

Reconocimiento Automático del Habla 2023-2024

Compromiso social y medioambiental

DSIC

DEPARTAMENT DE SISTEMES
INFORMÀTICS I COMPUTACIÓ



MIARFID

Máster en Inteligencia Artificial
Reconocimiento de Formas
e Imagen Digital

MIARFID-RAH mcastro@dsic.upv.es

¿Qué es una competencia transversal?

Podemos definir las competencias transversales como aquellas habilidades relacionadas con el desarrollo personal, que no dependen de un ámbito temático o disciplinario específico sino que aparecen en todos los dominios de la actuación profesional y académica (González y Wagenaar, 2003). Se trata de un saber hacer muy complejo, por lo que es necesario concretarla en resultados de aprendizaje más específicos.

<http://www.upv.es/contenidos/COMPTRAN/info/955270normalc.html>

- **¿Qué significa ser punto de control de una competencia transversal?**

Ser punto de control implica plantear actividades para, en el desarrollo de los contenidos, trabajar la competencia transversal y evaluarla, recogiendo evidencias de los logros alcanzados.

- **¿Cómo se evalúan?**

- Todas las asignaturas evalúan contenidos y competencias. Entre estas últimas están incluidas las competencias transversales. Por tanto, son curriculares y se evalúan dentro de las asignaturas.
- Una competencia transversal se evalúa como “Satisfactorio” o “En proceso”. No hay nota numérica.

Competencias transversales

- **Compromiso social y medioambiental**

Actuar con ética y responsabilidad profesional ante los desafíos sociales, ambientales y económicos.

<https://www.upv.es/entidades/vecal/compromiso-social-y-medioambiental/>

- Innovación y creatividad
- Trabajo en equipo y liderazgo
- Comunicación efectiva
- Responsabilidad y toma de decisiones



Algunas lecturas

- [“Privacy in Speech Technology”, Tom Bäckström](#) (Survey Talk Interspeech 2022, a partir de minuto 47). Capítulo [“Security and privacy in speech technology”](#) de su libro [“Introduction to Speech Processing”](#) III 3
- Un informe ([“Always on”](#)) donde se exponen algunas ideas y controversias relacionadas con las tecnologías del lenguaje y, en particular, con el reconocimiento del habla. IIII 5
- La noticia que saltó a los medios en enero de 2021, [Microsoft patented a chatbot that would let you talk to dead people](#). ¿Viste el capítulo de 'Black Mirror' se empezaba con un chatbot y se terminaba con un androide? IIIIIII 9
- ["Ethical and Technological Challenges of Conversational AI", Pascale Fung](#) (Keynote Interspeech 2021).
- [AI Ethics: What It Is and Why It Matters](#) (curso)
- [Ethics of artificial intelligence \(wikipedia\)](#)

<https://bigthink.com/thinking/deepfake-editing-morality-ai/>

Always on*

Is your Smart TV listening to your conversations?

Are your children's toys spying on your family?

- These types of questions are increasingly raised as the next generation of internet-connected devices enter the market. Such devices, often dubbed “always on,” include mobile phones, televisions, cars, toys, and home personal assistants—many of which are powered and enhanced by speech recognition technology.
- There is no doubt that the increasing prevalence of voice integration into everyday appliances enables companies to collect, store, analyze, and share increasing amounts of personal data.
- But.... **what kinds of data are these devices actually collecting,**
when are they collecting it, and
what are they doing with it?

(*) “Always On: Privacy Implications of Microphone-Enabled Devices”, by STACEY GRAY APRIL 2016

Microphone-enabled devices:

Activation

ACTIVATION: Manual, Always Ready, or Always On?

By their method of **activation**, consumer devices can be categorized as **manual**, **always ready**, or **always on**. In the past, most recording devices could be considered either on or off. Many new voice-based home assistants today can be considered “always ready” because they do not begin transmitting data off-site until they detect a wake phrase.

METHOD OF ACTIVATION



MANUAL

Device begins transmitting audio externally when a **button or switch** is pressed or held down.



Examples: Smart TVs (some);
Mattel's Hello Barbie



ALWAYS READY

Device processes locally to detect a “wake phrase*” which **wakes/triggers** the device to begin transmitting data.



Examples: Smart TVs (some); Home Assistant Devices,
e.g. Google Home, Amazon Echo

*Familiar wake phrases include: “Hey, Siri” “OK, Google,”
“Hey Cortana,” and “Alexa”



ALWAYS ON

Device transmits data 100% of the time on a standalone basis, and further processing occurs externally.



Examples: Home security systems;
CCTV; Body-worn cameras;
Baby monitors

BENEFITS

- ability to prevent unauthorized access through a hardware-linked microphone
- avoids unintentional activation

- convenience of verbal activation
- accessibility for users with physical limitations, e.g. mobility or visual impairment
- contextual responses, e.g. a home security system that alerts the owner and begins transmitting data when it detects a noise

- enabling physical security for people and property
- child safety

Microphone-enabled devices

Each category presents different privacy implications, influenced in part by whether data is

- stored locally (an increasingly rare practice) or
- whether it is transmitted from the device to a third party or external cloud storage.

Another key issue is whether the device is used for

- voice recognition, the biometric identification of an individual by the characteristics of her voice, or
- for speech recognition, the mere translation of voice into text.

These are among the many factors that must be assessed in order to evaluate potential privacy issues and determine appropriate notice, consent, and default frameworks.

Privacy implications

Privacy implications will vary by social and legal context

- Biometric Identification
- One and Two-Party Consent
- Employment and Workplaces
- Hospitals and Medical Environments
- Homes (Historically Protected Spaces)

Emergency privacy questions and best practices

1. Does processing and storage occur locally or externally (i.e. cloud-based)?
2. Does the device arrive with speech recognition, or other audio recording functionality, pre-enabled?
3. Does the device contain a hard on/off switch that can disable the microphone?
4. Does the device provide visual cues that clearly indicate when it is recording and/or transmitting information?
5. Use limitation is appropriate to alleviate concerns over mis-use of audio.
6. Ability to access and delete stored audio files will build consumer trust.
7. The difference between far-field or near-field microphone technology will influence appropriate privacy frameworks.

CONCLUSIONES ???

