Lignes directrices 02/2021 sur les assistants vocaux virtuels

Version 2.0

Adoptées le 7 juillet 2021

Historique des versions

Version 2.0	7 juillet 2021	Adoption des lignes directrices après consultation publique
Version 1.0	9 mars 2021	Adoption des lignes directrices pour consultation publique

SYNTHÈSE

Un assistant vocal virtuel (VVA, de l'anglais «virtual voice assistants») est un service qui comprend les commandes vocales et les exécute ou assure les échanges avec d'autres systèmes informatiques si nécessaire. Les VVA sont actuellement disponibles sur la plupart des téléphones intelligents et tablettes, sur les ordinateurs traditionnels et, ces dernières années, même sur des appareils autonomes tels que des enceintes intelligentes.

Les VVA servent d'interface entre les utilisateurs et leurs appareils informatiques et services en ligne tels que les moteurs de recherche ou les boutiques en ligne. En raison de leur rôle, les VVA ont accès à un volume considérable de données à caractère personnel, y compris à toutes les commandes des utilisateurs (par exemple, l'historique de navigation ou de recherche) et aux réponses (par exemple, les rendez-vous de l'agenda).

Si la grande majorité des services de VVA ont été mis au point par quelques concepteurs de VVA, les VVA peuvent travailler conjointement avec des applications programmées par des tiers (développeurs d'applications de VVA) afin de permettre des commandes plus sophistiquées.

Pour fonctionner correctement, un VVA a besoin d'un terminal équipé de microphones et de haut-parleurs. L'appareil stocke des données vocales et d'autres données que les VVA actuels transfèrent vers des serveurs de VVA à distance.

Les responsables du traitement qui fournissent des services de VVA et leurs sous-traitants doivent donc tenir compte à la fois du RGPD[1] et de la directive «vie privée et communications électroniques»[2].

Les présentes lignes directrices recensent quelques-uns des problèmes de conformité les plus pertinents et fournissent des recommandations aux parties prenantes concernées quant à la manière d'y remédier.

Les responsables du traitement qui fournissent des services de VVA au moyen d'appareils terminaux sans écran doivent toujours informer les utilisateurs conformément au RGPD lorsqu'ils mettent en place le VVA ou l'installent, ou utilisent une application de VVA pour la première fois. Par conséquent, nous recommandons aux fournisseurs/concepteurs et développeurs de VVA d'élaborer des interfaces vocales afin de faciliter la communication des informations obligatoires.

Actuellement, tous les VVA requièrent l'enregistrement d'un utilisateur au moins auprès du service. Conformément à l'obligation de protection des données dès la conception et par défaut, les fournisseurs/concepteurs et les développeurs de VVA devraient examiner la nécessité de disposer d'un utilisateur enregistré pour chacune de leurs fonctionnalités.

Le compte utilisateur employé par de nombreux concepteurs de VVA regroupe le service de VVA avec d'autres services tels que les courriers électroniques ou les services de transmission vidéo. Le CEPD estime que les responsables du traitement devraient s'abstenir de telles pratiques, dans la mesure où

[1] Règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»).

[2] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive relative à la vie privée et aux communications électroniques), telle que modifiée par la directive 2006/24/CE et la directive 2009/136/CE (ci-après la «directive "vie privée et communications électroniques"»).

elles impliquent des politiques longues et complexes en matière de protection de la vie privée qui ne seraient pas conformes au principe de transparence du RGPD.

Les lignes directrices tiennent compte de quatre des finalités les plus courantes pour lesquels les VVA traitent des données à caractère personnel: l'exécution des demandes, l'amélioration du modèle d'apprentissage automatique du VVA, l'identification biométrique et l'établissement d'un profil pour le contenu personnalisé ou la publicité.

Dans la mesure où les données des VVA sont traitées afin d'exécuter les demandes de l'utilisateur, c'est-à-dire dans la mesure strictement nécessaire pour fournir un service demandé par l'utilisateur, les responsables du traitement des données sont exemptés de l'obligation d'obtenir le consentement préalable prévue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». À l'inverse, le consentement requis à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» est nécessaire au stockage ou à l'obtention de l'accès à des informations à des fins autres que l'exécution de la demande des utilisateurs.

Certains services de VVA conservent des données à caractère personnel jusqu'à ce que leurs utilisateurs demandent leur suppression. Cette pratique n'est pas conforme au principe de limitation de la conservation. Les VVA devraient stocker les données à caractère personnel pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

Si un responsable du traitement se rend compte (par exemple, en raison de processus d'évaluation de la qualité) de la collecte accidentelle de données à caractère personnel, il devrait vérifier qu'il existe une base juridique valide pour chaque finalité du traitement de ces données. Dans le cas contraire, les données collectées accidentellement devraient être supprimées.

Les VVA peuvent traiter les données de plusieurs personnes concernées. Les fournisseurs/concepteurs de VVA devraient dès lors mettre en œuvre des mécanismes de contrôle d'accès pour garantir la confidentialité, l'intégrité et la disponibilité des données à caractère personnel. Toutefois, certains mécanismes traditionnels de contrôle de l'accès, tels que les mots de passe, ne sont pas adaptés au contexte des VVA, puisque ces mots de passe devraient être prononcés à voix haute. Les lignes directrices présentent quelques considérations à cet égard, y compris une section dédiée au traitement de catégories particulières de données aux fins d'identification biométrique.

Les fournisseurs/concepteurs de VVA devraient tenir compte du fait qu'en collectant la voix de l'utilisateur, l'enregistrement peut contenir la voix d'autres personnes ou des données telles que du bruit de fond, qui ne sont pas nécessaires pour le service. Dans la mesure du possible, les concepteurs de VVA devraient donc envisager des technologies permettant de filtrer les données inutiles et de veiller à ce que seule la voix de l'utilisateur soit enregistrée.

Lorsqu'il évalue la nécessité d'une analyse d'impact sur la protection des données (AIPD), le CEPD estime qu'il est très probable que les services de VVA relèvent des catégories et conditions considérées comme nécessitant une AIPD.

Les responsables du traitement qui fournissent des services de VVA devraient veiller à ce que les utilisateurs puissent exercer leurs droits en utilisant des commandes vocales faciles à suivre. Les fournisseurs/concepteurs de VVA ainsi que les développeurs d'applications devraient, à la fin du processus, informer les utilisateurs que leurs droits ont été dûment pris en compte, par message vocal ou en envoyant une notification écrite au téléphone mobile ou au compte de l'utilisateur, ou encore par tout autre moyen choisi par l'utilisateur.

Table des matières

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, points e) et j), du règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[3],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 GÉNÉRALITÉS

1. Les récentes avancées technologiques ont considérablement accru la précision et la popularité des assistants vocaux virtuels (VVA, de l'anglais «virtual voice assistants»). Les VVA ont été intégrés, entre autres appareils, aux téléphones intelligents, aux véhicules connectés, aux enceintes intelligentes et aux télévisions intelligentes. Cette intégration a permis aux VVA d'accéder à des informations à caractère intime qui, si elles ne sont pas correctement gérées, pourraient porter atteinte aux droits des personnes à la protection des données et à la vie privée. Par conséquent, les VVA et les dispositifs qui les intègrent ont été examinés par différentes autorités chargées de la protection des données.

2. Le recours à des interactions fondées sur la parole présente plusieurs avantages, tels que: le caractère naturel de l'interaction, qui n'implique pas un apprentissage spécifique de la part des utilisateurs, la rapidité d'exécution de la commande et l'extension du champ d'action qui permet un accès plus rapide à l'information. Toutefois, le fait de s'appuyer sur la parole soulève également des difficultés pour interpréter correctement le message: variabilité du signal audio entre les différents locuteurs, environnement acoustique, ambiguïté du langage, etc.

3. Dans la pratique, la fluidité ou la simplification des tâches reste la principale motivation pour s'équiper de VVA. Il peut s'agir, par exemple, de passer un appel ou d'y répondre, de régler un minuteur, entre autres manipulations, en particulier lorsque les utilisateurs ont les mains occupées. La domotique est la principale application proposée par les concepteurs de VVA. En proposant de simplifier l'exécution des tâches (allumer la lumière, régler le chauffage, abaisser les volets, etc.) et de les centraliser au moyen d'un outil unique pouvant être facilement activé à distance, ils agissent en tant que facilitateur domestique. Outre l'usage personnel ou domestique, les commandes vocales peuvent présenter un intérêt dans des environnements professionnels où il est difficile de manipuler des outils informatiques et d'utiliser des commandes écrites (par exemple, des travaux de manufacture).

[3] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».

4. En théorie, les principaux bénéficiaires de l'interface vocale pourraient être les personnes handicapées ou dépendantes, pour lesquelles l'utilisation d'interfaces traditionnelles pose problème. L'assistance vocale virtuelle peut faciliter l'accès à l'information et aux ressources informatiques et promouvoir ainsi des logiques inclusives, étant donné que l'utilisation de la voix permet de surmonter les difficultés liées au mot écrit, qui apparaissent chez certaines catégories d'utilisateurs.

5. Enfin, la santé est également un domaine où il existe de nombreux cas d'utilisation pour des dialogueurs, vocaux ou non. Par exemple, au cours de la pandémie de COVID-19, divers robots d'appel (de l'anglais «callbots») ont été déployés pour offrir un diagnostic préalable aux appelants. À long terme, certains estiment que l'ensemble du processus de soins au patient pourrait être transformé par les interactions entre l'homme et l'assistant: non seulement à des fins de bien-être et de prévention, mais aussi pour le traitement et le soutien.

6. Il existe actuellement plus de 3 milliards de téléphones intelligents et tous ont des VVA intégrés, la plupart d'entre eux étant activés par défaut. Certains des systèmes d'exploitation les plus répandus dans les ordinateurs personnels et les ordinateurs portables intègrent également des VVA. La récente augmentation du nombre d'enceintes intelligentes (147 millions d'entre elles ont été vendues en 2019[4]) introduit les VVA dans des millions de foyers et de bureaux. Toutefois, les modèles actuels de VVA ne proposent pas de mécanismes d'authentification ou de contrôle d'accès par défaut.

7. Le présent document vise à fournir des orientations sur l'application du RGPD dans le contexte des VVA.

2 CONTEXTE TECHNOLOGIQUE

2.1 Caractéristiques fondamentales des assistants vocaux virtuels

8. Un VVA peut être défini comme une application logicielle qui permet de dialoguer oralement avec un utilisateur en langage naturel.

9. Le langage naturel possède une sémantique spécifique au langage humain. En fonction des caractéristiques du langage et de la diversité du lexique, la même instruction peut être formulée de multiples manières, tandis que certaines commandes peuvent sembler similaires mais se rapporter à deux objets différents. Des mécanismes de déduction sont alors fréquemment utilisés pour lever ces ambiguïtés, par exemple, en fonction de ce qui a été dit précédemment, du moment où l'instruction a été donnée, du lieu, des intérêts de la personne, etc.

10. Un VVA peut être subdivisé en modules permettant d'exécuter différentes tâches: captation et restitution du son, transcription automatique de la parole (conversion de la parole en texte), traitement automatique du langage, stratégies de dialogue, accès aux ontologies (jeux de données et concepts structurés liés à un domaine donné) et sources de connaissances externes, génération de langage, synthèse vocale (conversion du texte en parole), etc. Concrètement, l'assistant devrait permettre une interaction afin de réaliser des actions (par exemple, «allumer la radio», «éteindre la lumière») ou d'accéder à des informations (par

[4] Voir à titre d'exemple un communiqué de presse publié le 1er août 2019 par l'autorité de la protection des données et de l'information de Hambourg: https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant

exemple, «quel temps fera-t-il demain?», «est-ce que le train de 7 h 43 circule?»). Il joue ainsi le rôle d'intermédiaire et d'orchestrateur censé faciliter la réalisation des tâches de l'utilisateur.

11. Dans la pratique, un VVA n'est pas une enceinte intelligente, mais une enceinte intelligente peut être équipée d'un assistant vocal. Il est courant de confondre les deux, mais le second n'est qu'une incarnation matérielle de la première. Un VVA peut être déployé dans un téléphone intelligent, une enceinte intelligente, une montre connectée, un véhicule, un appareil électroménager, etc.

12. L'organisation du traitement des données sous-jacent peut faire intervenir de multiples schémas de flux d'informations. Il est possible d'isoler trois entités principales:

    L'instance physique: l'élément matériel dans lequel l'assistant est incorporé (téléphone intelligent, enceinte, télévision intelligente, etc.) et qui est doté de microphones, de haut-parleurs et de capacités de réseau et de calcul (plus ou moins développées selon les cas).

    L'instance logicielle: la partie qui met en œuvre l'interaction entre l'homme et la machine à proprement parler et qui intègre les modules de reconnaissance vocale automatique, de traitement du langage naturel, de dialogue et de synthèse vocale. Cette opération peut être effectuée directement à l'intérieur de l'équipement physique, mais, dans de nombreux cas, elle est effectuée à distance.

    Les ressources: des données externes telles que des bases de données de contenus, des ontologies ou des applications commerciales qui fournissent des connaissances (par exemple, «donner l'heure de la côte Ouest des États-Unis», «lire mes courriels») ou qui permettent d'exécuter l'action demandée de manière concrète (par exemple, «augmenter la température de 1,5 °C»).

13. Les VVA permettent l'installation de composants ou d'applications de tiers qui élargissent leurs fonctionnalités de base. Chaque VVA désigne les composants différemment, mais ils impliquent tous l'échange de données à caractère personnel des utilisateurs entre le concepteur du VVA et le développeur de l'application.

14. Bien que la plupart des VVA ne partagent pas l'extrait vocal avec les développeurs d'applications, ces acteurs traitent malgré tout des données à caractère personnel. En outre, selon la nature de la fonctionnalité fournie, le développeur d'applications reçoit des intentions et des variables d'informations (de l'anglais «slots») qui pourraient inclure des informations sensibles telles que des données relatives à la santé.

2.2 Acteurs de l'écosystème des VVA

15. Un VVA peut faire intervenir un grand nombre d'acteurs et d'intermédiaires tout au long de la chaîne d'exécution. Dans la pratique, il est possible de recenser jusqu'à cinq acteurs différents. En fonction des modèles commerciaux et des choix technologiques, certains acteurs peuvent toutefois assumer plusieurs combinaisons de rôles, par exemple le concepteur et l'intégrateur ou le concepteur et le développeur d'applications:

    a. **Le fournisseur (ou concepteur) de VVA:** responsable du développement du VVA, conçoit et définit ses possibilités et ses fonctionnalités par défaut : modalités d'activation, choix

de l'architecture, accès aux données, gestion des enregistrements, spécifications matérielles, etc.

b. **Le développeur d'applications de VVA:** comme pour les applications mobiles, crée des applications élargissant les fonctionnalités par défaut des VVA. Pour ce faire, il est nécessaire de respecter les contraintes de développement imposées par le concepteur.

c. **L'intégrateur:** le fabricant d'objets connectés, qui souhaite les équiper d'un VVA. Il devrait respecter les exigences définies par le concepteur.

d. **Le propriétaire:** étant en charge d'espaces physiques accueillant des personnes (lieux d'habitation, environnements professionnels, véhicules de location, etc.), il/elle souhaite fournir un VVA à son public (éventuellement avec des applications spécifiques).

e. **L'utilisateur:** le maillon final de la chaîne de valeur du VVA, qui peut l'utiliser sur divers appareils (enceinte, télévision, téléphone intelligent, montre, etc.) en fonction de comment et où le VVA a été déployé et mis en place.

2.3 Description étape par étape

16. Pour qu'un VVA puisse effectuer une action ou accéder à des informations, une succession de tâches est réalisée:

1) Lorsqu'il est déployé à l'intérieur d'un équipement (téléphone intelligent, enceinte, véhicule), le VVA est en veille. Plus précisément, il est constamment à l'écoute. Toutefois, tant qu'une expression de réveil spécifique n'est pas détectée, aucun message audio n'est transmis hors de l'appareil recevant la voix et aucune autre opération que la détection de l'expression de réveil n'est effectuée. À cette fin, un délai tampon de quelques secondes est utilisé (voir la section suivante pour plus de détails).

2) L'utilisateur prononce l'expression de réveil et le VVA compare localement le message audio à l'expression de réveil. S'ils correspondent, le VVA ouvre un canal d'écoute et le contenu audio est immédiatement transmis.

3) Dans de nombreux cas, si le traitement de la commande s'effectue à distance, une deuxième vérification de la prononciation du mot-clé est exécutée du côté du serveur afin de limiter les activations indésirables.

4) L'utilisateur formule sa demande, qui est instantanément transmise au fournisseur de VVA. La séquence des paroles prononcées est alors automatiquement transcrit (conversion de la parole en texte).

5) La commande est interprétée à l'aide des technologies de traitement du langage naturel (TLN). Les intentions du message sont extraites et des variables d'informations (slots) sont identifiées. Un module de gestion du dialogue est ensuite utilisé pour préciser le scénario d'interaction à mettre en œuvre avec l'utilisateur en fournissant le schéma de réponse approprié.

6) Si la commande implique une fonctionnalité fournie par une application tierce (compétence, action, raccourci, etc.), le fournisseur de VVA envoie au développeur d'applications les intentions et les variables d'informations (slots) du message.

7) Une réponse adaptée à la demande de l'utilisateur est identifiée – en principe du moins, la réponse «Je n'ai pas la réponse à votre question» étant une réponse adaptée au cas où le VVA n'aurait pas pu interpréter correctement la demande. Si nécessaire, des ressources à distance sont employées: les bases de données de connaissances accessibles au public (encyclopédie en ligne, etc.) ou par authentification (compte bancaire, application musicale, compte client pour l'achat en ligne, etc.) et les variables d'informations (slots) sont complétées par les connaissances récupérées.

8) Une phrase de réponse est créée et/ou une action est identifiée (abaisser les stores, augmenter la température, jouer une musique, répondre à une question, etc.). La phrase est synthétisée (conversion du texte en parole) et/ou l'action à exécuter est transmise à l'équipement et exécutée.

9) Le VVA retourne en mode veille.

Il convient de noter que si la plupart des traitements vocaux s'effectuent actuellement sur des serveurs à distance, certains fournisseurs de VVA développent des systèmes qui pourraient assurer une partie de ce traitement au niveau local[5].

2.4 Expressions de réveil

17. Pour être utilisé, un VVA devrait être «en alerte». Cela signifie que l'assistant passe à un mode d'écoute active afin de recevoir les ordres et commandes de son utilisateur. Alors que cette mise en éveil peut aussi parfois être obtenue par une action physique (par exemple, en pressant un bouton, en appuyant sur l'enceinte intelligente, etc.), presque tous les VVA présents sur le marché se fondent sur la détection d'une expression de réveil ou d'un mot pour passer à un mode d'écoute active (également appelé mot d'activation ou mot de réveil).

18. Pour ce faire, l'assistant se fonde sur l'utilisation du microphone et sur des capacités informatiques de base pour détecter si le mot-clé a été prononcé. Cette analyse, qui a lieu de manière continue dès la mise en service du VVA, s'effectue exclusivement au niveau local. Ce n'est que lorsque le mot-clé a été reconnu que les enregistrements audio sont traités pour l'interprétation et l'exécution de la commande, ce qui signifie souvent qu'ils sont envoyés à des serveurs à distance via l'internet. La détection de mots-clés repose sur des techniques d'apprentissage automatique. Le principal défi lié à l'utilisation de ces méthodes réside dans le fait que la détection est probabiliste. Ainsi, pour chaque mot ou expression prononcé, le système attribue une note de confiance pour déterminer si le mot-clé a bien été prononcé. Si cette note s'avère supérieure à une valeur seuil prédéfinie, l'appareil considère que c'est le cas. Un tel système n'est donc pas exempt d'erreurs : dans certains cas, il se peut que l'activation ne soit pas détectée alors que le mot-clé a été prononcé (rejet erroné) et, dans d'autres cas, il se peut que le VVA soit activé même si l'utilisateur n'a pas prononcé le mot-clé (acceptation erronée).

19. Dans la pratique, un compromis acceptable devrait être trouvé entre ces deux types d'erreurs pour définir la valeur seuil. Toutefois, étant donné que la conséquence d'une détection erronée du mot-clé pourrait être l'envoi d'enregistrements audio, des transmissions inattendues et non désirées de données sont susceptibles de se produire. Très souvent, les

[5] Cette possibilité a été signalée ici par exemple: https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech

fournisseurs de VVA qui se servent du traitement à distance utilisent un mécanisme à deux étapes pour cette détection: une première étape intégrée localement au niveau de l'équipement et une seconde sur des serveurs à distance, où s'effectue le traitement de données suivant. Dans ce cas, les développeurs ont tendance à fixer un seuil relativement bas afin d'améliorer l'expérience de l'utilisateur et de veiller à ce que le mot-clé soit presque toujours reconnu lorsque l'utilisateur le prononce – même si cela implique une «sur détection» –, avant de mettre en œuvre une seconde étape de détection du côté du serveur, ce qui est plus restrictif.

2.5 Extraits vocaux et apprentissage automatique

20. Les VVA se fondent sur des méthodes d'apprentissage automatique pour effectuer un large éventail de tâches (détection de mots-clés, reconnaissance vocale automatique, traitement du langage naturel, synthèse vocale, etc.), ce qui nécessite dès lors la collecte, la sélection, l'étiquetage, etc., de grands ensembles de données.

21. La surreprésentation ou la sous-représentation de certaines caractéristiques statistiques peut influencer le développement des tâches fondées sur l'apprentissage automatique et, par la suite, la refléter dans ses calculs, et donc dans son mode de fonctionnement. Ainsi, tout comme leur quantité, la qualité des données joue un rôle majeur dans la finesse et la précision du processus d'apprentissage.

22. Afin d'accroître la qualité des VVA et de renforcer les méthodes d'apprentissage automatique déployées, les concepteurs de VVA pourraient souhaiter accéder aux données relatives à l'utilisation de l'appareil dans des conditions réelles - c'est-à-dire aux extraits vocaux - afin de travailler à son amélioration.

23. Qu'il s'agisse d'améliorer la qualité de la base de données d'apprentissage ou de corriger les erreurs commises lors du déploiement de l'algorithme, l'apprentissage et la formation des systèmes d'intelligence artificielle requièrent nécessairement une intervention humaine. Cette partie du travail, connue sous le nom de «travail numérique» (de l'anglais «digital labor»), soulève des questions tant sur les conditions de travail que sur la sécurité. Dans ce contexte, les médias d'information ont également fait état de transferts de données entre des concepteurs de VVA et des sous-traitants qui n'offriraient pas les garanties nécessaires en matière de protection de la vie privée.

3 ÉLÉMENTS DE LA PROTECTION DES DONNÉES

3.1 Cadre juridique

24. Le cadre juridique de l'UE applicable aux VVA est, en premier lieu, le RGPD, étant donné que la fonction essentielle des VVA implique le traitement de données à caractère personnel. Outre le RGPD, la directive «vie privée et communications électroniques»[6] établit une norme spécifique pour tous les acteurs qui souhaitent conserver des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur dans l'EEE ou accéder à ces informations.

[6] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2006/24/CE et la directive 2009/136/CE (ci-après la «directive "vie privée et communications électroniques"»).

25. Conformément à la définition d'un «*équipement terminal*»[7], les téléphones intelligents, les télévisions intelligentes et les dispositifs IdO similaires sont des exemples de terminaux. Même si les VVA sont en soi des services logiciels, ils fonctionnent toujours au moyen d'un dispositif physique tel qu'une enceinte intelligente ou une télévision intelligente. **Les VVA utilisent des réseaux de communications électroniques pour accéder aux dispositifs physiques qui constituent des «équipements terminaux» au sens de la directive «vie privée et communications électroniques». Par conséquent, les dispositions de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'appliquent chaque fois qu'un VVA conserve des informations dans le dispositif physique qui y est lié ou accède à ces informations**.[8]

26. Toutes opérations de traitement de données à caractère personnel postérieure aux opérations de traitement susmentionnées, y compris le traitement de données à caractère personnel obtenues en accédant à des informations dans l'équipement terminal, doit également avoir une base juridique au titre de l'article 6 du RGPD pour être licite[9].

27. Étant donné que le responsable du traitement, lorsqu'il demande le consentement pour conserver des informations ou obtenir l'accès à ces dernières en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», devra informer la personne concernée de toutes les finalités du traitement (à savoir le «traitement ultérieur») – y compris tout traitement à la suite des opérations susmentionnées –, le consentement au titre de l'article 6 du RGPD constituera généralement la base juridique la plus appropriée pour couvrir le traitement ultérieur des données à caractère personnel. Partant, le consentement constituera probablement la base juridique tant pour conserver des informations déjà stockées et obtenir l'accès à ces dernières que pour traiter des données à caractère personnel à la suite des opérations de traitement susmentionnées. En effet, lors de l'évaluation du respect de l'article 6 du RGPD, il convient de tenir compte du fait que le traitement dans son ensemble entraîne des activités spécifiques pour lesquelles le législateur de l'UEa cherché à fournir une protection supplémentaire[10]. En outre, lorsqu'ils déterminent la base juridique appropriée, les responsables du traitement doivent tenir compte de l'incidence sur les droits des personnes concernées, afin de respecter le principe de loyauté[11]. Le principe de base est que les responsables du traitement ne peuvent pas s'appuyer sur l'article 6 du RGPD pour

[7] L'article 1er de la directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications définit un «*équipement terminal*» comme a) «tout *équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public, b) les équipements de stations terrestres de satellites*»;

[8] Voir les lignes directrices 1/2020 du CEPD, paragraphe 12, pour un raisonnement similaire concernant les véhicules connectés (ci-après les «lignes directrices 1/2020 du CEPD»). Voir également CEPD, avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données.

[9] Idem, paragraphe 41.

[10] Avis 5/2019, paragraphe 41.

[11] Voir les lignes directrices 2/2019 du CEPD sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, 8 octobre 2019, paragraphe 1.

réduire la protection supplémentaire prévue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

28. Comme indiqué à la section 2.3 (étapes 2 et 3), les VVA actuels nécessitent l'accès aux données vocales stockées par le dispositif VVA[12]. Par conséquent, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique. L'applicabilité de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» signifie que la conservation d'informations ainsi que l'accès à des informations déjà stockées dans un VVA nécessitent, en règle générale, le consentement préalable de l'utilisateur final[13], mais prévoit deux exceptions: premièrement, lorsqu'ils visent à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques ou, deuxièmement, lorsqu'ils sont strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

29. La deuxième exception («strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur») permettrait à un fournisseur de services de VVA de traiter les données des utilisateurs pour exécuter les demandes de ces derniers (voir paragraphe 72 de la section 3.4.1) sans le consentement prévu à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». À l'inverse, le **consentement requis à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» serait nécessaire à** la conservation des informations ou à l'obtention de l'accès à ces dernières à **des fins autres que l'exécution de la demande des utilisateurs** (par exemple, l'établissement du profil des utilisateurs). Les responsables du traitement devraient obtenir le consentement d'utilisateurs spécifiques. Par conséquent, les responsables du traitement ne devraient traiter les données des utilisateurs non-enregistrés que pour exécuter leurs demandes.

30. Les VVA peuvent capturer accidentellement un message audio de personnes qui n'avaient pas l'intention d'utiliser un service de VVA. Premièrement, dans une certaine mesure et en fonction des VVA, l'expression de réveil peut être modifiée. Les personnes qui n'ont pas connaissance de ce changement pourraient utiliser accidentellement la nouvelle expression de réveil. Deuxièmement, il se peut que les VVA détectent l'expression de réveil par erreur ou en effectuant une faute. Il est très peu probable que l'une ou l'autre des exceptions prévues à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» soit applicable en cas d'activation accidentelle. En outre, le consentement tel que défini dans le RGPD doit être la «*manifestation de volonté [...] univoque [de] la personne concernée*». Il est donc très peu probable qu'une activation accidentelle puisse être interprétée comme un consentement valide. Si les responsables du traitement de données se rendent compte (par exemple, lors d'un examen automatisé ou manuel) que le service de VVA a accidentellement traité des données à caractère personnel, ils devraient vérifier qu'il existe une base juridique valable pour chaque finalité du traitement de ces données. Dans le cas contraire, les données recueillies accidentellement devraient être supprimées.

31. En outre, il convient de noter que les données à caractère personnel traitées par les VVA peuvent revêtir un caractère très sensible. Il peut s'agir de données à caractère personnel tant

[12] Il est possible que les futurs dispositifs de VVA adoptent le paradigme de l'informatique de périphérie (de l'anglais «edge computing») et soient capables de fournir certains services localement. En pareil cas, il sera nécessaire de réévaluer l'applicabilité de la directive «vie privée et communications électroniques».
[13] Voir également les lignes directrices 1/2020 du CEPD, paragraphe 14.

dans leur contenu (signification du texte parlé) que dans leurs métadonnées (sexe ou âge du locuteur, etc.). Le CEPD rappelle que les données vocales sont intrinsèquement des données à caractère personnel biométriques[14]. Par conséquent, lorsque ces données sont traitées dans le but d'identifier une personne physique de manière unique ou sont intrinsèquement des données à caractère personnel de catégorie particulière ou sont considérées comme telles, le traitement doit relever d'une base juridique valable en vertu de l'article 6 et s'accompagner d'une dérogation tel que prévue à l'article 9 du RGPD (voir section 3.7 ci-après).

3.2 Identification du traitement des données et des parties prenantes

32. Compte tenu des multiples possibilités d'assistance qu'offre un VVA dans autant d'environnements différents de la vie quotidienne d'une personne concernée[15], il convient d'accorder une attention toute particulière au traitement des données à caractère personnel, qui peut également être influencé par différentes parties prenantes.

3.2.1 Traitement des données à caractère personnel

33. Du point de vue de la protection des données à caractère personnel, plusieurs constantes peuvent être observées quel que soit le type de VVA (c'est-à-dire le type d'appareil, les fonctionnalités, les services ou leur combinaison) qui peut être utilisé par une personne concernée. Ces constantes ont trait à la pluralité des données à caractère personnel, des personnes concernées et des traitements de données en jeu.

Pluralité des types de données à caractère personnel

34. La définition des données à caractère personnel au sens de l'article 4, paragraphe 1, du RGPD englobe un large éventail de données différentes et s'applique, dans un contexte de neutralité technologique, à toute information qui concerne «*une personne physique identifiée ou identifiable*»[16]. Toute interaction d'une personne concernée avec un VVA peut relever du champ d'application de cette définition. Une fois que l'interaction a eu lieu, divers types de données à caractère personnel peuvent être traités tout au long de l'exploitation du VVA, comme décrit à la section 2.4.

35. De la demande initiale à la réponse, à l'action ou au suivi correspondants (par exemple, mise en place d'une alerte hebdomadaire), la première saisie de données à caractère personnel générera donc des données à caractère personnel subséquentes. Cela inclut les données primaires (par exemple, données de compte, enregistrements vocaux, historique des demandes), les données observées (par exemple, données d'un appareil qui se rapportent à une personne concernée, journaux d'activité, activités en ligne), ainsi que les données

[14] Conformément à l'article 4, paragraphe 14, du RGPD, on entend par données biométriques les «données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques».

[15] Par exemple: à domicile, dans un véhicule, dans la rue, au travail ou dans tout autre espace privé, public ou professionnel, ou dans une combinaison de ces espaces.

[16] L'article 4, paragraphe 1, du RGPD précise également qu'une personne physique identifiable est «*une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*».

déduites ou dérivées (par exemple, l'établissement du profil des utilisateurs). Les VVA utilisent la parole pour assurer les échanges entre les utilisateurs et tous les services connectés (par exemple, un moteur de recherche, une boutique en ligne ou un service de diffusion de musique), mais contrairement à d'autres intermédiaires, les VVA peuvent avoir pleinement accès au contenu des demandes et, par conséquent, fournir au concepteur du VVA un large éventail de données à caractère personnel en fonction des finalités du traitement.

36. La pluralité des données à caractère personnel traitées lors de l'utilisation d'un VVA fait également référence à une pluralité de catégories de données à caractère personnel auxquelles une attention toute particulière devrait être accordée (voir section 3.7 ci-après). Le CEPD rappelle que lorsque des catégories particulières de données[17] sont traitées, l'article 9 du RGPD exige du responsable du traitement qu'il identifie une dérogation valable à l'interdiction de traitement prévue à l'article 9, paragraphe 1, et une base juridique valable en vertu de l'article 6, paragraphe 1, en utilisant un moyen approprié défini à l'article 9, paragraphe 2. Le consentement explicite peut constituer une dérogation appropriée lorsque le consentement est la base juridique invoquée en vertu de l'article 6, paragraphe 1. L'article 9 fait également observer (en détail) que les États membres peuvent introduire des conditions supplémentaires pour le traitement des données biométriques ou d'autres catégories particulières de données.

Pluralité des personnes concernées

37. Lors de l'utilisation d'un VVA, les données à caractère personnel sont traitées dès la première interaction avec le VVA. Pour certaines personnes concernées, il s'agit de l'achat d'un VVA et/ou de la configuration d'un compte utilisateur (c'est-à-dire les utilisateurs enregistrés). Pour d'autres personnes concernées, il s'agit de la première fois qu'elles interagissent sciemment avec le VVA d'une autre personne concernée qui a acheté et/ou configuré ce VVA (c'est-à-dire les utilisateurs non enregistrés). Outre ces deux catégories de personnes concernées, il existe une troisième catégorie: les utilisateurs accidentels qui, enregistrés ou non, adressent des demandes au VVA à leur insu (par exemple, en prononçant la bonne expression de réveil sans savoir que le VVA est actif, ou en prononçant d'autres termes que le VVA reconnaît erronément comme étant l'expression de réveil).

38. Les termes pluralité des personnes concernées désignent également plusieurs utilisateurs pour un VVA (par exemple, un appareil partagé entre des utilisateurs enregistrés et non enregistrés, entre des collègues, dans une famille ou à l'école) et différents types d'utilisateurs en fonction de leur condition (par exemple, un adulte, un enfant, une personne âgée ou une personne handicapée). Bien qu'un VVA puisse garantir une interaction simplifiée avec un outil numérique et apporter de nombreux avantages pour certaines catégories de personnes concernées, il importe de tenir compte des spécificités propres à chaque catégorie de personnes concernées et du contexte dans lequel le VVA est utilisé.

Pluralité des traitement de données

[17] L'article 9, paragraphe 1, du RGPD définit les «catégories particulières de données à caractère personnel» comme des «*données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique [...]*».

39. Les technologies employées pour fournir un VVA ont également une incidence sur la quantité de données traitées et sur les types de traitement. Plus un VVA fournit de services ou présente de fonctionnalités et est connecté à d'autres dispositifs ou services gérés par d'autres parties, plus la quantité de données à caractère personnel traitées et réaffectées à d'autres finalités augmente. Il en résulte une pluralité de traitements effectués par des moyens automatisés, comme décrit à la section 2. Outre les moyens automatisés, certains traitements peuvent également impliquer des moyens humains. C'est le cas, par exemple, lorsque la technologie mise en œuvre suppose une intervention humaine, comme la révision de la transcription des paroles en textes ou la fourniture d'annotations sur des données à caractère personnel qui peuvent être utilisées pour insérer de nouveaux modèles dans une technologie d'apprentissage automatique. C'est également le cas lorsque des êtres humains analysent des données à caractère personnel (par exemple, des métadonnées) afin d'améliorer le service fourni par un VVA.

3.2.2 Traitement par les responsables du traitement et les sous-traitants

40. Les personnes concernées devraient être en mesure de comprendre et de déterminer les rôles en jeu et devraient pouvoir contacter chaque partie prenante ou agir envers chacune d'entre elles, comme l'exige le RGPD. La répartition des rôles ne devrait pas se faire au détriment des personnes concernées, même si les scénarios peuvent être compliqués ou susceptibles d'évoluer. Afin d'évaluer leurs rôles, les parties prenantes sont renvoyées aux lignes directrices 7/2020 du CEPD sur les notions de responsable du traitement et de sous-traitant dans le RGPD[18].

41. Comme indiqué au paragraphe 15, les principales parties prenantes peuvent être définies sous le rôle de fournisseur ou de concepteur, de développeur d'applications, d'intégrateur, de propriétaire ou d'une combinaison de ces rôles. Différents scénarios sont possibles en fonction des rôles définis dans la relation professionnelle des parties prenantes, de la demande de l'utilisateur, des données à caractère personnel, des activités de traitement des données et de leurs finalités. Elles devraient clairement décider des conditions dans lesquelles chacune d'entre elles agira et en informer les personnes concernées, ainsi que se conformer aux rôles correspondants de responsables de traitements, de responsables conjoints de traitements ou de sous-traitants, comme le prévoit le RGPD[19]. Chacune d'elles peut assumer un ou plusieurs rôles, car elles peuvent remplir la fonction de responsable du traitement des données, de responsable conjoint du traitement ou de sous-traitant pour un certain traitement de données, et assumer une autre position pour un autre traitement de données.

42. D'un point de vue général, le concepteur peut agir en tant que responsable du traitement lorsqu'il détermine les finalités et les moyens d'un traitement, mais peut intervenir comme sous-traitant lorsqu'il traite des données à caractère personnel pour le compte d'autres parties telles qu'un développeur d'applications. L'utilisateur du VVA serait donc soumis à plusieurs responsables de traitements: le développeur de l'application et le concepteur. Il est également possible que le concepteur, l'intégrateur et le développeur soient regroupés en un seul organe agissant en tant que responsable unique du traitement des données. Dans tous les cas, les qualifications applicables doivent être établies sur la base d'une analyse au cas par cas.

[18] Lignes directrices 07/2020 du CEPD sur les notions de responsable du traitement et de sous-traitant dans le RGPD, V2.0, adoptées le 7 juillet 2021 (ci-après les «lignes directrices 7/2020»).
[19] Articles 12 à 14, article 26 du RGPD.

Exemple 1:

Le concepteur du VVA traite les données des utilisateurs pour de nombreuses finalités, notamment pour améliorer les compétences de compréhension vocale du VVA et répondre avec précision aux demandes. Par conséquent, même si cette finalité peut conduire au traitement de données résultant de l'utilisation d'applications fournies par des tiers, il n'existe qu'un seul responsable du traitement: le concepteur du VVA, pour le compte duquel le traitement est effectué en tenant compte de ses finalités.

Exemple 2:

Une banque propose à ses clients une application qui peut être directement interrogée par l'intermédiaire du VVA afin de gérer leurs comptes.

Deux acteurs participent au traitement des données à caractère personnel: le concepteur du VVA et le développeur de l'application bancaire.

Dans le scénario présenté, la banque est responsable du traitement des données pour la prestation du service, puisqu'elle détermine les finalités et les principaux moyens de traitement liés à l'application permettant d'interagir avec l'assistant. En effet, elle propose une application spécifique qui permet à l'utilisateur, client de la banque, de gérer ses comptes à distance. En outre, elle décide des moyens de traitement en choisissant le sous-traitant approprié, à savoir le concepteur du VVA, et peut jouer un rôle important en offrant son expertise pour déterminer ces moyens (par exemple, elle peut exploiter la plateforme de développement qui permet l'intégration d'applications tierces dans le VVA, et fixe ainsi le cadre et les conditions que doivent respecter les développeurs d'applications).

43. Du côté de la personne concernée, il convient de noter que plusieurs parties prenantes peuvent traiter les mêmes données à caractère personnel, même si la personne concernée ne s'attend pas réellement à ce que d'autres parties que le fournisseur de VVA soient associées à la chaîne de traitement. Ainsi, lorsqu'une personne concernée interagit avec le fournisseur de VVA en ce qui concerne ses données à caractère personnel (par exemple, l'exercice de ses droits), cela ne signifie pas automatiquement que cette action s'appliquera aux mêmes données à caractère personnel qui sont traitées par une autre partie prenante. Lorsque ces parties prenantes sont des responsables de traitements indépendants, il est important qu'une notice d'informations claires expliquant les différentes étapes et les différents acteurs du traitement soit donnée aux personnes concernées. En outre, en cas de responsabilité conjointe, il convient de clarifier si chaque responsable du traitement est compétent pour veiller au respect de tous les droits de la personne concernée ou de définir le responsable du traitement compétent pour chaque droit[20].

Exemple 3:

Dans ce scénario, le concepteur du VVA souhaite utiliser les données collectées et traitées pour le service fourni par la banque afin d'améliorer son système de reconnaissance vocale.

[20] Lignes directrices 7/2020, paragraphe 165.

Le concepteur du VVA, qui traite les données pour ses propres finalités, aura alors le statut de responsable du traitement pour ce traitement spécifique.

44. Étant donné que de nombreuses parties prenantes peuvent contribuer à la chaîne de traitement, et respectivement plusieurs membres du personnel, des situations risquées peuvent se présenter si aucunes mesures ni garanties appropriées ne sont mises en place. Les responsables du traitement doivent répondre de celles-ci et devraient donc porter une attention particulière à la protection des données à caractère personnel, notamment en choisissant des partenaires commerciaux et des sous-traitants de données appropriés, en appliquant les principes de protection de la vie privée par défaut et dès la conception[21], en mettant en œuvre des outils de sécurité adéquats et d'autres outils du RGPD tels que les audits et les accords juridiques (par exemple, l'article 26 pour les responsables conjoints du traitement ou l'article 28 du RGPD pour les sous-traitants).

45. L'écosystème des VVA est un environnement complexe, dans lequel de nombreux acteurs peuvent être amenés à échanger et traiter des données à caractère personnel en tant que responsables de traitements ou sous-traitants de données. Il est de la plus haute importance que le rôle de chaque acteur à l'égard de chaque traitement soit clarifié et que le principe de minimisation des données soit respecté, aussi en ce qui concerne l'échange de données.

46. En outre, les responsables du traitement devraient être vigilants vis-à-vis des transferts de données à caractère personnel et garantir le niveau de protection requis tout au long de la chaîne de traitement, en particulier lorsqu'ils utilisent des services situés en dehors de l'EEE.

3.3 Transparence

47. Étant donné que les VVA traitent des données à caractère personnel (par exemple, la voix, la localisation ou le contenu de la communication des utilisateurs), ils doivent respecter les exigences de transparence du RGPD telles que définies à l'article 5, paragraphe 1, point a), ainsi qu'à l'article 12 et à l'article 13 (éclairés par le considérant 58). Les responsables du traitement sont tenus d'informer les utilisateurs du traitement de leurs données à caractère personnel sous une forme concise, transparente, compréhensible et aisément accessible.

48. Le fait de ne pas fournir les informations nécessaires constitue un manquement aux obligations susceptible d'affecter la légitimité du traitement des données. Le respect de l'exigence de transparence est un impératif, car elle sert de mécanisme de contrôle du traitement des données et permet aux utilisateurs d'exercer leurs droits. Informer correctement les utilisateurs sur la manière dont leurs données à caractère personnel sont utilisées complique, pour les responsables du traitement, l'emploi abusif du VVA à des fins qui vont bien au-delà des attentes des utilisateurs. Par exemple, des technologies brevetées visent à déduire l'état de santé ainsi que l'état émotionnel de la voix d'un utilisateur et à adapter les services fournis en conséquence.

49. Le respect des exigences de transparence peut être particulièrement difficile pour le fournisseur de services de VVA ou toute autre entité agissant en tant que responsable du traitement des données. Compte tenu de la nature spécifique des VVA, les responsables du traitement se heurtent à plusieurs obstacles pour se conformer aux exigences de transparence du RGPD:

[21] Voir lignes directrices 4/2019 du CEPD relatives à l'article 25 sur la protection des données dès la conception et par défaut, version 2.0, adoptées le 20 octobre 2020.

- **Utilisateurs multiples**: les responsables du traitement de données devraient informer tous les utilisateurs (utilisateurs enregistrés, non enregistrés et accidentels), et pas seulement l'utilisateur qui installe le VVA.
- **Complexité des écosystèmes**: comme expliqué dans la section relative au contexte technologique, les identités et les rôles de ceux qui traitent des données à caractère personnel lors de l'utilisation d'un VVA sont loin d'être évidents pour les utilisateurs.
- **Spécificités de l'interface vocale**: les systèmes numériques ne sont pas encore adaptés aux interactions uniquement vocales, comme le prouve l'usage quasi systémique d'un écran auxiliaire. Toutefois, il est nécessaire de s'adapter à l'interface vocale et de pouvoir informer l'utilisateur de manière claire et correcte par ce moyen.

50. Les VVA peuvent être considérés comme des machines à état défini qui passent par un certain nombre d'états au cours de leur fonctionnement normal. S'ils peuvent écouter localement pour détecter les expressions de réveil ou interagir avec un serveur à distance pour résoudre une commande, ils peuvent deviner de nombreux autres états en fonction du contexte (par exemple, s'il y a un bruit de fond) ou de l'utilisateur qui leur parle (par exemple, ils peuvent parler à un utilisateur identifié ou inconnu). Malheureusement, ces situations se déroulent dans une asymétrie informationnelle importante par rapport à l'utilisateur, qui ne se rend guère compte si l'appareil écoute et encore moins du statut qui est le sien.

51. Il est fortement recommandé que les concepteurs et développeurs de VVA prennent les mesures appropriées pour combler ces asymétries, en rendant le fonctionnement des VVA plus interactif. Les utilisateurs devraient être informés du statut actuel de l'appareil. Il est possible d'atteindre une meilleure transparence à la fois en rendant le dialogue entre l'homme et la machine plus interactif (par exemple, l'appareil peut confirmer d'une manière ou d'une autre la réception d'une commande vocale), ou en transmettant le statut de la machine avec des signaux spécifiques. De nombreuses options peuvent être examinées à cet égard, qu'il s'agisse de l'emploi de confirmations vocales spécifiques et d'icônes ou de lumières visibles, ou encore de l'utilisation d'affichages sur l'appareil.

52. Ces questions se révèlent particulièrement pertinentes compte tenu de la pluralité des utilisateurs et de la présence, parmi eux, de catégories de personnes vulnérables, telles que les enfants, les personnes âgées ou les personnes souffrant d'handicaps audiovisuels.

53. Deux questions importantes ressortent clairement de ce qui précède: quel est le moyen le plus réaliste d'informer les utilisateurs et quand est-il opportun de le faire? Ces questions méritent d'être examinées plus en détails dans deux situations différentes, selon que le VVA ne compte qu'un seul utilisateur (comme un téléphone intelligent personnel) ou potentiellement plusieurs utilisateurs (par exemple, un appareil domestique intelligent). Grâce à la technologie des VVA, une sous-version de ces deux paramètres de base pourrait également se présenter, par exemple lorsqu'un utilisateur possède un téléphone intelligent personnel et le connecte à une voiture. Le VVA du téléphone intelligent, dont on peut raisonnablement attendre qu'il soit uniquement utilisé par cet utilisateur, est désormais «étendu» aux autres personnes présentes dans la voiture.

54. Actuellement, tous les VVA sont connectés à un compte utilisateur et/ou sont installés par une application qui en requiert un. La question de savoir comment les responsables du traitement pourraient informer ces utilisateurs de la politique de confidentialité lors de la mise en place du VVA devrait être abordée, comme indiqué dans les lignes directrices du groupe de travail «Article 29» sur la transparence. Les applications devraient mettre les informations

nécessaires à disposition dans une boutique en ligne avant d'être téléchargées[22]. Ainsi, les informations sont communiquées le plus tôt possible et, au plus tard, au moment de l'obtention des données à caractère personnel. Certains fournisseurs de VVA incluent des applications tierces dans la configuration par défaut du VVA, de sorte que ces applications peuvent les exécuter en utilisant des expressions de réveil spécifiques. Les VVA qui utilisent cette stratégie de déploiement d'une application tierce devraient veiller à ce que les utilisateurs obtiennent également les informations nécessaires quant au traitement des données par des tiers.

55. Toutefois, de nombreux concepteurs de VVA requièrent des comptes utilisateurs de VVA qu'ils associent le service de VVA à de nombreux autres services tels que les courriers électroniques, les services de diffusion vidéo ou les achats pour n'en citer que quelques-uns. La décision du concepteur de VVA de relier le compte à de nombreux services différents a pour effet de nécessité des politiques de confidentialité très longues et complexes. La longueur et la complexité de ces politiques de confidentialité de la vie privée entravent considérablement le respect du principe de transparence.

> Exemple 4:
>
> Un concepteur de VVA requiert que ses utilisateurs disposent d'un compte pour accéder au service de VVA. Ce compte utilisateur n'est pas spécifique au service de VVA et peut être utilisé pour d'autres services proposés par le concepteur de VVA, tels que les courriers électroniques, le stockage en nuage et les médias sociaux. Pour créer le compte, les utilisateurs doivent lire et accepter une politique de confidentialité de 30 pages. La politique comprend des informations sur le traitement des données à caractère personnel par tous les services qui pourraient être liés au compte.
>
> Les informations fournies par le concepteur de VVA dans ce cas ne devraient pas être considérées comme concises, et leur complexité réduit la transparence requise. Par conséquent, le concepteur de VVA ne serait pas en conformité avec les exigences de transparence énoncées aux articles 12 et 13 du RGPD.

56. Bien que la manière la plus courante de fournir les informations nécessaires soit l'écrit, le RGPD autorise également «d'autres moyens». Le considérant 58 indique explicitement que les informations peuvent être fournies sous forme électronique, par exemple par l'intermédiaire d'un site web. En outre, il convient de tenir compte de circonstances spécifiques telles que la manière dont le responsable du traitement et la personne concernée interagissent l'un avec l'autre autrement, lorsqu'il s'agit de choisir la méthode appropriée pour informer les personnes concernées[23]. Pour les appareils dépourvus d'écran, une option pourrait consister à fournir un lien facile à comprendre, soit directement, soit dans un courriel. Les solutions déjà existantes pourraient servir d'exemple quant à la fourniture de l'information, par exemple les pratiques déployées par les centres d'appel, qui informent l'appelant qu'un appel téléphonique est enregistré et l'orientent vers la politique de confidentialité. Les contraintes posées par les VVA dépourvus d'écran ne dispensent pas le responsable du traitement de fournir les informations nécessaires conformément au RGPD lors de la mise en place du VVA ou encore de l'installation ou de l'utilisation d'une application de VVA. Les fournisseurs et

[22] Lignes directrices sur la transparence au titre du règlement 2016/679, WP260 rév. 01, approuvées par le CEPD (ci-après les «lignes directrices WP260 du GT29»), paragraphe 11.
[23] Lignes directrices WP260 du GT29, paragraphe 19.

développeurs de VVA devraient développer des interfaces vocales afin de faciliter la communication des informations obligatoires.

57. Les VVA pourraient présenter un grand intérêt pour les utilisateurs malvoyants, dans la mesure où ils offrent un moyen d'interaction alternatif avec les services informatiques qui s'appuient traditionnellement sur des informations visuelles. Conformément à l'article 12, paragraphe 1, du RGPD, la communication orale des informations nécessaires n'est possible que si la personne concernée en fait la demande, mais n'est pas employée comme méthode par défaut. Toutefois, les contraintes posées par les VVA dépourvus d'écran nécessiteraient de recourir à des outils d'information verbale automatisée, qui pourraient être compléter par des supports écrits. Lorsqu'ils utilisent un message audio pour informer les personnes concernées, les responsables du traitement devraient fournir les informations nécessaires d'une manière concise et claire. En outre, les personnes concernées devraient pouvoir être en mesure de les réécouter[24].

58. Il est plus complexe de prendre les mesures appropriées en vue de se conformer aux exigences de transparence du RGPD lorsqu'il y a plusieurs utilisateurs du VVA autres que le propriétaire de l'appareil. Les concepteurs de VVA doivent réfléchir à la manière d'informer correctement les utilisateurs non-enregistrés et accidentels lors du traitement de leurs données à caractère personnel. Lorsque le consentement constitue la base juridique du traitement des données des utilisateurs, ces derniers doivent être correctement informés pour que le consentement soit valide[25].

59. Afin de se conformer au RGPD, les responsables du traitement devraient trouver un moyen d'informer non seulement les utilisateurs enregistrés, mais aussi les utilisateurs non-enregistrés et les utilisateurs accidentels du VVA. Ces utilisateurs devraient être informés le plus rapidement possible **et <u>au plus tard au moment du</u>** traitement. Dans la pratique, cette condition peut être particulièrement difficile à remplir.

60. Certaines spécificités du monde des entreprises ne devraient pas non plus porter préjudice aux personnes concernées. Étant donné que de nombreuses parties prenantes sont des entreprises mondiales ou sont bien connues pour une activité commerciale spécifique (par exemple, télécommunications, commerce électronique, technologies de l'information, activités web), la manière dont elles fournissent un service de VVA devrait être claire. Des informations adéquates devraient permettre aux personnes concernées de comprendre si leur utilisation du VVA impliquera ou non d'autres activités de traitement gérées par le prestataire de services de VVA (par exemple, télécommunications, commerce électronique, technologies de l'information ou activités web) en dehors de l'utilisation stricte du VVA.

> Exemple 5:
>
> Pour utiliser son assistant, un concepteur de VVA, qui fournit également une plateforme de médias sociaux et un moteur de recherche, exige de l'utilisateur qu'il/elle relie son compte à l'assistant. Si l'utilisateur relie son compte à l'utilisation du VVA, le concepteur peut ainsi améliorer le profil de ses utilisateurs grâce à l'usage qui est fait de l'assistant, aux applications (ou compétences) qui sont installées, aux commandes passées, etc. De ce fait, les interactions de l'assistant constituent une nouvelle source d'information attachée à un utilisateur. Le concepteur de VVA devrait fournir aux utilisateurs des informations claires sur

[24] Lignes directrices WP260 du GT29, paragraphe 21.

[25] Article 4, paragraphe 11, du RGPD.

la manière dont leurs données seront traitées pour chaque service et proposer des commandes permettant à l'utilisateur de choisir si les données seront utilisées ou non pour établir un profil.

Recommandations

61. Lorsque les utilisateurs sont informés que le VVA traite des données à caractère personnel dans la politique de confidentialité d'un compte utilisateur, et que le compte est lié à d'autres services indépendants (par exemple, le courrier électronique ou les achats en ligne), le CEPD recommande que la politique de confidentialité comporte une section clairement séparée concernant le traitement des données à caractère personnel par le VVA.

62. Les informations fournies à l'utilisateur devraient correspondre à la collecte et au traitement exacts qui sont effectués. Si certaines métadonnées sont contenues dans un échantillon vocal (par exemple, niveau de stress du locuteur), il n'est pas automatiquement clair qu'une telle analyse est effectuée. Il est essentiel que les responsables du traitement fassent preuve de transparence quant aux aspects spécifiques des données brutes qu'ils traitent.

63. En outre, le statut du VVA devrait être clair à tout moment. Les utilisateurs devraient être en mesure de déterminer si un VVA est actuellement à l'écoute, en circuit fermé et, en particulier, s'il envoie des informations en flux continu en arrière-plan. Ces informations devraient également être accessibles aux personnes ayant des handicaps tels que le daltonisme ou la surdité (anacousie). Il convient d'accorder une attention toute particulière au fait que les VVA proposent un scénario d'utilisation ne nécessitant pas de contact visuel avec le dispositif. Par conséquent, tous les retours utilisateurs, y compris les changements d'état, devraient être disponibles au moins sous forme visuelle et acoustique.

64. Il convient d'accorder une attention particulière aux dispositifs permettant l'ajout de fonctionnalités tierces («applications» pour les VVA). Si certaines informations générales peuvent être fournies à l'utilisateur lorsqu'il ajoute cette fonctionnalité (en considérant que c'est son choix), les frontières entre les différents responsables de traitements concernés peuvent être beaucoup moins claires dans le cadre d'une utilisation normale de l'appareil, c'est-à-dire, il est possible que l'utilisateur ne soit pas suffisamment informé tant sur les personnes qui traitent ses données que sur la manière dont elles le sont (et dans quelle mesure elles le sont) pour une requête spécifique.

65. Toutes les informations relatives au traitement fondé sur les données collectées et dérivées du traitement des voix enregistrées devraient également être mises à la disposition des utilisateurs conformément à l'article 12 du RGPD.

66. Les responsables du traitement de VVA devraient rendre transparents les types d'informations qu'un VVA peut obtenir au sujet de son environnement, par exemple – mais pas exclusivement – concernant les autres personnes présentes dans la pièce, la musique de fond, tout traitement de la voix pour des raisons médicales ou d'autres raisons commerciales, les animaux de compagnie, etc.

3.4 Limitation de la finalité et base juridique

67. Si le traitement des demandes vocales par les VVA a une finalité évidente, à savoir l'exécution de la demande, il existe souvent d'autres finalités qui ne sont pas aussi évidentes, comme l'amélioration des capacités de compréhension du langage naturel du VVA en entraînant le

modèle de VVA aux techniques d'apprentissage automatique. Parmi les finalités les plus courantes pour le traitement des données à caractère personnel par les VVA figurent:

- l'exécution des demandes des utilisateurs;
- l'amélioration du VVA, en entraînant le modèle d'apprentissage automatique ainsi qu'en examinant et en étiquetant manuellement les transcriptions vocales;
- l'identification de l'utilisateur (à l'aide de données vocales);
- l'établissement du profil de l'utilisateur pour le contenu personnalisé ou la publicité.

68. En raison de leur rôle d'intermédiaires et de la manière dont ils sont conçus, les VVA traitent un large éventail de données à caractère personnel et non personnel. Cela permet de traiter des données à caractère personnel pour de nombreuses finalités, qui dépassent celle consistant à répondre aux demandes des utilisateurs et qui pourrait passer totalement inaperçues. En analysant les données collectées au moyen des VVA, il est possible de connaître ou de déduire les intérêts, les horaires, les trajets en voiture ou les habitudes des utilisateurs. Cela pourrait permettre le traitement de données à caractère personnel à des fins non prévues (par exemple, l'analyse des sentiments ou l'évaluation de l'état de santé[26]), ce qui irait bien au-delà des attentes raisonnables des utilisateurs.

69. Les responsables du traitement devraient clairement préciser leur(s) finalité(s) par rapport au contexte dans lequel le VVA est utilisé, de manière à ce qu'elles soient clairement comprises par les personnes concernées (par exemple, en présentant les finalités par catégorie). Conformément à l'article 5, paragraphe 1, du RGPD, les données à caractère personnel devraient être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

3.4.1 Exécuter les demandes des utilisateurs

70. L'utilisation principale d'un VVA consiste à émettre des commandes vocales qui doivent être exécutées par le VVA ou une application ou un service associé (par exemple, un service de diffusion de musique, un service de cartographie ou un verrouillage électronique). La voix de l'utilisateur et éventuellement d'autres données (par exemple, la position de l'utilisateur lorsqu'il demande un itinéraire pour une destination donnée) pourraient donc être traitées.

> Exemple 6:
>
> Le passager d'une voiture intelligente comprenant un VVA demande un itinéraire vers la station-service la plus proche. Le VVA traite la voix de l'utilisateur pour comprendre la commande et la position de la voiture afin de trouver l'itinéraire, et l'envoie au composant intelligent pour qu'il l'affiche sur l'écran de la voiture.

71. Dans la mesure où le traitement des commandes vocales implique de conserver des informations stockées dans les terminaux de l'utilisateur final ou d'accéder à ces informations, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» doit être respecté. Si l'article 5, paragraphe 3, inclut le principe général selon lequel cette conservation ou cet accès requiert le consentement préalable de l'utilisateur final, il prévoit également une dérogation à l'obligation de consentement lorsqu'ils sont «strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé

[26] Eoghan Furey, Juanita Blue, «Alexa, Emotion, Privacy and GDPR», document de conférence, conférence sur l'interaction homme-machine, juillet [2018].

par l'abonné ou l'utilisateur». Étant donné que les données vocales sont traitées pour exécuter les demandes de l'utilisateur, elles sont exemptées de l'obligation de consentement préalable.

72. Comme indiqué précédemment, toute opération de traitement de données à caractère personnel subséquente à la conservation d'informations dans le terminal des utilisateurs finaux ou à l'accès à ces informations doit avoir une base juridique au titre de l'article 6 du RGPD pour être licite.

73. Deux opérations de traitement consécutives ont lieu en ce qui concerne le VVA. Comme indiqué auparavant, la première action requiert l'accès au VVA (et les conditions de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» doivent donc être remplies). Outre les conditions énoncées à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», la deuxième étape nécessite également une base juridique au titre de l'article 6 du RGPD.

74. Lorsqu'une personne décide d'utiliser un VVA, cette action implique généralement que l'utilisateur initial doit d'abord enregistrer un compte pour activer le VVA. En d'autres termes, cette situation fait référence à une relation contractuelle[27] entre l'utilisateur enregistré et le responsable du traitement du VVA. Compte tenu de son contenu et de son objectif fondamental, ce contrat a pour objet principal d'utiliser le VVA pour exécuter la demande d'assistance de l'utilisateur.

75. Tout traitement de données à caractère personnel nécessaire pour répondre à la demande de l'utilisateur peut par conséquent se fonder sur la base juridique de l'exécution du contrat[28]. Ce traitement comprend notamment la capture de la demande vocale de l'utilisateur, sa transcription en texte, son interprétation, les informations échangées avec des sources de connaissances pour préparer la réponse, puis la transcription en une réponse vocale finale qui met fin à la demande de l'utilisateur.

76. L'exécution d'un contrat peut constituer une base juridique pour le traitement de données à caractère personnel au moyen de l'apprentissage automatique lorsque cela est nécessaire à la fourniture du service. Le traitement de données à caractère personnel qui utilise l'apprentissage automatique pour d'autres finalités qui ne sont pas nécessaires, telles que l'amélioration du service, ne devrait pas s'appuyer sur cette base juridique.

77. Enfin, et surtout, il convient de ne pas confondre les bases juridiques de l'exécution du contrat et du consentement au titre du RGPD. Le consentement donné pour conclure le contrat, c'est-à-dire pour l'accepter, fait partie des conditions de validité de ce contrat et ne fait pas référence à la signification spécifique du consentement au sens du RGPD[29].

78. Lorsqu'il n'est pas nécessaire de configurer au préalable un compte utilisateur pour utiliser un VVA, le consentement peut constituer une base juridique possible.

---

[27] Sous réserve de la «*validité du contrat en vertu du droit national des contrats applicable*», extrait des lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées (ci-après les «lignes directrices 2/2019»), paragraphe 26.

[28] Conformément aux lignes directrices 2/2019, qui indiquent en outre que l'avis 06/2014 reste pertinent au regard de l'article 6, paragraphe 1, point b), et du RGPD (voir en particulier les pages 11, 16, 17, 18 et 55 de cet avis 06/2014).

[29] Voir les lignes directrices 2/2019, respectivement paragraphes 18, 19, 20, 21 et 27.

3.4.2 Améliorer le VVA en entraînant les systèmes d'apprentissage automatique et en examinant manuellement les voix et les transcriptions

79. Les accents et les variations du langage humain sont considérables. Si tous les VVA sont fonctionnels une fois sortis de leur boîte, leurs performances peuvent s'améliorer en les adaptant aux caractéristiques propres au langage des utilisateurs. Comme indiqué au paragraphe 2.6, ce processus d'ajustement repose sur des méthodes d'apprentissage automatique et se compose de deux composantes: l'ajout de nouvelles données collectées auprès de ses utilisateurs à l'ensemble de données d'entraînement du VVA et l'examen manuel des données traitées pour exécuter une fraction des demandes.

> Exemple 7:
>
> Un utilisateur de VVA doit émettre trois fois la même commande vocale parce que le VVA ne la comprend pas. Les trois commandes vocales et les transcriptions associées sont transmises aux examinateurs humains afin qu'ils examinent et corrigent les transcriptions. Les commandes vocales et les transcriptions révisées sont ajoutées à l'ensemble de données d'entraînement du VVA afin d'améliorer ses performances.

80. Les activités de traitement décrites dans cet exemple ne devraient pas être considérées comme (strictement) «*nécessaires à l'exécution d'un contrat*» au sens de l'article 6, paragraphe 1, point b), du RGPD, et requièrent donc une autre base juridique de l'article 6 du RGPD. Cela s'explique principalement par le fait que les VVA sont déjà fonctionnels lorsqu'ils sortent de leur boîte et peuvent déjà fonctionner en opérant des traitements (strictement) nécessaires à l'exécution du contrat. Le CEPD ne considère pas que l'article 6, paragraphe 1, point b), constituerait généralement une base juridique appropriée pour un traitement destiné à améliorer un service ou à développer de nouvelles fonctions au sein d'un service existant. Dans la plupart des cas, un utilisateur conclut un contrat pour bénéficier d'un service existant. Si la possibilité d'apporter des améliorations ou des modifications à un service peut être régulièrement intégrée aux termes du contrat, un tel traitement ne peut généralement pas être considéré comme objectivement nécessaire à l'exécution du contrat conclu avec l'utilisateur.

3.4.3 Identification[30] de l'utilisateur (à l'aide de données vocales)

81. L'utilisation de données vocales pour l'identification de l'utilisateur suppose le traitement de données biométriques telles que définies à l'article 4, paragraphe 14, du RGPD. Par conséquent, le responsable du traitement devra définir une dérogation au titre de l'article 9 du RGPD en plus de l'identification d'une base juridique au titre de l'article 6 du RGPD[31].

[30] Techniquement, la notion d'identification doit se distinguer de la vérification (authentification). L'identification est une recherche et une comparaison de type multilatéral (1: N) et nécessite en principe une base de données dans laquelle plusieurs individus sont répertoriés. En revanche, le traitement à des fins de vérification est une comparaison unilatérale (1:1) et sert à vérifier et à confirmer, par une comparaison biométrique, si un individu est la même personne que celle de laquelle proviennent les données biométriques. À la connaissance du CEPD, les VVA sur le marché se fondent sur le seul recours aux technologies d'identification du locuteur.

[31] Il est considéré, dans le RGPD, que la simple nature des données n'est pas toujours suffisante pour déterminer si elles constituent des catégories particulières de données, étant donné que «*le traitement des photographies […] ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique*» (considérant 51). Le même raisonnement s'applique à la voix.

82. Parmi les exemptions énumérées à l'article 9 du RGPD, seul le consentement explicite des personnes concernées semble applicable à cette fin spécifique.

83. Toutefois, étant donné que cet objectif exige l'application du régime juridique spécifique prévu à l'article 9 du RGPD, de plus amples détails figurent à la section 3.8 concernant le traitement des catégories particulières de données.

3.4.4 L'établissement du profil de l'utilisateur pour le contenu personnalisé ou la publicité

84. Comme indiqué précédemment, les VVA ont accès au contenu de toutes les commandes vocales, même lorsqu'elles sont destinées à des services fournis par des tiers. Cet accès permet au concepteur de VVA de construire des profils d'utilisateur très précis qui peuvent être utilisés pour proposer des services ou des publicités personnalisés.

> Exemple 8:
>
> Chaque fois qu'un utilisateur de VVA effectue une recherche sur l'internet, le VVA ajoute des étiquettes signalant les sujets d'intérêt au profil de l'utilisateur. Les résultats de chaque nouvelle recherche sont présentés à l'utilisateur, dans un ordre tenant compte de ces étiquettes.
>
> Exemple 9:
>
> Chaque fois qu'un utilisateur de VVA effectue un achat auprès d'un service de commerce électronique, le VVA conserve un enregistrement du bon de commande. Le fournisseur de VVA permet à des tiers d'atteindre l'utilisateur du VVA au moyen de publicités ciblées en fonction des achats précédents.

85. La personnalisation du contenu peut (mais pas toujours) constituer un élément intrinsèque et attendu d'un VVA. La question de savoir si un tel traitement peut être considéré comme un aspect intrinsèque d'un service de VVA dépendra de la nature précise du service fourni, des attentes de la personne concernée moyenne au regard non seulement des conditions du service, mais aussi de la manière dont le service est promu auprès des utilisateurs, ainsi que de la question de savoir si ce service peut être fourni sans personnalisation[32].

86. Lorsque la personnalisation se déroule dans le cadre d'une relation contractuelle et d'un service explicitement demandé par l'utilisateur final (et que le traitement est limité à ce qui est strictement nécessaire pour fournir ce service), ce traitement peut être fondé sur l'article 6, paragraphe 1, point b), du RGPD.

87. Si le traitement n'est pas strictement «*nécessaire à l'exécution d'un contrat*» au sens de l'article 6, paragraphe 1, point b), du RGPD, le fournisseur de VVA doit, en principe, demander le consentement de la personne concernée. En effet, étant donné que le consentement sera requis en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» pour conserver des informations ou obtenir l'accès à ces dernières (voir paragraphes 28 et 29 ci-dessus), le consentement au titre de l'article 6, paragraphe 1, point a), du RGPD constituera également, en principe, la base juridique appropriée pour le traitement de données à caractère personnel à la suite de ces opérations, puisque l'invocation d'un intérêt

[32] Voir également les lignes directrices 2/2019, paragraphe 57.

légitime pourrait, dans certains cas, porter atteinte au niveau supplémentaire de protection prévu à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

88. En ce qui concerne l'établissement du profil des utilisateurs à des fins de publicité, il convient de noter que cette finalité n'est jamais considérée comme un service explicitement demandé par l'utilisateur final. Par conséquent, en cas de traitement à cette fin, le consentement des utilisateurs devrait être systématiquement recueilli.

Recommandations

89. Les utilisateurs devraient être informés de la finalité du traitement des données à caractère personnel, et cette dernière devrait correspondre à leurs attentes vis-à-vis du dispositif qu'ils achètent. Dans le cas d'un VVA, cette finalité - du point de vue de l'utilisateur - est clairement le traitement de sa voix dans le seul but d'interpréter sa requête et d'apporter des réponses appropriées (qu'il s'agisse de réponses à une demande ou d'autres réactions telles que le contrôle à distance d'un interrupteur).

90. Lorsque le traitement des données à caractère personnel est fondé sur le consentement, ce consentement «*doit être donné en lien avec «une ou plusieurs finalités spécifiques» et que la personne concernée a un choix concernant chacune de ces finalités*». En outre, «*un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques*»[33]. Par exemple, les utilisateurs devraient être en mesure de donner leur consentement séparément ou non à l'examen et à l'étiquetage manuels des transcriptions vocales ou à l'utilisation de leurs données vocales pour l'identification/l'authentification de l'utilisateur (voir section 3.7).

3.5 Traitement des données des enfants

91. Les enfants peuvent également interagir avec les VVA ou créer leurs propres profils liés à ceux des adultes. Certains VVA sont intégrés dans des dispositifs spécifiquement destinés aux enfants.

92. Lorsque la base juridique du traitement est l'exécution d'un contrat, les conditions de traitement des données des enfants dépendront du droit national des contrats.

93. Conformément à l'article 8, paragraphe 1, du RGPD, lorsque la base juridique du traitement est le consentement, le traitement des données des enfants n'est licite que «*lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant*». Par conséquent, pour se conformer au RGPD, lorsque le consentement est la base juridique, il convient de demander aux parents ou aux tuteurs l'autorisation explicite de collecter, traiter et stocker les données des enfants (voix, transcriptions, etc.).

94. Les contrôles parentaux sont disponibles dans une certaine mesure, mais sous leur forme actuelle, ils ne sont pas conviviaux (par exemple, il est nécessaire de s'inscrire à un nouveau service) ou ont des capacités limitées. Les responsables du traitement de données devraient

[33] Voir les lignes directrices 05/2020 du CEPD sur le consentement en vertu du règlement 2016/679, adoptées le 4 mai 2020, section 3.2

investir dans le développement de moyens permettant aux parents ou aux tuteurs de contrôler l'utilisation des VVA par les enfants.

3.6 Conservation des données

95. Les VVA traitent et génèrent un large éventail de données à caractère personnel telles que la voix, les transcriptions vocales, les métadonnées ou les journaux système. Ces types de données pourraient être traités à des fins très diverses, telles que la fourniture d'un service, l'amélioration du TLN, la personnalisation ou la recherche scientifique. Conformément au principe de limitation de la conservation des données du RGPD, les VVA devraient stocker les données pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles les données à caractère personnel sont traitées. Par conséquent, les durées de conservation des données devraient être liées aux différentes finalités du traitement. Les fournisseurs de services de VVA ou les tiers fournissant des services par l'intermédiaire de VVA devraient évaluer la durée maximale de conservation pour chaque ensemble de données et pour chaque finalité.

96. Le principe de minimisation des données est étroitement lié au principe de la limitation de la conservation des données. Non seulement les responsables du traitement doivent limiter la durée de conservation des données, mais aussi le type et la quantité de données.

97. Les responsables du traitement de données devraient se poser, entre autres, les questions suivantes: Est-il nécessaire de conserver tous les enregistrements vocaux ou toutes les transcriptions pour atteindre la finalité X? Est-il nécessaire de conserver les données vocales une fois que la transcription a été stockée? Dans ce cas, pour quelle finalité? Pour combien de temps les données vocales ou les données de transcription sont-elles nécessaires à chaque finalité? La réponse à ces questions et à d'autres questions similaires définira les durées de conservation qui devraient faire partie des informations dont disposent les personnes concernées.

98. Certains VVA stockent par défaut des données à caractère personnel telles que des extraits vocaux ou des transcriptions pour une période indéterminée, tout en donnant aux utilisateurs les moyens de les effacer. La conservation illimitée des données à caractère personnel va à l'encontre du principe de limitation de la conservation. Donner aux personnes concernées les moyens de supprimer leurs données à caractère personnel n'enlève en rien au responsable du traitement, la responsabilité de définir et d'appliquer une politique de conservation des données.

99. Lors de la conception de VVA, il convient d'intégrer des commandes permettant aux utilisateurs d'effacer leurs données à caractère personnel dans leurs appareils et dans tous les systèmes de stockage à distance. Ces commandes peuvent s'avérer nécessaires pour répondre à différents types de demandes provenant des utilisateurs, par exemple une demande de suppression ou le retrait du consentement donné précédemment. Cette exigence n'a pas été prise en compte lors de la conception de certains VVA[34].

100. Comme dans d'autres contextes, les responsables du traitement peuvent avoir besoin de conserver des données à caractère personnel comme preuve d'un service fourni à un utilisateur pour se conformer à une obligation légale. Le responsable du traitement peut

[34] Voir la lettre d'Amazon du 28 juin 2019 en réponse au sénateur américain Christopher Coons: https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf

conserver des données à caractère personnel sur cette base. Toutefois, les données conservées devraient rester le minimum nécessaire pour se conformer à cette obligation légale et pour une durée minimale. Bien entendu, les données conservées dans le but se de conformer à une obligation légale ne devraient pas être utilisées à d'autres fins sans utiliser l'une des bases juridiques de l'article 6 du RGPD.

> Exemple 10:
>
> Un utilisateur achète une télévision auprès d'un service de commerce électronique au moyen d'une commande vocale délivrée à un VVA. Même si l'utilisateur demande par la suite la suppression de ses données, le fournisseur ou le développeur du VVA pourrait conserver certaines données en raison de l'obligation légale de conserver des preuves d'achat prévue par la réglementation fiscale. Toutefois, les données conservées à cette fin ne devraient pas dépasser le minimum nécessaire pour se conformer à l'obligation légale et ne peuvent être traitées à aucune autre fin sans utiliser l'une des bases juridiques de l'article 6 du RGPD.

101. Comme indiqué à la section 2, la capacité de reconnaissance vocale des VVA s'améliore grâce à l'entraînement des systèmes d'apprentissage automatique avec les données des utilisateurs. Si les utilisateurs ne consentent pas ou retirent leur consentement à l'utilisation de leurs données à cette fin, leurs données ne pourraient pas être légalement utilisées pour former un autre modèle et devraient être supprimées par le responsable du traitement, en supposant qu'il n'existe aucune autre finalité justifiant la poursuite de la conservation. Toutefois, il est prouvé qu'il peut y avoir des risques de ré-identification dans certains modèles d'apprentissage automatique.[35]

102. Les responsables du traitement et les sous-traitants ne devraient ni utiliser des modèles qui restreignent leur capacité à interrompre le traitement en cas de révocation du consentement par une personne, ni recourir à des modèles qui limitent leur capacité à favoriser les droits des personnes concernées. Les responsables du traitement et les sous-traitants devraient appliquer des mesures d'atténuation afin de réduire le risque de ré-identification à un seuil acceptable.

103. Si l'utilisateur retire son consentement, les données collectées auprès de l'utilisateur ne peuvent plus être utilisées pour poursuivre l'entraînement du modèle. Néanmoins, le modèle précédemment entraîné à l'aide de ces données ne doit pas être supprimé. Le CEPD souligne toutefois qu'il peut y avoir des risques de fuite de données à caractère personnel dans certains modèles d'apprentissage automatique. En particulier, de nombreuses études ont montré que des attaques visant à la reconstruction et à découvrir si un individu fait partie de la base de données d'entraînement peuvent être perpétrées, permettant aux attaquants de récupérer des informations sur les individus[36]. Les responsables du traitement et les sous-traitants devraient dès lors appliquer des mesures d'atténuation afin de réduire le risque de ré-identification à un seuil acceptable pour s'assurer qu'ils utilisent des modèles ne contenant pas de données à caractère personnel.

104. Les personnes concernées ne devraient pas être incitées à conserver leurs données indéfiniment. Bien que la suppression des données vocales ou des transcriptions stockées

[35] Veale Michael, Binns Reuben et Edwards Lilian, 2018, «Algorithms that remember: model inversion attacks and data protection law», Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083

[36] N. Carlini et al., «Extracting Training Data from Large Language Models», décembre 2020.

puisse avoir une incidence sur la performance du service, cette incidence devrait être expliquée aux utilisateurs de manière claire et mesurable. Les fournisseurs de services de VVA devraient éviter de faire des déclarations générales sur la dégradation du service après la suppression des données à caractère personnel.

105. L'anonymisation des enregistrements vocaux est particulièrement difficile, car il est possible d'identifier les utilisateurs grâce au contenu du message lui-même et aux caractéristiques de la voix elle-même. Néanmoins, des recherches[37] sont en cours sur des techniques qui pourraient supprimer les informations contextuelles, telles que les bruits de fond, et anonymiser la voix.

Recommandations

106. Du point de vue de l'utilisateur, la principale finalité du traitement de ses données est de poser des questions et de recevoir des réponses et/ou de déclencher des actions telles que jouer de la musique, allumer ou éteindre des lumières. Une fois qu'une requête a reçu une réponse ou qu'une commande a été exécutée, les données à caractère personnel devraient être supprimées, à moins que le concepteur ou le développeur de VVA ne dispose d'une base juridique valide pour les conserver à des fins spécifiques.

107. Avant d'envisager l'anonymisation comme un moyen de respecter le principe de limitation de la conservation des données, les fournisseurs et les développeurs de VVA devraient vérifier si le processus d'anonymisation rend bien la voix non identifiable.

108. Les paramètres par défaut de la configuration devraient refléter ces exigences en proposant par défaut un minimum absolu d'informations utilisateur stockées. Si ces options sont présentées dans le cadre d'un assistant de configuration, le paramétrage par défaut devrait en tenir compte, et toutes les options devraient être présentées comme des possibilités égales, sans discrimination visuelle.

109. Lorsque, au cours du processus d'examen, le fournisseur ou le développeur de VVA détecte un enregistrement provenant d'une activation erronée, l'enregistrement et toutes les données associées devraient être immédiatement supprimés et n'être utilisés à aucune fin.

3.7 Sécurité

110. Pour traiter en toute sécurité les données à caractère personnel, les VVA devraient protéger leur confidentialité, leur intégrité et leur disponibilité. Outre les risques liés aux éléments de l'écosystème des VVA, l'utilisation de la voix comme moyen de communication crée un nouvel ensemble de risques pour la sécurité.

111. Les VVA sont multi-utilisateurs: ils peuvent autoriser plus d'un utilisateur enregistré et quiconque se trouvant dans son environnement peut émettre des commandes et utiliser ses services. Chaque service de VVA exigeant de la confidentialité, impliquera un mécanisme de contrôle d'accès et une authentification de l'utilisateur. Sans contrôle d'accès, toute personne capable d'adresser des commandes vocales au VVA pourrait y accéder, modifier ou supprimer les données à caractère personnel de n'importe quel utilisateur (par exemple, demander les

[37] Voir à titre d'exemple VoicePrivacy (https://www.voiceprivacychallenge.org), une initiative visant à élaborer des solutions de protection de la vie privée pour les technologies vocales.
Voir également les outils d'anonymisation de la voix libres d'accès élaborés par le projet de recherche et d'innovation Horizon 2020 COMPRISE: https://gitlab.inria.fr/comprise/voice_transformation.

messages reçus, l'adresse de l'utilisateur ou des événements au calendrier). Il n'est pas nécessaire de se trouver à proximité immédiate du VVA pour émettre des commandes vocales car ces dernières peuvent être modifiées, par exemple par la diffusion de signaux[38] (radio ou télévision). Certaines des méthodes connues pour adresser à distance des commandes au VVA, comme les ondes laser[39] ou ultrasoniques (inaudibles)[40], ne sont même pas décelables par les sens de l'être humain.

112. L'authentification de l'utilisateur peut s'appuyer sur un ou plusieurs des facteurs suivants: un élément que vous connaissez (comme un mot de passe), un objet que vous possédez (comme une carte à puce) ou une donnée qui vous définit (comme une empreinte vocale). Un examen plus approfondi de ces facteurs d'authentification dans le contexte des VVA révèle que:

   - L'authentification à l'aide d'un élément que connaît l'utilisateur pose problème. Le secret qui permettrait aux utilisateurs de prouver leur identité devrait être prononcé à voix haute, l'exposant ainsi à toutes les personnes se trouvant dans les environs. Le canal de communication des VVA est l'air ambiant, un type de canal qui ne peut pas être fortifié comme les canaux traditionnels (par exemple, en limitant l'accès au canal ou en cryptant son contenu).

   - L'authentification à l'aide d'un objet que possède l'utilisateur obligerait les fournisseurs de services de VVA à créer, distribuer et gérer des «jetons» qui pourraient servir de preuve d'identité.

   - L'authentification par une donnée qui définit l'utilisateur suppose l'utilisation de données biométriques aux fins d'identifier de manière unique une personne physique (voir section 3.7 ci-après).

113. Les comptes utilisateurs de VVA sont associés aux appareils dans lesquels le service est fourni. Souvent, le même compte que celui utilisé pour gérer le VVA est employé pour gérer d'autres services. Par exemple, les propriétaires d'un téléphone mobile Android et d'une enceinte Google Home peuvent associer – et associent très probablement – leur compte Google aux deux appareils. La plupart des VVA n'exigent ni ne proposent aucun mécanisme d'identification ou d'authentification lorsqu'un appareil fournissant un service de VVA n'a qu'un seul compte utilisateur.

114. Lorsque plus d'un compte utilisateur est associé à l'appareil, certains VVA offrent la possibilité de mettre un contrôle d'accès de base sous la forme d'un code PIN sans véritable authentification de l'utilisateur. D'autres VVA ont pour option d'utiliser la reconnaissance de l'empreinte digitale comme mécanisme d'identification.

115. Bien que l'identification ou l'authentification de l'utilisateur ne soit pas nécessaire pour accéder à tous les services de VVA, elle le sera assurément pour certains. Sans mécanisme d'identification ou d'authentification, n'importe qui pourrait accéder aux données d'autres utilisateurs et les modifier ou les effacer à son gré. Par exemple, toute personne se trouvant à proximité d'une enceinte intelligente pourrait supprimer les listes de lecture d'autres

[38] X. Yuan et al., «All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo», Conférence mondiale sur les communications 2018 de l'IEEE (GLOBECOM), Abu Dhabi, Émirats arabes unis, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647762.

[39] Voir à titre d'exemple https://lightcommands.com

[40] Voir à titre d'exemple https://surfingattack.github.io

utilisateurs du service de diffusion de musique, les commandes de l'historique des commandes ou les contacts de la liste de contacts.

116. La plupart des VVA se fient aveuglément à leurs réseaux locaux. Tout dispositif compromis dans le même réseau pourrait modifier les paramètres de l'enceinte intelligente ou permettre l'installation de logiciels malveillants ou d'y associer de fausses applications/compétences à l'insu de l'utilisateur et sans son accord[41].

117. Comme tout autre logiciel, les VVA sont exposés à des vulnérabilités. Toutefois, en raison de la concentration du marché des VVA[42], toute vulnérabilité pourrait affecter des millions d'utilisateurs de VVA. S'ils fonctionnent comme prévu actuellement, les VVA n'envoient aucune information au service de reconnaissance vocale en nuage tant que l'expression de réveil n'est pas détectée. Néanmoins, des vulnérabilités logicielles pourraient permettre à un attaquant de contourner la configuration et les mesures de sécurité du VVA. Il serait alors possible, par exemple, d'obtenir une copie de toutes les données envoyées au nuage du VVA et de les transmettre à un serveur contrôlé par l'attaquant.

118. Les données licitement traitées ou obtenues par les VVA permettent d'établir un profil relativement précis de leurs utilisateurs, étant donné que les VVA connaissent ou peuvent déduire la localisation, les relations et les intérêts de leurs utilisateurs. Les VVA sont de plus en plus présents au sein des foyers et dans les téléphones intelligents des utilisateurs. Cette circonstance accroît le risque de surveillance de masse et de profilage de masse. Par conséquent, les mesures de sécurité visant à protéger les données tant en transit qu'au repos dans les appareils et dans le nuage devraient couvrir ces risques.

119. L'utilisation croissante des VVA, associée à des droits d'accès mal équilibrés par les autorités chargées de l'application de la loi, pourrait avoir un effet dissuasif qui porterait atteinte à des droits fondamentaux tels que la liberté d'expression.

120. Les autorités chargées de l'application de la loi, tant à l'intérieur[43] qu'à l'extérieur[44] de l'UE, ont déjà manifesté leur intérêt pour accéder aux extraits vocaux capturés par les VVA. L'accès aux données traitées ou obtenues par des VVA dans l'UE devrait être conforme au cadre réglementaire de l'UE existant en matière de protection des données et de protection de la vie privée. Si certains États membres envisagent d'adopter une législation spécifique limitant les droits fondamentaux relatifs à la vie privée et à la protection des données, ces restrictions devraient toujours respecter l'exigence énoncée à l'article 23 du RGPD[45].

121. L'examen manuel des enregistrements vocaux et des données connexes afin d'améliorer la qualité du service de VVA est une pratique courante parmi les fournisseurs de VVA. En raison de la nature sensible des données traitées par ces examinateurs humains et du fait que ce processus est souvent sous-traité à un sous-traitant, il est extrêmement important que des mesures de sécurité adéquates soient mises en place.

---

[41] Voir à titre d'exemple, Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, août 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/kumar
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping*, novembre 2019, https://srlabs.de/bites/smart-spies

[42] Le marché des VVA est actuellement partagé entre moins d'une douzaine de fournisseurs de services.

[43] Voir à titre d'exemple, https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2.

[44] Voir à titre d'exemple, https://cdt.org/insights/alexa-is-law-enforcement-listening.

[45] Voir également les lignes directrices 10/2020 du CEPD sur les restrictions prévues à l'article 23 du RGPD.

Recommandations

122. Les concepteurs de VVA et les développeurs d'applications devraient fournir aux utilisateurs des procédures d'authentification à la pointe de la technologie.

123. Les examinateurs humains devraient toujours recevoir les données strictement nécessaires qui ont été pseudonymisées. Les accords juridiques régissant cet examen devraient expressément interdire tout traitement susceptible de conduire à l'identification de la personne concernée.

124. Si la fonctionnalité d'appel d'urgence est un service fourni par l'intermédiaire du VVA, une disponibilité stable[46] devrait être garantie.

3.8 Traitement de catégories particulières de données

125. Comme indiqué précédemment, les VVA ont accès à des informations à caractère intime qui peuvent être protégées en vertu de l'article 9 du RGPD (voir section 3.7.1), telles que les données biométriques (voir section 3.7.2). Par conséquent, les concepteurs et développeurs de VVA doivent soigneusement déterminer dans quels cas le traitement porte sur des catégories particulières de données.

3.8.1 Considérations générales lors du traitement de catégories particulières de données

126. Les VVA peuvent traiter des catégories particulières de données dans différentes circonstances:

- Dans le cadre de leurs propres services, par exemple lors de la gestion des rendez-vous médicaux dans les agendas des utilisateurs.
- Lorsqu'ils agissent en tant qu'interface pour des services fournis par des tiers, les fournisseurs de VVA traitent le contenu des commandes. En fonction du type de service demandé par l'utilisateur, les fournisseurs de VVA peuvent traiter des catégories particulières de données. À titre d'exemple prenons le cas d'une utilisatrice qui envoie des requêtes à un VVA pour utiliser une application tierce afin de suivre son ovulation[47].
- Lorsqu'une donnée vocale est utilisée à des fins d'identification unique de l'utilisateur, comme indiqué ci-après.

3.8.2 Considérations particulières lors du traitement de données biométriques

127. Certains VVA ont la capacité d'identifier leurs utilisateurs de manière unique sur la seule base de leur voix. Ce processus est connu sous le nom de reconnaissance du modèle vocal. Au cours de la phase d'enregistrement de la reconnaissance vocale, le VVA traite la voix d'un utilisateur afin de créer un modèle vocal (ou une empreinte vocale). Par une utilisation régulière, le VVA peut calculer le modèle vocal de n'importe quel utilisateur et le comparer aux modèles enregistrés afin d'identifier de manière unique l'utilisateur qui a exécuté une commande.

Exemple 11:

[46] Le temps pendant lequel un appareil ou un service peut être laissé sans surveillance, sans connaître de plantage ou nécessiter un redémarrage à des fins administratives ou de maintenance.

[47] Voir à titre d'exemple, un produit disponible ici: https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY

Un groupe d'utilisateurs a mis en place un VVA pour utiliser la reconnaissance du modèle vocal. Après cela, chacun d'entre eux enregistre son modèle vocal.

Par la suite, un utilisateur demande au VVA d'accéder aux réunions figurant dans son agenda. Étant donné que l'accès à l'agenda nécessite l'identification de l'utilisateur, le VVA extrait le modèle de la voix qui a formulé la demande, calcule son modèle vocal et vérifie s'il correspond à un utilisateur enregistré et si cet utilisateur spécifique a accès à l'agenda.

128. Dans l'exemple ci-avant, la reconnaissance de la voix d'un utilisateur sur la base d'un modèle vocal équivaut au traitement de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD (traitement de données biométriques aux fins d'identifier une personne physique de manière unique)[48]. Le traitement de données biométriques aux fins d'identifier l'utilisateur, comme exigé dans cet exemple, nécessitera le consentement explicite de la ou des personne(s) concernée(s) (article 9, paragraphe 2, point a), du RGPD). Par conséquent, lorsqu'ils obtiennent le consentement des utilisateurs, les responsables du traitement doivent respecter les conditions énoncées à l'article 7 et telles que précisées au considérant 32 du RGPD et devraient proposer une méthode alternative d'identification autre que la biométrie, en tenant compte de la nature libre du consentement.

129. Lorsqu'ils utilisent des données vocales à des fins d'identification ou d'authentification biométrique, les responsables du traitement de données sont tenus de faire preuve de transparence quant à l'endroit où l'identification biométrique est utilisée et à la manière dont les empreintes vocales (modèles biométriques) sont stockées et envoyées à l'ensemble des appareils. Afin de satisfaire à cette exigence de transparence, le CEPD recommande de répondre aux questions suivantes:

- L'activation de l'identification vocale sur un appareil active-t-elle automatiquement cette fonction sur tous les autres dispositifs fonctionnant avec le même compte?
- L'activation de l'identification vocale se propage-t-elle, par l'intermédiaire de l'infrastructure du responsable du traitement des données du VVA, aux dispositifs appartenant à d'autres utilisateurs?
- Où les modèles biométriques sont-ils générés, stockés et mis en correspondance?
- Les modèles biométriques sont-ils accessibles aux fournisseurs et développeurs de VVA ou à d'autres personnes?

130. Lorsque l'utilisateur enregistré configure le VVA pour identifier la voix de ses utilisateurs, la voix des utilisateurs non enregistrés et accidentels sera également traitée aux fins de leur identification unique.

131. En effet, la détection de la voix du bon locuteur implique également de la comparer avec celle d'autres personnes se trouvant à proximité de l'assistant. En d'autres termes, la fonctionnalité de reconnaissance du locuteur mise en œuvre dans les assistants vocaux peut nécessiter l'enregistrement des données biométriques vocales des personnes qui parlent dans le ménage, afin de pouvoir distinguer les caractéristiques vocales de l'utilisateur de celles de la personne qui souhaite être reconnue. L'identification biométrique peut donc avoir pour conséquence de soumettre les personnes non informées au traitement de leurs données

biométriques de par l'enregistrement de leur modèle, qui est comparé à celui de l'utilisateur souhaitant être reconnu.

132. Afin d'éviter une telle collecte de données biométriques à l'insu des personnes concernées tout en permettant à un utilisateur d'être reconnu par l'assistant, il convient d'accorder la priorité à des solutions s'appuyant uniquement sur les données de l'utilisateur. Concrètement, cela signifie que la reconnaissance biométrique n'est activée qu'à chaque utilisation initiée par l'utilisateur et non grâce à l'analyse permanente des voix entendues par l'assistant. Par exemple, un mot-clé ou une question spécifique pourrait être adressé aux personnes présentes afin d'obtenir leur consentement pour déclencher le traitement biométrique. Par exemple, l'utilisateur peut dire «identification» ou l'assistant peut demander «Souhaitez-vous être identifié?» et attendre une réponse positive avant d'activer le traitement biométrique.

Exemple 12:
Si l'utilisateur souhaite mettre en place une authentification biométrique pour accéder à certaines données protégées, telles que son compte bancaire, l'assistant vocal peut activer la vérification du locuteur, uniquement lorsqu'il/elle lance l'application, et vérifier son identité de cette manière.

Recommandations

133. Les modèles vocaux devraient être générés, stockés et mis en correspondance exclusivement sur l'appareil local et non sur des serveurs à distance.

134. En raison de la sensibilité des empreintes vocales, il convient d'appliquer scrupuleusement des normes telles que la norme ISO/CEI 24745 et les techniques de protection des modèles biométriques[49].

135. Si un VVA utilise une identification biométrique vocale, les fournisseurs de VVA devraient:

- veiller à ce que l'identification soit suffisamment précise pour associer de manière fiable les données à caractère personnel aux bonnes personnes concernées;
- faire en sorte que tous les groupes d'utilisateurs bénéficient de la même précision, en vérifiant qu'il n'existe aucun biais conséquent à l'égard des différents groupes démographiques.

3.9 Minimisation des données

136. Les responsables du traitement devraient réduire au maximum la quantité de données collectées directement ou indirectement et obtenues par traitement et analyse, par exemple ne pas effectuer d'analyse sur la voix de l'utilisateur ou d'autres informations audibles pour obtenir des informations sur leur état mental, leur maladie éventuelle ou leurs conditions de vie.

[49] Voir par exemple:
Jain, Anil & Nandakumar, Karthik & Nagar, Abhishek, (2008), "*Biometric Template Security*", EURASIP Journal on Advances in Signal Processing, 2008, 10.1155/2008/579416.
S. K. Jami, S. R. Chalamala et A. K. Jindal, «*Biometric Template Protection Through Adversarial Learning*», *IEEE International Conference on Consumer Electronics (ICCE) de 2019*, Las Vegas, Nevada, États-Unis, 2019, pp. 1-6, doi: 10.1109/ICCE.2019.8661905.

137. Ils devraient mettre en place des paramètres par défaut qui limitent la collecte et/ou le traitement des données à la quantité minimale requise pour fournir le service.

138. En fonction de la localisation, du contexte de l'utilisation et de la sensibilité du microphone, le VVA pourrait collecter les données vocales de tiers qui se retrouvent dans le bruit de fond lors de la collecte de la voix des utilisateurs. Même si le bruit de fond n'inclut pas de données vocales, il peut toujours inclure des données contextuelles qui pourraient être traitées pour obtenir des informations sur la personne (par exemple, la localisation).

Recommandations

139. Les concepteurs de VVA devraient tenir compte des technologies qui suppriment le bruit de fond afin d'éviter l'enregistrement et le traitement des voix de fond et des informations contextuelles.

3.10 Responsabilité

140. Pour tout traitement fondé sur le consentement, les responsables du traitement sont tenus de prouver le consentement des personnes concernées conformément à l'article 7, paragraphe 1, du RGPD. Les données vocales peuvent être utilisées à des fins de responsabilité (par exemple, pour prouver le consentement). L'obligation de conservation de ces données vocales serait alors dictée par les exigences en matière de responsabilité prévues par la législation spécifique pertinente.

141. Lorsqu'il s'agit d'évaluer la nécessité d'effectuer une analyse d'impact sur la protection des données («AIPD»), le CEPD a défini les critères[50] que doivent utiliser les autorités chargées de la protection des données, en créant des listes d'opérations de traitement requérant une AIPD obligatoire et en fournissant des exemples de traitements susceptibles d'engendrer une AIPD. Il est très probable que les services de VVA relèvent des catégories et conditions définies comme nécessitant une AIPD. Il convient notamment d'examiner si le dispositif peut observer, surveiller ou contrôler les personnes concernées ou surveiller systématiquement à grande échelle, conformément à l'article 35, paragraphe 3, point c), l'utilisation de «nouvelles technologies» ou le traitement de données sensibles ou relatives à des personnes vulnérables.

142. Toutes les activités de collecte et de traitement des données doivent être documentées conformément à l'article 30 du RGPD, y compris tous les traitements impliquant des données vocales.

Recommandations

143. Si des messages vocaux devaient être utilisés pour informer les utilisateurs conformément à l'article 13, les responsables du traitement devraient publier ces messages sur leur site web afin qu'ils soient accessibles aux utilisateurs et aux autorités chargées de la protection des données.

3.11 Protection des données dès la conception et par défaut

144. Les fournisseurs et développeurs de VVA devraient tenir compte de la nécessité d'avoir un utilisateur enregistré pour chacune de leurs fonctionnalités. Si la nécessité de disposer d'un utilisateur enregistré pour gérer un agenda ou un carnet d'adresses semble claire, le besoin

[50] Groupe de travail «article 29», Lignes directrices concernant l'analyse d'impact sur la protection des données (AIPD), wp248, rév.01, validées par le CEPD.

d'enregistrer un utilisateur au sein du VVA pour passer un appel téléphonique ou réaliser une recherche sur Internet est moins évident.

145. Par défaut, les services qui ne nécessitent pas d'utilisateur identifié ne devraient associer aucun des utilisateurs identifiés du VVA à la commande. Par défaut, un VVA respectueux de la vie privée et de la protection des données ne devrait traiter les données des utilisateurs que pour exécuter les demandes des utilisateurs et ne devrait conserver ni les données vocales, ni un registre des commandes exécutées.

146. Alors que certains appareils ne peuvent exploiter qu'un seul VVA, d'autres peuvent choisir entre plusieurs VVA. Les fournisseurs de VVA devraient développer des normes sectorielles permettant la portabilité des données conformément à l'article 20 du RGPD.

147. Certains fournisseurs de VVA ont affirmé que leurs VVA ne pouvaient pas supprimer toutes les données des utilisateurs, même à la demande de la personne concernée. Les fournisseurs de VVA devraient veiller à ce que toutes les données des utilisateurs puissent être effacées à la demande de l'utilisateur, conformément à l'article 17 du RGPD.

4 MÉCANISMES POUR L'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

148. Conformément au RGPD, les responsables du traitement fournissant des services de VVA doivent permettre à tous les utilisateurs, enregistrés ou non, d'exercer leurs droits en tant que personnes concernées.

149. Les fournisseurs et développeurs de VVA devraient faciliter le contrôle des personnes concernées sur leurs données pendant toute la durée du traitement, en particulier, faciliter leur droit d'accès, de rectification et d'effacement, leur droit de limiter le traitement et, en fonction de la base juridique du traitement, leur droit à la portabilité des données et leur droit d'opposition.

150. Le responsable du traitement devrait fournir des informations sur les droits de la personne concernée au moment où celle-ci allume un VVA et, au plus tard, au moment du traitement de la première demande vocale de l'utilisateur.

151. Étant donné que le principal moyen d'interaction pour les VVA est la voix, les concepteurs de VVA devraient veiller à ce que les utilisateurs, enregistrés ou non, puissent exercer tous leurs droits en utilisant des commandes vocales faciles à suivre. À la fin de l'exercice des droits, les concepteurs de VVA ainsi que les développeurs d'applications devraient, s'ils font partie de la solution, informer l'utilisateur que ses droits ont été dûment pris en compte, par message vocal ou en envoyant une notification écrite au téléphone mobile ou au compte de l'utilisateur, ou encore par tout autre moyen choisi par l'utilisateur.

152. À tout le moins, les concepteurs de VVA et les développeurs d'applications, notamment, devraient mettre en œuvre des outils spécifiques offrant un moyen efficace et efficient d'exercer ces droits. Ils devraient dès lors proposer, pour leurs appareils, un moyen qui permette aux personnes concernées d'exercer leurs droits, en fournissant des outils en libre-

service comme système de gestion de profil[51]. Ainsi, il sera possible de traiter efficacement et en temps utile les droits des personnes concernées, et le responsable du traitement pourra inclure le mécanisme d'identification dans l'outil en libre-service.

153. En ce qui concerne l'exercice des droits des personnes concernées en cas d'utilisateurs multiples, lorsqu'un utilisateur, enregistré ou non, exerce l'un de ses droits, il ou elle devrait le faire sans préjudice des droits des autres utilisateurs. Tous les utilisateurs, enregistrés et non enregistrés, peuvent exercer leurs droits tant que le responsable du traitement des données continue de traiter les données. Le responsable du traitement devrait mettre en place un processus garantissant l'exercice des droits des personnes concernées.

4.1 Droit d'accès

154. Conformément à l'article 12, paragraphe 1, du RGPD, la communication au titre de l'article 15 devrait s'effectuer par écrit ou par d'autres moyens, y compris, le cas échéant, par voie électronique. En ce qui concerne l'accès aux données à caractère personnel faisant l'objet d'un traitement, l'article 15, paragraphe 3, dispose que lorsque la personne concernée présente sa demande par voie électronique, les informations devraient être fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement. Ce qui pourrait être considéré comme un format électronique couramment utilisé devrait tenir compte des attentes raisonnables des personnes concernées et non du format utilisé par le responsable du traitement dans ses opérations quotidiennes. La personne concernée ne devrait pas être obligée d'acheter un logiciel ou du matériel spécifique pour accéder aux informations.

155. Sur demande, les responsables du traitement devraient donc envoyer une copie des données à caractère personnel et des données audio (y compris les enregistrements vocaux et les transcriptions) en particulier, dans un format courant pouvant être lu par la personne concernée.

156. Lorsqu'il décide du type de format dans lequel les informations visées à l'article 15 devraient être fournies, le responsable du traitement doit garder à l'esprit que ce format devrait présenter les informations d'une manière à la fois intelligible et facile d'accès. Les responsables du traitement devraient également adapter, sur mesure, les informations à la situation spécifique de la personne concernée qui fait la demande.

> Exemple 13:
>
> Un responsable du traitement fournissant un service de VVA reçoit, de la part d'un utilisateur, à la fois une demande d'accès et une demande de portabilité des données. Le responsable du traitement décide de fournir les informations visées à l'article 15 et à l'article 20 dans un fichier PDF. Dans ce cas, il ne peut pas être considéré que le responsable du traitement traite les deux demandes correctement. Si un fichier PDF remplit techniquement les obligations incombant au responsable du traitement des données en vertu de l'article 15, il ne remplit pas les obligations qui lui incombent en vertu de l'article 20[52].

[51] Un système de gestion de profil, fait référence à un endroit au sein du système de VVA où l'utilisateur peut, à tout moment, enregistrer ses préférences, effectuer des modifications et changer facilement ses paramètres de confidentialité.

[52] Lignes directrices du GT29 relatives au droit à la portabilité des données, approuvées par le CEPD, p. 18.

Il convient de noter que le simple fait de renvoyer les utilisateurs à un historique de leurs interactions avec l'assistant vocal, ne semble pas permettre au responsable du traitement de remplir toutes les obligations qui lui incombent en vertu du droit d'accès, étant donné que les données accessibles ne représentent généralement qu'une partie des informations traitées dans le cadre de la prestation du service.

157. Le droit d'accès ne devrait pas être utilisé pour contrer/contourner les principes de minimisation et de conservation des données.

4.2 Droit de rectification

158. Afin de faciliter la rectification des données, les utilisateurs enregistrés ou non, devraient être en mesure de gérer et de mettre à jour, à tout moment, leurs données par l'utilisation de leur voix directement auprès du VVA, comme décrit plus tôt. En outre, un outil en libre-service devrait être installé dans l'appareil ou dans une application afin d'aider les utilisateurs à rectifier facilement leurs données à caractère personnel. Les utilisateurs devraient être avertis par message vocal ou par écrit de la mise à jour.

159. Plus généralement, le droit de rectification s'applique à tous les avis et déductions[53] du responsable du traitement, y compris l'établissement d'un profil, et devrait tenir compte du fait que la grande majorité des données sont hautement subjectives[54].

4.3 Droit à l'effacement

160. Les utilisateurs, enregistrés ou non, devraient avoir la possibilité, à tout moment, d'effacer les données les concernant par l'utilisation de leur voix auprès du VVA ou à partir d'un outil en libre-service intégré à tout dispositif associé au VVA. À cet égard, les données à caractère personnel peuvent être effacées par une personne concernée aussi facilement qu'elles ont été soumises. En raison des difficultés inhérentes à l'anonymisation des données vocales et de la grande diversité des données à caractère personnel collectées auprès de la personne concernée, observées et déduites,[55] le droit à l'effacement peut difficilement être garanti dans ce contexte par l'anonymisation des ensembles de données à caractère personnel. Étant donné que le RGPD est neutre sur le plan technologique et que la technologie évolue rapidement, il n'est toutefois pas exclu que le droit à l'effacement puisse être rendu effectif par l'anonymisation.

161. Dans certains cas, sans écran tiers ou possibilité d'afficher les données stockées (par exemple, une application mobile ou un dispositif tabulaire), il est difficile d'avoir un aperçu des éléments enregistrés pour juger de la pertinence des suggestions. Un tableau de bord (ou une application) largement accessible aux utilisateurs afin de faciliter son utilisation devrait être

[53] Le fait que des avis et des déductions puissent être qualifiés de données à caractère personnel a été confirmé par la CJUE, qui a relevé que le terme «toute information» dans la définition des données à caractère personnel inclut des informations «tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci "concernent" la personne en cause» – affaire C-434/16, *Peter Nowak/Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

[54] Getting Data Subject Rights Right, A submission to the EDPB from data protection academics, novembre 2019.

[55] Avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation, adopté le 10 avril 2014.

fourni avec l'assistant vocal afin de supprimer l'historique des requêtes et de personnaliser l'outil en fonction des besoins de l'utilisateur[56].

162. Pour tout traitement de données et, en particulier, lorsque les personnes concernées enregistrées consentent à ce que les enregistrements vocaux soient transcrits et utilisés par le fournisseur pour améliorer ses services, les fournisseurs de VVA devraient, à la demande de l'utilisateur, être en mesure de supprimer l'enregistrement vocal initial ainsi que toute transcription connexe des données à caractère personnel.

163. Le responsable du traitement devrait veiller à ce que les données ne puissent plus être traitées après l'exercice du droit à l'effacement. En ce qui concerne les actions antérieures, le droit à l'effacement peut rencontrer certaines limites juridiques et techniques, notamment.

> Exemple 14:
>
> Si, avant la demande d'effacement, un utilisateur a effectué un achat en ligne au moyen de son VVA, le fournisseur de VVA peut supprimer l'enregistrement vocal relatif à l'achat en ligne et s'assurer de ne plus utiliser plus à l'avenir. Toutefois, l'achat restera effectif, de même que la commande vocale ou la transcription écrite traitée par le site web de commerce électronique (ici, la dérogation est fondée sur l'obligation légale du site web de commerce électronique).
>
> Dans le même ordre d'idées, si l'utilisateur a ajouté une chanson spécifique à sa liste de lecture au moyen de son VVA avant de demander l'effacement de ses données, les fournisseurs de VVA pourront supprimer la demande orale, mais pas les conséquences antérieures d'une telle requête (l'effacement n'aura pas d'incidence sur la liste de lecture de l'utilisateur).

164. Sur la base de ce qui précède, si les mêmes données à caractère personnel sont traitées à des fins différentes, les responsables du traitement devraient considérer les demandes d'effacement comme le signal clair de mettre un terme au traitement des données à toutes les fins qui ne sont pas légalement exemptées.

Conformément aux conditions énoncées à l' article 21, paragraphe 1, du RGPD, les données traitées sur la base d'intérêts légitimes des fournisseurs de VVA ne devraient pas constituer une dérogation au droit à l'effacement, notamment parce que les personnes concernées ne s'attendent pas raisonnablement à un traitement ultérieur de leurs données à caractère personnel.

4.4 Droit à la portabilité des données

165. Le traitement des données effectué par les fournisseurs de VVA relève du champ d'application de la portabilité des données, étant donné que les opérations de traitement sont principalement fondées sur le consentement de la personne concernée (en vertu de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), lorsqu'il s'agit de catégories particulières de données à caractère personnel) ou sur un contrat auquel la personne concernée est partie en vertu de l'article 6, paragraphe 1, point b).

[56] «Assistants vocaux et enceintes connectées, l'impact de la voix sur l'offre et les usages culturels et médias», Conseil Supérieur de l'Audiovisuel français, mai 2019.

166. Dans la pratique, le droit à la portabilité des données devrait faciliter le changement de fournisseur de VVA. Puisque les VVA opèrent dans un environnement numérique en particulier et que la voix de la personne concernée est enregistrée dans une application ou sur une plateforme, le droit à la portabilité des données devrait être accordé pour toutes les données à caractère personnel fournies par la personne concernée. En outre, le responsable du traitement devrait offrir aux utilisateurs la possibilité de récupérer directement leurs données à caractère personnel depuis leur espace utilisateur, en tant qu'outil en libre-service. Les utilisateurs devraient également pouvoir exercer ce droit au moyen d'une commande vocale.

167. Les fournisseurs et développeurs de VVA devraient confier aux personnes concernées un contrôle étendu des données à caractère personnel les concernant, afin de leur permettre de transférer des données à caractère personnel d'un fournisseur de VVA à un autre. Les personnes concernées devraient donc recevoir leurs données à caractère personnel fournies au responsable du traitement dans un format structuré, couramment utilisé et exploitable sur machine, par des moyens[57] qui permettent de faire droit aux demandes de portabilité des données (tels que les outils de téléchargement et les interfaces de programmation d'applications)[58]. Comme indiqué dans les lignes directrices relatives au droit à la portabilité des données, en cas de collecte de données à caractère personnel de grande ampleur ou complexe, ce qui pourrait être le cas en l'espèce, le responsable du traitement devrait fournir une vue d'ensemble «*d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples*» (voir article 12, paragraphe 1, du RGPD), de manière à ce que les personnes concernées disposent toujours d'informations claires sur les données à télécharger ou à transmettre à un autre responsable du traitement en rapport avec une finalité donnée. Par exemple, les personnes concernées devraient être en mesure d'utiliser des applications logicielles afin d'identifier, de reconnaître et de traiter facilement des données spécifiques de celles-ci.

168. Ce droit devrait permettre à l'utilisateur de récupérer, pour son usage personnel, les données qu'il/elle a communiquées au moyen de sa voix (par exemple, l'historique des interactions vocales) et dans le cadre de la création de son compte utilisateur (par exemple, nom et prénom), notamment.

[57] Voir à titre d'illustration, le raisonnement du groupe de travail «article 29» dans les lignes directrices relatives au droit à la portabilité des données, approuvées par le CEPD, p. 16:
«*Du point de vue technique, les responsables du traitement devraient envisager et évaluer deux modes différents et complémentaires pour mettre les données portables à la disposition des personnes concernées ou d'autres responsables du traitement:*
- une transmission directe de l'intégralité de l'ensemble de données portables (ou plusieurs extraits de parties de l'ensemble global de données);
- un outil automatisé permettant l'extraction des données pertinentes.
Le deuxième mode de transmission peut être privilégié par les responsables du traitement dans les cas impliquant des ensembles de données volumineux et complexes, étant donné qu'il permet l'extraction de toute partie de l'ensemble de données pertinente pour la personne concernée dans le cadre de sa demande, peut contribuer à réduire le risque au minimum et permet éventuellement l'utilisation de mécanismes de synchronisation (par exemple, dans le contexte d'une communication régulière entre responsables du traitement). Il peut s'agir d'une meilleure manière d'assurer la conformité pour le "nouveau" responsable du traitement et constituerait une bonne pratique en ce qui concerne la réduction des risques liés à la confidentialité de la part du responsable du traitement initial».

[58] À cet égard, voir les Lignes directrices du Groupe de travail «Article 29» relatives au droit à la portabilité des données, approuvées par le CEPD, p. 1.

169. Pour la pleine application de ce droit des personnes concernées dans le contexte d'un marché unique numérique, les concepteurs de VVA et les développeurs d'applications, notamment, devraient développer des formats courants exploitables sur machine facilitant l'interopérabilité du format des données entre les systèmes de VVA[59], y compris les formats standard pour les données vocales. Les technologies devraient être structurées de manière à garantir que les données à caractère personnel traitées, y compris les données vocales, sont facilement et entièrement réutilisables par le nouveau responsable du traitement[60].

170. En ce qui concerne le format, les fournisseurs de VVA devraient fournir les données à caractère personnel en utilisant des formats ouverts couramment utilisés (par exemple, mp3, wav, csv, gsm, etc.) ainsi que les métadonnées appropriées utilisées pour décrire précisément la signification des informations échangées[61].

5 ANNEXE: RECONNAISSANCE AUTOMATIQUE DE LA PAROLE, SYNTHÈSE VOCALE ET TRAITEMENT DU LANGAGE NATUREL

171. À la suite des fondements théoriques du traitement des signaux, notamment les théories d'information et d'échantillonnage de Claude Shannon, le traitement automatique de la parole est devenu un élément fondamental des sciences de l'ingénierie. Au carrefour de la physique (acoustiques, propagation des ondes), des mathématiques appliquées (modélisation, statistiques), de l'informatique (algorithmes, techniques d'apprentissage) et des sciences humaines (perception, raisonnement), le traitement de la parole s'est rapidement décomposé en de nombreux sujets d'étude: identification et vérification du locuteur, reconnaissance vocale automatique, synthèse vocale, détection de l'émotion, etc. Au cours des quinze dernières années, la discipline dans son ensemble a accompli des progrès considérables, avec divers facteurs y contribuant : l'amélioration des méthodes, l'augmentation significative des capacités de calcul et l'accroissement des volumes de données disponibles.

5.1 Reconnaissance automatique de la parole (RAP)

172. La reconnaissance automatique de la parole (également appelée «conversion de la parole en texte») supposait généralement trois étapes distinctes visant à: 1) déterminer les phonèmes qui ont été communiqués à l'aide d'un modèle acoustique; 2) déterminer les mots qui ont été prononcés à l'aide d'un dictionnaire phonétique; 3) transcrire la séquence de mots (phrase) la plus probable à l'aide d'un modèle linguistique. Aujourd'hui, grâce aux progrès réalisés grâce à l'apprentissage profond (une technique d'apprentissage automatique), de nombreux

[59] À cet égard, voir le considérant 68 des lignes directrices du GT29 relatives au droit à la portabilité des données, approuvées par le CEPD, p. 17.

[60] «*À cet égard, le considérant 68 énonce qu'[i]l y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données, mais sans créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles. Le règlement général sur la protection des données interdit toutefois aux responsables du traitement d'entraver la transmission*», lignes directrices du GT29 relatives au droit à la portabilité des données, approuvées par le CEPD, p. 5.

[61] Le CEPD encourage vivement la coopération entre les parties prenantes du secteur et les associations professionnelles afin qu'elles œuvrent de concert à un ensemble commun de normes et de formats interopérables visant à satisfaire aux exigences du droit à la portabilité des données.

systèmes offrent une reconnaissance automatique de la parole «de bout en bout». Cela évite de devoir passer par l'entraînement complexe de trois modèles différents tout en offrant de meilleures performances en termes de résultats et de temps de traitement. Presque tous les grands acteurs numériques proposent désormais leurs propres modèles de RAP qui peuvent être facilement utilisés par les systèmes API, mais il existe également des systèmes libres d'accès (DeepSpeech[62]ou Kaldi[63], par exemple).

5.2 Traitement du langage naturel (TLN)

173. Le traitement du langage naturel est un domaine multidisciplinaire comprenant la linguistique, l'informatique et l'intelligence artificielle, qui vise à créer des outils de traitement du langage naturel pour diverses applications. Les domaines de recherches et d'applications sont nombreux: analyse syntaxique, traduction automatique par machine, production et synthèse automatiques de textes, vérification de l'orthographe, systèmes de réponse aux questions, fouille de textes, reconnaissance nominative de l'entité, analyse de sentiments, etc. De fait, l'objectif du TLN est de donner aux ordinateurs la capacité de lire, de comprendre et de déduire un sens à partir du langage humain. Le développement d'applications de TLN est difficile, car les outils informatiques exigent traditionnellement une interaction humaine dans un langage de programmation formel, c'est-à-dire précis, univoque et hautement structuré. Toutefois, la parole humaine n'est pas toujours précise. Elle est souvent ambigüe et la structure linguistique peut dépendre de nombreuses variables complexes comme l'argot, les dialectes régionaux et le contexte social.

174. L'analyse syntaxique et sémantique sont les deux techniques principales utilisées avec le TLN. La syntaxe désigne l'agencement de mots dans une phrase pour donner un sens grammatical. Le TLN utilise la syntaxe pour évaluer le sens à partir d'un langage fondé sur des règles grammaticales. Les techniques de syntaxe utilisées comprennent l'analyse syntaxique (analyse grammaticale pour une phrase), la segmentation des mots (qui divise un long texte en unités), la segmentation de la phrase (qui place les limites des phrases dans les grands textes), la segmentation morphologique (qui divise les mots en groupes) et la racinisation (qui divise les mots comportant une inflexion en racines). La sémantique implique l'utilisation et la signification des mots. Le TLN applique des algorithmes pour comprendre la signification et la structure des phrases. Parmi les techniques que le TLN emploie avec la sémantique figurent la désambiguïsation du sens du terme (qui donne le sens d'un mot grâce au contexte), la reconnaissance de l'entité désignée (qui détermine les mots pouvant être classés en groupes) et la génération naturelle du langage (qui s'appuiera sur une base de données pour déterminer la sémantique derrière les mots). Alors que les précédentes approches du TLN étaient fondées sur des règles qui informaient des algorithmes d'apprentissage automatique simples des mots et phrases à rechercher dans un texte et leur fournissaient des réponses spécifiques lorsque ces phrases apparaissent, les approches actuelles du TLN reposent sur un apprentissage profond, un type d'IA qui examine et utilise les schémas des données pour améliorer la compréhension d'un programme.

5.3 Synthèse de la parole

175. La synthèse de la parole est la production artificielle de la parole humaine. Cette technique a principalement été mise en œuvre par concaténation d'unités vocales qui sont conservées dans une base de données. Elle consiste à sélectionner, parmi tous les enregistrements d'un

[62] https://github.com/mozilla/DeepSpeech
[63] https://github.com/kaldi-asr/kaldi

acteur qui ont été préalablement transcrits en phonèmes, syllabes et mots, les bribes de son qui correspondent aux mots que l'on souhaite faire prononcer au VVA et assembler l'un après l'autre pour former une phrase intelligible avec une élocution naturelle. Un synthétiseur vocal peut également intégrer un modèle du tractus vocal et d'autres caractéristiques de la voix humaine afin de modéliser les paramètres d'une voix tels que l'intonation, le rythme et le timbre, par des modèles statistiques génératifs (tels que WaveNet[64], Tacotron[65] ou DeepVoice)[66] et de créer une sortie vocale entièrement synthétique.

[64] Aäron van den Oord et Sander Dieleman, *WaveNet: A generative model for raw audio*, Deepmind blog, septembre 2016, https://deepmind.com/blog/article/wavenet-generative-model-raw-audio

[65] Yuxuan Wang, *Expressive Speech Synthesis with Tacotron*, Google AI blog, mars 2018, https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html

[66] *Deep Voice 3: 2000-Speaker Neural Text-to-Speech*, Baidu Research blog, octobre 2017 http://research.baidu.com/Blog/index-view?id=91