Actualité
Données **P**ersonnelles

Contrôle 2022 de la CNIL: le *Cloud* en ligne de mire et 5 ministères dans le viseur

Chaque année, la CNIL choisit plusieurs thématiques de contrôle prioritaires.

Ces thématiques sont souvent liées à des enjeux forts de société sur lesquels la CNIL souhaite avoir un positionnement stratégique.

Les contrôles réalisés sur ces thématiques représentent environ 1/3 des contrôles annuels de la CNIL.

Ils complètent les contrôles suite à des plaintes ou déclenchés par l'actualité.

Trois thématiques de contrôle prioritaires

La prospection commerciale :

l'un des « irritants du quotidien » auquel la CNIL veut s'attaquer.

La surveillance dans le cadre du télétravail :

nécessité de trouver un juste équilibre entre vie privée au travail et contrôle légitime de l'activité des travailleurs.

Utilisation de l'informatique en nuage *(Cloud)* :

la pierre angulaire du programme de contrôle 2022.

Le *Cloud* au cœur des priorités de la CNIL

Transferts de données

Les technologies du *Cloud* impliquent généralement l'utilisation de prestations fournies (directement ou indirectement) par des **acteurs américains**.

La plupart du temps **ces solutions entrainent donc des transferts de données hors Europe**.

Même en cas d'hébergement en Europe, du fait des accès par les sous-traitants en chaîne (maintenance, assistance…) depuis des pays tiers (Etats-Unis, Inde...).

Dans l'immense majorité des cas, les pays de destination n'assurent pas un niveau de protection des données « ***substantiellement équivalent*** » à celui garanti en Europe.

Les entreprises adhérant au dispositif américain d'auto-certification du *Safe Harbor* **ne sont plus considérées comme établies dans un pays « adéquat »** depuis la décision de la Cour de justice de l'Union européenne C-311/18 du 16 juillet 2020 (« Schrems II »).

La seule alternative est la **signature de clauses contractuelles types** mais ce, sous réserve d'être complétées par des « ***mesures supplémentaires*** » capables de contrarier de manière effective les risques d'accès aux données (par exemple par les services de renseignements) à destination.

Les **principaux fournisseurs de solutions de *Cloud* sont concernés** : Microsoft (Office 365, Azur…), Google (Google Cloud Platform…), Amazon (Amazon Web Services…).

D’autres pays de destination des données soulèvent les **mêmes difficultés**.

Les législations de l’Inde, de la Chine et de la Russie ont récemment été évaluées à l’initiative du Comité européen à la protection des données (CEPD – Government access to data in third countries, final report, EDPS/2019/02-13).

Sans surprise, leur législation n’est **pas au niveau des standards européens**.

Quelle que soit l’origine des fournisseurs de *Cloud* non européens, les contraintes sont les mêmes que pour les fournisseurs américains (qui utilisent d’ailleurs souvent eux-mêmes des fournisseurs de ces pays).

Les autorités de contrôle européennes sont **actuellement particulièrement sévères** sur le sujet des transferts de données par des fournisseurs d'origine américaine.

Google Analytics jugé illicite par l'autorité autrichienne de protection des données en décembre 2021.

Cookiebot jugé illicite par la cour administrative de Wiesbaden (Allemagne) en **décembre** 2021

Google Analytics et Stripe jugés illicites par le Contrôleur européen de la protection des données (la « CNIL » des institutions européennes) en janvier 2022.

Google Analytics jugé illicite par la CNIL (février 2022).

Les offres de *Cloud*, offertes pour la plupart par des acteurs d'origine américaine, sont donc **largement concernées par ces enjeux, même lorsqu'ils hébergent les données en Europe.**

L’utilisation du *Cloud* par le secteur public particulièrement ciblée

Action conjointe des autorités européennes

Le **secteur public est particulièrement visé** par une procédure coordonnée de contrôle de l'EDPB.

- **22 autorités européennes de protection des données** vont lancer, de manière coordonnée, des investigations sur l'utilisation du *Cloud* par le secteur public.
- **75 autorités publiques**, dont des institutions européennes, vont être concernées par ces investigations au niveau européen.

En France, la CNIL annonce participer à cette action coordonnée en **contrôlant 5 ministères**.

Doctrine française du « *Cloud* au centre »

(circulaire n°6282/SG)

Si le recours au *Cloud* interne de l'Etat n'est pas obligatoire, **le recours aux offres commerciales de Cloud doit respecter plusieurs conditions**, notamment :

- Comporter des **conditions de fin de contrat et de réversibilité soutenables** pour l'administration.
- Être **conformes au RGPD**, et, le cas échéant à la législation sur l'hébergement des données de santé.
- Pour les données sensibles (données de citoyens, d'entreprises…), être **immunisée contre toute réglementation extracommunautaire**.

Les experts Oyat

Marie-Hélène TONNELLIER

Avocat fondateur

Digital / IP

Charlotte BARRACO-DAVID

Counsel

Digital / IP

Avec l’aimable assistance de **Clyde COUTELLIER**

Images:Flaticon.com

OYAT

www.oyat.law