Pour nous contacter

–

Equipe IP/IT & Data Protection

ebarbry@racine.eu | (+33) 6.13.28.91.28

Sanction de 800 000 € prononcée contre DISCORD :

Un manquement au principe du *Privacy by default* relevé pour la première fois par la CNIL, le premier d'une longue liste ?

Le 10 novembre 2022, la CNIL a prononcé à l'encontre de la société DISCORD une amende de 800 000 euros pour avoir manqué à plusieurs obligations du Règlement général sur la protection des données (RGPD). Si cette décision illustre, une fois de plus, que le sujet de la durée de conservation et de la sécurité des données personnelles est particulièrement surveillé par la CNIL, elle consacre, pour la première fois, un manquement à l'obligation de garantir la protection des données par défaut.

DISCORD est un réseau social permettant aux personnes de partager du contenu et de communiquer par service de voix et de messagerie. Cette plateforme est particulièrement populaire parmi la communauté des joueurs de jeux vidéo et a connu une forte croissance pendant le confinement lié à la pandémie de Covid-19.

Si la société ne dispose pas d'établissement dans l'Union Européenne, elle reste soumise au RGPD car traite des données à caractère personnel d'utilisateurs situés en France. En effet, le Règlement s'applique à chaque fois qu'une personne au sein de l'UE est directement concernée par un traitement de données à caractère personnel, même si le responsable de traitement ou ses sous-traitants sont basés hors de l'UE (**article 3 du RGPD**).

Suite à un contrôle en ligne sur le site web "discord.com" et sur l'application mobile DISCORD ainsi qu'un contrôle sur pièces auprès de la société, la CNIL a relevé plusieurs manquements au RGPD.

La décision de la CNIL est particulièrement novatrice sur le sujet de l'obligation de garantir la protection des données par défaut.

L'**article 25 du RGPD** consacre le principe de protection de la vie privée dès la conception -- ***Privacy by design*** (article 25.1) et son corollaire, celui de protection de la vie privée par défaut -- ***Privacy by default*** (article 25.2). Autrement dit, ces principes imposent que le respect de la vie privée soit une préoccupation des développeurs dès la conception du traitement et que, sans aucune intervention de la part de l'utilisateur, l'ensemble des mesures disponibles visant à protéger les données personnelles et à en limiter la collecte soit activé.

C'est justement sur le **fondement de l'article 25.2 du RGPD que la CNIL sanctionne DISCORD**. Lors de ses contrôles, la CNIL a constaté que, lorsqu'un utilisateur connecté à la plateforme fermait l'application DISCORD en cliquant sur l'icône « X » située en haut à droite sous Microsoft Windows, l'application restait toujours en cours d'exécution et l'utilisateur restait connecté à la plateforme. L'utilisateur pouvait continuer à être entendu par les autres membres présents dans le salon vocal alors qu'il pensait l'avoir quitté. A la différence des autres plateformes proposant un service similaire à celui de DISCORD, aucune notification n'était portée à l'attention de l'utilisateur sur ce risque.

La Commission reproche ainsi à la société de ne pas avoir assuré la protection des données des utilisateurs de la plateforme par défaut. Pour se mettre en conformité avec cette exigence du RGPD, la société DISCORD a mis en place une fenêtre « pop-up » pour informer l'utilisateur que, lorsque la fenêtre a été fermée pour la première fois, l'application est toujours en fonctionnement et que ce paramètre peut directement être modifié par l'utilisateur.

C'est la première fois que la CNIL sanctionne un responsable de traitement de ne pas avoir assuré, par défaut, la protection des données personnelles. Cela laisse à penser que, plus de 4 ans après l'entrée en vigueur du RGPD, le temps d'adaptation des sociétés aux exigences du règlement est fini et que la Commission est désormais moins indulgente dans ses analyses et sanctions.

Au cours de son investigation, la CNIL a relevé d'autres manquements au RGPD.

D'abord, un manquement à l'obligation de conserver les données pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5 du RGPD). La CNIL relève que la société n'a pas défini de politique de durée de conservation des données. Elle constate également que 2 474 000 millions de comptes d'utilisateurs français inactifs depuis plus de trois ans et 58 000 comptes inactifs depuis plus de cinq ans étaient conservées au sein de la base de données DISCORD.

En défense, DISCORD justifie la conservation de ces données en faisant valoir que la durée de conservation mise en œuvre correspond à la durée de la relation contractuelle avec ses utilisateurs. Mais la CNIL rejette cet argument en relevant que cette relation, étant à durée indéterminée, conduit à conserver des données de manière illimitée, ce qu'interdit le RGPD.

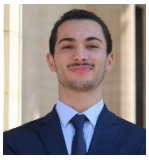
Egalement, la CNIL a constaté que la politique de gestion des mots de passe de DISCORD n'était pas suffisamment robuste et contraignante pour garantir la sécurité des comptes des utilisateurs (article 32 du RGPD), un mot de passe composé de six caractères incluant seulement des lettres et des chiffres était accepté par la plateforme.

Enfin, la Commission reproche à la société de ne pas avoir effectué d'analyse d'impact relative à la protection des données (AIPD) alors, qu'au regard du volume de données traitées et de l'utilisation des services par des mineurs, le traitement aurait dû faire l'objet d'une telle analyse.

La sanction de 800 000 € prononcée par la CNIL à l'encontre de DISCORD tient ainsi compte de l'ensemble de ces manquements mais également des efforts réalisés par la société pour se mettre en conformité tout au long de la procédure.

Auteurs

Eric Barbry
Avocat associé
ebarbry@racine.eu



Robin Genest
Juriste
rgenest@racine.eu