Protection des données personnelles : actualité des sanctions

Par Emmanuel JOUFFIN.

Intérêt légitime du responsable de traitement, violation de sécurité et cookies, telle est la trilogie des sujets ayant récemment donné l'occasion à la CNIL de s'exprimer sur sa doctrine…. par le biais de sanctions.

♦ **Intérêt légitime du responsable de traitement : point trop n'en faut !**

Le 10 décembre 2020, le Conseil d'Etat[1] a tranché la question de la conservation par CDISCOUNT des données relatives à la carte de paiement pour les ventes à distance.

La CNIL, le 6 septembre 2018[2], avait indiqué que ces données ne pouvaient être collectées et traitées par une société de vente à distance qu'afin de permettre la réalisation d'une transaction dans le cadre de l'exécution d'un contrat.

Par conséquent, la conservation de ces données afin de faciliter d'éventuels paiements ultérieurs ne pouvait être envisageable que si les personnes concernées avaient préalablement et explicitement donné leur consentement, sauf à avoir souscrit un abonnement. Sur saisine de CDISCOUNT, le Conseil d'Etat devait trancher entre l'intérêt légitime du responsable de traitement désireux de conserver les données de paiements de ses clients en vue d'achats ultérieurs et la protection des données personnelles.

La décision penche en faveur de la seconde. En effet, le Conseil d'Etat estime que la conservation des numéros de cartes bancaires pour faciliter des achats ultérieurs n'est nécessaire ni au respect d'une obligation légale, ni à l'exécution d'une mission d'intérêt public, ni à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne.

« Le recours à la notion d'intérêt légitime du responsable de traitement est un exercice qui connaît des limites.»

S'agissant de l'exécution d'un contrat auquel la personne concernée est partie, la conservation du numéro de carte bancaire peut se justifier une fois le contrat exécuté.

Moralité, si le recours à la notion d'intérêt légitime du responsable de traitement est tentant, l'exercice a ses limites. La CNIL en a fixé les contours, confirmés par le Conseil d'Etat.

♦ **Violation de sécurité : le responsable de traitement et son sous-traitant dos à dos.**

Le 27 janvier 2021, la CNIL[3] a sanctionné un responsable de traitement (à hauteur de 150.000 euros) ainsi que son sous-traitant (à hauteur de 75.000 euros). Etaient reprochés plusieurs éléments : l'accès à des données clients du site web par des tiers non autorisés pendant près d'une année, une durée de

[1] https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-12-10/429571

[2] Délibération n°2018-303 du 06 septembre 2018 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance et abrogeant la délibération n° 2017-222 du 20 juillet 2017.

[3] https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant

développement trop longue d'un outil de détection et de blocage des attaques, ainsi que le retard dans de déploiement de mesures préventives (limitation du nombre d'accès, CAPTCHA, etc.).

Moralité : le responsable de traitement doit décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant, tandis que le sous-traitant doit aussi rechercher les solutions techniques et organisationnelles les plus appropriées pour assurer la sécurité des données personnelles et les proposer au responsable de traitement. En somme : instructions d'un côté, devoir de collaboration de l'autre.

lesquels étaient pourtant déjà déposés sur l'ordinateur, dès l'accès au site, tandis que le dispositif d'opposition était défaillant.

Pour Amazon, le manque de transparence était également souligné. Le bandeau d'information ne permettait ni de comprendre que les cookies déposés avaient pour principal objectif d'afficher des publicités personnalisées, ni de comprendre qu'il était possible de les refuser.

Pour mémoire, la période de mise en conformité des sites internet arrive à son terme le 31 mars 2021. Il est donc temps de détailler, dans les bandeaux informatifs, les finalités pour lesquelles les cookies sont déposés sur les