



HAL
open science

Pour la CNIL, on ne badine pas avec la sécurité des données

Philippe Mouron

► **To cite this version:**

Philippe Mouron. Pour la CNIL, on ne badine pas avec la sécurité des données. Revue européenne des médias et du numérique, 2019, 49, pp.21-23. hal-02064820v2

HAL Id: hal-02064820

<https://amu.hal.science/hal-02064820v2>

Submitted on 24 May 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License



POUR LA CNIL, ON NE BADINE PAS AVEC LA SÉCURITÉ DES DONNÉES

-

Revue Européenne des Médias et du Numérique, n° 49, hiver 2018-2019, pp. 21-23

MOURON Philippe

Maître de conférences HDR en droit privé
LID2MS – Aix-Marseille Université

La CNIL a infligé, pendant l'année 2018, trois sanctions pécuniaires, allant de 250000 à 400000 €, à l'encontre des sociétés Optical Center, Bouygues et Uber pour manquement à l'obligation de sécurité des traitements de données personnelles.

L'entrée en vigueur du Règlement général relatif à la protection des données personnelles (RGPD) a certainement été l'un des événements les plus importants de l'année 2018.

Le nouveau cadre ainsi établi a entraîné, en France, une réécriture de la loi du 6 janvier 1978, dont la dernière version vient d'être achevée au mois de décembreⁱ. Sur le plan pratique, la CNIL a pu dresser un bilan plutôt positif de son applicationⁱⁱ. La prise de conscience des professionnels ayant établi leur mise en conformité a pu être saluée par l'autorité ; 24500 organismes ont ainsi désigné un délégué à la protection des données. Il en est de même pour les particuliers titulaires des données ; en atteste le nombre de plaintes enregistrées auprès de la CNIL en 2018, qui a augmenté de 64 % par rapport à l'année 2017. Si ces chiffres sont pour l'instant encourageants, on peut néanmoins déplorer le nombre important des notifications de violations de données signalées auprès de la Commission qui s'élève à 742, lesquelles concernent les données de plus de 33 millions de personnesⁱⁱⁱ. Ces atteintes porteraient tant sur l'intégrité que la disponibilité et la confidentialité des données, et 65 % d'entre elles auraient pour origine un acte malveillant. Ces constats nous rappellent l'importance de l'obligation de sécurisation des données mise à la charge des responsables de traitement par l'article 32 du Règlement.

La CNIL en a sanctionné le non-respect à plusieurs reprises pendant l'année 2018, s'agissant du défaut de sécurisation de l'accès à des bases de données personnelles.

Le défaut de sécurisation d'adresses URL : les cas Optical Center et Bouygues

Les deux sanctions pécuniaires prononcées par la CNIL à l'égard des sociétés Optical Center et Bouygues ont mis en lumière deux manquements très similaires à l'obligation de sécurisation s'agissant de services web.

Dans le premier cas^{iv}, les données étaient accessibles, sans procédure d'authentification, sur des adresses URL du site de la société Optical Center. Les informations concernées étaient

notamment les suivantes : « *nom, prénom, adresse postale, correction ophtalmologique et, pour certaines d'entre elles, la date de naissance des clients ainsi que leur numéro d'inscription au répertoire national d'identification des personnes physiques (NIR)* ». Des factures et bons de commandes relatifs à des achats passés sur le site étaient également impliqués. Bien que la faille ait été ultérieurement corrigée, les données en cause sont restées accessibles pendant plusieurs semaines. Le défaut tenait à l'absence de procédure d'authentification des clients avant de leur permettre l'accès aux documents les concernant. Une modification « élémentaire » du code source du site internet a suffi pour corriger ce défaut. Aussi la CNIL a-t-elle décidé, dans sa délibération du 7 mai 2018, de sanctionner la société Optical Center sans mise en demeure préalable, le manquement ne pouvant plus faire l'objet d'une mise en conformité. Compte-tenu de la gravité du défaut de sécurité du site, du nombre de documents concernés (334000) et des risques afférents à la libre collecte des données (notamment en termes de phishing), la Commission a infligé une sanction pécuniaire de 250000€.

Le même montant a été retenu pour la sanction infligée à la société Bouygues le 26 décembre 2018^v. Le manquement reproché était le même que dans le cas précédent, à savoir que les contrats de souscription des clients à l'offre B&YOU par une manipulation d'adresse URL. Cette faille ne concernait qu'une seule base de données clients et sa source pourrait remonter à 2015, année pendant laquelle plusieurs systèmes informatiques ont été fusionnés. La Commission a ainsi constaté l'insuffisance des mesures de sécurité déployées par la société, et notamment le fait qu'elle n'ait prévu aucune mesure complémentaire d'authentification des utilisateurs du site. De même, les tests effectués par la société s'avéraient inadaptés aux spécificités de la base de données en cause et ne permettaient pas de déceler la faille de sécurité. Enfin, une revue manuelle des lignes de code litigieuses aurait permis de mieux garantir la protection des données sans constituer un effort disproportionné pour la société.

Ces manquements, qui rappellent l'affaire déjà ancienne du site web des magasins Tati^{vi}, restent donc relativement communs tout en étant aisés à corriger.

L'absence de mesure de prévention des intrusions malveillantes : le cas Uber

Dans un autre registre intéressant la sécurité des données, la société Uber s'est vu infliger une sanction pécuniaire de 400000€ pour ne pas avoir su prévenir une intrusion malveillante dans ses bases de données clients^{vii}.

La société a en effet reconnu, en novembre 2017, que deux individus avaient pu dérober les données de 57 millions d'utilisateurs dans le monde, dont 1,4 millions sont situés en France, ce pourquoi elle aurait versé une rançon. Les données concernées étaient encore d'une particulière importance pour la vie privée : « *nom, prénom, adresse de courrier électronique, ville ou pays de résidence, numéro de téléphone mobile et statut des utilisateurs (conducteur, passager ou les deux)* ». Le G29 a par la suite créé un groupe de travail spécialement chargé de l'investigation sur cette faille de sécurité. S'agissant du volet français, la CNIL a à nouveau constaté plusieurs manquements de la part de la société Uber. En effet, celle-ci a négligé de prendre certaines précautions qui auraient permis de prévenir cette attaque informatique. La procédure d'authentification des ingénieurs ayant accès aux bases de données piratées (via la

plateforme Github) s'avérait peu adéquate en l'absence de mesure d'identification multifactorielle. Aucune procédure concernant le retrait des habilitations des ingénieurs ayant quitté la société n'avait de plus été prévue. La présence d'identifiants de connexion dans des fichiers et lignes de code non sécurisés a également pu être relevé par la Commission. Enfin, un système de filtrage des adresses IP aurait du être déployé afin de garantir que les seules personnes habilitées puissent accéder aux données. L'absence de préjudice avéré à l'égard des utilisateurs est sans effet sur la gravité du manquement, qui justifie pour la CNIL de retenir une sanction pécuniaire plus élevée.

On rappellera que les manquements à l'obligation de sécurité des traitements de données personnelles peuvent désormais être sanctionnés d'une amende allant jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial depuis l'entrée en vigueur du RGPD.

ⁱ Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel

ⁱⁱ « RGPD : quel premier bilan 4 mois après son entrée en application ? », www.cnil.fr, 25 septembre 2018

ⁱⁱⁱ « Violations de données personnelles : 1er bilan après l'entrée en application du RGPD », www.cnil.fr, 16 octobre 2018

^{iv} Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société Optical Center

^v Délibération de la formation restreinte n° SAN-2018-012 du 26 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Bouygues Télécom

^{vi} CA Paris, 12ème Ch. A, 30 octobre 2002, *CCE*, janvier 2003, comm. n° 5, L. Grynbaum

^{vii} Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Uber France SAS