

Données personnelles : une approche dynamique, contextuelle et pragmatique

Michael Montavon, le 21 janvier 2022

Formulée de manière volontairement large, la définition de ce qu'est une donnée personnelle n'en appelle pas moins une analyse circonstanciée. La jurisprudence montre en effet que la question de l'application de la loi sur la protection des données dépend aussi du contexte et des circonstances autour d'un traitement de données. Cela va dans le sens de la nouvelle approche de la protection des données « fondée sur les risques ».

La nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données (nLPD ; [FF 2020 7397](#)) reprend pour l'essentiel les fondamentaux de l'actuelle LPD (définitions, principes, droits des personnes concernées, surveillance par une autorité indépendante), mais y ajoute de nouvelles obligations pour les responsables du traitement et les sous-traitants (cf. <http://www.swissprivacy.law/12> et www.swissprivacy.law/13). L'application concrète de ces nouvelles règles représentera un défi important pour les responsables du traitement nécessitant beaucoup d'efforts, de moyens et d'apprentissage. Une des premières phases de cet apprentissage consistera à se montrer capable d'évaluer quand la nLPD s'applique et quand elle ne s'applique pas.

La nLPD régit le traitement de données personnelles concernant des personnes physiques effectué par des personnes privées et des organes fédéraux ([art. 2 al. 1 nLPD](#)). Les notions de « traitement » et de « données personnelles » se définissent ainsi :

- Un traitement correspond à toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données ([art. 5 let. d nLPD](#)). Il s'agit d'une définition extrêmement large qui, en raison de l'usage du terme « notamment », se révèle plus exemplative que normative. Il n'y a en soi pas grand-chose à en tirer sur le plan pratique.
- Une donnée personnelle correspond à toutes les informations concernant une personne physique identifiée ou identifiable ([art. 5 let. a nLPD](#)). Il s'agit à nouveau d'une définition extrêmement large. Contrairement à la définition d'un traitement, son contenu est néanmoins normatif même s'il ne se laisse pas facilement interpréter. C'est donc à partir de cette définition qu'il sera en partie possible de déterminer si la nLPD

s'applique ou non.

Une information concerne une personne lorsqu'elle peut lui être rattachée de manière à la rendre identifiable. Cette condition est remplie quand le lien entre une information et une personne est explicite (p. ex. les informations contenues sur une carte d'assurance-maladie nominative), mais également quand ce lien découle d'une corrélation d'informations tenant au contexte.

Certaines lois cantonales, à l'instar de la Loi fribourgeoise du 25 novembre 1994 sur la protection des données (LPrD ; [RSF 17.1](#)), définissent dans ce sens une donnée personnelle comme toute information « qui se rapporte » à une personne identifiée ou identifiable ([art. 3 al. 1 let. a LPrD](#)). Intuitivement, on se rend compte qu'il ne peut s'agir que d'un concept dynamique, qui doit être évalué au cas par cas. Savoir si une donnée peut être rapportée à une personne ne peut ainsi pas toujours être établi de manière catégorique *ex ante* mais peut dépendre de toute une série de circonstances qui sont susceptibles d'apparaître seulement lors d'un examen *in concreto* d'une certaine situation.

Ainsi, il est certes notoire que l'augmentation exponentielle des performances des technologies numériques peut aboutir au résultat que des données *a priori* sans lien avec une personne puissent grâce à des techniques de croisement devenir des données personnelles. Cela ne veut pas dire pour autant que toutes ces données doivent dès le départ être considérées comme des données personnelles et être traitées comme telles.

Il ressort de la jurisprudence du Tribunal fédéral que toute possibilité théorique de rattacher des données à un individu n'entraîne pas systématiquement l'application des dispositions relatives à la protection des données. Il faut en plus qu'on puisse raisonnablement admettre qu'une personne aura un intérêt à procéder à cette identification et que cette identification ne nécessite pas des moyens disproportionnés ([ATF 138 II 346, consid. 6.1 ; arrêt du TF 4A_588/2018 du 27 juin 2019, consid. 4](#)).

Cette approche pragmatique s'insère parfaitement dans le nouveau paradigme de la protection des données qui s'appuie sur une approche « fondée sur les risques ». Elle implique qu'une information pouvant éventuellement concerner une personne ne devrait être qualifiée comme une donnée personnelle que dans la mesure où, compte tenu des circonstances, il existe une probabilité raisonnable qu'elle puisse lui être rattachée et qu'elle puisse être utilisée pour déterminer ou influencer la façon dont elle sera traitée ou évaluée. À l'inverse, la seule possibilité qu'une information sans lien direct avec une personne puisse concerner cette dernière dans des circonstances inconnues et pour des finalités indéterminées ne

devrait pas conduire à appliquer à cette information les règles plus contraignantes de la législation sur la protection des données, même si un risque résiduel d'identification existe.

Dans cette approche, le verbe « concerner » qu'on retrouve dans la définition de ce qu'est une donnée personnelle acquiert un sens et une portée renouvelés. Ce n'est plus un élément passif de la définition mais un élément constitutif de celle-ci, nécessitant un examen dynamique et contextuel. Dans la plupart des cas, le résultat d'un tel examen sera assez clair et permettra d'aboutir sans grand effort à la conclusion qu'une information correspond ou non à une donnée personnelle, quel que soit le contexte. Dans d'autres cas, la probabilité qu'une information puisse réellement concerner une personne (c'est-à-dire lui être rattachée) dépendra en revanche des circonstances. Il est donc tout à fait possible qu'une information puisse dans un certain contexte être qualifiée de donnée personnelle sans que cette qualification ne s'applique nécessairement à n'importe quel autre contexte.

Un arrêt du Tribunal cantonal fribourgeois de 2019 illustre parfaitement cette approche. Dans un litige qui opposait deux frères, l'un d'eux a demandé à obtenir le résultat d'une expertise immobilière au sujet d'un bien qu'ils se querellaient et dont l'autre frère était inscrit comme propriétaire. Le Tribunal cantonal a dans ce cas estimé qu'« une expertise immobilière contient des informations relatives au bien expertisé mais aussi, indirectement, au sujet du propriétaire dudit bien, qu'il soit nommément cité dans l'expertise ou non ». Il est parvenu à ce résultat car :

« [e]n l'espèce, [l'un des protagonistes] fait valoir qu'il est propriétaire d'un bien en Albanie et que son frère, dans les procès-verbaux qu'il sollicite, a fait des déclarations le concernant en lien avec la propriété dudit bien. De par cet élément de contexte et la corrélation entre les questions posées par le juge d'instruction et les réponses du prévenu, ces informations se rapportent, au moins indirectement, à la personne du recourant, en ce qu'elles concernent sa qualité de propriétaire, respectivement le fait qu'il soit seul propriétaire ou non, du bien immobilier litigieux ». (cf. [arrêt du TC/FR 601 2018 76](#), consid. 4.2 et 5, in : RFJ 2019. P. 161 ss).

À la lecture de cet arrêt, on comprend que ça n'est pas l'expertise immobilière en elle-même qui a conduit à appliquer la LPrD (apparemment elle ne mentionnait même pas le nom du propriétaire) mais bien les circonstances du cas d'espèce. Il n'est dès lors pas impossible qu'en d'autres circonstances, cette expertise n'eût pas été traitée sous l'angle de la LPrD.

Le Tribunal fédéral est parvenu à un résultat similaire dans un tout autre contexte. Comme des données pseudonymisées permettent toujours d'identifier les personnes concernées, elles sont généralement toujours considérées comme des données personnelles et restent donc soumises aux législations relatives à la protection des données.

Toutefois, en cas de transmission de données pseudonymisées à des tiers, le Tribunal fédéral a jugé que ces données ne sont plus simplement pseudonymisées mais qu'elles sont anonymisées si les tiers en question ne disposent pas de la table de concordance nécessaire à une réidentification. À condition que des mesures suffisantes soient prises pour garantir le maintien de cet anonymat, la transmission peut ainsi échapper aux règles de la protection des données, car, pour le destinataire, les données ne concernent pas une personne identifiée ou même identifiable (cf. arrêt du TF 4A_365/2017 du 26 février 2018, consid. 5, Emilie Jacot-Guillarmod in : www.lawinside.ch/660).

Dans cet arrêt, le Tribunal fédéral a fait une distinction selon que les mêmes données sont en possession d'une personne capable de les rattacher à une personne ou pas. Dans le premier cas, il a considéré qu'il s'agissait de données personnelles, mais pas dans le second. Conformément à l'approche fondée sur les risques, il a accepté l'existence d'un risque résiduel de réidentification considérant que ces données n'avaient pas vocation à être rattachées à une personne déterminée.

Il est certain qu'avec l'usage toujours plus répandu des technologies numériques dans tous les secteurs d'activité le droit de la protection des données prend une dimension et une importance toujours plus grandes dans notre société. Cela nécessite toutefois une approche nuancée et pragmatique des lois sur la protection des données. Si l'on n'accepte pas l'existence d'un risque résiduel, aucune information ne pourra au bout du compte jamais plus sortir du champ d'application des lois sur la protection des données. Loin d'améliorer la situation des personnes dont les données sont traitées, cette situation risque plutôt de l'affaiblir.

Le but des lois sur la protection des données est la protection de la personnalité et des droits fondamentaux des personnes concernées dont les données font l'objet d'un traitement. Il n'est pas souhaitable que les règles prévues s'appliquent en définitive à des situations dans lesquelles ni la personnalité, ni les droits fondamentaux des personnes concernées ne sont réellement concernés. Tant du point de vue des personnes concernées que des autorités de contrôle de la protection des données, il vaut en effet mieux une protection efficace mais ciblée qu'une protection prétendument tous azimuts mais impossible à mettre en œuvre.

Proposition de citation : Michael MONTAVON, Données personnelles : une approche dynamique, contextuelle et pragmatique, 21 janvier 2022 *in* www.swissprivacy.law/115

 Les articles de [swissprivacy.law](http://www.swissprivacy.law) sont publiés sous licence creative commons CC BY 4.0.