# La Cnil tance Cdiscount pour manquements « graves » à la sécurité des données

La Commission nationale de l'informatique et des libertés a annoncé, mercredi, avoir prononcé un *« avertissement public »* pour des *« manquements graves »* en matière de sécurité et de traitement des données à l'encontre de Cdiscount, société du pôle e-commerce du groupe Casino. La charge, sévère, est complétée d'une mise en demeure. La Cnil exhorte l'entreprise à rectifier le tir.

## Données bancaires conservées en clair

À la suite de plaintes (80 depuis 2015), et de contrôles effectués entre février et mars 2016, le régulateur des données personnelles explique avoir constaté les manquements suivants : *« la conservation de plus de 4 000 données bancaires, associées pour certaines à des cryptogrammes visuels, de manière non sécurisée »*. Cdiscount ayant conservé en clair, dans un champ commentaire de sa base de données, les numéros de cartes bancaires de ses clients. Et *« la conservation en base de données de plusieurs millions de comptes d'anciens clients et prospects sans limitation de durée »*.

En raison de la gravité des manquements constatés et *« du volume potentiel de personnes concernées »*, la Cnil a donc prononcé, lors d'une délibération en formation restreinte, le 20 septembre dernier, un avertissement public, avec désignation d'un rapporteur (procédure de sanction). Et ce n'est pas tout : une procédure de mise en demeure est engagée. Les contrôles ayant révélé d'autres manquements.

## Stockage et cookies à durée illimitée

Ces autres manquements incluent l'absence de consentement à la conservation de données bancaires d'utilisateurs et la mise en œuvre d'un traitement de lutte contre la fraude sans autorisation de la Cnil. Mais aussi : le dépôt de cookies *« sans finalité déterminée, sans information des personnes quant à leurs droits et pour des durées excessives (30 ans) »*, des commentaires non pertinents sur des clients dans la base de l'entreprise (un handicap supposé, une inclinaison personnelle présumée…). Sans oublier : le défaut de politique de mots de passe suffisamment robustes.

Au total, dix manquements ont été relevés. Dans cette affaire, il n'est pas question de fuite de données, mais de manquements sérieux aux bonnes pratiques en matière de cybersécurité et d'entorses à la législation sur les données personnelles. La Cnil a donc choisi de les rendre publics pour *« sensibiliser les responsables de traitement à leurs obligations en matière de confidentialité des données personnelles collectées. »* Et sa présidente, Isabelle Falque-Pierrotin, a décidé d'adresser une mise en demeure à Cdiscount. La société doit engager des mesures correctives et se conformer à la loi informatique et libertés, *« dans un délai de trois mois, renouvelable une fois »*. À défaut, elles risque l'amende.

# « Des pratiques isolées », plaide Cdiscount

Mercredi soir, le distributeur a indiqué à l'AFP, après enquête interne, *« que ces dysfonctionnements étaient limités à un seul centre d'appels auquel [Cdiscount] a retiré l'activité depuis plusieurs mois »*. L'entreprise a ajouté que ces pratiques *« isolées »* sont *« contraires aux valeurs de Cdiscount »* et que « *des contrôles quotidiens ont été renforcés pour veiller au strict respect des règles* ». Le groupe ajoute : *« aucune faille de sécurité n'a été relevée »* concernant les mots de passe des clients. Et assure que le renforcement de leur robustesse, attendu par la Cnil, *« est effectif depuis mars dernier »*....

Peut-être, mais une vulnérabilité du système, donc une faille, a bien été mise à jour par l'autorité de contrôle : le stockage en clair de données bancaires ! C'est un problème de taille pour un site marchand comme Cdiscount.com qui revendique 2 millions de visiteurs et 85 000 ventes par jour.

**Lire aussi :**

La Cnil épingle Windows 10 sur la collecte des données
Sous la pression de la CNIL, le PS finit par colmater ses fuites
Sécurité et vie privée portent l'activité de la CNIL en 2015