Interfaces de programmation applicatives : Recommandations techniques de la CNIL

Charlotte Beck, le 23 janvier 2024

Cette contribution examine les recommandations techniques de la CNIL sur l'utilisation des interfaces de programmation applicatives, qui donne des indications sur les bonnes pratiques à suivre.

Recommandation technique du 7 juillet 2023 relative à l'utilisation des interfaces de programmation applicatives (API) pour le partage sécurisé de données à caractère personnel

Le 7 juillet 2023, la CNIL publie des recommandations techniques relatives à l'utilisation des interfaces de programmation applicatives (API, *Application Programming Interface*). Ces recommandations ont été suivies d'une publication de la CNIL le 24 novembre 2023, apportant des clarifications d'ordre général ainsi que sur la méthodologie. Une liste d'outils a également été partagée, ainsi que des liens utiles concernant d'autres lignes directrices ou guides sur des sujets connexes.

Les API sont des outils informatiques permettant la communication entre applications, souvent utilisées dans l'objectif d'échanger des données ou services. Une API définit l'ensemble des requêtes qu'une application visant à utiliser ce service peut effectuer. Elles sont créées par les développeurs d'applications.

L'API peut notamment être utilisée dans le but d'obtenir des données. Ce serait notamment le cas d'une entreprise permettant l'accès à des données de ses clients, sur la base de leur consentement, à des tiers agréés afin que ceux-ci puissent proposer à ces mêmes clients un service. Ces tiers accèderont aux données par voie d'API. Un exemple de ce cas de figure est la possibilité de se connecter via Facebook, Google ou Apple sur certains sites, notamment de vente. En donnant son consentement, l'internaute permet à l'éditeur du site de vente (le réutilisateur) de faire une requête envers, par exemple, Facebook (le détenteur des données et également gestionnaire d'API) afin d'obtenir le nom et prénom de l'internaute et pouvoir l'afficher dans son compte utilisateur.

L'utilisation d'API est recommandée dans le cadre de traitement de données personnelles,

car il permet de minimiser la quantité de données échangées, permettant à la personne faisant la requête d'obtenir uniquement des données pertinentes pour elle. Les mesures de sécurité et la gestion des droits d'accès sont un autre avantage de cet outil. Si l'on reprend l'exemple de l'API de Facebook, celle-ci sera définie de manière à ce que les réutilisateurs adressent des requêtes définies, par exemple obtenir le nom. Ceci permet de minimiser la quantité de données obtenues, évitant ainsi un accès à l'intégralité des données détenues par Facebook sur un de ses utilisateurs.

Invoquant ces facteurs, la CNIL indique dans sa publication vouloir « promouvoir l'usage des API lorsqu'il est bénéfique ». En effet, les échanges de données et leur réutilisation peuvent être facilités par le recours à des API, que ce soit entre administrations publiques ou acteurs privés. De plus, les API sont une opportunité d'intégrer les principes de *privacy by design* et *by default* si essentiels en matière de protection des données.

Les recommandations de CNIL se divisent en quatre parties principales. La première partie est d'ordre générale et analyse différents facteurs liés aux API. Les trois parties suivantes présentent des recommandations spécifiques, visant chacune des parties prenantes dans l'utilisation d'une API, soit les détenteurs des données, les gestionnaires d'API et les réutilisateurs.

La première partie présente les cas de figure dans lesquels l'utilisation des API est à privilégier – soit lorsque les données ou les mesures de sécurités sont susceptibles d'être régulièrement mises à jour, que les réutilisateurs n'ont besoin que d'une partie des données ou que de manière ponctuelle –, ainsi que les risques liés à cette utilisation. La CNIL met en avant les bonnes pratiques à suivre pour s'assurer de leur respect en cas d'utilisation d'API. Outre le respect des principes généraux de la protection des données, il est recommandé de mettre en place une gouvernance efficace entre les différents acteurs impliqués dans l'utilisation d'API. Cette gouvernance peut être atteinte par la mise en place d'un cadre documentaire, clarifiant et décrivant les rôles et responsabilités de chaque acteur ainsi que les modalités d'usage de l'API (l'art. 26 par. 1 RGPD prévoit que les responsabilités conjointes doivent être contractuellement déterminées). Les protocoles d'urgence devraient également être formalisés, prévoyant les mesures techniques à prendre en cas d'incident relatif à la sécurité des données.

Similairement, il est recommandé de définir une politique de gestion des droits d'accès, qui devrait en particulier porter sur les informations à fournir par les réutilisateurs afin de vérifier la licéité de leur accès à l'API. Les informations à fournir comportent, entre autres, l'identité

du réutilisateur, les finalités de réutilisation, les catégories de données nécessaires, ainsi que le volume, la fréquence et le type de requêtes envisagés. La CNIL recommande que ces informations soient transmises, tant pour les API en accès restreint que les API ouvertes, et que les habilitations soient accordées selon des niveaux, en fonction de la durée des accès (usage unique ou durée déterminée).

Ces informations sont également nécessaires et pourraient être fournies aux personnes concernées. Les données relatives aux accès par des réutilisateurs peuvent être collectées par des mesures de journalisation (*logging*). La CNIL précise les différentes informations à fournir, prônant une transparence élevée envers les personnes concernées, indiquant que « *a minima* [les informations soient] présentées sur un site web porté à l'attention des personnes ».

La deuxième partie vise les détenteurs de données, qui pourrait la plupart du temps tenir le rôle de responsable du traitement, du fait du contrôle qu'ils exercent sur les données, tant au niveau technique qu'organisationnel. Les recommandations spécifiques visent l'information des réutilisateurs, des aspects relatifs à l'exactitude et l'intégrité des données et la sécurité. Sur les aspects sécuritaires, la CNIL indique en particulier les mesures relatives au cloisonnement et la disponibilité, l'authentification et la journalisation. Sur la journalisation, la CNIL indique qu'une analyse proactive doit être effectuée, tant pour les journaux internes qu'externes, dans l'objectif de vérifier la légitimité des accès. Sur la durée de conservation des informations de journalisation, la Commission renvoie vers les recommandations relatives à la durée de conservation (cf. Recommandation de la CNIL du 18 novembre 2021 relative aux mesures de journalisation).

La troisième partie concerne les gestionnaires d'API, qui sont les acteurs principaux pouvant assurer la sécurité de la mise en œuvre de l'API. En effet, les gestionnaires d'API sont en charge de la gestion technique de l'outil. Dans leurs activités, les gestionnaires d'API assurent le lien entre les détenteurs et les réutilisateurs, agissant souvent comme sous-traitants de l'un ou l'autre. Les recommandations spécifiques à leur intention portent sur la documentation, la minimisation — en particulier sur l'utilisation de *sandbox* (bac à sable) comprenant des données synthétiques avant d'avoir recours à des données réelles et un accent sur les mesures visant à éviter la réidentification des données —, l'exercice des droits des personnes concernées et la sécurité. En matière de sécurité, la confidentialité des communications doit être garantie, la CNIL recommandant d'avoir recours aux références en matière cryptographique (cf. référentiel général de sécurité).

Enfin, la dernière partie concerne les recommandations à destination des réutilisateurs des données. Ceux-ci, dans le cadre d'utilisation d'API pour accéder ou recevoir des données, doivent strictement respecter les instructions fournies dans le cadre d'une charte ou licence de réutilisation. La CNIL préconise ici une sorte d'obligation de collaboration des réutilisateurs, notamment dans le cadre de l'information des personnes concernées et de minimisation des données traitées. Comme pour les autres acteurs, des exigences particulières de sécurité sont décrites, la principale visant la sécurité des clés.

Les recommandations de la CNIL comportent de plus des définitions et cas d'usage particuliers permettant de clarifier les différentes recommandations faites. Cette ressource peut être particulièrement intéressante pour les acteurs publics et privés concernés par les API et donner une ligne directrice dans l'élaboration d'une politique spécifique en matière d'API ou tout autre documentation visant à assurer la gouvernance des données dans ce cadre. De manière plus générale, ces recommandations donnent des indications utiles sur les bonnes pratiques à suivre en cas de partage des données entre différents destinataires.

Au niveau suisse, le thème des API fait partie des trois thèmes prioritaires dans la stratégie Suisse numérique de la Confédération. Il est de la responsabilité du secteur de la Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale, qui soutient et coordonne la transformation numérique de l'administration fédérale en étroite collaboration avec les départements.

Proposition de citation : Charlotte Beck, Interfaces de programmation applicatives : Recommandations techniques de la CNIL , 23 janvier 2024 *in* www.swissprivacy.law/279

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.