POUR LES INTÉGRATEURS D'ASSISTANTS VOCAUX

S'ils sont des constructions logicielles, les assistants vocaux ont cependant vocation à être incarnés dans des équipements physiques. Ces objets connectés peuvent être très divers : smartphone, véhicule, robot ménager, enceinte de salon, jouet pour enfant, etc.

Dans certains cas, les développeurs et intégrateurs d'assistants vocaux peuvent être la même entité, mais ce n'est pas nécessairement le cas. Si les développeurs d'assistants vocaux se concentrent sur les aspects logiciels (tout en apportant des indications en termes de spécifications requises), les intégrateurs se focalisent eux sur les contraintes matérielles. En tout état de cause, il convient de noter que les cas d'usage sont nombreux, les contextes d'utilisation multiples et les publics visés différents en fonction des applications. Les conseils proposés ici sont donc génériques, mais peuvent être enrichis en fonction des modalités d'usages. Dans tous les cas, il convient d'être particulièrement attentif aux modalités d'information des personnes.

Établir la transparence, fondement de la confiance

Comme pour tout traitement de données personnelles, le RGPD impose une information des personnes concernées par les traitements mis en œuvre par des assistants vocaux. Plus encore que pour les services accessibles en ligne, l'usage d'un assistant vocal impose aux utilisateurs de faire confiance à un dispositif qui donne peu d'information sur son fonctionnement et dont les modalités de maîtrise ne sont aujourd'hui pas aussi intégrées que celles qui s'exercent sur un ordinateur ou un smartphone.

Nos conseils

- Vérifier que les conditions d'information et de transparence prévues par le concepteur de l'assistant sont bien satisfaisantes pour permettre de traiter les données des personnes conformément à la législation (voir les conseils pour les concepteurs d'assistants ci-dessus, page 68).
- Mettre en œuvre l'information prévue et, le cas échéant, une information complémentaire adéquate.
- S'il est envisagé, dans une évolution logicielle à venir, de doter un objet d'un assistant vocal, bien préciser dans les spécifications de l'équipement si des capacités de production de son (haut-parleur), d'écoute (microphone) et de traitement (processeur) sont embarquées.
- Informer spécifiquement les utilisateurs quand une fonctionnalité d'assistant vocal vient à être déployée sur un équipement qui ne le proposait pas initialement, et leur permettre de continuer à bénéficier d'un équipement pleinement fonctionnel sans activer l'assistant vocal s'ils le souhaitent.

Donner des moyens de contrôle aux utilisateurs

Autre exigence majeure portée par le RGPD, la mise en œuvre de moyens permettant aux personnes de maîtriser les usages qui sont faits de leurs données et d'exercer leurs droits de façon simple et effective. Ces modalités de contrôle et d'exercice doivent être adaptées à l'interface vocale de l'assistant.

Nos conseils

- Réfléchir préalablement à l'intérêt et aux attendus de l'intégration d'un assistant vocal dans l'équipement en question.
- Si un tel choix est effectivement pertinent, choisir l'assistant à intégrer en fonction des objectifs poursuivis et de l'impératif de protection de la vie privée.
- Laisser le choix à l'utilisateur d'utiliser ou non l'assistant intégré à son équipement si celui-ci n'est pas absolument nécessaire au service proposé, tout en continuant à bénéficier d'un équipement pleinement fonctionnel.

- Mettre en œuvre un bouton de désactivation physique du microphone (électriquement non alimenté).

Satisfaire l'impératif de sécurité

De la même manière que pour les concepteurs d'assistants vocaux, le RGPD précise que la protection des données personnelles nécessite de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques. La mise en œuvre de tout traitement de données à caractère personnel implique donc une obligation de sécurité. Outre les mesures génériques qui peuvent être retrouvées dans le Guide sur la sécurité des données personnelles[151] et dans le Guide développeur[152] (présenté dans l'encadré page 75), des bonnes pratiques spécifiques aux assistants vocaux peuvent être précisées.

Nos conseils

- Déployer les assistants vocaux sur des équipements mis à jour et correctement sécurisés (voir par exemple l'encadré sur les jouets connectés, ci-après).
- Privilégier les assistants dont le fonctionnement est maîtrisable, c'est-à-dire pour lesquels il est possible d'agir sur l'ensemble du paramétrage technique et de la sélection des fonctionnalités.
- Éviter les assistants susceptibles de transmettre des données à un tiers sans connaître les conditions de traitement des données par celui-ci.
- Éviter les assistants opérés par des acteurs qui réutilisent les données pour leur propre compte ou veiller à encadrer contractuellement les traitements réalisés par le concepteur de l'assistant.
- Réaliser une Analyse d'Impact relative à la Protection des Données et la mettre régulièrement à jour afin d'assurer que les mesures techniques et organisationnelles prises sont en adéquation avec les risques que le traitement de données fait peser sur les personnes (pour plus de précisions sur l'AIPD, voir l'encadré page 56).

ZOOM SUR...

Les jouets connectés pas toujours sécurisés

En 2017, la CNIL a effectué des missions de vérification sur deux jouets connectés. Ces jouets, équipés d'un microphone et d'un haut-parleur, répondent aux questions des enfants sur des sujets divers tels que les fées et les dinosaures. La réponse est extraite d'Internet et donnée à l'enfant par l'intermédiaire de ces objets.

Les contrôles réalisés ont permis de relever que la société qui commercialise ces jouets collecte par leur intermédiaire une multitude d'informations personnelles sur les enfants et leur entourage, notamment leur voix et le contenu des conversations échangées. Plus encore, il a été constaté que le défaut de sécurisation des jouets permet à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des adultes les entourant, et d'avoir ainsi accès aux discussions échangées dans un cercle familial ou amical.

Au vu de ces éléments, la Présidente de la CNIL a considéré que les traitements mis en œuvre n'étaient pas conformes à la loi Informatique et Libertés, en raison du non-respect de la vie privée des personnes et de l'absence d'information des personnes concernées, et a décidé en conséquence de mettre en demeure le responsable de traitement d'adopter des mesures correctrices sous un délai de deux mois. Cette mise en demeure a été rendue publique en décembre 2017.

151 - CNIL, Le guide de sécurité des données personnelles, édition 2018 https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
152 - CNIL, La CNIL publie un guide RGPD pour les développeurs, janvier 2020, https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeurs