_swissprivacy.law

Enquête contre Digitec Galaxus : les recommandations du Préposé sont justifiables, mais sont-elles justes ?

Christophe Hensler, le 13 mai 2024

Le Préposé estime que l'obligation d'ouvrir un compte client pour procéder à un achat viole le principe de proportionnalité et recommande à Digitec Galaxus plusieurs modifications de sa déclaration de protection des données. La présente contribution analyse les différentes recommandations du Préposé d'un œil critique et tire des enseignements à la lumière de la nouvelle loi sur la protection des données.

I. Introduction

Le Préposé fédéral à la protection des données et à la transparence a récemment publié son rapport final sur l'enquête ouverte contre Digitec Galaxus SA.

Cette affaire remonte à fin mars 2020 avec l'interpellation du Préposé par une cliente qui avait accepté la déclaration de protection des données de Digitec Galaxus, mais s'était opposée par la suite à l'enregistrement et à la transmission de ses données relatives à son adresse et sa carte de crédit, ainsi qu'à toute exploitation de ses données personnelles à des fins publicitaires et de marketing. La cliente reprochait également à Digitec Galaxus le fait que les clients étaient contraints d'accepter tous les traitements de données décrits dans la déclaration de protection des données pour pouvoir passer une commande.

Dans son rapport final, le Préposé arrive à la conclusion que l'obligation de créer un compte client pour procéder à un achat viole le principe de proportionnalité et recommande également à Digitec Galaxus plusieurs adaptations de sa déclaration de protection des données.

La présente contribution analyse les différentes recommandations du Préposé d'un œil critique et tire des enseignements à la lumière de la nouvelle loi sur la protection des données.

II. Remarques préliminaires

Tout d'abord, il est important de souligner que cette affaire était soumise à l'ancienne LPD (aLPD) conformément à la disposition transitoire de l'art. 70 nLPD. Le Préposé a ainsi procédé

à un établissement des faits selon l'art. 29 al. 1 let. a aLPD en appliquant les règles matérielles de l'ancien droit. L'application de l'aLPD s'étend également aux mesures à disposition du Préposé qui se limitent à des recommandations non contraignantes (art. 29 al. 3 aLPD) avec la possibilité, en cas de rejet par le maître du fichier (responsable du traitement selon la nLPD), de porter l'affaire devant le Tribunal administratif fédéral pour décision (art. 29 al. 4 aLPD).

Par ailleurs, on relèvera la durée particulièrement longue de cette affaire, dont les prémices ont commencé en mars 2020 pour aboutir à un rapport final en avril 2024, soit après plus de 4 ans. Avec l'entrée en vigueur de la nLPD, et malgré la disposition transitoire, les délais de traitement ont malheureusement pour effet de créer un décalage important entre le droit qui est, ou était, déterminant lors de l'établissement des faits et le droit auquel Digitec Galaxus est soumise au moment de la publication du rapport final.

Enfin, on notera que le rapport final se base sur l'état de fait et les documents soumis à fin 2021, alors que Digitec Galaxus a informé le Préposé en juin 2023 qu'elle avait révisé sa déclaration de protection des données en vue de l'entrée en vigueur de la nLPD. On peut dès lors se demander pourquoi le Préposé n'a pas tenu compte de la nouvelle déclaration de protection des données dans ses recommandations, dont la plupart étaient déjà dépassées au moment où le rapport final a été publié.

III. Adaptations de la déclaration de protection des données

Dans son rapport final, le Préposé formule cinq recommandations à Digitec Galaxus portant sur des adaptations de sa déclaration de protection des données.

1) Identification des outils d'analyse web

Le Préposé recommande d'identifier clairement les outils d'analyse web utilisés et les traitements de données personnelles qui en résultent. De son côté, Digitec Galaxus semble estimer que cette recommandation est sans objet avec l'adoption de la nouvelle déclaration de protection des données.

Cette recommandation soulève des questions intéressantes sur l'application de la LPD (ancienne comme nouvelle) aux données récoltées au moyen d'outils d'analyse web, en particulier les fameux cookies dont les bannières de consentement sont devenues omniprésentes sur tous les sites internet depuis l'entrée en vigueur du RGPD en 2018.

Cela n'est pas abordé dans le rapport du Préposé, mais il est utile de rappeler qu'en droit suisse l'utilisation de cookies est régie en premier lieu par l'art. 45c de la Loi sur les télécommunications (LTC) qui exige notamment d'informer l'utilisateur sur le traitement et sa finalité, ainsi que sur la possibilité de refuser ce traitement. Contrairement au droit européen, qui prévoit un mécanisme d'opt-in nécessitant d'obtenir le consentement préalable de l'utilisateur (cf. art. 5 (3) de la de la directive 2002/58/CE surnommée aussi « ePrivacy Directive »), le droit suisse prévoit uniquement un devoir d'information, lequel peut parfaitement être rempli par le biais de la déclaration de protection des données, avec possibilité d'opt-out. C'est d'ailleurs l'approche choisie par les sites digitec.ch et galaxus.ch qui n'ont pas de bannière de cookies mais où l'information se fait par la déclaration de protection des données, complétée par une notice d'information sur les cookies et les technologies similaires.

Au final, la règlementation sur la protection des données ne trouve application que si les données traitées au moyen de cookies se rapportent à une personne déterminée ou identifiable. La notion de données personnelles a connu des évolutions ces dernières années avec plusieurs arrêts, suisses et européens, qui penchent de plus en plus vers une approche dite « *relative* » (où le caractère identifiable de l'information doit être analysé du point de vue de la personne qui détient l'information ; sur cette notion voir notamment Alexandre Jotterand, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?, 13 juin 2023 in www.swissprivacy.law/232). Or, il est intéressant de voir que le Préposé semble continuer à se baser sur l'approche « absolue » en considérant que des données pseudonymisées constituent des données personnelles dans la mesure où elles peuvent être potentiellement réidentifiées, sans effort disproportionné, par un procédé d'individualisation, de corrélation ou d'inférence (soit dans la version originale en allemand, « *durch Herausgreifen, Verknüpfung und Inferenz* » qui est une terminologie reprise de l'Avis 05/2014 du G29 sur les techniques d'anonymisation [allemand/français]).

2) Identification des finalités et profil de la personnalité

Le Préposé recommande ensuite d'identifier clairement pour quelles finalités les données personnelles sont traitées et d'indiquer que certains traitements peuvent conduire à des profils de la personnalité (devenus des « profilages » sous la nLPD). Digitec Galaxus rejette partiellement cette recommandation tout en ayant adapté sa nouvelle déclaration de protection des données sur ce point.

Cette recommandation pose notamment la question de la granularité de l'information sur les finalités, à savoir s'il est acceptable d'indiquer dans la déclaration une liste de finalités sans

préciser quelles données personnelles sont traitées en rapport avec chaque finalité.

Il est utile de rappeler que l'aLPD prévoyait un devoir d'information moins étendu que la nLPD avec une information limitée à la collecte de données sensibles et aux profils de la personnalité (l'art. 19 nLPD s'applique à la collecte de toute donnée personnelle). En ce qui concerne le contenu de l'information, la LPD (ancienne comme nouvelle) impose entre autres au responsable du traitement de communiquer les finalités du traitement (art. 14 al. 2 let. a aLPD ; art. 19 al. 2 let. a nLPD), sans toutefois exiger explicitement de lier les données personnelles traitées aux finalités.

Dans son rapport final, le Préposé semble d'avantage baser sa réflexion sur les principes généraux de bonne foi (art. 4 al. 2 aLPD ; art. 6 al. 2 nLPD) et de reconnaissabilité des finalités (art. 4 al. 3 et 4 aLPD ; art 6 al. 3 nLPD) que sur les dispositions relatives au devoir d'information (art. 14 aLPD ; art. 19 nLPD). Il estime que les personnes concernées ne peuvent pas valablement exercer leur droit à l'autodétermination informationnelle (comme donner leur consentement ou s'opposer à un traitement) si elles ne savent pas clairement quelles données personnelles sont traitées en lien avec quelles finalités.

La nLPD apporte une précision dans ce sens en exigeant que les informations à communiquer doivent être celles nécessaires pour que la personne concernée puisse faire valoir ses droits et pour que la transparence des traitements soit garantie (art. 19 al. 2 nLPD). Le degré de détails de l'information est en principe déterminé par le responsable du traitement et dépend du type de données personnelles traitées ainsi que de la nature et de l'ampleur du traitement (cf. message du Conseil fédéral relatif à la nLPD, p. 6669).

De manière générale, on peut se demander si le rattachement des données personnelles à chaque finalité est réellement nécessaire pour que les personnes concernées puissent faire valoir leurs droits. En effet, dans l'exercice de leurs droits, les personnes concernées attacheront souvent plus d'importance aux finalités en tant que telles qu'aux données personnelles qui y sont rattachées. Par exemple, le client qui souhaite s'opposer à l'exploitation de ses données personnelles à des fins publicitaires et de marketing ne s'abstiendra pas de le faire parce qu'il ne connaît pas l'étendue exacte des données personnelles traitées en lien avec cette finalité.

Une interprétation trop stricte de la granularité de l'information irait également à l'encontre de la possibilité de traiter ultérieurement des données personnelles de manière compatible avec les finalités initiales. A titre d'exemple, on peut présumer que si la personne concernée transmet son adresse dans le cadre de l'obtention d'une carte client ou pour une commande

(en ligne ou non), l'utilisation ultérieure de cette adresse à des fins commerciales par l'entreprise elle-même peut être considérée comme correspondant à une finalité initialement reconnaissable, et donc compatible avec les finalités initiales (cf. message du Conseil fédéral relatif à la nLPD, p. 6645).

A notre sens, il convient de lire la recommandation du Préposé dans le contexte spécifique des traitements effectués par Digitec Galaxus, en particulier le fait que certaines données personnelles sont utilisées à des fins d'analyse du comportement de la clientèle et qu'elles peuvent être transmises à d'autres entreprises du groupe Migros pour les mêmes finalités. Tout en laissant ouverte la question, le Préposé évoque l'existence potentielle d'un « profilage à risque élevé », ce qui explique peut-être l'approche stricte qui a été prise dans cette affaire.

3) Traitement de données personnelles « à titre de réserve »

Le Préposé recommande également de ne pas mentionner de traitements de données à « titre de réserve » mais uniquement ceux qui sont vraiment effectués. Cette recommandation est rejetée par Digitec Galaxus.

Le Préposé estime qu'une personne concernée s'attend de bonne foi à ce que les informations contenues dans la déclaration de protection des données soient exactes. Selon lui, une déclaration de protection des données incluant des traitements de données « à titre de réserve » laisserait les personnes concernées dans l'ignorance et il ne leur serait plus possible de distinguer les traitements de données qui ont effectivement lieu de ceux qui pourraient éventuellement avoir lieu à l'avenir.

Sur ce point, les explications du Préposé ne sont pas convaincantes et cette recommandation doit être relativisée.

La mention de traitement de données personnelles « à titre de réserve » ne signifie pas nécessairement que les informations communiquées sont inexactes. Si la déclaration de protection des données est formulée de manière non-équivoque, en distinguant les traitements actuels de ceux envisagés, on ne devrait pas pouvoir reprocher au responsable du traitement un manque de transparence.

Par ailleurs, la mention de futurs traitements évite de devoir modifier la déclaration et permet aux personnes concernées d'être informées d'emblée sur les développements envisagés du traitement. Une telle réserve permet vraisemblablement une meilleure transparence

qu'une modification ultérieure de la déclaration, qui ne sera vraisemblablement jamais lue par le client et réputée comme acceptée tacitement.

Enfin, il ne faut pas perdre de vue que la déclaration de protection des données est une information générale ex-ante et que les personnes concernées ont toujours la possibilité de demander des informations plus précises ex-post sur les traitements effectués par le biais du droit d'accès (art. 8 aLPD ; art. 25 LPD).

Si la position du Préposé parait trop stricte, il convient toutefois de poser des limites pour éviter des abus. La mention de traitements de données « à titre de réserve » devrait rester une exception réservée à des traitements qui sont réellement envisagés dans un futur proche. La multiplication de traitements purement hypothétiques viderait de sens l'information qui est donnée et ne serait vraisemblablement plus compatible avec le principe de bonne foi.

4) Identification des atteintes à la personnalité et des motifs justificatifs invoqués

Le Préposé recommande aussi d'informer les personnes concernées sur les traitements entraînant des atteintes à la personnalité et sur les motifs justificatifs invoqués. Cette recommandation est elle aussi rejetée par Digitec Galaxus.

Le fondement de cette recommandation ne ressort pas clairement du rapport final.

En ce qui concerne le traitement de données personnelles par des personnes privées, il est important de rappeler que la LPD a adopté une approche différente du RGPD qui part du principe qu'un traitement de données n'est licite que s'il existe un motif justificatif (art. 6 RGPD) et exige explicitement de communiquer aux personnes concernées la base juridique du traitement (art. 13(1)© RGPD). Dans la LPD, il n'est pas nécessaire d'avoir un motif justificatif pour traiter des données personnelles, mais celui-ci permet de justifier une atteinte à la personnalité (présumée dans les cas énumérés à l'art. 12 al. 2 aLPD et 30 al. 2 nLPD) qui rendrait le traitement illicite.

Comme nous l'avons vu ci-dessus, le devoir d'information de l'aLPD était moins étendu que celui de la nLPD et aucun des deux textes n'impose explicitement de communiquer des informations sur les atteintes à la personnalité ou sur les motifs justificatifs. L'aLPD prévoyait tout au plus de communiquer « éventuellement la base juridique du traitement » dans le cadre du droit d'accès (art. 8 LPD), ce qui n'a pas été repris dans la nLPD.

Néanmoins, en fonction du type de données personnelles traitées ainsi que de la nature et de l'ampleur du traitement, on pourrait envisager qu'il existe un devoir d'information à tout le moins sur les motifs justificatifs du traitement pour que les personnes concernées puissent évaluer la licéité du traitement et le cas échéant faire valoir leurs droits.

5) Effacement et opposition

Le Préposé recommande encore de décrire les possibilités d'effacement, respectivement d'opposition, applicables pour chaque motif justificatif et de les mettre correctement en œuvre en pratique. Digitec Galaxus estime avoir anticipé cette recommandation avec l'adoption de sa nouvelle déclaration de protection des données.

On notera que, contrairement au RGPD (art. 14(2)© RGPD), la LPD (ancienne comme nouvelle) n'exige pas explicitement d'informer les personnes concernées de leurs droits. Cette information pourrait tout au plus rentrer dans les informations nécessaires pour que la personne concernée puisse faire valoir ses droits selon l'art. 19 al. 2 *ab initio* nLPD. Sous réserve des informations minimales expressément prévues à l'art. 19 al. 2 nLPD qui sont requises, le contenu et degré de détails de l'information est déterminé par le responsable du traitement qui pourrait défendre un point de vue minimaliste en se réfugiant derrière le principe « *nul n'est censé ignorer la loi* ».

En pratique, on peut toutefois constater que de nombreux responsables de traitement ont adopté des déclarations de protection des données plus détaillées pour se conformer également aux exigences du RGPD et qu'ils fournissent ainsi cette information.

IV. Obligation de créer un compte client

Enfin, le Préposé arrive à la conclusion principale que le fait de lier le traitement de données à l'obligation de créer un compte client viole le principe de nécessité et donc le principe de proportionnalité du traitement des données de l'art. 4 al. 2 aLPD (art. 6 al. 2 nLPD). Il formule une recommandation alambiquée par laquelle il suggère que l'offre alternative d'une possibilité d'achat en tant qu'invité, c'est-à-dire un achat pouvant être effectué sur la plateforme en ligne sans enregistrement préalable, constituerait un moyen d'aménagement proportionné du traitement des données. Il semble que Digitec Galaxus ait accepté de mettre en œuvre cette alternative, sans toutefois reconnaitre l'existence d'une obligation légale.

La conclusion du Préposé peut sembler justifiée sous l'angle de la protection des données, mais est-elle vraiment juste ?

La nécessité d'un traitement, et donc sa proportionnalité, doit être mise en rapport avec la finalité poursuivie, qui est en principe définie par le responsable du traitement.

Le Préposé estime que la création d'un compte client ne devrait pas être nécessaire pour l'utilisateur qui souhaite simplement commander une marchandise en ligne, alors que Digitec Galaxus considère que le compte client fait partie intégrante d'une offre de services plus large (notamment gestion des commandes, personnalisation d'offres et participation à la communauté).

D'un côté, le Préposé n'a pas totalement tort d'estimer que le compte client n'est pas nécessaire pour un simple achat mais, d'un autre côté, il intervient dans une relation de services plus large qui reste en rapport avec la finalité initiale poursuivie par Digitec Galaxus. La création d'un compte client peut présenter des avantages pour les clients en facilitant le suivi des commandes et l'exercice des droits de garantie, voire même de certains droits de la protection des données (il sera par exemple plus facile d'exercer les droits de rectification, d'effacement ou de portabilité par le biais d'un compte client). En tant que responsable du traitement, Digitec Galaxus doit rester libre de structurer son offre de services de la façon qu'elle juge appropriée tant que les personnes concernées sont conscientes des traitements effectués et qu'elles ont la possibilité de faire valoir leurs droits (comme le droit de s'opposer au traitement à des fins publicitaires et de marketing). En effet, c'est bien le responsable du traitement qui détermine non seulement les finalités mais aussi les moyens du traitement (art. 3 let. i aLPD ; art. 5 let. j nLPD). Il en irait bien entendu autrement si Digitec Galaxus collectait des données personnelles sans utilité pour l'accomplissement des finalités poursuivies. Sauf en cas de violation évidente, le Préposé ne devrait pas intervenir pour surprotéger des clients qui ont volontairement fourni leurs données personnelles et accepté la déclaration de protection des données. Les clients restent libres de s'adresser à un concurrent qui propose l'achat en tant qu'invité. Il ne faut pas non plus oublier que les utilisateurs peuvent supprimer à tout moment leur compte client et demander la suppression des données personnelles qui y sont rattachées.

Enfin, on peut se demander si l'alternative de l'achat en tant qu'invité constitue réellement un moyen d'aménagement proportionné du traitement des données. L'achat en tant qu'invité donne l'illusion que la boutique en ligne traite moins de données personnelles, ce qui n'est souvent pas le cas en réalité. En effet, les données personnelles collectées dans le cadre d'un achat en tant qu'invité sont généralement identiques à celles demandées pour la création d'un compte client (à l'exception peut-être d'un mot de passe). La création d'un compte client doit être vue comme un moyen pour récolter des données personnelles. Lors d'un

achat en tant qu'invité, le responsable de traitement peut traiter, par des moyens techniques (cookies ou autres traceurs), exactement les mêmes données personnelles qu'avec la création d'un compte client. Par ailleurs, le client qui achète des biens en tant qu'invité sera, dans tous les cas, amené à accepter une déclaration de protection des données, dont les finalités sont librement déterminées par le responsable du traitement. Il n'est en effet pas exclu qu'un responsable du traitement puisse utiliser certaines données personnelles récoltées lors d'un achat en tant qu'invité pour d'autres finalités (par exemple envoi par courrier ou email de publicités). D'ailleurs, si on analyse les déclarations de protection des données des boutiques en ligne qui proposent un achat en tant qu'invité, on se rend très rapidement compte qu'il n'existe souvent pas de distinction entre les données personnelles collectées avec ou sans compte client et qu'elles sont utilisées de manière générale pour toutes les finalités. Au final, ce qui importe ne devrait pas être la méthode par laquelle les données personnelles sont collectées, mais plutôt les finalités et traitements effectués par le responsable du traitement, conformément à sa déclaration de protection des données.

En pratique, la tendance est de prévoir la possibilité d'un achat en tant qu'invité, qui ne change dans le fond pas grand-chose pour le responsable du traitement, mais qui donne l'illusion d'un meilleur respect de la protection des données. On notera qu'en mars 2022 la Conférence de protection des données allemande (« DSK » qui regroupe les autorités indépendantes de contrôle de la protection des données au niveau fédéral et des Länder) a pris une position allant dans le même sens que notre Préposé en concluant que les responsables du traitement offrant des biens ou services en ligne sont généralement tenus de permettre aux clients de passer des commandes via un accès invité.

V. Conclusion

Le rapport final du Préposé est particulièrement sévère à l'encontre de Digitec Galaxus avec des recommandations très (trop ?) strictes et formalistes.

Les recommandations du Préposé paraissent extrêmement strictes au vu des circonstances et de l'adaptation de la déclaration de protection des données de Digitec Galaxus.

Par ailleurs, les principes qui se dégagent des recommandations méritent également d'être relativisés, en particulier la mention dans la déclaration de protection des données de traitements « à titre de réserve » qui devrait être possible dans la mesure du raisonnable.

Enfin, il sera intéressant de voir si le Préposé est cohérent et poursuivra son action en prenant des mesures contre les autres boutiques en ligne (dont certaines sont identifiées

dans son rapport final) qui exigent la création d'un compte client. À cet égard, il est particulièrement amusant de constater que l'utilisateur qui souhaite commander une copie papier du 30e Rapport d'activités du Préposé 2022/2023 dans le Shop officiel en ligne des publications fédérales devra obligatoirement créer un compte pour passer commande et qu'il est étonnamment impossible de procéder à un achat en tant qu'invité.

Proposition de citation : Christophe HENSLER, Enquête contre Digitec Galaxus : les recommandations du Préposé sont justifiables, mais sont-elles justes ?, 13 mai 2024 *in* www.swissprivacy.law/299