée des intérêts en présence. Celui-ci aurait notamment dû prendre en compte le fait que X avait lui-même rendu publiques de nombreuses informations sur sa situation ; que l'autorisation de consulter pouvait être grevée de charges limitant la divulgation des informations ; que plusieurs décennies s'étaient écoulées depuis les faits ; que la recherche ne portait pas sur la vie privée de la famille, mais sur la gestion du dossier par l'administration ; et qu'elle était menée dans un cadre universitaire formel, garantissant (potentiellement) un usage responsable des données.

Cet arrêt souligne l'importance, pour les organes publics, d'opérer une mise en balance complète et circonstanciée des intérêts en présence, notamment en tenant compte du contexte de la recherche (but, procédés, garanties de sécurité).

En outre, dans l'arrêt 1C_595/2021,[118] le Tribunal fédéral a procédé à une pesée des intérêts entre le droit d'accès aux documents publics et la protection des intérêts légitimes des institutions de recherche. Dans le cas d'espèce, un ancien collaborateur scientifique de l'Université de Genève avait demandé l'accès à des documents relatifs à plusieurs projets de recherche en coopération avec des partenaires privés, ce que l'Université avait partiellement refusé en invoquant la protection d'intérêts prépondérants selon la loi cantonale sur l'information du public (LIPAD).[119] Le litige portait sur le caviardage des informations liées à la propriété intellectuelle, aux plans et objectifs de recherche ainsi qu'aux données financières, protégées en tant que secrets d'affaires. Le Tribunal fédéral a confirmé que l'Université pouvait légitimement protéger ces informations afin de préserver ses intérêts patrimoniaux et ceux de ses partenaires, notamment pour éviter un désavantage concurrentiel.

Cet arrêt reconnaît ainsi que les universités, en tant qu'organes publics, disposent d'un intérêt légitime à préserver la confidentialité de certaines informations pour ne pas compromettre leurs partenariats ni leur compétitivité. Cela conforte la marge de manœuvre des institutions académiques pour gérer la diffusion de leurs résultats et préserver leur capacité d'innovation.

---

[118] TF, 1C_595/2021, 19.5.2022.

[119] Loi du 5 octobre 2001sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD ; rsGE A 2 08).