

Orientări



Orientările 02/2021 privind asistenții vocali virtuali

Versiunea 2.0

Adoptate la 7 iulie 2021

Istoricul versiunii

Versiunea 2.0	7 iulie 2021	Adoptarea orientărilor în urma consultării publice
Versiunea 1.0	9 martie 2021	Adoptarea orientărilor pentru consultare publică

REZUMAT

Un asistent vocal virtual (AVV) este un serviciu care înțelege comenzile vocale și le execută sau face legătura cu alte sisteme IT, dacă este necesar. AVV-urile sunt disponibile în prezent pe majoritatea telefoanelor inteligente și tabletelor, a computerelor tradiționale și, în ultimii ani, chiar și pe dispozitive independente precum boxele inteligente.

AVV-urile acționează ca o interfață între utilizatori și dispozitivele lor de calcul și serviciile online, precum motoare de căutare sau magazine online. Prin rolul lor, ele au acces la o cantitate imensă de date cu caracter personal, printre care toate comenzile utilizatorilor (de exemplu, istoricul de navigare sau de căutare) și răspunsurile lor (de exemplu, programările din agendă).

Marea majoritate a serviciilor AVV au fost proiectate de câțiva specialiști AVV. Asistenții vocali virtuali pot funcționa însă în combinație cu aplicații programate de terți (dezvoltatori de aplicații pentru AVV-uri), pentru a oferi comenzi mai sofisticate.

Pentru a funcționa corect, un AVV are nevoie de un dispozitiv terminal prevăzut cu microfoane și difuzoare. Dispozitivul stochează date vocale și alte tipuri de date, pe care AVV-urile actuale le transferă la servere AVV aflate la distanță.

Prin urmare, operatorii de date care furnizează servicii AVV și persoanele împuternicite de aceștia trebuie să țină seama atât de RGPD¹, cât și de Directiva privind viața privată și comunicațiile electronice².

Prezentele orientări identifică unele dintre cele mai relevante provocări legate de conformitate și oferă recomandări părților interesate relevante cu privire la modul de abordare a acestora.

Operatorii de date care furnizează servicii AVV prin dispozitive terminale fără ecran trebuie încă să informeze utilizatorii, conform dispozițiilor RGPD, atunci când configurează sau instalează AVV-ul sau atunci când folosesc o aplicație AVV pentru prima dată. În consecință, recomandăm furnizorilor/proiectanților și dezvoltatorilor de AVV să dezvolte interfețele pe bază de voce astfel încât să faciliteze transmiterea informațiilor obligatorii.

În prezent, toate AVV-urile necesită cel puțin un utilizator înregistrat în serviciu. Ca urmare a obligației de protecție a datelor din faza de proiectare și în mod implicit, furnizorii/proiectanții și dezvoltatorii de AVV-uri ar trebui să aibă în vedere necesitatea de a avea câte un utilizator înregistrat pentru fiecare dintre funcționalitățile lor.

Contul de utilizator folosit de mulți proiectanți de AVV combină serviciul AVV cu alte servicii, precum e-mail sau streaming video. CEPD consideră că operatorii de date ar trebui să se abțină de la astfel de practici, deoarece ele implică utilizarea unor politici de confidențialitate extinse și complexe, care nu ar respecta principiul transparenței din RGPD.

¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”).

² Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea vieții private în sectorul comunicațiilor publice (Directiva privind viața privată și comunicațiile electronice), astfel cum a fost modificată prin Directiva 2006/24/CE și prin Directiva 2009/136/CE (denumită în continuare „Directiva privind viața privată și comunicațiile electronice”).

Orientările analizează patru din cele mai frecvente scopuri pentru care AVV-urile prelucrează date cu caracter personal: executarea cererilor, îmbunătățirea modelului de învățare automată folosit de AVV, identificarea biometrică și crearea de profiluri pentru conținut personalizat sau pentru publicitate.

În măsura în care datele obținute de AVV sunt prelucrate pentru a executa cererile utilizatorului, adică prelucrarea este strict necesară pentru a furniza un serviciu solicitat de utilizator, operatorii de date sunt exonerati de obligația privind consimțământul prealabil prevăzută la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. În schimb, consimțământul prevăzut la articolul 5 alineatul (3) din directivă ar fi necesar pentru stocarea sau obținerea accesului la informații în orice alt scop decât executarea cererii utilizatorilor.

Unele servicii AVV păstrează datele cu caracter personal până când utilizatorii solicită ștergerea lor. Acest lucru nu este în conformitate cu principiul limitării legate de stocare. AVV-urile ar trebui să stocheze date pe o perioadă nu mai mare decât este necesar în scopurile pentru care sunt prelucrate datele cu caracter personal.

Dacă un operator de date are cunoștință (de exemplu, în urma proceselor de analiză a calității) de colectarea accidentală de date cu caracter personal, ar trebui să verifice dacă există un temei legal valabil pentru fiecare scop în care sunt prelucrate aceste date. În caz contrar, datele colectate accidental trebuie șterse.

AVV-urile pot prelucra date ale mai multor persoane vizate. De aceea, furnizorii/proiectanții de AVV ar trebui să implementeze mecanisme de control al accesului pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal. Cu toate acestea, unele mecanisme tradiționale de control al accesului, cum ar fi parolele, nu sunt însă potrivite în contextul AVV, deoarece ar trebui să fie spuse cu voce tare. Orientările prezintă câteva considerații în acest sens, inclusiv o secțiune specifică pe tema prelucrării categoriilor speciale de date în vederea identificării biometrice.

Furnizorii/proiectanții de AVV ar trebui să aibă în vedere faptul că, atunci când colectează vocea utilizatorului, înregistrarea ar putea conține și vocea altor persoane sau date precum zgomotul de fond care nu sunt necesare pentru serviciu. Din acest motiv, proiectanții AVV-urilor ar trebui să ia în considerare, ori de câte ori este posibil, tehnologii care filtrează datele inutile și care asigură că doar vocea utilizatorului este înregistrată.

Atunci când analizează necesitatea unei evaluări a impactului asupra protecției datelor (DPIA), CEPD consideră că serviciile AVV se încadrează foarte probabil în categoriile și condițiile identificate ca necesitând o DPIA.

Operatorii de date care furnizează servicii AVV ar trebui să se asigure că utilizatorii își pot exercita drepturile de persoane vizate folosind comenzi vocale ușor de urmat. Furnizorii/proiectanții de AVV, precum și dezvoltatorii de aplicații ar trebui, la sfârșitul procesului, să informeze utilizatorii că drepturile lor au fost luate în considerare în mod corespunzător, printr-un mesaj vocal sau prin trimiterea unei notificări scrise pe telefonul mobil sau în contul utilizatorului ori prin orice alt mijloc ales de acesta.

Cuprins

REZUMAT	3
1 GENERALITĂȚI	7
2 DETALII PRIVIND TEHNOLOGIA	8
2.1 Caracteristicile de bază ale asistenților vocali virtuali.....	8
2.2 Actorii din ecosistemul AVV	9
2.3 Descrierea pas cu pas.....	10
2.4 Expresiile de activare.....	11
2.5 Fragmentele de cod care prelucrează vocea și învățarea automată	12
3 ELEMENTE DE PROTECȚIE A DATELOR	12
3.1 Cadru juridic	12
3.2 Identificarea prelucrării datelor și a părților interesate.....	14
3.2.1 Prelucrarea datelor cu caracter personal.....	15
3.2.2 Prelucrarea de către operatorii de date și persoanele împuternicite de aceștia.....	17
3.3 Transparența	19
3.4 Limitarea scopului și temeiul juridic.....	23
3.4.1 Executarea cererilor utilizatorilor.....	24
3.4.2 Îmbunătățirea AVV-ului prin antrenarea sistemelor de învățare automată și revizuirea manuală a vocii și a transcrierilor vocii	25
3.4.3 Identificarea utilizatorilor (folosind date vocale).....	26
3.4.4 Crearea de profiluri ale utilizatorilor pentru conținut personalizat sau publicitate personalizată	26
3.5 Prelucrarea datelor referitoare la copii.....	28
3.6 Păstrarea datelor.....	28
3.7 Securitatea	31
3.8 Prelucrarea categoriilor speciale de date.....	33
3.8.1 Considerații generale cu privire la prelucrarea categoriilor speciale de date.....	33
3.8.2 Considerații specifice cu privire la prelucrarea datelor biometrice	34
3.9 Reducerea la minimum a datelor	36
3.10 Responsabilitatea	36
3.11 Asigurarea protecției datelor din faza de proiectare și în mod implicit.....	37
4 Mecanisme de exercitare a drepturilor persoanei vizate	37
4.1 Dreptul de acces	38
4.2 Dreptul la rectificare.....	39
4.3 Dreptul la ștergerea datelor	39
4.4 Dreptul la portabilitatea datelor	40

5	Anexă: Recunoașterea automată a vorbirii, sinteza vorbirii și procesarea limbajului natural	42
5.1	Recunoașterea automată a vorbirii (RAV).....	42
5.2	Procesarea limbajului natural (PLN).....	42
5.3	Sinteza vorbirii.....	43

Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) literele (e) și (j) din Regulamentul 2016/679/UE al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE și în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018³,

având în vedere articolul 12 și articolul 22 din Regulamentul său de procedură,

A ADOPTAT URMĂTOARELE ORIENTĂRI

1 GENERALITĂȚI

1. Progresele tehnologice din ultimul timp au crescut mult acuratețea și popularitatea asistențelor vocale virtuale (AVV). Printre alte dispozitive, AVV-urile au fost integrate în telefoane inteligente, în vehicule conectate, în difuzoare inteligente și în televizoare inteligente, printre alte dispozitive. Această integrare a oferit AVV-urilor acces la informații de natură intimă care, dacă nu sunt gestionate corespunzător, ar putea afecta drepturile persoanelor la protecția datelor și la viața privată. În consecință, AVV-urile și dispozitivele care le integrează s-au aflat sub controlul a diferite autorități de protecție a datelor.
2. Utilizarea interacțiunilor bazate pe voce prezintă mai multe avantaje, de exemplu: natura leșea interacțiunii care nu presupune învățarea unor comenzi specifice din partea utilizatorilor, viteza de execuție a comenzii și extinderea câmpului de acțiune, care poate facilita un acces mai rapid la informații. Cu toate acestea, aplicațiile care se bazează pe voce implică însă și dificultăți în interpretarea corectă a mesajului: variația semnalului audio între diferiți vorbitori, mediul acustic, ambiguitatea lingvistică etc.
3. În practică, fluiditatea sau simplificarea execuției sarcinilor rămân motivația principală pentru dotarea cu AVV. Aceasta poate implica, de exemplu, inițierea unui apel sau răspunsul la un apel, setarea unui cronometru etc., mai ales atunci când utilizatorii au mâinile ocupate. Principala aplicabilitate propusă de proiectanții AVV-urilor este domotica (automatizarea locuinței). Prin propunerea simplificării execuției sarcinilor (aprinderea luminii, reglarea încălzirii, coborârea obloanelor etc.) și centralizarea acestora printr-un singur instrument, care poate fi ușor activat de la distanță, AVV-urile se încadrează în categoria instrumentelor care ușurează activitățile casnice. În plus față de utilizarea personală sau casnică, comenzile vocale pot prezenta interes și în mediile profesionale în care este dificil să se manipuleze instrumente computerizate și să se utilizeze comenzi scrise (de exemplu, munca pe liniile de producție).
4. În teorie, principalii beneficiari ai interfeței vocale ar putea fi persoanele cu dizabilități sau dependente de ajutor, pentru care utilizarea interfețelor tradiționale este problematică. Asistența vocală virtuală poate oferi un acces mai ușor la informații și resurse informatice,

³ Referirile la „statele membre” din acest document trebuie înțelese ca referiri la „statele membre ale SEE”.

promovând astfel logica incluzivă, deoarece utilizarea vocii face posibilă depășirea dificultăților asociate cuvântului scris pe care le pot întâmpina anumite clase de utilizatori.

5. În sfârșit, sănătatea este un alt domeniu în care sunt multe cazuri de utilizare a agenților de conversație, de tip vocal sau de alt tip. De exemplu, în timpul pandemiei de COVID-19 au fost implementate diverse programe bot pentru apeluri care au oferit un diagnostic preliminar apelanților. Pe termen lung, unii anticipează că întregul proces de îngrijire a pacienților ar putea fi impactat de interacțiunile om/asistent: nu numai pentru menținerea stării de bine și prevenție, ci și pentru tratament și sprijin.
6. În prezent există mai mult de 3 miliarde de telefoane inteligente și toate au AVV-uri integrate, majoritatea fiind activate în mod implicit. Unele dintre cele mai răspândite sisteme de operare instalate pe computerele personale și pe laptopuri integrează de asemenea AVV-uri. Popularitatea din ultimul timp a difuzoarelor inteligente (147 de milioane vândute în 2019⁴) aduce AVV-urile în milioane de locuințe și birouri. Însă AVV-urile proiectate în prezent nu oferă implicit mecanisme de autentificare sau de control al accesului.
7. Prezentul document își propune să ofere îndrumări cu privire la aplicarea RGPD în contextul AVV-urilor.

2 DETALII PRIVIND TEHNOLOGIA

2.1 Caracteristicile de bază ale asistenților vocali virtuali

8. Un AVV poate fi definit ca o aplicație software care oferă posibilitatea unui dialog oral cu un utilizator, în limbaj natural.
9. Limbajul natural are o semantică specifică limbajului uman. În funcție de caracteristicile limbii și de diversitatea sa lexicală, aceeași instrucțiune poate fi formulată în mai multe moduri, iar unele comenzi pot să pară similare, dar să se refere la două obiecte diferite. Pentru a lămurii aceste ambiguități se folosesc în mod frecvent mecanisme de inferență – care depind, de exemplu, de cele spuse anterior, de momentul în care a fost dată instrucțiunea, locul, interesele persoanei etc.
10. Un AVV poate fi împărțit în module care fac posibilă îndeplinirea a diverse sarcini: înregistrare și redare a sunetului, transcriere automată a vorbirii (recunoaștere vocală), procesare automată a limbajului, strategii de dialog, acces la ontologii (seturi de date și concepte structurate legate de un anumit domeniu) și la surse de cunoștințe externe, generarea limbajului, sinteza vocală (text transpus în vorbire) etc. Concret, asistentul ar trebui să facă posibilă interacțiunea pentru a efectua acțiuni (de exemplu, „Pornește radioul”, „Închide lumina”) sau a obține informații (de exemplu, „Cum va fi vremea mâine?”, „Trenul de la 7:43 circulă?”). Astfel, el joacă rolul unui intermediar și orchestrator care ar trebui să ajute utilizatorul în îndeplinirea sarcinilor.
11. În practică, un AVV nu este o boxă inteligentă, dar o boxă inteligentă poate fi echipată cu un asistent vocal. Se întâmplă frecvent ca cele două să fie confundate, însă cea de a doua este doar una din întrupările materiale ale primului. Un AVV poate fi integrat într-un telefon

⁴ De exemplu, a se vedea comunicatul de presă din 1 august 2019 al Autorității pentru protecția datelor și informații din Hamburg: <https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistent>

inteligent, într-o boxă inteligentă, într-un ceas conectat, într-un vehicul, într-un aparat electrocasnic etc.

12. Organizarea prelucrării datelor inerente poate implica mai multe modele de flux de informații. Se pot izola trei entități principale:

Instanța fizică: elementul hardware în care este încorporat asistentul (telefon inteligent, boxă, televizor inteligent etc.) și care este echipat cu microfoane, difuzoare și capacități de rețea și de calcul (mai mult sau mai puțin dezvoltate, după caz).

Instanța software: partea care implementează propriu-zis interacțiunea om-mașină și care integrează modulele de recunoaștere automată a vorbirii, procesare a limbajului natural, dialog și sinteză vocală. Aceasta poate fi operată direct în cadrul echipamentului fizic, dar în multe cazuri se efectuează de la distanță.

Resursele: date externe, precum baze de date de conținut, ontologii sau aplicații comerciale care oferă informații (de exemplu, „Spune-mi cât este ora pe coasta de vest a Statelor Unite”, „Citește-mi e-mailurile”) sau fac posibilă efectuarea concretă a acțiunii solicitate (de exemplu, „Crește temperatura cu 1,5 °C”).

13. AVV-urile permit instalarea de componente sau aplicații ale terților care extind funcționalitățile lor de bază. Fiecare AVV denumește componentele diferit, dar toate implică schimbul de date cu caracter personal ale utilizatorilor între proiectantul AVV și dezvoltatorul aplicațiilor.
14. Deși majoritatea AVV-urilor nu comunică fragmentul de voce cu dezvoltatorii de aplicații, totuși acești actori prelucrează date cu caracter personal. În plus, în funcție de natura funcției oferite, dezvoltatorul aplicațiilor primește intenții și sloturi care ar putea conține informații sensibile, precum date privind sănătatea.

2.2 Actorii din ecosistemul AVV

15. Un AVV poate implica un număr mare de actori și intermediari de-a lungul lanțului de execuție. În practică se pot identifica până la cinci actori diferiți. În funcție de modelele de afaceri și de opțiunile tehnologice, unii actori își pot asuma mai multe combinații de roluri – de exemplu, proiectant și integrator sau proiectant și dezvoltator de aplicații:
 - a. **Furnizorul (sau proiectantul) AVV:** responsabil cu dezvoltarea AVV-ului, proiectează și definește posibilitățile și funcționalitățile implicite ale acestuia: modalități de activare, alegerea arhitecturii, accesul la date, gestionarea înregistrărilor, specificațiile hardware etc.
 - b. **Dezvoltatorul de aplicații pentru AVV:** la fel ca în cazul aplicațiilor mobile, creează aplicații care extind funcționalitățile implicite ale AVV-ului. Pentru aceasta, este necesar să se respecte constrângerile de dezvoltare impuse de proiectant.
 - c. **Integratorul:** producător de obiecte conectate, pe care dorește să le echipeze cu un AVV. Ar trebui să respecte cerințele definite de proiectant.
 - d. **Proprietarul:** responsabil de spațiile fizice în care se află persoane (locuri de cazare, medii profesionale, vehicule de închiriat etc.); dorește să ofere un AVV publicului său (eventual împreună cu aplicații dedicate).

- e. **Utilizatorul:** veriga finală în lanțul valoric al AVV-ului, care îl poate folosi pe diferite dispozitive (boxă, televizor, telefon inteligent, ceas etc.), în funcție de modul și locul în care a fost implementat și configurat AVV-ul.

2.3 Descrierea pas cu pas

16. Pentru ca un AVV să execute o acțiune sau să acceseze informații, se efectuează o succesiune de sarcini:

- 1) Instalat în cadrul unui echipament (telefon inteligent, difuzor, vehicul), AVV-ul este în standby. Mai precis, AVV-ul ascultă în mod constant. Totuși, până când nu detectează o expresie de activare specifică, dispozitivul care recepționează vocea nu emite sunete și nu efectuează nicio altă operațiune în afara celei de detectare a expresiei de activare. În acest scop, se utilizează o întârziere de câteva secunde (vezi secțiunea următoare pentru mai multe detalii).
- 2) Utilizatorul rostește expresia de activare și AVV-ul compară local sunetul recepționat cu expresia de activare. Dacă se potrivesc, AVV-ul deschide un canal de ascultare și conținutul audio este transmis imediat.
- 3) În multe cazuri, dacă procesarea comenzii se face de la distanță, se face o a doua verificare pe server a pronunției cuvintelor-cheie, pentru a reduce numărul de activări nedorite.
- 4) Utilizatorul rostește solicitarea care este transmisă în timp real către furnizorul AVV-ului. Secvența de sunete vorbite este apoi transcrisă automat (vorbire în text).
- 5) Comanda este interpretată prin utilizarea tehnologiilor de procesare a limbajului natural (PLN). Se extrag intențiile mesajului și se identifică variabilele (sloturile) de informație. Apoi se folosește un manager de dialog pentru a specifica schema de interacțiune care să fie implementată de utilizator prin furnizarea schemei de răspuns adecvate.
- 6) În cazul în care comanda implică o funcționalitate furnizată de o aplicație terță (abilitate, acțiune, comandă rapidă etc.), furnizorul AVV-ului trimite dezvoltatorului aplicației intențiile și variabilele (sloturile) de informație ale mesajului.
- 7) Se identifică un răspuns adaptat cererii utilizatorului – cel puțin în teorie, răspunsul „Nu am un răspuns la întrebarea dvs.” fiind un răspuns adaptat în cazul în care AVV-ul nu a putut să interpreteze corect solicitarea. Dacă este necesar, se utilizează resurse aflate la distanță: baze de cunoștințe accesibile publicului (enciclopedii online etc.) sau resurse accesibile prin autentificare (cont bancar, aplicație pentru muzică, cont de client pentru achiziții online etc.), iar variabilele (sloturile) de informație se completează cu cunoștințele recuperate.

8) Se creează o frază de răspuns și/sau se identifică o acțiune (coborârea jaluzelelor, creșterea temperaturii, redarea unei piese muzicale, răspunsul la o întrebare etc.). Se sintetizează o propoziție (text transpus în vorbire) și/sau acțiunea care trebuie efectuată se trimite la echipamentul corespunzător.

9) AVV-ul revine în standby.

Rețineți că, deși în prezent majoritatea procesărilor vocale se realizează pe servere la distanță, unii furnizori de AVV-uri dezvoltă sisteme care ar putea efectua o parte din aceste procesări la nivel local⁵.

2.4 Expresiile de activare

17. Pentru a putea fi utilizat, un AVV trebuie să fie „activ”. Aceasta înseamnă că asistentul comută într-un mod de ascultare activ pentru a putea să primească ordine și comenzi de la utilizator. Deși această activare poate fi realizată uneori și printr-o acțiune fizică (de exemplu apăsând un buton, apăsând pe boxa inteligentă etc.), aproape toate AVV-urile de pe piață se bazează pe detectarea unei expresii sau a unui cuvânt de activare (cunoscut și sub numele de cuvânt de trezire/cuvânt-cheie) pentru a comuta în modul de ascultare activă.
18. În acest scop, asistentul se bazează pe utilizarea microfonului și a unor capacități de calcul simple pentru a detecta dacă a fost rostit cuvântul-cheie. Această analiză, care are loc în mod continuu din momentul în care este pornit AVV-ul, este realizată exclusiv local. Abia după ce este recunoscut cuvântul-cheie se procesează înregistrările audio în vederea interpretării și a executării comenzii, ceea ce presupune în multe cazuri trimiterea lor către servere de la distanță prin internet. Detectarea cuvântului-cheie se bazează pe tehnici de învățare automată. Problema majoră în utilizarea de astfel de metode este faptul că detectarea se face în mod probabilistic. Astfel, pentru fiecare cuvânt sau expresie pronunțată, sistemul dă un scor de încredere care stabilește dacă acel cuvânt-cheie a fost de fapt pronunțat. Dacă punctajul se dovedește mai mare decât valoarea unui prag predefinit, se consideră că a fost rostit cuvântul-cheie. Prin urmare, un astfel de sistem nu este lipsit de erori: în unele cazuri, activarea poate să nu fie detectată chiar dacă a fost pronunțat cuvântul-cheie (respingere falsă), iar în alte cazuri activarea poate să fie detectată deși utilizatorul nu a rostit cuvântul-cheie (acceptare falsă).
19. În practică ar trebui să se ajungă la un compromis acceptabil între aceste două tipuri de erori, pentru a defini valoarea pragului. Totuși, deoarece detectarea falsă a cuvântului-cheie ar putea avea drept consecință transmiterea de înregistrări audio, este probabil să apară transmiteri neașteptate și nedorite de date. Foarte des, furnizorii de AVV-uri care implementează prelucrarea de la distanță folosesc un mecanism în doi pași pentru această detectare: un prim pas se realizează local la nivelul echipamentului, iar al doilea are loc pe serverele de la distanță unde are loc următoarea prelucrare a datelor. În acest caz, dezvoltatorii tind să stabilească de obicei un prag relativ scăzut, pentru a îmbunătăți experiența utilizatorului și pentru a asigura că atunci când utilizatorul pronunță cuvântul-cheie, acesta este recunoscut aproape de fiecare

⁵ Acest fapt a fost semnalat, de exemplu, aici: <https://www.amazon.science/blog/alexa-new-speech-recognition-abilities-showcased-at-interspeech>

dată – chiar dacă acest lucru înseamnă „supra-detectarea” lui –, apoi aplică un al doilea test de detecție pe server, care este mai restrictiv,.

2.5 Fragmentele de cod care prelucrează vocea și învățarea automată

20. AVV-urile se bazează pe metode de învățare automată pentru a efectua o gamă largă de sarcini (detectarea cuvântului-cheie, recunoașterea automată a vorbirii, procesarea limbajului natural, sinteza vorbirii etc.), și astfel necesită colectarea, selectarea, etichetarea etc. a unor seturi mari de date.
21. Suprareprezentările sau subreprezentările anumitor caracteristici statistice pot influența dezvoltarea sarcinilor bazate pe învățare automată și ulterior o reflectă în calculele AVV-ului și, deci, în modul său de funcționare. Astfel, calitatea datelor joacă un rol major în finețea și acuratețea procesului de învățare, la fel de mult ca și volumul datelor.
22. Pentru a crește calitatea AVV-urilor și a îmbunătăți metodele de învățare automată utilizate, proiectanții AVV ar putea dori să aibă acces la date referitoare la utilizarea dispozitivului în condiții reale – adică la fragmente de voce –, pentru a lucra la îmbunătățirea acestuia.
23. Fie că este vorba de validarea bazei de date de învățare sau de corectarea erorilor făcute la implementarea algoritmului, procesul de învățare și antrenare a sistemelor de inteligență artificială necesită obligatoriu intervenția umană. Această parte a activității, cunoscută sub numele de muncă digitală, ridică întrebări atât despre condițiile de muncă, cât și despre siguranță. În acest context, mass-media a semnalat și transferuri de date între proiectanții de AVV-uri și subcontractanți cu privire la care se presupune că nu au existat garanțiile necesare de protecție a vieții private.

3 ELEMENTE DE PROTECȚIE A DATELOR

3.1 Cadrul juridic

24. Cadrul juridic relevant al UE pentru AVV-uri este, în primă instanță, RGPD, deoarece prelucrarea datelor cu caracter personal face parte din funcția de bază a AVV-urilor. În plus față de RGPD, Directiva privind viața privată și comunicațiile electronice⁶ stabilește un standard specific pentru toți actorii care doresc să stocheze sau să acceseze informații stocate în echipamentele terminale ale unui abonat sau utilizator din SEE.
25. În conformitate cu definiția sintagmei „*echipament terminal*”⁷, telefoanele inteligente, televizoarele inteligente și dispozitivele IoT similare sunt exemple de echipamente terminale. Chiar dacă AVV-urile în sine sunt servicii software, ele operează întotdeauna prin intermediul unui dispozitiv fizic, de exemplu o boxă inteligentă sau un televizor inteligent. **AVV-urile utilizează rețele de comunicații electronice pentru a accesa aceste dispozitive fizice care sunt**

⁶ Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea vieții private în sectorul comunicațiilor publice (Directiva privind viața privată și comunicațiile electronice), astfel cum a fost modificată prin Directiva 2006/24/CE și prin Directiva 2009/136/CE (denumită în continuare „Directiva privind viața privată și comunicațiile electronice”).

⁷ Articolul 1 din Directiva 2008/63/CE a Comisiei din 20 iunie 2008 privind concurența pe piețele echipamentelor terminale de telecomunicații definește „*echipamentul terminal*” astfel: „(a) *echipamentul racordat în mod direct sau indirect la interfața unei rețele publice de telecomunicații, în scopul trimiterii, prelucrării sau recepționării de informații; în ambele cazuri de racordare (directă sau indirectă), aceasta se poate efectua prin cablu, fibre optice sau electromagnetic; racordarea este indirectă atunci când echipamentul este amplasat între terminal și interfața rețelei; (b) echipament pentru stațiile de sol pentru comunicații prin satelit;*”

„echipamente terminale” în sensul Directivei privind viața privată și comunicațiile electronice. În consecință, ori de câte ori un AVV stochează sau accesează informații în dispozitivul fizic conectat la acesta, se aplică dispozițiile articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiilor electronice⁸.

26. Orice operațiuni de prelucrare a datelor cu caracter personal care urmează după operațiunile de prelucrare menționate anterior, inclusiv prelucrarea datelor cu caracter personal obținute prin accesarea informațiilor din echipamentul terminal, trebuie să aibă de asemenea un temei legal în conformitate cu articolul 6 din RGPD pentru a fi legale⁹.
27. Atunci când solicită consimțământul pentru stocarea sau obținerea accesului la informații în conformitate cu articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice, operatorul de date va trebui să informeze persoana vizată despre toate scopurile prelucrării (adică despre „prelucrarea ulterioară”), inclusiv orice prelucrare ulterioară operațiunilor menționate mai sus. Consimțământul în conformitate cu articolul 6 din RGPD va fi, în general, cel mai potrivit temei juridic care să acopere prelucrarea ulterioară a datelor cu caracter personal. Prin urmare, consimțământul va reprezenta probabil temeiul juridic atât pentru stocarea informațiilor și obținerea accesului la informațiile deja stocate, cât și pentru prelucrarea datelor cu caracter personal ulterioară operațiunilor de prelucrare menționate anterior, va consta cel mai probabil în consimțământ. Într-adevăr, atunci când se evaluează conformitatea cu articolul 6 din RGPD, ar trebui să se țină seama de faptul că prelucrarea în ansamblu presupune activități specifice pentru care organul legislativ al UE a dorit să ofere o protecție suplimentară¹⁰. Mai mult, operatorii de date sunt obligați să ia în considerare impactul asupra drepturilor persoanelor vizate atunci când identifică temeiul juridic adecvat pentru a respecta principiul echității¹¹. Concluzia este că articolul 6 din RGPD nu poate fi invocat de către operatorii de date pentru a reduce protecția suplimentară prevăzută la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.
28. Astfel cum se arată în secțiunea 2.3 (pașii 2 și 3), AVV-urile actuale necesită acces la datele vocale stocate de dispozitivul AVV¹². Prin urmare, se aplică articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. Aplicabilitatea articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice înseamnă că stocarea informațiilor, precum și accesul la informațiile deja stocate într-un AVV necesită, de regulă, consimțământul prealabil al utilizatorului final¹³, dar permite două excepții: în primul rând, efectuarea sau facilitarea transmiterii unei comunicări printr-o rețea de comunicații electronice; sau, în al

⁸ A se vedea punctul 12 din Orientările CEPD 1/2020, pentru un raționament similar cu privire la vehiculele conectate (denumite în continuare „Orientările CEPD 1/2020”). A se vedea și CEPD, Avizul nr. 5/2019 privind interacțiunea dintre Directiva privind viața privată și comunicațiile electronice și RGPD, în special în ceea ce privește competența, sarcinile și prerogativele autorităților pentru protecția datelor.

⁹ Ibidem, punctul 41.

¹⁰ Avizul 5/2019, punctul 41.

¹¹ CEPD, Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, versiunea 2.0, 8 octombrie 2019, punctul 1.

¹² Este posibil ca viitoarele dispozitive AVV să adopte paradigma tehnicii de calcul de margine și să fie capabile să ofere local unele servicii. În acest caz, va fi necesar să se reevalueze aplicabilitatea Directivei privind viața privată și comunicațiile electronice.

¹³ A se vedea și Orientările 1/2020 ale CEPD, punctul 14.

doilea rând, în măsura în care este strict necesar pentru a furniza un serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.

29. A doua excepție („strict necesar pentru a furniza un serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator”) ar permite unui furnizor de servicii AVV să prelucreze datele utilizatorilor pentru a executa cererile acestora (vezi punctul 72 din secțiunea 3.4.1.) fără acordul prevăzut la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. În schimb, **consimțământul prevăzut la articolul 5 alineatul (3) din directivă ar fi necesar pentru** stocarea sau obținerea accesului la informații în **orice scop diferit de executarea cererii utilizatorilor** (de exemplu, pentru crearea de profiluri ale utilizatorilor). Operatorii de date ar trebui să coreleze acest consimțământ cu fiecare utilizator în parte. În consecință, operatorii ar trebui să prelucreze doar datele utilizatorilor neînregistrați în scopul de a le executa cererile.
30. AVV-urile pot capta accidental vocea unor persoane care nu intenționau să utilizeze un serviciu AVV. În primul rând, într-o anumită măsură și în funcție de AVV, expresia de activare poate fi schimbată. Persoanele care nu au cunoștință de această schimbare ar putea folosi accidental expresia de activare actualizată. În al doilea rând, AVV-urile pot detecta expresia de activare din greșeală sau în urma unei erori. Este foarte puțin probabil ca în cazul activării accidentale să se aplice vreuna dintre excepțiile prevăzute la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. În plus, consimțământul definit în RGPD trebuie să reprezinte o „manifestare de voință [...] lipsită de ambiguitate a persoanei vizate”. Astfel, este foarte puțin probabil ca o activare accidentală să poată fi interpretată drept consimțământ valabil. Dacă operatorii de date au cunoștință (de exemplu, prin analiză automată sau umană) de faptul că serviciul AVV a prelucrat accidental date cu caracter personal, ar trebui să verifice dacă există un temei juridic valabil pentru fiecare scop în care sunt prelucrate aceste date. În caz contrar, datele colectate accidental trebuie șterse.
31. Mai mult, trebuie precizat că datele cu caracter personal prelucrate de AVV-uri pot avea o natură extrem de sensibilă. Ele pot să conțină date cu caracter personal atât în ceea ce privește conținutul (semnificația cuvintelor rostite), cât și din punct de vedere al metainformațiilor (sexul sau vârsta vorbitorului etc.). CEPD reamintește că datele vocale sunt, în mod inerent, date biometrice cu caracter personal¹⁴. În consecință, atunci când datele de acest tip sunt prelucrate în scopul identificării unice a unei persoane fizice sau când sunt în mod inerent sau considerate a fi date cu caracter personal dintr-o categorie specială, prelucrarea trebuie să aibă drept temei juridic valabil în baza articolului 6 și să fie însoțită de o derogare de la articolul 9 din RGPD (vezi secțiunea 3.7 de mai jos).

3.2 Identificarea prelucrării datelor și a părților interesate

32. Având în vedere posibilitățile multiple de asistență pe care le poate oferi un AVV în atât de multe medii diferite în care își trăiește viața de zi cu zi o persoană vizată¹⁵, merită reamintit că

¹⁴ Articolul 4 punctul 14 din RGPD definește datele biometrice ca „date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice”.

¹⁵ De exemplu: acasă, într-un vehicul, pe stradă, la locul de muncă sau în orice alt spațiu privat, public sau profesional ori într-o combinație de astfel de spații.

este nevoie de multă grijă cu privire la prelucrarea datelor cu caracter personal, aceasta putând fi influențată și de diversele părți interesate.

3.2.1 Prelucrarea datelor cu caracter personal

33. Din perspectiva protecției datelor cu caracter personal, se observă mai multe constante indiferent de tipul AVV-ului (adică indiferent de tipul dispozitivului, de funcționalități, de servicii sau de combinația acestora) care poate fi utilizat de o persoană vizată. Aceste constante se referă la pluralitatea datelor cu caracter personal, a persoanelor vizate și a prelucrării datelor respective.

Pluralitatea tipurilor de date cu caracter personal

34. Definiția datelor cu caracter personal conform articolului 4 punctul 1 din RGPD include o mare varietate de date diferite și se aplică, într-un context neutru din punct de vedere tehnologic, oricărei informații care se referă la „o persoană fizică identificată sau identificabilă”¹⁶. Orice interacțiune a unei persoane vizate cu un AVV poate intra sub incidența acestei definiții. Odată ce are loc interacțiunea, pe durata funcționării AVV-ului pot fi prelucrate diverse date cu caracter personal, astfel cum este descris în secțiunea 2.4.
35. Prin urmare, de la cererea inițială până la răspunsul, executarea sau o acțiune ulterioară (de exemplu, configurarea unei alerte săptămânale), prima introducere de date cu caracter personal va continua să genereze astfel date cu caracter personal ulterioare. Acestea includ date primare (de exemplu, date privind contul, înregistrări vocale, istoricul comenzilor), date observate (de exemplu, date privind dispozitivul care au legătură cu persoana vizată, jurnale de activitate, activități online), precum și și date deduse sau derivate (de exemplu, crearea unui profil al utilizatorului). AVV-urile folosesc vorbirea pentru a intermedia între utilizatori și toate serviciile conectate (de exemplu, un motor de căutare, un magazin online sau un serviciu de streaming de muzică); dar, spre deosebire de alți intermediari, AVV-urile pot avea acces complet la conținutul cererilor și, prin urmare, furnizează proiectantului AVV o mare varietate de date cu caracter personal, în funcție de scopurile prelucrării.
36. Pluralitatea datelor cu caracter personal prelucrate atunci când se utilizează un AVV se referă și la pluralitatea categoriilor de date cu caracter personal cărora ar trebui să li se acorde atenție (vezi secțiunea 3.7 de mai jos). CEPD reamintește că, atunci când se prelucrează categorii speciale de date¹⁷, articolul 9 din RGPD impune operatorului să identifice o derogare valabilă de la interdicția de prelucrare prevăzută la articolul 9 alineatul (1) și un temei juridic valabil în conformitate cu articolul 6 alineatul (1), utilizând un mijloc adecvat dintre cele identificate la articolul 9 alineatul (2). Consimțământul explicit poate fi una dintre derogările adecvate în cazul în care temeiul juridic aplicat conform articolului 6 alineatul (1) este consimțământul. Articolul 9 menționează (în detaliu) și faptul că statele membre pot introduce condiții suplimentare referitoare la prelucrarea datelor biometrice sau a altor categorii speciale de date.

Pluralitatea persoanelor vizate

37. Atunci când se utilizează un AVV, se prelucrează date cu caracter personal chiar de la prima interacțiune cu AVV-ul. Pentru unele persoane vizate (utilizatorii înregistrați), aceasta înseamnă achiziționarea AVV-ului și/sau configurarea unui cont de utilizator. Pentru alte persoane vizate (utilizatorii neînregistrați), prelucrarea are loc prima dată când interacționează în mod conștient cu AVV-ul unei alte persoane vizate, care a achiziționat și/sau a configurat acest AVV. Pe lângă aceste două categorii de persoane vizate, există și o a treia: utilizatorii

¹⁶ Tot la articolul 4 punctul 1 din GDPR specifică și faptul că „o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale”.

¹⁷ Articolul 9 alineatul (1) din RGPD definește categoriile speciale de date cu caracter personal precizând următoarele: „Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice”.

accidentali care, înregistrați sau nu, transmit cereri către AVV în mod involuntar (de exemplu, rostind expresia corectă de activare fără să știe că AVV-ul este activ sau pronunțând alte cuvinte care sunt identificate în mod eronat de AVV ca expresie de activare).

38. Termenul „pluralitate a persoanelor vizate” se referă, de asemenea, la mai mulți utilizatori ai aceluiși AVV (de exemplu, un dispozitiv folosit în comun de utilizatori înregistrați și neînregistrați, de colegi, în familie, la școală) și la diferite tipuri de utilizatori pe baza condiției/stării lor (de exemplu, un adult, un copil, o persoană vârstnică sau cu handicap). În timp ce un AVV poate oferi o interacțiune mai ușoară cu un instrument digital, aducând multe avantaje pentru unele categorii de persoane vizate, este important să se aibă în vedere specificitățile fiecărei categorii de persoane vizate și contextul de utilizare a AVV-ului.

Pluralitatea prelucrării datelor

39. Tehnologiile utilizate pentru a pune la dispoziție un AVV au, de asemenea, impact asupra volumului de date prelucrat, și asupra tipurilor de prelucrări. Cu cât un AVV furnizează mai multe servicii sau funcții și cu cât este mai conectat la alte dispozitive sau servicii gestionate de alte părți, cu atât crește volumul de date cu caracter personal prelucrate, la fel ca și prelucrarea datelor în alte scopuri. Aceasta conduce la o multitudine de prelucrări efectuate prin mijloace automate, astfel cum se descrie în secțiunea 2. Pe lângă mijloacele automate, unele prelucrări pot implica și mijloace umane. Un exemplu în acest sens este cazul în care tehnologia implementată presupune intervenția umană, de pildă la revizuirea transcrierii vorbirii în text sau la furnizarea de adnotări privind datele cu caracter personal care pot fi utilizate pentru a insera modele noi într-o tehnologie de învățare automată. Acesta este cazul și atunci când oamenii analizează date cu caracter personal (de exemplu, metadate) pentru a îmbunătăți serviciul furnizat de un AVV.

3.2.2 Prelucrarea de către operatorii de date și persoanele împuternicite de aceștia

40. Persoanele vizate ar trebui să fie în măsură să înțeleagă și să identifice rolurile implicate și să poată contacta sau acționa cu fiecare dintre părțile interesate astfel cum este cerut de RGPD. Distribuția rolurilor nu ar trebui să fie în detrimentul persoanelor vizate, chiar dacă scenariile pot să fie complicate sau să evolueze în timp. Pentru evaluarea rolurilor lor, părțile interesate sunt invitate să consulte Orientările CEPD 7/2020 privind conceptele de operator de date și persoană împuternicită de operator în cadrul RGPD¹⁸.
41. După cum se indică la punctul 15, principalele părți interesate pot fi identificate ca având rol de furnizor sau proiectant, de dezvoltator de aplicații, de integrator, de proprietar sau o combinație între acestea. Sunt posibile diferite scenarii, în funcție de: activitatea fiecăruia în relația de afaceri a părților interesate, cererea utilizatorului, datele cu caracter personal, activitățile de prelucrare a datelor și scopurile părților interesate. Acestea ar trebui să decidă clar și să informeze persoanele vizate cu privire la condițiile în care va acționa fiecare dintre ele și să respecte rolurile care le revin ca operatori de date, operatori asociați sau persoane împuternicite de operatori, astfel cum sunt prevăzute pentru ei de RGPD¹⁹. Fiecare dintre ei poate prelua unul sau mai multe roluri, putând fi operator de date unic, operator asociat sau

¹⁸ CEPD, Orientările 7/2020 privind conceptele de operator de date și persoană împuternicită de operator în cadrul RGPD, V2.0, adoptate la 7 iulie 2021 (denumite în continuare „Orientările 7/2020”).

¹⁹ RGPD, articolele 12-14, articolul 26.

persoană împuternicită de un operator în contextul unei prelucrări de date și, în același timp, îndeplinind un alt rol în contextul unei alte prelucrări de date.

42. Dintr-o perspectivă la nivel înalt, proiectantul poate acționa ca operator de date atunci când stabilește scopurile și mijloacele unei prelucrări, dar poate interveni ca persoană împuternicită de operator atunci când prelucrează date cu caracter personal în numele altor părți, de exemplu în numele unui dezvoltator de aplicații. Prin urmare, datele utilizatorului AVV-ului ar fi prelucrate de mai mulți operatori: dezvoltatorul de aplicații și proiectantul. Este posibil și ca proiectantul, integratorul și dezvoltatorul să fie grupați într-un singur organism, care să acționeze ca operator unic. În orice caz, calificările aplicabile trebuie stabilite pe baza unei analize de la caz la caz.

Exemplul 1:

Proiectantul AVV-ului prelucrează datele utilizatorului în mai multe scopuri, inclusiv îmbunătățirea abilităților de înțelegere vocală ale AVV-ului și răspunsul cu precizie la solicitări. Prin urmare, cu toate că acest scop poate duce la prelucrarea unor date rezultate din utilizarea aplicațiilor furnizate de terți, există un singur operator de date: proiectantul AVV-ului, în numele căruia și pentru scopurile căruia se efectuează prelucrarea.

Exemplul 2:

O bancă oferă clienților săi o aplicație cu ajutorul căreia își pot gestiona conturile făcând interogări direct prin intermediul AVV-ului.

În prelucrarea datelor cu caracter personal sunt implicați doi actori: proiectantul AVV-ului și dezvoltatorul aplicației bancare.

În scenariul prezentat, banca este operatorul de date pentru furnizarea serviciului, deoarece stabilește scopurile și mijloacele esențiale de prelucrare aferente aplicației care permite interacțiunea cu asistentul. Într-adevăr, ea oferă o aplicație dedicată care permite utilizatorului, client al băncii, să-și gestioneze conturile de la distanță. În plus, decide asupra mijloacelor de prelucrare alegând o persoană împuternicită potrivită, care este proiectantul AVV-ului și care poate juca un rol important în asistarea cu cunoștințele sale de specialitate pentru a stabili aceste mijloace (de exemplu, poate opera platforma de dezvoltare care permite integrarea în AVV a aplicațiilor furnizate de terți, stabilind așadar cadrul și condițiile care trebuie respectate de dezvoltatorii de aplicații).

43. Din perspectiva persoanei vizată, trebuie precizat că mai multe părți interesate pot prelucra aceleași date cu caracter personal, chiar dacă persoana vizată nu se așteaptă cu adevărat ca în lanțul de procesare să fie implicate și alte părți în afară de furnizorul AVV-ului. Prin urmare, atunci când o persoană vizată realizează demersuri legate de datele sale cu caracter personal pe lângă furnizorul AVV-ului (de exemplu, în exercitarea drepturilor persoanei vizate), nu înseamnă automat că această acțiune se va aplica și prelucrării acelorași date cu caracter personal care sunt prelucrate de către o altă parte interesată. În cazul în care aceste părți interesate sunt operatori de date independenți, este important ca persoanele vizate să fie informate clar, prin explicarea diferitelor etape ale prelucrării și diferiților actori ai prelucrării. Mai mult, în cazurile cu operatori asociați ar trebui stabilit clar dacă fiecare operator are

competență să gestioneze toate drepturile persoanei vizate sau care operator este competent și pentru ce drept²⁰.

Exemplul 3:

În acest scenariu, proiectantul AVV-ului dorește să utilizeze datele colectate și prelucrate pentru serviciul furnizat de bancă pentru a-și îmbunătăți sistemul de recunoaștere vocală. Proiectantul AVV-ului, care prelucrează datele în scopuri proprii, va avea în acest caz statutul de operator pentru această prelucrare specifică.

44. Deoarece în lanțul de prelucrare pot fi implicate multe părți interesate, respectiv mulți angajați, pot apărea situații de risc dacă nu se instituie măsuri și garanții de protecție adecvate. Operatorii de date sunt responsabili pentru acestea și, prin urmare, ar trebui să se concentreze pe protejarea datelor cu caracter personal, în special prin alegerea unor parteneri de afaceri și a unor împuterniciți potriviți, prin aplicarea principiilor de protejare a vieții private începând cu momentul conceperii și în mod implicit²¹ prin implementarea unui nivel de securitate adecvat și a altor instrumente RGPD, precum audituri și acorduri juridice (de exemplu, articolul 26 în cazul operatorilor asociați sau articolul 28 din RGPD în cazul persoanelor împuternicite de operatori).
45. Ecosistemul unui AVV este unul complex, în care potențial mulți actori ar putea să prelucreze și să facă schimb de date cu caracter personal în calitate de operatori sau de persoane împuternicite de operatori. Este extrem de important să se clarifice rolul fiecărui actor în cadrul fiecărei prelucrări și să se respecte principiul reducerii la minimum a datelor inclusiv în ceea ce privește schimbul de date.
46. În plus, operatorii ar trebui să fie vigilenți la transferurile de date cu caracter personal și să garanteze nivelul de protecție necesar pe tot parcursul lanțului de prelucrare, în special atunci când utilizează servicii din afara SEE.

3.3 Transparența

47. Deoarece prelucrează date cu caracter personal (de exemplu, vocea utilizatorilor, locația sau conținutul comunicării), AVV-urile trebuie să respecte cerințele privind transparența din RGPD, astfel cum sunt reglementate la articolul 5 alineatul (1) litera (a), precum și la articolul 12 și articolul 13 (cu explicații în considerentul 58). Operatorii de date sunt obligați să informeze utilizatorii cu privire la prelucrarea datelor lor cu caracter personal într-o formă concisă, transparentă, inteligibilă și ușor accesibilă.
48. Nefurnizarea informațiilor necesare reprezintă o încălcare a obligațiilor, care poate afecta legitimitatea prelucrării datelor. Respectarea cerinței de transparență este un imperativ, deoarece servește ca mecanism de control al prelucrării datelor și permite utilizatorilor să își exercite drepturile. Informarea corespunzătoare a utilizatorilor cu privire la modul în care le sunt utilizate datele cu caracter personal face mai dificilă utilizarea abuzivă a AVV-ului de către operatorii de date în scopuri care depășesc cu mult de așteptările utilizatorilor. De exemplu,

²⁰ Orientările 7/2020, punctul 165.

²¹ Vezi CEPD, Orientările nr. 4/2019 privind articolul 25 „Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit”, versiunea 2.0, adoptată la 20 octombrie 2020.

tehnologiile brevetate care își propun să determine starea de sănătate și stările emoționale ale utilizatorului pe baza vocii acestuia și să adapteze în consecință serviciile furnizate.

49. Respectarea cerințelor de transparență poate fi o sarcină deosebit de dificilă pentru furnizorul de servicii AVV sau pentru orice altă entitate care acționează ca operator de date. Având în vedere natura specifică a AVV-urilor, operatorii se confruntă cu o serie de obstacole în încercarea de a respecta cerințele de transparență din RGPD:
- J **Utilizatori multipli:** operatorii ar trebui să informeze toți utilizatorii (înregistrați, neînregistrați și accidentali), nu numai utilizatorul care configurează AVV-ul.
 - J **Complexitatea ecosistemului:** astfel cum a fost explicat în secțiunea de detalii privind tehnologia, identitățile și rolurile celor care prelucrează date cu caracter personal atunci când se utilizează un AVV sunt departe de a fi evidente pentru utilizatori.
 - J **Particularitățile interfeței vocale:** sistemele digitale nu sunt încă potrivite pentru interacțiuni exclusiv vocale, așa cum demonstrează utilizarea aproape sistemică a unui ecran însoțitor. Cu toate acestea, este o necesitate adaptarea informării la interfața vocală și trebuie să existe posibilitatea de a informa utilizatorul în mod clar și corect prin acest mijloc.
50. AVV-urile pot fi considerate mașini cu stări finite care trec printr-o serie de stări în timpul funcționării obișnuite. Ele pot asculta local, pentru a detecta expresiile de activare, sau pot interacționa cu un server aflat la distanță pentru a răspunde unei comenzi, dar se pot afla în multe alte stări în funcție de context (de exemplu, dacă există un sunet ambiental de fundal) sau de utilizatorul care vorbește cu ele (de exemplu, pot vorbi cu un utilizator identificat sau necunoscut). Din păcate, aceste situații sunt caracterizate de o asimetrie substanțială a informațiilor în raport cu utilizatorul, acesta neputând ști cu siguranță dacă dispozitivul ascultă, și cu atât mai puțin în ce stare se află dispozitivul.
51. Este foarte recomandat ca proiectanții și dezvoltatorii de AVV-uri să ia măsuri adecvate pentru a compensa aceste asimetrii, făcând ca funcționarea AVV-urilor să fie mai interactivă. Utilizatorii trebuie informați cu privire la starea în care se află dispozitivul în momentul respectiv. Această îmbunătățire a transparenței poate fi realizată atât făcând dialogul om-mașină mai interactiv (de exemplu, dispozitivul ar putea confirma într-un fel sau altul primirea unei comenzi vocale), fie comunicând starea mașinii prin semnale specifice. Există multe opțiuni care pot fi explorate în acest sens, care variază de la utilizarea unor confirmări vocale specifice și a unor pictograme sau semnale luminoase vizibile până la utilizarea de afișaje pe dispozitiv.
52. Aceste aspecte sunt deosebit de relevante având în vedere pluralitatea utilizatorilor și prezența printre aceștia a unor categorii vulnerabile de persoane, precum copiii, vârstnicii sau utilizatorii cu deficiențe de vedere și auz.
53. Din problemele de mai sus se desprind două întrebări importante: care este cel mai fezabil mod de informare a utilizatorilor și când este momentul potrivit pentru a-i informa? Aceste probleme ar trebui examinate în continuare în două situații diferite, în funcție de existența unui singur utilizator al AVV-ului (de exemplu, în cazul unui telefon inteligent personal) sau a mai multor utilizatori posibili (de exemplu, un dispozitiv inteligent casnic). Folosirea tehnologiei AVV, o versiune secundară a acestor două setări de bază, ar putea de asemenea să existe de exemplu atunci când un utilizator are un telefon inteligent personal și îl conectează la un automobil. Sistemul AVV al telefonului inteligent, despre care se preconizează în mod

rezonabil că va fi folosit doar de acel utilizator, este acum „extins” la celelalte persoane din automobil.

54. În prezent, toate AVV-urile sunt conectate la un cont de utilizator și/sau sunt configurate de o aplicație care necesită un astfel de cont. Întrebarea cu privire la modalitatea în care operatorii de date pot aborda informarea acestor utilizatori cu privire la politica de confidențialitate în timp ce configurează AVV-ul ar trebui abordată astfel cum se descrie în Orientările privind transparența ale Grupului de lucru articolul 29. Aplicațiile ar trebui să pună la dispoziție informațiile necesare într-un magazin online înainte de descărcare²². În acest fel, informațiile ar fi oferite cât mai curând posibil, și cel târziu la momentul obținerii datelor cu caracter personal. Unii furnizori de AVV-uri includ aplicații ale terților în configurarea implicită a AVV-ului, astfel încât aceste aplicații să poată executa aceste aplicații folosind expresii de activare specifice. AVV-urile care utilizează această strategie de implementare a aplicațiilor terților ar trebui să se asigure că utilizatorii primesc informațiile necesare și despre prelucrarea de către terți.
55. Cu toate acestea, mulți proiectanți de AVV-uri solicită conturi de utilizator AVV care asociază serviciul AVV cu o serie de alte servicii precum e-mail, streaming video sau achiziții, pentru a numi doar câteva. Decizia proiectantului AVV de a asocia contul cu multe servicii diferite are ca efect impunerea unor politici de confidențialitate foarte extinse și complexe. Lungimea și complexitatea acestor politici de confidențialitate împiedică în mare măsură îndeplinirea principiului transparenței.

Exemplul 4:

Proiectantul unui AVV cere utilizatorilor săi să aibă un cont pentru a accesa serviciul AVV. Acest cont de utilizator nu este specific serviciului AVV și poate fi utilizat pentru alte servicii oferite de proiectantul AVV-ului, cum ar fi e-mail, stocare în cloud și platforme de comunicare socială. Pentru a crea contul, utilizatorii trebuie să citească și să accepte o politică de confidențialitate de 30 de pagini. Politica cuprinde informații privind prelucrarea datelor cu caracter personal de către toate serviciile care ar putea fi asociate contului.

Informațiile furnizate de proiectantul AVV în acest caz nu pot fi considerate concise, iar complexitatea lor reduce transparența necesară. Prin urmare, proiectantul AVV-ului nu ar respecta cerințele de transparență prevăzute la articolele 12 și 13 din RGPD.

56. Deși cel mai comun mod de a furniza informațiile necesare este în scris, RGPD permite și „alte mijloace”. Considerentul 58 prevede în mod explicit că informațiile pot fi furnizate în format electronic, de exemplu printr-un site. În plus, la alegerea metodei adecvate de informare a persoanelor vizate, ar trebui să se țină seama de circumstanțele specifice, cum este modul în care operatorul de date și persoana vizată interacționează de obicei unul cu celălalt²³. O opțiune pentru dispozitivele fără ecran ar putea fi furnizarea unui link care este ușor de înțeles, fie direct, fie într-un e-mail. Soluțiile deja existente ar putea servi drept exemplu pentru informare – de exemplu, practicile centrelor de intermediere telefonică de a notifica apelantul cu privire la înregistrarea apelului și de a-l direcționa către politicile lor de confidențialitate. Constrângerile AVV-urilor fără ecran nu scutesc operatorul de date de obligația de a furniza informațiile necesare conform RGPD la configurarea AVV-ului sau la instalarea sau utilizarea

²² Orientări privind transparența în temeiul Regulamentului 2016/679, GL260 rev. 01, aprobate de CEPD (denumite în continuare „Orientările GL260 ale GL29”), punctul 11.

²³ Orientările GL260 ale GL29, punctul 19.

unei aplicații AVV. Furnizorii și dezvoltatorii AVV-urilor ar trebui să dezvolte interfețe vocale care să faciliteze informarea obligatorie.

57. AVV-urile ar putea fi de mare interes pentru utilizatorii cu deficiențe de vedere, deoarece oferă un mijloc alternativ de interacțiune cu servicii informatice care se bazează în mod tradițional pe informații vizuale. În conformitate cu articolul 12 alineatul (1) din RGPD, furnizarea informațiilor necesare este posibilă pe cale verbală exclusiv la solicitarea persoanei vizate, dar nu ca metodă implicită. Totuși, constrângerile AVV-urilor fără ecran ar necesita mijloace automate de informare verbală, care ar putea fi potențate prin mijloace scrise. Atunci când utilizează mesaje audio pentru informarea persoanelor vizate, operatorii de date ar trebui să furnizeze informațiile necesare într-un mod concis și clar. Mai mult, persoanele vizate ar trebui să aibă posibilitatea de a asculta din nou mesajul²⁴.
58. Luarea măsurilor corespunzătoare pentru a respecta cerințele de transparență din RGPD este un demers mai complex atunci când AVV-ul este folosit de mai mulți utilizatori, alții decât proprietarul dispozitivului. Proiectanții AVV-urilor trebuie să aibă în vedere cum să informeze în mod corespunzător utilizatorii neînregistrați și pe cei accidentali atunci când le sunt prelucrate datele cu caracter personal. Atunci când consimțământul reprezintă temeiul juridic pentru prelucrarea datelor utilizatorilor, aceștia trebuie informați în mod corespunzător pentru a avea un consimțământ valabil²⁵.
59. Pentru a se conforma RGPD, operatorii de date ar trebui să găsească o modalitate de a informa nu doar utilizatorii înregistrați, ci și utilizatorii neînregistrați și pe cei accidentali ai AVV-ului. Acești utilizatori ar trebui informați cât mai curând posibil, și cel mai **târziu la momentul** prelucrării datelor. Această condiție ar putea fi deosebit de greu de îndeplinit în practică.
60. De asemenea, particularitățile corporațiilor nu ar trebui folosite în detrimentul persoanelor vizate. Deoarece multe părți interesate sunt companii active la nivel mondial sau sunt bine cunoscute pentru o anumită activitate comercială (de exemplu, telecomunicații, comerț electronic, tehnologii informaționale, activități pe web), modul în care furnizează un serviciu AVV ar trebui să fie clar. Informarea adecvată ar trebui să permită persoanelor vizate ar trebui să înțeleagă dacă utilizarea AVV-ului va fi legată de alte activități de prelucrare gestionate de furnizorul de servicii AVV (de exemplu, telecomunicații, comerț electronic, tehnologii informaționale sau activități pe web), în afară de utilizarea strictă a AVV-ului.

Exemplul 5:

Pentru a utiliza asistentul său, proiectantul unui AVV care oferă și o platformă de socializare și un motor de căutare impune utilizatorului să își asocieze contul cu asistentul. Prin asocierea contului cu AVV-ul utilizat, proiectantul poate îmbunătăți profilul utilizatorilor săi prin folosirea asistentului, a aplicațiilor (sau abilităților) instalate, a comenzilor plasate etc. Prin urmare, interacțiunile cu asistentul sunt o nouă sursă de informații referitoare la un utilizator. Proiectantul AVV-ului ar trebui să furnizeze utilizatorilor informații clare cu privire la modul în care vor fi prelucrate datele lor pentru fiecare serviciu și să instituie mijloace de control care să permită utilizatorului să aleagă dacă datele vor fi utilizate sau nu pentru crearea profilului.

²⁴ Orientările GL260 ale GL29, punctul 21.

²⁵ RGPD, articolul 4 punctul 11.

Recomandări

61. Atunci când utilizatorii sunt informați despre prelucrarea prin AVV a datelor cu caracter personal prin utilizarea unei politici de confidențialitate a contului de utilizator, iar contul este asociat altor servicii independente (de exemplu, e-mail sau achiziții online), CEPD recomandă ca politica de confidențialitate să aibă o secțiune clar separată referitoare la prelucrarea datelor cu caracter personal prin intermediul AVV-ului.
62. Informațiile furnizate utilizatorului trebuie să corespundă exact operațiunilor de colectare și prelucrare care sunt efectuate. În timp ce eșantioanele de voce conțin și unele metainformații (de exemplu, nivelul de stres al vorbitorului), nu este în mod automat clar dacă și cum se realizează o astfel de analiză. Este crucial ca operatorii să fie transparenți cu privire la aspectele specifice ale datelor brute pe care le prelucrează.
63. În plus, ar trebui să fie întotdeauna evident în ce stare se află AVV-ul. Utilizatorii ar trebui să fie capabili să își dea seama dacă AVV-ul ascultă în momentul respectiv pe circuitul său în buclă închisă și mai ales dacă transmite informații către partea sa de back-end. Aceste informații ar trebui să fie accesibile și persoanelor cu dizabilități, de exemplu celor care suferă de daltonism sau de surditate (anacuzie). Trebuie acordată o atenție specială faptului că AVV-urile presupun un scenariu de utilizare în care contactul vizual cu dispozitivul nu este necesar. Prin urmare, toate feedbackurile oferite utilizatorilor, inclusiv schimbări privind starea ar trebui să fie disponibile cel puțin în formă vizuală și acustică.
64. Ar trebui acordată o atenție specială cazului în care dispozitivele permit adăugarea de funcționalități ale terților („aplicații” pentru AVV). În timp ce anumite informații generale pot fi furnizate utilizatorului atunci când aceștia sunt cei care adaugă o astfel de funcționalitate (având în vedere că este alegerea utilizatorului), în timpul utilizării normale a dispozitivului, limitele dintre diferiții operatori implicați pot fi mult mai puțin clare, de exemplu utilizatorul poate să nu fie suficient de informat cu privire la modul în care îi sunt prelucrate datele, precum și cu privire la persoana care realizează prelucrarea într-o anumită interogare.
65. În conformitate cu articolul 12 din RGPD, toate informațiile despre prelucrarea pe baza datelor colectate și derivate din prelucrarea vocii înregistrate ar trebui să fie disponibile utilizatorilor.
66. Operatorii datelor provenite de la AVV-uri ar trebui să fie transparenți cu privire la tipul de informații care pot fi obținute de AVV despre mediul în care se află, de exemplu, dar fără a se limita la alte persoane din cameră, muzica din fundal, orice prelucrare a vocii în scopuri medicale sau de marketing sau în alte scopuri, animale de companie etc.

3.4 Limitarea scopului și temeiul juridic

67. Prelucrarea de către AVV-uri a cererilor transmise vocal are un scop evident: executarea cererii. Adesea există însă și scopuri suplimentare care nu sunt atât de evidente, cum ar fi îmbunătățirea capacităților AVV-ului de înțelegere a limbajului natural prin antrenarea modelului AVV cu tehnici de învățare automată. Printre cele mai frecvente scopuri pentru care un AVV prelucrează date cu caracter personal regăsim:

) Executarea cererilor utilizatorilor

) Îmbunătățirea AVV-ului prin antrenarea modelului de învățare automată, revizuire umană și etichetarea transcrierilor vocale

) Identificarea utilizatorilor (folosind date vocale)

J Crearea de profiluri ale utilizatorilor pentru conținut personalizat sau publicitate personalizată

68. Datorită rolului lor de intermediari și modului în care sunt proiectate, AVV-urile prelucrează o mare varietate de date cu și fără caracter personal. Acest lucru face posibilă prelucrarea datelor cu caracter personal în numeroase scopuri, nu doar pentru a răspunde la cererile utilizatorilor și care ar putea trece complet neobservate. Analizând datele colectate prin intermediul AVV-urilor se pot afla sau deduce interesele utilizatorilor, programul acestora, rutele pe care conduc sau obiceiurile lor. Ar putea fi astfel posibilă prelucrarea datelor cu caracter personal în scopuri neprevăzute (de exemplu, pentru analiza sentimentelor sau evaluarea stării de sănătate²⁶), care ar fi cu mult peste așteptările rezonabile ale utilizatorilor.
69. Operatorii de date ar trebui să își specifice în mod clar scopul (scopurile) în raport cu contextul în care este utilizat AVV-ul, astfel încât să fie înțelese în mod clar de persoanele vizate (de exemplu, prezentarea scopurilor pe categorii). În conformitate cu articolul 5 alineatul (1) din RGPD, datele cu caracter personal trebuie colectate în scopuri specifice, explicite și legitime și nu trebuie prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

3.4.1 Executarea cererilor utilizatorilor

70. Principalul scop pentru un AVV este de a emite comenzi vocale care trebuie executate de AVV sau de o aplicație sau un serviciu asociat (de exemplu, un serviciu de difuzare de muzică, un serviciu de hărți sau un sistem de blocare electronică). Prin urmare, ar putea fi prelucrată vocea utilizatorului, eventual și alte date (de exemplu, poziția utilizatorului atunci când solicită un traseu către o anumită destinație).

Exemplul 6:

Pasagerul unei mașini inteligente, dotată cu AVV, cere să afle traseul către cea mai apropiată benzinărie. AVV-ul procesează vocea utilizatorului pentru a înțelege comanda și poziția mașinii pentru a găsi traseul, pe care îl trimite apoi la componenta inteligentă pentru afișare pe ecranul mașinii.

71. În măsura în care procesarea comenzilor vocale implică stocarea de date sau accesul la informațiile stocate în dispozitivele terminale ale utilizatorului final, trebuie respectate dispozițiile articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. În timp ce articolul 5 alineatul (3) include și principiul general conform căruia stocarea sau accesul respectiv necesită acordul prealabil al utilizatorului final, acesta prevede și o derogare de la cerința privind consimțământul atunci când este „strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator”. În măsura în care datele vocale sunt prelucrate pentru a executa cererile utilizatorului, acestea sunt exceptate de la cerința privind consimțământul prealabil.
72. După cum s-a indicat anterior, orice operațiune de prelucrare a datelor cu caracter personal ulterioară stocării sau accesării informațiilor în dispozitivul terminal al utilizatorilor finali trebuie să aibă un temei juridic în conformitate cu articolul 6 din RGPD pentru a fi legală.
73. În cadrul unui AVV au loc două operațiuni de prelucrare consecutive. După cum s-a menționat mai sus, pentru prima este nevoie de acces la AVV [și, prin urmare, trebuie îndeplinite

²⁶ Eoghan Furey, Juanita Blue, „Alexa, Emotion, Privacy and GDPR”, prezentare în cadrul Conferinței Human Computer Interaction, iulie [2018].

condițiile de la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice]. În plus față de condițiile impuse de articolul 5 alineatul (3) din directivă, al doilea pas necesită de asemenea un temei juridic conform articolului 6 din RGPD.

74. Atunci când o persoană ia decizia de a utiliza un AVV, această acțiune presupune în general ca utilizatorul inițial să înregistreze mai întâi un cont pentru a activa AVV-ul. Cu alte cuvinte, această situație se referă la o relație contractuală²⁷ între utilizatorul înregistrat și operatorul datelor obținute de AVV. Având în vedere fondul și obiectivul său fundamental, scopul principal al acestui contract constă în utilizarea AVV-ului pentru a executa cererea de asistență venită din partea utilizatorului.
 75. Prin urmare, orice prelucrare a datelor cu caracter personal care este necesară pentru a executa cererea utilizatorului se poate baza pe temeiul juridic al executării contractului²⁸. Prelucrarea respectivă include în special captarea solicitării vocale a utilizatorului, transcrierea sa în format text, interpretarea sa, schimbul de informații cu sursele de cunoștințe pentru a pregăti răspunsul și apoi transcrierea în forma unui răspuns vocal final, cu care se încheie cererea utilizatorului.
 76. Executarea unui contract poate reprezenta temeiul juridic pentru prelucrarea datelor cu caracter personal în cadrul procesului de învățare automată atunci când este necesar pentru furnizarea serviciului. Prelucrarea datelor cu caracter prin intermediul învățării automate în alte scopuri care nu sunt necesare, cum ar fi îmbunătățirea serviciului, nu trebuie să se bazeze pe temeiul juridic respectiv.
 77. Nu în ultimul rând, temeiurile juridice ale executării contractului și consimțământul conform RGPD nu trebuie confundate. Consimțământul dat pentru a fi parte la un contract, adică agrearea contractului, face parte din valabilitatea contractului respectiv și nu se referă la sensul specific al termenului „consimțământ” conform RGPD²⁹.
 78. Atunci când utilizarea unui AVV nu necesită configurarea în prealabil a unui cont de utilizator pentru AVV, consimțământul ar putea reprezenta un posibil temei juridic.
- 3.4.2 Îmbunătățirea AVV-ului prin antrenarea sistemelor de învățare automată și revizuirea manuală a transcrierilor și vocii
79. Accentele și variațiile vorbirii umane sunt vaste. În timp ce toate AVV-urile sunt funcționale odată scoase din cutie, performanța lor se poate îmbunătăți prin ajustarea lor în funcție de caracteristicile specifice ale vorbirii utilizatorilor. Astfel cum s-a menționat în secțiunea 2.6, acest proces de ajustare se bazează pe metode de învățare automată și constă în două procese: adăugarea la setul de date folosit pentru antrenarea AVV-ului a unor noi date colectate de la utilizatorii săi și revizuirea umană a datelor prelucrate pentru executarea unei fracțiuni din cereri.

Exemplul 7:

²⁷ Sub condiția existenței unui „contract valabil încheiat cu persoana vizată”, extras din Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate („Orientările 2/2019”), punctul 26.

²⁸ În conformitate cu Orientările 2/2019, care afirmă în plus că Avizul 06/2014 rămâne relevant pentru articolul 6 alineatul (1) litera (b) și RGPD (vezi în special, paginile 11, 16, 17, 18 și 55 din Avizul 06/2014).

²⁹ Vezi Orientările 2/2019, respectiv punctele 18, 19, 20, 21 și 27.

Un utilizator de AVV trebuie să rostească de trei ori aceeași comandă vocală, pentru că AVV-ul nu o înțelege. Cele trei comenzi vocale și transcrierile aferente sunt transmise unor revizori umani care verifică și corectează transcrierile. Comenzile vocale și transcrierile revizuite sunt adăugate la setul de date folosit pentru antrenarea AVV-ului, în vederea îmbunătățirii performanței sale.

80. Activitățile de prelucrare descrise în exemplu nu trebuie considerate (strict) „*necesare pentru executarea unui contract*” în sensul articolului 6 alineatul (1) litera (b) din RGPD și, prin urmare, necesită un alt temei juridic dintre cele menționate la articolul 6 din RGPD. Principalul motiv este faptul că AVV-urile sunt deja funcționale atunci când sunt scoase din cutie și pot funcționa deja în modul (strict) necesar pentru executarea contractului. CEPD nu consideră că articolul 6 alineatul (1) litera (b) ar constitui la modul general un temei juridic adecvat pentru prelucrarea în scopul îmbunătățirii unui serviciu sau în scopul realizării de funcții noi în cadrul unui serviciu existent. În majoritatea cazurilor, un utilizator devine parte a unui contract pentru a folosi un serviciu existent. Deși posibilitatea de a aduce îmbunătățiri și modificări serviciului poate fi inclusă în mod curent printre clauzele contractuale, de obicei prelucrarea în acest scop nu poate fi considerată ca fiind necesară în mod obiectiv pentru executarea contractului încheiat cu utilizatorul.

3.4.3 Identificarea utilizatorilor³⁰ (prin utilizarea de date vocale)

81. Utilizarea datelor vocale pentru identificarea utilizatorilor presupune prelucrarea unor date biometrice, astfel cum sunt definite la articolul 4 punctul 1 din RGPD. În consecință, operatorul de date va trebui să identifice o derogare în temeiul articolului 9 din RGPD, pe lângă identificarea unui temei juridic în conformitate cu articolul 6 din RGPD³¹.
82. Dintre derogările enumerate la articolul 9 din RGPD, numai consimțământul explicit al persoanelor vizate pare să fie aplicabil în acest scop specific.
83. Totuși, întrucât acest scop necesită aplicarea regimului juridic specific al articolului 9 din RGPD, în secțiunea 3.8 vor fi date mai multe detalii referitoare la prelucrarea categoriilor speciale de date.

3.4.4 Crearea de profiluri ale utilizatorilor pentru conținut personalizat sau publicitate personalizată

84. După cum s-a menționat mai sus, AVV-urile au acces la conținutul tuturor comenzilor vocale, chiar și atunci când acestea sunt destinate obținerii unor servicii furnizate de terți. Acest acces ar permite proiectantului unui AVV să construiască profiluri de utilizator foarte precise, care ar putea fi utilizate pentru a oferi servicii sau reclame personalizate.

³⁰ Din punct de vedere tehnic, trebuie făcută distincția între noțiunea de identificare și cea de verificare (autentificare). Identificarea este un proces de căutare și comparare de tip „unu-la-mai-multe” (1: N) și necesită în principiu o bază de date care cuprinde mai multe persoane. În schimb, prelucrarea în scop de verificare constă într-o comparație de tip „unu-la-unu” (1:1) și se utilizează pentru a verifica și confirma, prin comparare biometrică, dacă o persoană este aceeași cu cea de la care provin datele biometrice. Potrivit cunoștințelor CEPD, AVV-urile de pe piață se bazează exclusiv pe utilizarea tehnologiilor de identificare a vorbitorilor.

³¹ RGPD consideră că simpla natură a datelor nu este întotdeauna suficientă pentru a stabili dacă se încadrează într-o categorie specială de date, deoarece „prelucrarea fotografiilor [...] intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice” (considerentul 51). Același raționament se aplică și în cazul vocii.

Exemplul 8:

De fiecare dată când un utilizator AVV efectuează o căutare pe Internet, AVV-ul adaugă la profilul utilizatorului etichete care semnalizează subiecte de interes pentru acesta. Rezultatele pentru fiecare căutare nouă sunt prezentate utilizatorului într-o ordine determinată de etichetele respective.

Exemplul 9:

De fiecare dată când un utilizator AVV face o achiziție printr-un serviciu de comerț electronic, AVV-ul stochează o înregistrare a comenzii de cumpărare. Furnizorul AVV-ului permite unor terți să transmită utilizatorului acestui AVV reclame țintite, pe baza achizițiilor anterioare.

85. Personalizarea conținutului poate (dar nu întotdeauna) să constituie un element intrinsec și așteptat al unui AVV. Dacă prelucrarea în acest scop poate sau nu să fie considerată un aspect intrinsec al serviciului oferit de AVV va depinde de natura precisă a serviciului furnizat, de așteptările persoanei vizate obișnuite – având în vedere nu doar condițiile de furnizare a serviciului, ci și modul în care serviciul este promovat în rândul utilizatorilor – și dacă serviciul poate să fie furnizat nepersonalizat³².
86. În cazul în care personalizarea are loc în contextul unei relații contractuale și ca parte a unui serviciu cerut în mod expres de utilizatorul final (iar prelucrarea se limitează la ceea ce este strict necesar pentru a furniza acest serviciu), prelucrarea respectivă se poate întemeia pe articolul 6 alineatul (1) litera (b) din RGPD.
87. Dacă prelucrarea nu este strict „necesară pentru executarea unui contract” în sensul articolului 6 alineatul (1) litera (b) din RGPD, furnizorul AVV-ului trebuie, în principiu, să solicite consimțământul persoanei vizate. Mai precis, deoarece consimțământul va fi necesar în conformitate cu articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice pentru stocarea sau obținerea accesului la informații (vezi punctele 28-29 de mai sus), în principiu tot consimțământul – în conformitate cu articolul 6 alineatul (1) litera (a) din RGPD – va reprezenta temeiul juridic adecvat pentru prelucrarea datelor cu caracter personal în urma operațiunilor respective, întrucât justificarea lor prin interesul legitim ar putea risca, în anumite cazuri, să împiedice obținerea nivelului suplimentar de protecție prevăzut la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.
88. În ceea ce privește crearea de profiluri ale utilizatorilor în scopuri publicitare, trebuie precizat că acest scop nu este considerat niciodată ca fiind un serviciu cerut în mod explicit de utilizatorul final. Prin urmare, în cazul procesării în acest scop trebuie obținut în mod sistematic consimțământul utilizatorilor.

Recomandări

89. Utilizatorii trebuie să fie informați cu privire la scopul prelucrării datelor cu caracter personal, iar acest scop trebuie să corespundă așteptărilor pe care le au cu privire la dispozitivul pe care îl achiziționează. În cazul unui AVV, acest scop – din punctul de vedere al utilizatorului – este, în mod evident, prelucrarea vocii cu unicul scop de a interpreta cererea lor și de a oferi

³² A se vedea și Orientările 2/2019, punctul 57.

răspunsuri pertinente (fie răspunsuri la o întrebare, fie alte reacții, precum acționarea de la distanță a unui întrerupător).

90. Atunci când prelucrarea datelor cu caracter personal se bazează pe consimțământ, acesta *„trebuie să fie exprimat în raport cu unul sau mai multe scopuri specifice și [...] persoana vizată [trebuie] să aibă posibilitatea de a alege în legătură cu fiecare dintre acestea”*. Mai mult, *„un operator care solicită consimțământul pentru o serie de scopuri diferite ar trebui să ofere o opțiune separată pentru fiecare scop în parte, astfel încât să permită utilizatorilor să acorde un consimțământ specific pentru scopuri specifice”*³³. De exemplu, utilizatorii ar trebui să își poată exprima separat consimțământul sau refuzul pentru revizuirea manuală și etichetarea transcrierilor vocale sau pentru utilizarea datelor lor vocale în scopul identificării/autentificării utilizatorilor (vezi secțiunea 3.7).

3.5 Prelucrarea datelor referitoare la copii

91. Și copiii pot interacționa cu AVV-urile sau își pot crea propriile profiluri, conectate la cele ale adulților. Unele AVV-uri sunt încorporate în dispozitive destinate în mod special copiilor.
92. În cazul în care temeiul juridic al prelucrării este executarea unui contract, condițiile pentru prelucrarea datelor referitoare la copii vor depinde de dreptul național al contractelor.
93. În cazul în care temeiul juridic al prelucrării datelor este consimțământul, în conformitate cu articolul 8 alineatul (1) din RGPD, prelucrarea datelor copiilor este legală numai *„dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului”*. În consecință, pentru a respecta RGPD, atunci când temeiul juridic este reprezentat de consimțământ trebuie solicitată permisiunea explicită a părinților sau a tutorilor pentru a colecta, prelucra și stoca date referitoare la copii (voce, transcrieri etc.).
94. Controalele parentale sunt disponibile într-o anumită măsură, dar în forma lor actuală nu sunt ușor de utilizat (de exemplu, este necesară contractarea unui serviciu nou) sau au capacități limitate. Operatorii de date ar trebui să investească în realizarea unor mijloace prin care părinții sau tutorii să poată controla utilizarea AVV-urilor de către copii.

3.6 Păstrarea datelor

95. AVV-urile prelucrează și generează o mare varietate de date cu caracter personal, precum vocea, transcrierile vocale, metadatele sau jurnalele de sistem. Aceste tipuri de date ar putea fi prelucrate pentru o gamă largă de scopuri, de exemplu furnizarea unui serviciu, îmbunătățirea PLN, personalizare sau cercetare științifică. În conformitate cu principiul RGPD de limitare a stocării datelor, AVV-urile nu trebuie să stocheze date pe o perioadă mai lungă decât este necesar în scopurile pentru care sunt prelucrate datele cu caracter personal. Prin urmare, perioadele de păstrare a datelor ar trebui alese în funcție de diferitele scopuri ale prelucrării. Furnizorii de servicii AVV sau terții care furnizează servicii prin intermediul AVV-urilor ar trebui să evalueze perioada maximă de păstrare pentru fiecare set de date și fiecare scop în parte.

³³ A se vedea CEPD, [Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679](#), adoptate la 4 mai 2020, secțiunea 3.2.

96. Principiul reducerii la minimum a datelor este strâns legat de principiul limitării legate de stocare. Operatorii de date trebuie să limiteze nu doar perioada de stocare a datelor, ci și tipul și volumul de date.
97. Operatorii de date ar trebui să își pună, printre altele, următoarele întrebări: Este necesară stocarea tuturor înregistrărilor vocale sau a tuturor transcrierilor pentru a atinge scopul X? Mai este necesară stocarea datelor vocale odată ce a fost stocată transcrierea lor? Dacă da, în ce scop? Cât timp sunt necesare datele vocale sau cele transcrise, pentru fiecare scop? Răspunsurile la aceste întrebări și la altele similare vor defini perioadele de păstrare, care trebuie să facă parte din informațiile comunicate persoanelor vizate.
98. Unele AVV-uri stochează în mod implicit date personale, de exemplu fragmente vocale sau transcrieri, pe o perioadă nedeterminată, oferind în același timp utilizatorilor mijloace de ștergere a acestor date. Păstrarea datelor cu caracter personal pe termen nelimitat contravine principiului limitării legate de stocare. Faptul că se oferă persoanelor vizate mijloace de ștergere a datelor cu caracter personal nu elimină responsabilitatea operatorului de a defini și aplica o politică de păstrare a datelor.
99. Proiectarea AVV-urilor trebuie să se aibă în vedere comenzi prin care utilizatorii să-și poată șterge datele cu caracter personal din dispozitive și din toate sistemele de stocare la distanță. Aceste comenzi pot fi necesare pentru a răspunde unor tipuri diferite de solicitări ale utilizatorilor – de exemplu, o cerere de ștergere a datelor sau retragerea consimțământului dat anterior. La proiectarea unora dintre AVV-uri nu s-a ținut cont de această obligație³⁴.
100. Ca și în alte contexte, operatorii de date pot avea nevoie să păstreze date cu caracter personal ca dovadă a unui serviciu oferit unui utilizator, pentru a se conforma unei obligații legale. Operatorul poate să păstreze date cu caracter personal pe baza acestui temei juridic. Totuși, datele păstrate ar trebui să fie la nivelul minim necesar pentru respectarea obligației legale respective și pentru o perioadă minimă de timp. Desigur, datele păstrate în scopul respectării unei obligații legale nu trebuie utilizate în alte scopuri fără un temei juridic conform articolului 6 din RGPD.

Exemplul 10:

Un utilizator cumpără un televizor printr-un serviciu de comerț electronic, folosind o comandă vocală adresată unui AVV. Chiar dacă utilizatorul solicită ulterior ștergerea datelor sale, furnizorul sau dezvoltatorul AVV-ului ar putea totuși să păstreze unele date având drept motiv obligația legală de a păstra dovezi ale achiziției, stabilită de reglementările fiscale. Totuși, datele stocate în acest scop nu trebuie să depășească minimumul necesar pentru a se conforma obligației legale și nu pot fi prelucrate în alte scopuri fără un temei juridic conform articolului 6 din RGPD.

101. După cum s-a menționat în secțiunea 2, capacitatea de recunoaștere vocală a AVV-urilor se îmbunătățește prin antrenarea sistemelor de învățare automată cu ajutorul datelor utilizatorilor. În cazul în care utilizatorii nu își dau sau își retrag consimțământul cu privire la utilizarea datelor lor în acest scop, datele nu mai pot fi utilizate în mod legal pentru a mai

³⁴ A se vedea scrisoarea trimisă de Amazon la 28 iunie 2019 ca răspuns la întrebările senatorului SUA Christopher Coons:
[https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons_Response%20Letter_6.28.19\[3\].pdf](https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons_Response%20Letter_6.28.19[3].pdf)

antrena modelul și trebuie șterse de către operatorul de date, presupunând că nu există un alt scop care să justifice continuarea păstrării lor. Există însă dovezi că pot exista riscuri de reidentificare în unele modele de învățare automată.³⁵

102. Operatorii de date și persoanele împuternicite de aceștia ar trebui să utilizeze modele care nu le restricționează capacitatea de a opri prelucrarea dacă o persoană își retrage consimțământul, nu modele care le restrâng capacitatea de a facilita exercitarea drepturilor persoanei vizate. Operatorii și persoanele împuternicite ar trebui să aplice măsuri de atenuare pentru a diminua riscul de reidentificare până la un prag acceptabil.
103. În cazul în care utilizatorul își retrage consimțământul, datele colectate de la acesta nu mai pot fi folosite pentru antrenarea ulterioară a modelului. Cu toate acestea, modelul antrenat anterior cu ajutorul acestor date nu trebuie șters. CEPD subliniază totuși că există dovezi ale unor posibile riscuri de scurgeri de date cu caracter personal în unele modele de învățare automată. În special, numeroase studii au arătat că pot avea loc atât atacuri care reconstituie baze de date (*reconstruction attacks*), cât și atacuri care deduc datele folosite la învățare (*membership inference attacks*), permițând atacatorilor să obțină informații despre persoane³⁶. Prin urmare, operatorii de date și persoanele împuternicite de aceștia ar trebui să aplice măsuri de atenuare pentru a diminua riscul de reidentificare până la un prag acceptabil, asigurându-se că utilizează modele care nu conțin date cu caracter personal.
104. Persoanele vizate nu trebuie îndemnate să-și păstreze datele pe termen nelimitat. În timp ce ștergerea datelor vocale sau a transcrierilor stocate ar putea avea un impact asupra performanței serviciului, acest impact ar trebui explicat utilizatorilor într-un mod clar și măsurabil. Furnizorii de servicii AVV ar trebui să evite să facă declarații generale cu privire la degradarea serviciului după ce datele cu caracter personal sunt șterse.
105. Anonimizarea înregistrărilor vocale este deosebit de dificilă, deoarece este posibil să identifiți utilizatori prin intermediul conținutului mesajului propriu-zis și prin caracteristicile vocii sale. Cu toate acestea, se efectuează unele cercetări³⁷ privind tehnici care ar putea face posibilă eliminarea informațiilor contextuale, cum sunt zgomotele de fundal, și anonimizarea vocii.

Recomandări

106. Din perspectiva utilizatorului, scopul principal al prelucrării datelor constă în interogarea și primirea de răspunsuri și/sau declanșarea de acțiuni precum redarea muzicii sau aprinderea/stingerea luminilor. După ce s-a răspuns la o interogare sau s-a executat o comandă, datele personale ar trebui șterse, cu excepția cazului în care proiectantul sau dezvoltatorul AVV-ului are un temei juridic valabil care îi permite să le păstreze într-un anumit scop.

³⁵ Veale Michael, Binns Reuben și Edwards Lilian, 2018, „[Algorithms that remember: model inversion attacks and data protection law](https://doi.org/10.1098/rsta.2018.0083)”, Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083

³⁶ N. Carlini et al, „[Extracting Training Data from Large Language Models](https://arxiv.org/abs/2009.14794)”, dec. 2020.

³⁷ Vezi, de exemplu, VoicePrivacy (<https://www.voiceprivacychallenge.org>), o inițiativă destinată dezvoltării de soluții de păstrare a confidențialității pentru tehnologia legată de vorbire.

A se vedea și instrumentele de tip open-source pentru anonimizare vocală dezvoltate în cadrul proiectului de cercetare și inovare COMPRISE, derulat ca parte a programului Horizon 2020: https://gitlab.inria.fr/comprise/voice_transformation.

107. Înainte de a analiza opțiunea anonimizării ca mijloc pentru respectarea principiului de limitare a stocării datelor, furnizorii și dezvoltatorii AVV-urilor ar trebui să verifice dacă procesul de anonimizare face imposibilă identificarea vocii.
108. Configurația implicită trebuie să reflecte aceste cerințe prin setarea implicită la un nivel minim absolut a informațiilor despre utilizator stocate. Dacă aceste opțiuni sunt prezentate ca parte a unui asistent de configurare, setarea implicită trebuie să reflecte cele de mai sus, iar toate opțiunile trebuie prezentate ca posibilități egale, fără discriminare vizuală.
109. Atunci când în timpul procesului de revizuire furnizorul sau dezvoltatorul AVV-ului detectează o înregistrare provenită dintr-o activare greșită, înregistrarea și toate datele asociate trebuie șterse imediat și nu trebuie utilizate în niciun scop.

3.7 Securitatea

110. Pentru a prelucra în siguranță datele cu caracter personal, AVV-urile trebuie să protejeze confidențialitatea, integritatea și disponibilitatea acestora. În afară de riscurile care decurg din elementele ecosistemului AVV, utilizarea vocii ca mijloc de comunicare creează un nou set de riscuri de securitate.
111. AVV-urile sunt aplicații cu mai mulți utilizatori. Ele pot permite conectarea pentru mai mulți utilizatori înregistrați și orice persoană aflată în jurul lor poate să transmită comenzi și să folosească serviciile oferite. Orice serviciu AVV care necesită asigurarea confidențialității va include un mecanism de control al accesului și de autentificare a utilizatorilor. Fără controlul accesului, orice persoană care poate să emită comenzi vocale destinate AVV-ului ar putea să acceseze, să modifice sau să șteargă datele cu caracter personal ale oricărui utilizator (de exemplu, poate solicita mesajele primite, adresa utilizatorului sau evenimentele din calendar). Transmiterea de comenzi vocale AVV-ului nu necesită apropierea fizică de acesta, deoarece AVV-urile pot fi manipulate, de exemplu, prin transmiterea de semnale³⁸ (ex. radio sau TV). Unele dintre metodele cunoscute prin care se transmit comenzi de la distanță către AVV-uri, precum undele laser³⁹ sau ultrasunetele (inaudibile)⁴⁰, nu pot fi nici măcar detectate de simțurile umane.
112. Autentificarea utilizatorului se poate baza pe unul sau mai mulți dintre următorii factori: un element cunoscut (de exemplu, o parolă), un element deținut (de exemplu, un card inteligent) sau un element care face parte din utilizator (de exemplu, amprenta vocală). O privire mai atentă asupra acestor factori de autentificare în contextul AVV-urilor arată următoarele:
 -) Autentificarea prin folosirea unui element cunoscut de utilizator este problematică. Secretul care ar permite utilizatorilor să-și demonstreze identitatea ar trebui rostit cu voce tare, expunându-l oricărei persoane aflate în apropiere. Canalul de comunicație al AVV-ului este aerul înconjurător, un tip de canal care nu poate fi consolidat într-un mod similar canalelor tradiționale (de exemplu, prin limitarea accesului la canal sau prin criptarea conținutului său).

³⁸ X. Yuan et al., „All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo”, 2018, Conferința IEEE Global Communications (GLOBECOM), Abu Dhabi, Emiratele Arabe Unite, 2018, p. 1-6, doi: 10.1109/GLOCOM.2018.8647762.

³⁹ A se vedea, de exemplu, <https://lightcommands.com>

⁴⁰ A se vedea, de exemplu, <https://surfingattack.github.io>

-) Autentificarea prin folosirea unui element deținut de utilizator necesită ca furnizorii serviciilor AVV să creeze, să distribuie și să gestioneze „tokene” care să poată fi folosite ca dovadă a identității.
-) Autentificarea prin folosirea unui element care face parte din utilizator presupune utilizarea datelor biometrice în scopul identificării unice a unei persoane fizice (vezi secțiunea 3.7 de mai jos).
113. Conturile de utilizator al AVV-ului sunt asociate dispozitivelor prin care este furnizat serviciul. Adesea, același cont utilizat pentru gestionarea AVV-ului este folosit și pentru gestionarea altor servicii. De exemplu, proprietarii unui telefon mobil cu sistem Android și ai unei boxe Google Home își pot asocia contul Google la ambele dispozitive, și cel mai probabil chiar fac acest lucru. Majoritatea AVV-urilor nu necesită sau nu oferă un mecanism de identificare sau de autentificare atunci când dispozitivul care furnizează serviciul AVV are un singur cont de utilizator.
114. Când există mai multe conturi de utilizator asociate dispozitivului, unele AVV-uri oferă opțional un control de bază al accesului, sub forma unui cod PIN care nu necesită autentificarea reală a utilizatorului. Alte AVV-uri au opțiunea de a utiliza recunoașterea amprentei vocale ca mecanism de identificare.
115. Deși identificarea sau autentificarea utilizatorului ar putea să nu fie necesară pentru a accesa toate serviciile AVV, pentru unele dintre ele va fi cu siguranță necesară. În lipsa unui mecanism de identificare sau autentificare, oricine ar putea să acceseze datele altor utilizatori și să le modifice sau să le șteargă după bunul plac. De exemplu, orice persoană aflată în apropierea unei boxe inteligente ar putea șterge listele de redare ale altor utilizatori din serviciul de streaming muzical, comenzile din istoricul comenzilor sau contactele din lista de contacte.
116. Majoritatea AVV-urilor se încred orbește în rețelele lor locale. Orice dispozitiv compromis din aceeași rețea ar putea modifica setările boxei inteligente sau ar putea permite instalarea de programe malware sau asocierea unor aplicații/funcții false fără știrea sau acordul utilizatorului⁴¹.
117. AVV-urile, ca orice alt software, sunt supuse vulnerabilităților informatice. Totuși, din cauza concentrării pieței AVV-urilor⁴², orice vulnerabilitate ar putea afecta milioane de utilizatori. Dacă funcționează așa cum sunt proiectate în prezent, AVV-urile nu trimit informații la serviciul cloud de recunoaștere a vorbirii până când nu detectează expresia de activare. Cu toate acestea, vulnerabilitățile informatice ar putea permite unui atacator să ocolească această setare și măsurile de securitate ale AVV-urilor. Apoi, ar fi posibil, de exemplu, să obțină o copie a tuturor datelor trimise în cloud-ul AVV-ului și să le transmită către un server controlat de atacator.
118. Datele prelucrate sau deduse legal de AVV-uri permit crearea unui profil destul de precis al utilizatorilor, deoarece AVV-ul cunoaște sau poate deduce locul unde se află utilizatorul, relațiile și interesele sale. AVV-urile sunt din ce în ce mai prezente în casele și în telefoanele inteligente ale utilizatorilor. Această circumstanță crește riscul unor acțiuni de supraveghere

⁴¹ A se vedea, de exemplu, Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, august 2018, <https://www.usenix.org/conference/usenixsecurity18/presentation/kumar>
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping*, noiembrie 2019, <https://srlabs.de/bites/smart-spies>

⁴² În prezent, piața AVV-urilor este împărțită între mai puțin de o duzină de furnizori de servicii.

și crearea de profiluri în masă. În consecință, măsurile de securitate instituite pentru a proteja datele atât în tranzit, cât și în repaus, în dispozitive și în cloud, ar trebui să fie pe măsura acestor riscuri.

119. Utilizarea pe scară tot mai largă a AVV-urilor, dacă nu este însoțită de o echilibrare adecvată a drepturilor de acces de către autoritățile de aplicare a legii, ar putea avea drept efect inducerea unei stări de teamă care ar submina drepturi fundamentale precum libertatea de exprimare.
120. O serie de autorități de aplicare a legii, atât din cadrul⁴³, cât și din afara UE⁴⁴, și-au exprimat deja interesul pentru accesarea fragmentelor vocale captate de AVV-uri. Accesul la datele prelucrate sau deduse de AVV-uri în UE trebuie să respecte cadrul actual al Uniunii de reglementare a protecției datelor și a confidențialității. În cazul în care unele state membre vor lua în considerare opțiunea emiterii unor acte legislative specifice care să restricționeze drepturile fundamentale la confidențialitate și la protecția datelor, aceste restricții trebuie să respecte întotdeauna obligația prevăzută la articolul 23 din RGPD⁴⁵.
121. Revizuirea umană a înregistrărilor vocale și a datelor asociate, cu scopul de a îmbunătăți calitatea serviciilor AVV, este o practică obișnuită în rândul furnizorilor de AVV-uri. Având în vedere natura sensibilă a datelor prelucrate de acești revizori umani și faptul că acest proces este adesea subcontractat unor persoane împuternicite de operatori, este extrem de important să fie puse în aplicare măsuri de securitate adecvate.

Recomandări

122. Proiectanții AVV-urilor și dezvoltatorii de aplicații ar trebui să ofere utilizatorilor proceduri de autentificare sigure, la cel mai înalt nivel.
123. Revizorii umani ar trebui să primească întotdeauna doar datele strict necesare, pseudonimizate. Acordurile juridice care reglementează revizuirea ar trebui să interzică în mod expres orice prelucrare care ar putea duce la identificarea persoanei vizate.
124. Dacă unul dintre serviciile furnizate prin intermediul AVV-ului este apelarea serviciilor de urgență, ar trebui garantat un timp de funcționare⁴⁶ stabil.

3.8 Prelucrarea categoriilor speciale de date

125. După cum s-a menționat anterior, AVV-urile au acces la informații cu caracter intim care pot fi protejate în temeiul articolului 9 din RGPD (vezi secțiunea 3.7.1), de exemplu datele biometrice (vezi secțiunea 3.7.2). Prin urmare, proiectanții și dezvoltatorii de AVV-uri trebuie să identifice cu atenție cazurile în care prelucrarea implică date din categorii speciale.

3.8.1 Considerații generale cu privire la prelucrarea categoriilor speciale de date

126. AVV-urile pot prelucra categorii speciale de date în diverse circumstanțe:

) Ca parte a propriilor servicii, de exemplu atunci când gestionează programările medicale în agendele utilizatorilor.

⁴³ A se vedea, de exemplu, <https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2>.

⁴⁴ A se vedea, de exemplu, <https://cdt.org/insights/alexa-is-law-enforcement-listening>.

⁴⁵ A se vedea și CEPD, Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD.

⁴⁶ Perioada în care un dispozitiv sau un serviciu poate fi lăsat nesupravegheat, fără a se bloca și fără a trebui să fie repornit în scopuri administrative sau de întreținere.

- J Când acționează ca interfață pentru servicii ale terților, furnizorii de AVV-uri prelucrează conținutul comenzilor. În funcție de tipul serviciului solicitat de utilizator, furnizorii de AVV-uri ar putea prelucra categorii speciale de date. Un posibil exemplu ar fi acela în care o utilizatoare comandă AVV-ului să folosească o aplicație terță care ține evidența perioadelor sale de ovulație⁴⁷.
- J Atunci când datele vocale sunt utilizate în scopul identificării unice a utilizatorului, astfel cum se detaliază mai jos.

3.8.2 Considerații specifice cu privire la prelucrarea datelor biometrice

127. Unele AVV-uri au capacitatea de a identifica în mod unic utilizatorii doar pe baza vocii lor. Acest proces este cunoscut sub numele de recunoaștere a modelului vocal. În timpul fazei de înregistrare a recunoașterii vocale, AVV-ul prelucrează vocea unui utilizator pentru a crea un model vocal (sau o amprentă vocală). În timpul utilizării sale curente, AVV-ul poate calcula modelul vocal al oricărui utilizator și îl poate compara cu modelele înregistrate, pentru a identifica în mod unic utilizatorul care a emis comanda.

Exemplul 11:

Un grup de utilizatori configurează un AVV să folosească recunoașterea modelului vocal. Apoi, fiecare dintre ei își înregistrează modelul vocal.

Mai târziu, un utilizator solicită AVV-ului acces la întâlnirile din agenda sa. Deoarece accesul la agendă necesită identificarea utilizatorului, AVV-ul extrage modelul din vocea solicitantului, calculează modelul vocal aferent și verifică dacă se potrivește cu un utilizator înregistrat și dacă acel utilizator are acces la agendă.

128. În exemplul de mai sus, recunoașterea vocii utilizatorului pe baza unui model vocal echivalează cu prelucrarea unor categorii speciale de date cu caracter personal în sensul articolului 9 din RGPD (prelucrarea de date biometrice în scopul identificării unice a unei persoane fizice)⁴⁸. Prelucrarea datelor biometrice în scopul identificării utilizatorului, ca în exemplul prezentat, necesită consimțământul explicit al persoanei vizate [articolul 9 alineatul (2) litera (a) din RGPD]. Prin urmare, atunci când obțin consimțământul utilizatorilor, operatorii de date trebuie să respecte condițiile de la articolul 7, astfel cum sunt clarificate în considerentul 32 din RGPD, și să ofere o metodă de identificare alternativă la biometrie în ceea ce privește natura liberă a consimțământului.
129. Atunci când se utilizează date vocale pentru identificarea sau autentificarea biometrică, operatorii de date sunt obligați să comunice în mod transparent locul în care este utilizată identificarea biometrică și modul în care sunt stocate și propagate amprente vocale (modele biometrice) pe diferitele dispozitive. Pentru a îndeplini această obligație de transparență, CEPD recomandă ca operatorii să răspundă la următoarele întrebări:
- J Activarea identificării vocale pe un dispozitiv activează automat această caracteristică pe toate celelalte dispozitive care funcționează cu același cont?

⁴⁷ A se vedea, de exemplu, un produs disponibil aici: <https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY>

135. Dacă un AVV utilizează identificarea biometrică vocală, furnizorii săi ar trebui să asigure următoarele:
-) că identificarea este suficient de precisă pentru a asocia în siguranță datele cu caracter personal cu persoanele vizate corecte;
 -) că acuratețea similară pentru toate grupurile de utilizatori, verificând să nu existe o părtinire substanțială față de diferite grupuri demografice.

3.9 Reducerea la minimum a datelor

136. Operatorii de date trebuie să minimizeze cantitatea de date colectate direct sau indirect și obținute prin prelucrare și analiză, de exemplu să nu efectueze vreo analiză asupra vocii utilizatorului sau alte informații sonore pentru a deduce informații despre starea sa mentală, posibilele boli sau circumstanțele vieții sale.
137. Trebuie stabilite setări implicite care să limiteze orice colectare și/sau prelucrare a datelor la un minim necesar pentru furnizarea serviciului.
138. În funcție de loc, de contextul utilizării și de sensibilitatea microfonului, AVV-ul ar putea colecta date vocale ale terților ca parte a zgomotului de fond atunci când colectează vocea utilizatorilor. Chiar dacă zgomotul de fond nu include date vocale, poate include totuși date contextuale care ar putea fi prelucrate pentru a obține informații despre subiect (de exemplu, locul unde se află).

Recomandări

139. Proiectanții de AVV-uri ar trebui să aibă în vedere tehnologii care elimină zgomotul de fond, pentru a evita înregistrarea și prelucrarea vocilor din fundal și a informațiilor contextuale.

3.10 Responsabilitatea

140. Pentru orice prelucrare care se bazează pe consimțământ, operatorii de date au obligația de a putea dovedi consimțământul persoanelor vizate, în conformitate cu articolul 7 alineatul (1) din RGPD. Datele vocale pot fi utilizate în scopuri legate de responsabilitate (de exemplu, pentru a dovedi consimțământul). În acest caz, obligația de păstrare a datelor vocale respective ar fi dictată de cerințele referitoare la responsabilitate din legislația specifică relevantă.
141. Atunci când a evaluat necesitatea unei evaluări a impactului asupra protecției datelor (DPIA), CEPD a stabilit o serie de criterii⁵⁰ care trebuie utilizate de autoritățile de protecție a datelor pentru a crea liste de operațiuni de prelucrare care necesită o DPIA obligatorie și a oferit exemple de prelucrare care ar putea necesita în mod probabil o DPIA. Este foarte probabil ca serviciile AVV să se încadreze foarte probabil în categoriile și condițiile identificate ca având nevoie de o DPIA. Aceasta include analizarea posibilității ca dispozitivul să urmărească, să monitorizeze sau să controleze persoanele vizate sau să realizeze o monitorizare sistematică pe scară largă, conform articolului 35 alineatul (3) litera (c), să utilizeze „noi tehnologii” sau să prelucreze date sensibile și date referitoare la persoane vulnerabile.
142. Toate activitățile de colectare și prelucrare de date trebuie documentate în conformitate cu articolul 30 din RGPD. Aceasta include toate prelucrările care implică date vocale.

⁵⁰ Grupul de lucru „Articolul 29”, Orientări privind evaluarea impactului asupra protecției datelor (DPIA), GL248 rev. 01, aprobate de CEPD.

Recomandări

143. Dacă se folosesc mesaje vocale pentru a informa utilizatorii în conformitate cu articolul 13, operatorii de date ar trebui să publice mesajele respective pe site-ul lor, astfel încât să fie accesibile utilizatorilor și autorităților de protecție a datelor.

3.11 Asigurarea protecției datelor din faza de proiectare și în mod implicit

144. Furnizorii și dezvoltatorii de AVV-uri ar trebui să reanalizeze necesitatea de a avea un utilizator înregistrat pentru fiecare dintre funcționalități. Deși este clar că trebuie să existe un utilizator înregistrat pentru a gestiona o agendă sau o listă de adrese, nu este la fel de clar că efectuarea unui apel telefonic sau a unei căutări pe Internet ar necesita existența unui utilizator înregistrat al AVV-ului.
145. Ca setare implicită, serviciile care nu necesită un utilizator identificat ar trebui să nu asocieze comenzile cu niciunul dintre utilizatorii identificați ai AVV-ului. Un AVV care asigură în mod implicit protecția datelor și a confidențialității ar prelucra datele utilizatorilor doar pentru executarea cererilor acestora și nu ar stoca nici date vocale, nici un registru al comenzilor executate.
146. În timp ce pe unele dispozitive poate funcționa un singur AVV, altele pot alege dintre diferite AVV-uri. Furnizorii de AVV-uri ar trebui să elaboreze standarde în domeniu care să permită portabilitatea datelor, în conformitate cu articolul 20 din RGPD.
147. Unii furnizori de AVV-uri au susținut că asistenții lor virtuali nu ar putea să șteargă toate datele utilizatorilor nici dacă persoana vizată le-ar solicita acest lucru. Furnizorii de AVV-uri ar trebui să se asigure că toate datele utilizatorilor pot fi șterse la cererea acestora, în conformitate cu articolul 17 din RGPD.

4 MECANISME DE EXERCITARE A DREPTURILOR PERSOANEI VIZATE

148. În conformitate cu RGPD, operatorii de date care furnizează servicii AVV trebuie să permită tuturor utilizatorilor, înregistrați și neînregistrați, să își exercite drepturile în calitate de persoane vizate.
149. Furnizorii și dezvoltatorii de AVV-uri ar trebui să faciliteze controlul persoanelor vizate asupra datelor lor pe întreaga perioadă de prelucrare, în special să le ușureze dreptul de acces, rectificare, ștergere, dreptul de a restricționa prelucrarea și, în funcție de temeiul juridic al prelucrării, dreptul la portabilitatea datelor și dreptul de a se opune prelucrării.
150. Operatorul de date ar trebui să ofere persoanelor vizate informații cu privire la drepturile lor în momentul în care acestea pornesc un AVV, și în orice caz nu mai târziu de momentul prelucrării cererii vocale a primului utilizator.
151. Având în vedere că vocea este principalul mijloc de interacțiune cu AVV-urile, proiectanții AVV-urilor ar trebui să se asigure că utilizatorii (înregistrați sau nu) pot să-și exercite toate drepturile în calitate de persoane vizate utilizând comenzi vocale ușor de urmat. La sfârșitul procesului de exercitare, proiectanții AVV-urilor, precum și dezvoltatorii de aplicații în cazul în care fac parte din soluție, ar trebui să informeze utilizatorul că drepturile sale au fost luate în considerare în mod corespunzător, printr-o notificare verbală sau trimisă în scris pe telefonul mobil al utilizatorului, în contul acestuia sau prin orice alt mijloc ales de utilizator.

152. Cel puțin, proiectanții AVV-urilor și dezvoltatorii de aplicații, în special, ar trebui să implementeze cel puțin instrumente specifice care să ofere o modalitate eficace și eficientă de exercitare a acestor drepturi. Astfel, ei ar trebui să propună pentru dispozitivele lor o modalitate de exercitare a drepturilor persoanelor vizate, de exemplu prin furnizarea de instrumente de autoservire sub forma unui sistem de gestionare a profilului⁵¹. Acest lucru ar facilita o gestionare eficientă și promptă a drepturilor persoanei vizate, iar operatorul de date va putea să includă mecanismul de identificare în instrumentul de autoservire.
153. În ceea ce privește exercitarea drepturilor persoanelor vizate în cazul mai multor utilizatori, atunci când un utilizator (înregistrat sau nu) își exercită unul dintre drepturile sale, acțiunea sa nu ar trebui să aducă atingere drepturilor altor utilizatori. Toți utilizatorii, înregistrați și neînregistrați deopotrivă, își pot exercita drepturile atâta timp cât operatorul de date încă prelucrează datele. Operatorul de date ar trebui să instituie un proces care să asigure exercitarea drepturilor persoanei vizate.

4.1 Dreptul de acces

154. În conformitate cu articolul 12 alineatul (1) din RGPD, comunicarea în temeiul articolului 15 ar trebui făcută în scris sau prin alte mijloace, inclusiv în format electronic atunci când este oportun. În ceea ce privește accesul la datele cu caracter personal care se află în curs de prelucrare, articolul 15 alineatul (3) prevede că, atunci când persoana vizată introduce cererea prin mijloace electronice și cu excepția cazului în care persoana vizată solicită altfel, informațiile trebuie furnizate într-un format electronic utilizat în mod curent. Stabilirea „formatului electronic utilizat în mod curent” ar trebui să se bazeze pe așteptările rezonabile ale persoanelor vizate și nu pe formatul utilizat de operatorul de date în operațiunile sale de zi cu zi. Persoana vizată nu ar trebui să fie obligată să cumpere un software sau hardware specific pentru a obține acces la informații.
155. Prin urmare, operatorii de date ar trebui să trimită, la cerere, o copie a datelor cu caracter personal și în special a datelor audio (inclusiv înregistrări vocale și transcrieri), într-un format uzual care să poată fi citit de persoana vizată.
156. Atunci când decide asupra tipului de format în care ar trebui furnizate informațiile prevăzute la articolul 15, operatorul de date trebuie să țină cont de faptul că formatul trebuie să permită prezentarea informațiilor într-un mod atât inteligibil, cât și ușor accesibil. De asemenea, operatorii de date ar trebui să adapteze informațiile la situația specifică a persoanei vizate care face cererea.

Exemplul 13:

Un operator de date care furnizează un serviciu AVV primește de la un utilizator atât o cerere de acces, cât și o cerere de portabilitate a datelor. Operatorul decide să furnizeze informațiile, în conformitate cu articolul 15 și cu articolul 20, într-un fișier PDF. Într-un astfel de caz, nu ar trebui să se considere că operatorul a gestionat ambele cereri în mod corect. Un fișier PDF

⁵¹ Prin „sistem de gestionare a profilului” se înțelege un loc din cadrul sistemului AVV unde utilizatorii pot oricând să își salveze preferințele, să își modifice și să își schimbe cu ușurință setările de confidențialitate

îndeplinește, din punct de vedere tehnic, obligațiile care revin operatorului de date în temeiul articolului 15, dar nu și pe cele care îi revin în temeiul articolului 20⁵².

Trebuie precizat că simpla trimitere a utilizatorilor la istoricul interacțiunilor lor cu asistentul vocal, nu înseamnă că operatorul de date își îndeplinește toate obligațiile care îi revin conform dreptului de acces, deoarece datele accesibile reprezintă în general doar o parte din informațiile prelucrate în contextul furnizării serviciului.

157. Dreptul de acces nu ar trebui utilizat pentru a contracara sau a ocoli principiile privind reducerea la minimum și păstrarea datelor.

4.2 Dreptul la rectificare

158. Pentru a facilita rectificarea datelor, utilizatorii (înregistrați sau nu) ar trebui să își poată gestiona și actualiza în orice moment datele prin comandă vocală direct de pe dispozitivul AVV, astfel cum se descrie mai sus. În plus, instrumentul de autoservire ar trebui să fie implementat în cadrul dispozitivului sau al unei aplicații, pentru a-i ajuta să rectifice cu ușurință datele lor personale. Utilizatorii ar trebui să fie anunțați, prin voce sau prin scris, despre actualizare.
159. În sens mai general, dreptul la rectificare se aplică oricăror opinii și deducții⁵³ ale operatorului de date, inclusiv creării de profiluri, și ar trebui să se țină cont de faptul că marea majoritate a datelor sunt deosebit de subiective⁵⁴.

4.3 Dreptul la ștergerea datelor

160. Utilizatorii (înregistrați sau nu) ar trebui să poată șterge în orice moment datele care îi privesc, prin comandă vocală adresată dispozitivului AVV sau printr-un instrument de autoservire integrat în orice dispozitiv asociat AVV-ului. În acest sens, datele cu caracter personal pot fi șterse de persoana vizată la fel de ușor pe cât sunt transmise. Din cauza dificultăților inerente ale anonimizării a datelor vocale și a varietății mari de date cu caracter personal colectate, observate și deduse despre persoana vizată⁵⁵, cu greu ar putea fi aplicat în acest context dreptul la ștergere prin anonimizarea seturilor de date cu caracter personal. Deoarece RGPD este neutru din punct de vedere tehnologic și tehnologia evoluează rapid, nu se poate totuși exclude ipoteza că dreptul la ștergere poate fi realizat efectiv prin anonimizare.
161. În unele cazuri, fără un ecran al unui terț sau fără posibilitatea de a afișa datele stocate (de exemplu, printr-o aplicație mobilă sau un dispozitiv tabular), este dificil să se realizeze previzualizarea fragmentelor înregistrate, pentru a aprecia relevanța sugestiilor. Ar trebui ca împreună cu asistentul vocal să se furnizeze un tablou de bord (sau o aplicație) accesibil(ă) pe

⁵² Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 18.

⁵³ Faptul că opiniile și deducțiile se pot încadra în categoria datelor cu caracter personal a fost confirmat de CJUE, care a menționat că expresia „orice informație” din definiția noțiunii „date cu caracter personal” înglobează informații „atât obiective, cât și subiective, sub formă de opinii și de aprecieri, cu condiția ca acestea să fie «referitoare» la persoana în cauză”- Cauza 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, noiembrie 2019.

⁵⁵ Avizul 5/2014 al Grupului de lucru „Articolul 29” privind tehnicile de anonimizare, adoptat la 10 aprilie 2014.

scară largă utilizatorilor, pentru a fi mai ușor de folosit, care să ștergă istoricul cererilor exprimate și să personalizeze instrumentul în funcție de nevoile utilizatorului⁵⁶.

162. Pentru orice prelucrare a datelor, și în special, atunci când persoanele vizate înregistrate consimt ca înregistrările vocale să fie transcrise și utilizate de furnizor pentru îmbunătățirea serviciilor sale, furnizorii de AVV-uri ar trebui, la cererea utilizatorului, să fie capabili să ștergă înregistrarea vocală inițială, precum și orice transcriere aferentă a datelor cu caracter personal.
163. Operatorul de date ar trebui să se asigure că nu mai poate avea loc nicio prelucrare după exercitarea dreptului de ștergere. În ceea ce privește acțiunile anterioare, dreptul la ștergere se poate confrunta cu anumite limite juridice și, în special, tehnice.

Exemplul 14:

Dacă înainte de solicitarea de ștergere un utilizator a efectuat o achiziție online prin intermediul AVV-ului său, furnizorul serviciului AVV poate să ștergă înregistrarea vocală referitoare la achiziția online și să asigure că nu va mai fi folosită ulterior. Totuși, achiziția va rămâne însă valabilă, la fel și comanda vocală sau transcrierea scrisă procesată de site-ul de comerț electronic (aici derogarea se bazează pe obligația legală a site-ului respectiv).

În mod similar, dacă înainte de solicitarea de ștergere utilizatorul a adăugat o anumită melodie în lista sa de redare prin intermediul AVV-ului, furnizorii AVV-ului vor putea șterge cererea exprimată oral, dar nu și consecințele deja survenite ale solicitării respective (ștergerea nu va afecta lista de redare a utilizatorului).

164. Pe baza celor de mai sus, în cazul în care aceleași date cu caracter personal sunt prelucrate în scopuri diferite, operatorii de date ar trebui să interpreteze cererile de ștergere ca pe un semnal clar de încetare a prelucrării datelor în toate scopurile pentru care nu există o derogare legală.

În conformitate cu condițiile prevăzute la articolul 21 alineatul (1) din RGPD, datele prelucrate pe baza intereselor legitime ale furnizorilor de AVV-uri nu ar trebui să constituie o derogare de la dreptul la ștergerea datelor, în special pentru că în mod rezonabil persoanele vizate nu se mai așteaptă ca datele lor cu caracter personal să fie prelucrate în continuare.

4.4 Dreptul la portabilitatea datelor

165. Prelucrarea datelor efectuată de furnizorii AVV-urilor intră sub incidența portabilității datelor, deoarece operațiunile de prelucrare se bazează în principal pe consimțământul persoanei vizate [în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a) în cazul categoriilor speciale de date cu caracter personal] sau pe un contract la care persoana vizată este parte, în temeiul articolului 6 alineatul (1) litera (b).
166. În practică, dreptul la portabilitatea datelor ar trebui să faciliteze comutarea între diferiți furnizori de AVV-uri. Deoarece AVV-urile funcționează în special într-un mediu digital, iar vocea persoanei vizate este înregistrată într-o aplicație sau pe o platformă, dreptul la portabilitatea datelor ar trebui acordat pentru toate datele cu caracter personal furnizate de persoana vizată. Mai mult, operatorul de date ar trebui să ofere utilizatorilor posibilitatea de a-și recupera direct datele cu caracter personal din zona destinată utilizatorului, cu ajutorul unui instrument

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”, Franța, mai 2019.

de autoservire. De asemenea, utilizatorii ar trebui să își poată exercita acest drept prin comandă vocală.

167. Furnizorii și dezvoltatorii de AVV-uri ar trebui să ofere persoanelor vizate un control extins asupra datelor cu caracter personal care le privesc, pentru a le permite să-și transfere aceste date personale de la un furnizor AVV la altul. Prin urmare, persoanele vizate ar trebui să primească datele personale pe care le-au furnizat operatorului de date într-un format structurat, utilizat în mod curent și care poate fi prelucrat automat, precum și prin mijloace⁵⁷ care să ajute la efectuarea operațiunii de portare solicitate (de exemplu, instrumente de descărcare și interfețe de programare a aplicațiilor)⁵⁸. După cum se menționează în Orientările privind dreptul la portabilitatea datelor, în cazul colectării unor date cu caracter personal în volum mare sau complexe, situație care poate să corespundă cazului de față, operatorul ar trebui să ofere o imagine de ansamblu „într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu” [vezi articolul 12 alineatul (1) din RGPD], în așa fel încât persoanele vizate să aibă întotdeauna informații clare despre ce date să descarce sau să transmită altui operator de date, în raport cu un anumit scop. De exemplu, persoanele vizate ar trebui să fie în măsură să utilizeze aplicații software pentru a identifica, recunoaște și prelucra cu ușurință date specifice din acestea.
168. Acest drept ar trebui să permită utilizatorului să recupereze, pentru utilizarea sa personală, datele pe care le-a comunicat prin intermediul vocii sale (de exemplu, istoricul interacțiunilor vocale) și în special în cadrul creării contului său de utilizator (de exemplu: numele și prenumele).
169. Pentru exercitarea deplină a acestui drept al persoanelor vizate în contextul unei piețe digitale unice, proiectanții de AVV-uri și mai ales dezvoltatorii de aplicații ar trebui să dezvolte formate comune, care pot fi prelucrate automat, care să faciliteze interoperabilitatea formatului de date între sistemele AVV⁵⁹, inclusiv a formatelor standard pentru date vocale. Tehnologiile ar trebui structurate astfel încât să asigure faptul că datele cu caracter personal prelucrate, inclusiv datele vocale, pot fi utilizate ușor și pe deplin de către noul operator⁶⁰.

⁵⁷ Vezi, ca o ilustrare, raționamentul Grupului de lucru „Articolul 29” din Orientările privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 16:

„La nivel tehnic, operatorii de date ar trebui să exploreze și să evalueze două căi diferite și complementare pentru a pune la dispoziție datele portabile persoanelor vizate sau altor operatori de date:

o transmitere directă a întregului set de date portabile (sau a mai multor părți extrase din setul de date global); un instrument automat care să permită extragerea datelor relevante.

A doua modalitate poate fi preferată de către operatorii de date în cazurile care implică seturi de date complexe și mari, deoarece permite extragerea oricărei părți a setului de date care este relevantă pentru persoana vizată în contextul cererii sale, poate să contribuie la minimizarea riscului și să permită utilizarea unor mecanisme de sincronizare a datelor (de exemplu, în contextul unei comunicări regulate între operatorii de date). Poate fi o modalitate mai bună de a asigura conformitatea «noului» operator de date și ar constitui o bună practică în reducerea riscurilor legate de confidențialitate din partea operatorului de date inițial.”

⁵⁸ În acest sens: Orientările Grupului de lucru „Articolul 29” privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 1.

⁵⁹ În acest sens: considerentul 68 din RGPD; Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 17.

⁶⁰ *„În acest sens, considerentul 68 încurajează operatorii de date să dezvolte formate interoperabile care să permită portabilitatea datelor, fără a crea însă obligația operatorilor de a adopta sau a menține sisteme de prelucrare compatibile din punct de vedere tehnic. Pe de altă parte, RGPD interzice operatorilor să stabilească*

170. În ceea ce privește formatul, furnizorii de AVV-uri ar trebui să pună la dispoziție datele cu caracter personal utilizând formate deschise utilizate în mod curent (de exemplu, mp3, wav, csv, gsm etc.), împreună cu folosirea de metadate adecvate pentru a descrie cu exactitate semnificația informațiilor schimbate⁶¹.

5 ANEXĂ: RECUNOAȘTEREA AUTOMATĂ A VORBIRII, SINTEZA VORBIRII ȘI PROCESAREA LIMBAJULUI NATURAL

171. Urmând bazele teoretice ale prelucrării semnalelor, în special teoria informației și teoria eșantionării ale lui Claude Shannon, prelucrarea automată a vorbirii a devenit o componentă fundamentală a științelor ingineriei. Aflată la intersecția dintre fizică (acustică, propagarea undelor), matematică aplicată (modelare, statistică), informatică (algoritmi, tehnici de învățare) și științele umaniste (percepție, raționament), prelucrarea vorbirii a fost împărțită rapid în numeroase subiecte de studiu: identificarea și verificarea vorbitorilor, recunoașterea automată a vorbirii, sinteza vocii, detectarea emoțiilor etc. În ultimii aproximativ cincisprezece ani, disciplina în ansamblu a înregistrat progrese foarte mari, la care au contribuit factori diverși: metode îmbunătățite, creșterea semnificativă a capacității de calcul și volumele mai mari de date disponibile.

5.1 Recunoașterea automată a vorbirii (RAV)

172. Recunoașterea automată a vorbirii (cunoscută și sub denumirea de transcriere a vocii în text) presupunea trei etape distincte, care vizau următoarele aspecte: 1) determinarea fonemelor pronunțate, folosind un model acustic; 2) determinarea cuvintelor pronunțate, folosind un dicționar fonetic; 3) transcrierea secvenței de cuvinte (a propoziției) rostite cel mai probabil, folosind un model lingvistic. Astăzi, odată cu progresele posibile datorită învățării profunde (o tehnică de învățare automată), multe sisteme oferă recunoaștere automată a vorbirii „de la un cap la celălalt”. Se evită astfel nevoia de a realiza instruirea complexă a trei modele diferite, obținându-se totodată performanțe mai bune în ceea ce privește rezultatele și timpul de prelucrare. Aproape toți jucătorii majori de pe piața digitală oferă acum propriile lor implementări RAV care pot fi ușor utilizate de sistemele API, dar există și sisteme open-source (DeepSpeech⁶² sau Kaldi⁶³, de exemplu).

5.2 Procesarea limbajului natural (PLN)

173. Procesarea limbajului natural este un domeniu multidisciplinar, care implică lingvistică, informatică și inteligență artificială, și care își propune să creeze instrumente de procesare a limbajului natural pentru o varietate de aplicații. Domeniile de cercetare și aplicațiile sunt numeroase: analiză sintactică, traducere automată, generare și sintetizare automată a textelor, verificare ortografică, sisteme de răspuns la întrebări, extragere de text, recunoaștere a entității numite, analiză a sentimentelor etc. Concret, scopul PLN este de a oferi

bariere în calea transmisiei ” – Orientările WP29 privind dreptul la portabilitatea datelor – aprobate de CEPD, p. 5.

⁶¹ CEPD încurajează puternic cooperarea dintre părțile interesate din domeniu și organismele profesionale, pentru a lucra împreună la un set comun de standarde privind interoperabilitatea și formate interoperabile menit să ajute la îndeplinirea cerințelor referitoare la dreptul la portabilitatea datelor.

⁶² <https://github.com/mozilla/DeepSpeech>

⁶³ <https://github.com/kaldi-asr/kaldi>

computerelor capacitatea să citească, să înțeleagă și să extragă semnificație din limbile folosite de oameni. Dezvoltarea aplicațiilor de tip PLN este o provocare, deoarece instrumentele informatice se bazează în mod tradițional pe interacțiunea oamenilor cu acestea într-un limbaj de programare formal, adică precis, lipsit de ambiguitate și foarte structurat. În schimb, vorbirea umană nu este întotdeauna precisă. Este adesea ambiguă, iar structura lingvistică poate depinde de multe variabile complexe – inclusiv argoul, dialectele regionale și contextul social.

174. Sintaxa și analiza semantică sunt două tehnici principale utilizate în PLN. Sintaxa reprezintă aranjarea cuvintelor într-o propoziție pentru a avea sens gramatical. PLN folosește sintaxa pentru a evalua sensul dintr-o limbă bazată pe reguli gramaticale. Printre tehnicile sintactice utilizate se numără analiza gramaticală a unei propoziții (*parsing*), segmentarea în cuvinte (care împarte o bucată mare de text în unități), separarea frazelor (care stabilește limite ale propozițiilor în textele mari), segmentarea morfologică (care împarte cuvintele în grupuri) și analiza rădăcinii (care extrage rădăcina cuvintelor derivate). Semantica presupune utilizarea cuvintelor și sensului din spatele lor. PLN aplică algoritmi pentru a înțelege semnificația și structura propozițiilor. Printre tehnicile semantice folosite de PLN se numără dezambiguizarea sensului cuvântului (care deduce sensul unui cuvânt din context), recunoașterea entității numite (care determină cuvintele ce pot fi clasificate în grupuri) și generarea limbajului natural (care va utiliza o bază de date pentru a determina semantica din spatele cuvintelor). În timp ce abordările anterioare ale PLN erau bazate pe reguli, în care se indica unor algoritmi simpli de învățare automată ce cuvinte și expresii să caute în text și se dădeau răspunsuri specifice atunci când apăreau expresiile respective, abordările actuale ale PLN se bazează pe învățarea profundă, un tip de IA care examinează și folosește tiparele din date pentru a îmbunătăți capacitatea de înțelegere a unui program.

5.3 Sinteza vorbirii

175. Sinteza vorbirii reprezintă producerea artificială a vorbirii umane. Sinteza vorbirii a fost implementată în principal prin concatenarea unităților vocale stocate într-o bază de date. Această tehnică constă în selectarea – dintre toate înregistrările unui actor transcrise anterior în foneme, silabe și cuvinte – a acelor fragmente sonore care corespund cuvintelor care se doresc să fie pronunțate de AVV și asamblarea lor una după alta astfel încât să formeze o propoziție inteligibilă, cu dicție naturală. Ca alternativă, un sintetizator de vorbire poate încorpora un model al tractului vocal și alte caracteristici ale vocii umane, pentru a modela parametri vocali precum intonația, ritmul și timbrul, prin modele statistice generative (precum WaveNet⁶⁴, Tacotron⁶⁵ sau DeepVoice⁶⁶), și pentru a crea o producție vocală integral sintetică.

⁶⁴ Aäron van den Oord și Sander Dieleman, *WaveNet: A generative model for raw audio*, blogul Deepmind, septembrie 2016, <https://deepmind.com/blog/article/wavenet-generative-model-raw-audio>

⁶⁵ Yuxuan Wang, *Expressive Speech Synthesis with Tacotron*, blogul Google AI, martie 2018, <https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html>

⁶⁶ *Deep Voice 3: 2000-Speaker Neural Text-to-Speech*, blogul Baidu Research, octombrie 2017 <http://research.baidu.com/Blog/index-view?id=91>