_swissprivacy.law

La CNIL sanctionne une banque pour des atteintes à la protection des données

Philipp Fischer et Julien Levis, le 10 janvier 2021

Aux termes de sa délibération du 18 novembre 2020 (n° SAN-2020–009) concernant Carrefour Banque (la Banque), la Commission Nationale de l'Informatique et des Libertés (CNIL) a prononcé une décision portant amende de EUR 800'000 en application du Règlement général sur la protection des données (RGPD) et de la loi française dite « informatique et libertés ». La sanction est assortie d'une mesure de publication nominative de la délibération.

I. Résumé de la décision de la CNIL

La Banque (détenue à 60% par Carrefour S.A.) opérait deux programmes de paiement en lien avec sa carte *Pass*. La société Carrefour France (détenue à 99.61% par Carrefour S.A.) gérait un programme permettant le rattachement de la carte *Pass* au programme de fidélité Carrefour.

La CNIL a sanctionné la Banque aux motifs suivants :

I.1. La Banque aurait manqué au principe de loyauté (art. 5 RGPD).

La CNIL déduit ce manquement de la transmission à Carrefour France de davantage de données concernant les souscripteurs de la carte *Pass* que celles limitativement énumérées lors de la souscription en ligne. La CNIL souligne la nature « à la fois imprécise et trompeuse » de l'information fournie par la Banque (Décision, § 34) et note :

- L'absence d'explication : les personnes concernées n'étaient pas mises en capacité de comprendre que leurs données seraient transmises à une société tierce.
- L'indication selon laquelle seules certaines catégories de données seraient transmises : cette limitation n'a pas été respectée en pratique, ce qui matérialiserait la déloyauté.

I.2. L'information aux utilisateurs du site n'était pas aisément accessible (art. 12 RGPD).

La CNIL a – à ce titre – relevé :

- l'imprécision découlant d'un onglet intitulé « *Protection des données bancaires* » sur le site de la Banque. La Banque aurait – selon la CNIL – dû clairement mentionner les données personnelles et non la notion – équivoque – de « données bancaires » ;
- que la succession de « clics » nécessaires pour atteindre la politique de confidentialité du site était insuffisamment intuitive ;
- que si des informations de premier niveau étaient disponibles sur le site, elles manquaient de renvois vers des informations plus détaillées sur la protection des données.

I.3. L'information délivrée par la Banque était imprécise et incomplète.

La CNIL sanctionne la Banque au titre du caractère insuffisamment détaillé de sa politique de confidentialité quant aux durées de conservation des données.

I.4. Manquement relatif aux cookies

La CNIL sanctionne le dépôt de certains *cookies* sans recueil préalable du consentement pourtant requis.

II. Quelques enseignements de cette décision

II.1. Méthodologie des contrôles

La modalité mise en œuvre par la CNIL est celle du contrôle en ligne. Certaines analyses avaient pu souligner l'insuffisance des ressources allouées aux autorités nationales de contrôle et en déduire la faible probabilité statistique d'un contrôle. Le contrôle en ligne offre toutefois aux autorités de contrôle un outil économe tant en ressources financières qu'humaines : la probabilité de contrôles s'en trouve mécaniquement accrue.

II.2. Intensité du contrôle matériel exercé

Les violations sanctionnées le sont en suite d'un examen approfondi des mécanismes de traitement. Si certains ont pu envisager la mise en conformité au RGPD *on a best effort basis*, le contrôle détaillé effectué par la CNIL n'est pas de nature à conforter une telle approche.

II.3. Prise en considération des mesures correctrices intervenues en cours de procédure

La CNIL examine en détail les mesures correctrices adoptées par la Banque et ne prononce pas d'injonction sous astreinte du fait des corrections intervenues. L'amende prononcée est cependant lourde en chiffres absolus (EUR 800'000). Cette sévérité trouve apparemment sa source dans la volonté de la CNIL de sanctionner la déloyauté décelée (cf. *supra* I.1.).

II.4. Mesure de publicité nominative de la délibération

L'impact réputationnel de la décision est accru par le caractère nominatif dont est assortie sa publication.

II.5. Détails notables de la procédure

Il convient de relever ici :

- la limite dans le temps (deux ans) posée au caractère nominatif de la publication ;
- le refus opposé par le rapporteur (de la CNIL) à la demande formulée par la Banque de le rencontrer ;
- l'accueil positif réservé à la demande par la Banque d'une audience à huis clos ;
- les délais liés à la crise sanitaire.

III. Remarques conclusives

Les principaux enseignements à tirer de cette décision incluent :

- l'importance d'une formulation méticuleuse des mentions du site Internet d'une entreprise ayant pour objet de satisfaire à son obligation d'information ;
- le caractère significatif de l'amende prononcée pour des infractions relativement formelles. Cette décision pourrait marquer un renforcement de la sévérité des contrôles de conformité au RGPD ;
- une attention croissante peut-être portée par les autorités de contrôle en matière de protection des données au secteur bancaire. Quelques semaines après la décision commentée, l'homologue espagnol de la CNIL – l'AEPD –, semble lui avoir emboîté le pas : cette dernière a rendu le 11 décembre 2020 une décision de sanction à l'encontre de la banque BBVA (amende de EUR 5'000'000 là encore principalement axée sur des manquements au devoir d'information).

En Suisse, la décision ici commentée pourrait préfigurer certaines évolutions dans la pratique du Préposé fédéral à la protection des données et à la transparence, particulièrement après l'entrée en vigueur de la nouvelle LPD (nLPD) prévue en principe en 2022. La publication

d'une « recommandation » du Préposé est déjà possible (art. 30 al. 2 LPD actuelle) et la nLPD renforce les pouvoirs d'enquête du Préposé. Le Préposé reprendra-t-il au surplus certaines des exigences substantielles posées par la CNIL dans sa décision « Carrefour Banque » ? Cette question ne manquera pas de tenir en haleine le secteur bancaire et financier suisse.

Proposition de citation : Philipp FISCHER / Julien LEVIS, La CNIL sanctionne une banque pour des atteintes à la protection des données, 10 janvier 2021 *in* www.swissprivacy.law/47