31e Rapport d'activités du PFPDT – Un survol (Partie 1 : Protection des données)

Charlotte Beck, le 4 septembre 2024

Le 31e rapport annuel du PFPDT permet de plonger dans les activités de cette autorité, de passer en revue les différentes décisions importantes rendues ainsi que les travaux effectués.

31e Rapport d'activités 2023/2024

Mis en ligne le 26 juin 2024, le rapport est partagé en deux parties, à l'image des deux tâches de l'autorité, la protection des données personnelles et la transparence.

Sur le domaine de la protection des données, sur lequel cette contribution se focalise, le 31e rapport couvre la période du 1er avril 2023 au 31 mars 2024. Ce rapport est d'autant plus intéressant qu'il permet de revenir sur presque sept mois d'application de la LPD révisée. Les décisions rendues, interprétations et pratiques décrites donnent des indications aux personnes concernées, aux entités soumises, aux professionnels et au public sur les effets et l'application de cette loi.

Le rapport s'ouvre sur une section dédiée au « défis actuels », en répondant à sept questions : qu'est-ce que l'on protège, contre quoi et jusqu'où, la capacité à renoncer à ces droits, l'intérêt même de la discipline dans le contexte des réseaux sociaux, l'existence ou non de traitements interdits et la mesure politique de la protection des données. Cette section permet de rappeler la base de la protection des données, ainsi que la pertinence du domaine dans le contexte actuel. Deux phrases mises en avant dans le rapport permettent de résumer ces deux aspects. La première rappelle que :

> *« la personnalité humaine est au cœur de la protection des données ».*

La deuxième – en réponse à la question de savoir si la protection des données est une « notion dépassée », notamment dans le contexte des réseaux sociaux – indique que :

> *« ces adultes qui prétendent s'exposer librement devant un large public sont pour la plupart soucieux de se présenter dans un contexte mis en scène par eux-mêmes ».*

Les thèmes principaux abordés dans le rapport sont l'implications du PFPDT dans les projets fédéraux par le biais d'analyses d'impact, les décisions rendues dans les procédures d'enquêtes, les prises de positions et indications sur des sujets actuels et les développements ayant eu lieu à l'international.

Cloud fédéral

En matière d'informatique en nuage (*cloud*), le PFPDT a notamment été associé au projet *Cloud Enabling Büro-automation* (Bureautique permettant l'accès au nuage, CEBA) de la Chancellerie fédérale. Le PFPDT a notamment sur la directive d'application du logiciel Microsoft 365 ainsi que le projet d'analyse d'impact relative à la protection des données (AIPD). Sur ce point, le PFPDT rappelle que tous les risques devraient figurer dans l'AIPD, notamment les risques futurs, tels qu'une dépendance au fournisseur. Des solutions de remplacement devraient également être évaluée, afin de permettre aux offices un choix objectif entre les solutions.

Le préposé s'est également prononcé sur les « Principes relatifs à l'informatique en nuages » élaboré par le secteur Transformation numérique et gouvernance de l'informatique (TNI), critiquant la réduction du caractère contraignant des principes. Similairement, sur le projet « *Swiss Government Cloud* », le PFPDT a émis des propositions, prises en compte par l'Office fédéral de l'informatique et de la télécommunication (OFIT).

Identificateur des personnes, numéro AVS et e-ID

Sur le programme DigiSanté et le projet de révision de la loi sur les épidémies (LEp, RS : 818.101), le PFPDT s'est prononcé sur divers sujets, tels que la nécessité de procéder à des AIPD, les exigences relatives à l'utilisation systématique du numéro AVS et les mesures techniques et organisationnelles à mettre en place.

Sur le deuxième projet de la (e-ID : Message FF 2023 2843), la principale préoccupation émise a été de s'assurer que la quantité de données personnelles collectées soit appropriée et non excessive par rapport à la finalité poursuivie. Celle-ci a été prise en compte dans le cadre de la révision de la loi, par l'introduction d'un devoir de diligence des vérificateurs, permettant de limiter la « sur-identification ».

Portails et informations relatives à la nouvelle LPD

En plus des séances d'information, des guides et feuillets disponibles sur la page internet du PFPDT, le rapport fait état du retour d'expérience des trois portails introduits avec l'entrée en vigueur de la LPD révisée.

Sur le portail DataReg, sur lequel les organes fédéraux déclarent leurs traitements, le rapport note que sur les nouvelles entrées faites, celles-ci visent principalement les caisses de pension et fondation collectives qualifiées d'organes fédéraux.

Avec l'introduction de la nécessité de notifier les violations de la sécurité des données, le portail dédié DataBreach a été mis en place permettant de fournir toutes les informations nécessaires relatives à l'événement. Le PFPDT indique un intérêt particulier pour les cas impliquant des sous-traitants et dénombre un total de 245 notifications depuis le 9 mai 2023, dont 57 ont fait l'objet de suivi afin de fournir des informations supplémentaires.

Enfin, sur le portail contenant les données de contact des conseillers-ères à la protection des données, portail DPO, plus de 2000 responsables du traitement ont fournis des coordonnées.

Dans les autres nouveautés arrivées en parallèle de l'entrée en vigueur de la LPD, il y a l'ordonnance sur les certifications en matière de protection des données (OCPD ; RS 235.13), ainsi que de nombreuses ressources mises à disposition sur le site du PFPDT. Y figurent notamment les nouveaux modèles pour les règlements de traitement, des recommandations sur le thème de la journalisation (cette mesure étant devenue obligatoire pour les organes fédéraux), un guide relatif aux mesures techniques et organisationnelles et un aide-mémoire sur le sujet des analyses d'impact à la protection des données. Dernière nouveauté, la loi fédérale sur la procédure administrative (PA ; RS 172.021) est désormais applicable aux enquêtes du PFPDT.

Un rappel à l'ordre

Le PFPDT participe régulièrement à des consultations, comme cela a été le cas sur le de convention relative à l'échange de données policières impliquant la Confédération. Ce projet qui vise la numérisation de l'assistance administrative en matière de police comporte certains risques en matière de protection des données, notamment l'absence de conditions à remplir pour consulter les données par les différents corps de police. À cette occasion, le PFPDT précise que

> *« la numérisation ne doit pas donner carte blanche à des superautorités monolitiques »*

mention qui semble faire référence aux nombreux projets de numérisation et d'un certain manque de considération pour les questions de protection des données dans ces contextes. Il est rappelé que plusieurs critères doivent être rempli pour que ce type de projet soit conforme à la législation. En premier lieu, sur le plan « qualitatif », les bases légales doivent permettre un accès limité aux données, sur la base du principe de proportionnalité. En deuxième lieu, sur le plan « quantitatif », les accès doivent être limités aux membres ayant la compétence et formation requise pour remplir leurs tâches. Enfin, les analyses d'impact sont essentielles afin de mitiger les risques présents dans ce genre de projets importants, impliquant une mise en ligne de données.

Le risque d'une mise en commun de base de données entre des autorités distinctes, sans prendre en compte les limites de compétences d'un État de droit est relevé.

Enquêtes

Le rapport annuel revient sur plusieurs enquêtes et prises de positions, dont notamment celles visant : l'association Forum Civique Suisse, une gérance immobilière, Ricardo, Digitec Galaxus (abordé dans : swissprivacy.law/299/), Xplain (abordé dans : swissprivacy.law/306/), Once Dating SA (abordé dans : swissprivacy.law/242/) et Oracle America. Les différents échanges avec les parties concernées par les enquêtes sont évoqués. Il en ressort des niveaux de collaboration variable.

Santé

Dans le domaine de la santé, la période couverte par le rapport annuel a été prolifique. Du projet de sauvetage de la plateforme mesvaccins.ch (ayant eu pour solution la reprise des données par eHealth Argovie), aux échanges avec l'OFSP sur des questions de surveillance des assurances maladies, en passant par des recommandations sur les déclarations de consentement des patients, la réutilisation des données sur la base de la loi sur la recherche de l'être humain (LRH ; RS 810.30) ainsi que la révision de la loi sur le dossier électronique du patient (LDEP ; RS 816.1), ces sujets ont suscités différentes indications de la part du PFPDT.

Travail et transports

Sur les questions du droit du travail, ce sont principalement les caisses de pensions qui ont

intéressés l'autorité, que ce soit sur la gestion des dossiers personnelles, notamment sur les durées de conservation, que sur la qualification des caisses selon la LPD, qu'elles soient de nature fédérale, cantonale ou même communale. Il est en outre rappelé que lorsque des caisses de pension ont recours à des sous-traitants sous la forme de sociétés de services, celles-ci doivent être déclarées au registre des activités de traitement des organes fédéraux (Datareg).

Dans le domaine du transport ferroviaire, les principales revendications du PFPDT sont de préserver la possibilité du voyage anonyme ainsi que du paiement en liquide. Toujours en lien avec la mobilité, le PFPDT a répondu à la consultation relative à la loi sur les données de passager aériens (LDPa), qui a rappelé la nécessité d'effectuer une AIPD, ainsi que l'importance de la proportionnalité.

À l'internationale

Un des événements marquants, bien qu'attendu, du début de l'année 2024 a été la décision d'adéquation rendue par la Commission. Similairement, le *Data Privacy Framework* est abordé, bien que la décision du Conseil fédéral ne fût alors pas encore rendue (pour plus d'informations sur le sujet, cf : swissprivacy.law/313/).

Avec l'entrée en vigueur de la nouvelle LPD, la Suisse a également ratifié la Convention du Conseil de l'Europe sur la protection des données modernisée. Bien que le PFPDT prédise une entrée en vigueur dans le courant 2024, au moment de la parution de cette contribution, il manque encore la ratification de 7 États (voir la liste du Conseil de l'Europe).

L'autorité suisse était présente à diverses conférences et rencontres avec d'autres autorités de protection des données sur des différents sujets, tels que les dernières avancées technologiques, la coopération entre autorités, le moissonnage de données (*data scraping*), la gouvernance de données et l'intelligence artificielle entre autres.

Les questions liées à Schengen ont fait l'objet de groupes de coordination, comme pour le système d'information Schengen, le système d'information sur les visas ou le système européen de comparaison des empreintes digitales des demandeurs d'asile.

Enfin, l'autorité a participé à plusieurs rencontres et conférences à l'internationale, ayant débouché sur des prises de position et résolutions.

Conclusion

Cet article présente une brève synthèse des différents éléments approfondis dans le rapport. Certains sujets connus du grand public sont abordés (notamment certaines enquêtes, telles que celles concernant Xplain ou la vidéosurveillance des CFF) ainsi que d'autres moins connus. C'est en effet l'occasion de voir l'implication du PFPDT dans les consultations de projets ou lois, et de voir quelles suggestions ont été reprises par les autorités concernées.

Une prochaine contribution abordera la partie « transparence » du rapport.

Proposition de citation : Charlotte Beck, 31e Rapport d'activités du PFPDT – Un survol (Partie 1 : Protection des données), 4 septembre 2024 *in* www.swissprivacy.law/314

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.