ARTICLE

"QUIZZ" ET QUESTIONNAIRES EN LIGNE SUR LE THÈME DE LA SANTÉ : LES LEÇONS À RETENIR DE LA DÉCISION DE SANCTION DE LA CNIL À L'ENCONTRE DE LA SOCIÉTÉ DOCTISSIMO

IT et données personnelles | 28/06/23 | Florence Chafiol Roxane Blanc-Dubois

La CNIL a publié le 17 mai dernier une décision de sanction à l'encontre de Doctissimo[1], une société éditant un site d'information francophone sur la santé et le bien-être à destination du grand public.

Les manquements au RGPD constatés ont majoritairement trait aux tests c'est-à-dire des « quizz » et autres questionnaires de santé, accessibles à partir du site Doctissimo.

- **Leçon n°1 : les responsables de traitement doivent prendre conscience qu'ils ont pour obligation de surveiller les actions de leurs sous-traitants**

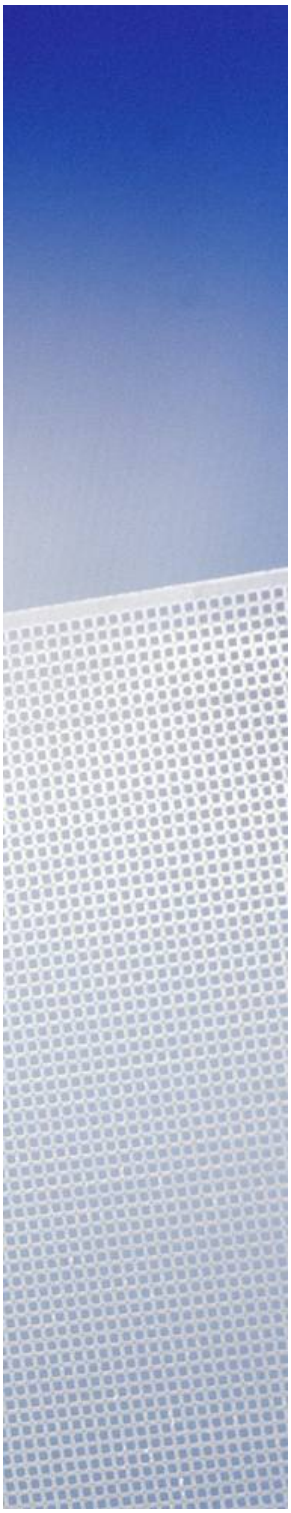
La CNIL a tout d'abord retenu un manquement de Doctissimo s'agissant de la durée de conservation des données personnelles des utilisateurs ayant procédé aux tests en ligne. Doctissimo conservait pendant plusieurs mois les réponses fournies aux tests et les adresses IP pouvant être associées aux informations des comptes utilisateurs. Cette durée de conservation a été considérée comme excessive dans la mesure où les résultats de ces tests s'affichaient sur l'écran de l'internaute ayant fait le test **dès la fin du formulaire** et qu'il n'était pas nécessaire pour Doctissimo de les conserver (Doctissimo n'ayant justifié d'aucune finalité permettant une conservation plus longue).

Doctissimo a eu beau indiquer que ce manquement était dû à son sous-traitant à qui la mise en œuvre et l'hébergement des tests rédigés par Doctissimo étaient confiés, cela n'a pas suffi, et ce, en dépit du fait que Doctissimo ait mis en avant les stipulations contractuelles claires qui figuraient dans le contrat avec son sous-traitant selon lesquelles ce dernier ne devait pas collecter les adresses IP des personnes concernant les tests dits « sensibles ».

Cette décision est ainsi l'occasion pour la CNIL de rappeler que le non-respect par le sous-traitant des stipulations contractuelles qui lui sont imposées n'est pas exonératoire de responsabilité pour le responsable de traitement. Ce dernier reste tenu de veiller à ce que la protection des données personnelles soit systématiquement et effectivement assurée, y compris lorsqu'il fait appel à des sous-traitants. Il est donc attendu du responsable de traitement qu'il mette en œuvre des diligences raisonnables pour vérifier les actions de son sous-traitant, ces diligences étant dépendantes des compétences et des moyens du responsable de traitement. En l'occurrence, la CNIL a souligné que Doctissimo **avait des compétences dans le domaine du numérique** et conclu qu'elle n'avait pas **suffisamment vérifié la bonne exécution de ses instructions par son sous-traitant, ni exercé de contrôle satisfaisant quant aux mesures techniques et organisationnelles mises en œuvre**. La CNIL relève de surcroît que Doctissimo avait accès à des tableaux de bord établis par son sous-traitant sur lesquels figuraient les réponses aux tests ainsi que les adresses IP sous forme pseudonymisée et qu'elle ne pouvait donc ignorer que son sous-traitant collectait les adresses IP.

- **Leçon n°2 : les responsables de traitement doivent se montrer prudents lorsqu'ils traitent des données de santé, en particulier lorsque leur secteur d'activité a trait au domaine de la santé**

La CNIL a pointé du doigt l'absence de recueil du **consentement explicite** des internautes répondant aux tests impliquant le traitement de **données de santé[2]**. Ces dernières sont des données dites « sensibles » qui bénéficient d'un régime de protection accrue : leur traitement implique de pouvoir mobiliser l'une des bases légales de l'article 6 du RGPD ainsi que l'une des exceptions à l'interdiction de traiter de telles données sensibles au titre de l'article 9 du RGPD. Compte tenu des circonstances de l'espèce, seul le consentement explicite des personnes constituait une exception mobilisable au titre de l'article 9 du RGPD (les autres exceptions, comme par exemple, la nécessité de traiter les données à des fins de recherche, n'étant pas remplies). Bien que Doctissimo se soit mise en conformité au cours de la procédure de contrôle (en insérant une case à cocher pour recueillir un consentement explicite), la CNIL a souligné que cela ne remettait pas en cause l'existence du manquement pour les faits passés. La société a donc également été sanctionnée à ce titre. Une fois encore, le secteur d'activité de Doctissimo a pesé dans la balance : la CNIL note dans sa



délibération que Doctissimo, diffusant des contenus numériques relatifs à la santé, ne pouvait éluder une telle obligation d'obtention du consentement.

- **Leçon n°3 : la sécurité des données est une réelle préoccupation de la CNIL qui peut sanctionner pour un défaut de sécurité même en l'absence de toute violation effective de données personnelles**

La CNIL reproche à Doctissimo de ne pas avoir mis en œuvre des mesures de sécurité suffisantes concernant (i) la navigation des utilisateurs sur le site internet et (ii) le stockage des mots de passe des utilisateurs du site. A l'argument selon lequel il n'y a eu aucune violation de données, la CNIL répond que « *la survenance d'une attaque ou d'une violation de données n'est pas nécessaire à la caractérisation d'un manquement à l'article 32 du RGPD* » imposant la mise en œuvre de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. En revanche, aucune injonction n'est formulée par la CNIL à cet égard puisque la situation a été régularisée.

- **Leçon n°4 : les cookies sont toujours dans le collimateur de la CNIL**

La CNIL relève enfin des manquements aux dispositions de la loi Informatique et Libertés relatives aux **cookies** (notamment le dépôt d'un cookie ayant pour finalité la diffusion de publicité ciblée déposé sur le terminal des utilisateurs sans leur consentement préalable alors que celui-ci était requis).

- **Leçon n°5 : il convient de ne pas négliger, dans le cadre des projets d'acquisition d'entreprises, la phase d'audit des opérations de traitements de données personnelles des cibles**

La formation restreinte de la CNIL a prononcé une sanction de 280 000 euros pour les manquements au RGPD et de 100 000 euros pour les manquements à la loi Informatique et Libertés concernant l'utilisation de cookies (soit une sanction financière totale de 380 000 euros). Elle a en cela suivi les réquisitions de la rapporteure qui avait requis de tels montants. Aucun des arguments opposés par Doctissimo n'auront permis d'écarter la sanction financière ni de diminuer son montant. A cet égard, la rapporteure avait indiqué lors de l'audience que les montants des sanctions qu'elle proposait étaient bas compte tenu du risque relativement faible pour les personnes.

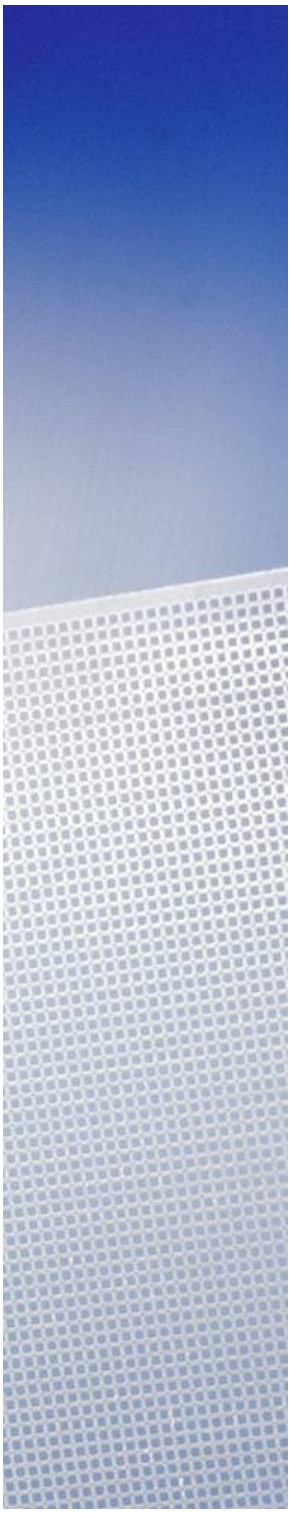
A noter qu'au moment des contrôles (2020), Doctissimo était détenue par la société UNIFY elle-même détenue par le groupe de médias français TF1. TF1 a cédé en juin 2022 au groupe REWORLD MEDIA « *les actifs média et des activités digitales du pôle Publishers de la société UNIFY dont fait partie la société Doctissimo* ». Doctissimo a été sanctionnée en 2023 pour des faits commis antérieurement à son acquisition par le groupe REWORLD MEDIA : la CNIL semble néanmoins avoir tenu compte du chiffre d'affaires et du résultat net réalisés par REWORLD MEDIA en 2021 puisqu'elle les mentionne dans sa délibération.

Cela rappelle donc l'importance pour les potentiels acquéreurs d'une cible de (i) réaliser des **audits** sur les traitements de données personnelles opérés par ladite cible et ses filiales et de vérifier l'existence (et la teneur) de contrôles en cours (ou de risques de contrôles à venir) d'une autorité de protection des données, ainsi que (ii) **d'inclure les garanties ou actions nécessaires** dans le contrat d'acquisition/de cession et, le cas échéant, de négocier le prix à la baisse en fonction des résultats de l'audit. Au-delà des sanctions financières, il existe un **impact réputationnel** en cas de publicité d'une décision de sanction de l'autorité de protection des données (risque dont il doit être tenu compte lors des opérations d'acquisition de cibles). En l'occurrence, à la suite de la publication de la décision de la CNIL sanctionnant nommément Doctissimo et mentionnant tant l'ancien que l'actuel groupe détenteur de la société sanctionnée, plusieurs médias ont relaté l'affaire en ne désignant que l'actuel groupe détenteur de Doctissimo (soit l'acquéreur qui n'était pourtant pas le groupe détenant Doctissimo au moment de la commission des faits litigieux).

- **Leçon n°6 : aucun accompagnement individualisé de la CNIL n'est possible à partir du moment où une procédure de contrôle est en cours (et ce, même si le rapporteur n'a pas encore été désigné)**

Un autre apport intéressant de cette délibération porte sur les précisions apportées par la formation restreinte de la CNIL au sujet de la charte d'accompagnement des professionnels éditée par la CNIL[3].

Dans ladite charte qui explique les différents axes d'accompagnement de la CNIL pour les professionnels, la CNIL indique « *que **l'accompagnement individualisé** offert par la CNIL porte sur une analyse globale (comment correctement appliquer le RGPD à mon activité ?) ou sur un projet de traitement à venir. Ainsi, en aucun cas, l'accompagnement à la conformité décrit dans la présente charte ne saurait servir à « régulariser » des comportements en cours ou passés contraires à la réglementation* ». A cet égard, la formation restreinte de la CNIL énonce explicitement dans sa délibération, l'impossibilité pour une entité d'obtenir un



accompagnement individualisé de la CNIL pour sa mise en conformité **dès lors qu'une procédure de contrôle est en cours à son encontre**[4]. Elle précise également que « (…) *la CNIL peut répondre à une demande de conseil* ***à l'issue du contrôle si la phase répressive n'est pas engagée*** (…) ».

Doctissimo avait sollicité un accompagnement individuel de la CNIL le 8 avril 2021, soit à une date postérieure aux opérations contrôles, raison pour laquelle le service compétent de la CNIL avait refusé à l'époque cet accompagnement.

---

[1] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047552103

[2] Au sens de l'article 4-15 du RGPD

[3] https://www.cnil.fr/sites/default/files/atoms/files/charte_accompagnement_des_professionnels.pdf (version française) ; https://www.cnil.fr/sites/default/files/atoms/files/charter_support_professionals.pdf (version anglaise)

[4] Points 10 et 59 de la délibération
