Systemy rozpoznawania głosu a ich wpływ na ochronę danych i prywatność

Posted on 2024-09-30

Technologie rozpoznawania głosu przeszły długą drogę, ewoluując od prostych aplikacji rozpoznających pojedyncze słowa, po zaawansowane systemy zdolne do interpretacji złożonych fraz, różnych akcentów oraz tonów emocjonalnych. Ta dynamicznie rozwijająca się dziedzina technologii staje się integralną częścią naszego codziennego życia, umożliwiając bardziej naturalną i intuicyjną interakcję z urządzeniami elektronicznymi.

Dzięki postępom w dziedzinie uczenia maszynowego i sztucznej inteligencji, tego typu systemy osiągają niespotykany wcześniej poziom precyzji i wszechstronności, otwierając drzwi do szerokiego zakresu zastosowań – od asystentów głosowych, poprzez transkrypcje mowy, aż po zaawansowane systemy biometryczne. Zdarza się, że termin „rozpoznawanie głosu” używany jest zamiennie z terminem „rozpoznawanie mowy”, mają one jednak nieco inne znaczenie. Różnica ta może wydawać się subtelna, ale ma istotne implikacje dla zrozumienia tego, jak działają te technologie i jakie są ich zastosowania. Rozpoznawanie głosu skupia się na identyfikacji osoby na podstawie unikalnych cech jej głosu, natomiast rozpoznawanie mowy skupia się na konwersji mowy na tekst i często obejmuje także

zrozumienie języka naturalnego.

Obie technologie są ze sobą ściśle powiązane i często wykorzystywane wspólnie. Na przykład, system rozpoznawania mowy może najpierw zidentyfikować osobę mówiącą (rozpoznawanie głosu), a następnie przetłumaczyć jej wypowiedź na inny język (rozpoznawanie mowy). Rozwój tych technologii jest wspierany przez postępy w dziedzinie sztucznej inteligencji, w szczególności uczenia maszynowego. Algorytmy te uczą się rozpoznawać wzorce na podstawie ogromnych ilości danych, co pozwala na ciągłe poprawianie ich precyzji i skuteczności. Obecnie, zarówno systemy rozpoznawania głosu, jak i systemy rozpoznawania mowy są wykorzystywane w wielu dziedzinach.

Zastosowania dotyczące rozpoznawania głosu:

ØAsystenci głosowi, np. Siri, Alexa czy Google Assistant, które stały się powszechnym elementem naszego codziennego życia.

• Umożliwiają one użytkownikom wykonywanie różnych zadań – od zarządzania kalendarzem, przez sterowanie urządzeniami domowymi, aż po szukanie informacji w Internecie – wszystko to za pomocą prostych komend głosowych. Dzięki funkcji rozpoznawania głosu, asystent może dostosować swoje odpowiedzi i usługi do indywidualnych potrzeb i preferencji każdej osoby, co sprawia, że interakcja staje się bardziej spersonalizowana.

Ø Systemy bezpieczeństwa i monitoringu, w których głos jest wykorzystywany jako dane biometryczne do identyfikacji i weryfikacji tożsamości.

• Takie rozwiązania są stosowane m.in. w bankowości, przy kontroli dostępu do

zabezpieczonych obszarów, a także w aplikacjach mobilnych.

ØNarzędzia do analizy emocji w głosie, które stają się coraz bardziej popularne, zwłaszcza w obsłudze klienta i badaniach rynkowych.

• Systemy te potrafią wykrywać emocje, takie jak radość, smutek, gniew, co pozwala firmom lepiej rozumieć swoich klientów i dostosowywać swoje usługi.

Zastosowania dotyczące rozpoznawania mowy:

ØTranskrypcja mowy na tekst, która jest niezwykle przydatna w wielu branżach, takich jak dziennikarstwo, medycyna, prawo, czy edukacja, gdzie transkrypcja wywiadów, wykładów lub rozmów jest codziennością.

ØTranskrypcja mowy na mowę, czyli tłumaczenie mowy w czasie rzeczywistym, co znacząco ułatwia komunikację międzynarodową i może być wykorzystywane podczas konferencji, podróży czy na polu edukacji.

Rozwój technologii do rozpoznawania głosu sprawił, że istotnym zagadnieniem stała się ochrona danych osobowych. W tym miejscu należy podkreślić, że głos uznaje się za daną osobową, gdyż umożliwia identyfikację osoby, której dotyczy. Głos dostarcza słuchaczowi dodatkowych informacji, np. o płci mówiącego, lokalizacji czy nastroju, które można wykorzystać do identyfikacji danej osoby. Co więcej, najnowocześniejsza nauka o danych biometrycznych umożliwia identyfikację lub weryfikację osoby na podstawie unikalnych cech jej głosu. W związku z tym, że głos bardzo często odnosi się (samodzielnie lub w połączeniu z innymi informacjami) do możliwej do zidentyfikowania osoby fizycznej, stanowi on dane osobowe w rozumieniu art. 4 RODO.

W wytycznych EROD 02/2021 w sprawie VVA czyli wirtualnych asystentów głosowych, zwrócono między innymi uwagę na to, że administratorzy danych świadczący usługi VVA i ich podmioty przetwarzające muszą brać pod uwagę zarówno ogólne rozporządzenie o ochronie danych (RODO), jak i dyrektywę o e-prywatności. W wytycznych określono najistotniejsze wyzwania związane
z zapewnieniem zgodności i przedstawiono zalecenia dla odpowiednich zainteresowanych stron dotyczące sposobów radzenia sobie z nimi.

Wyzwania związane z ochroną danych osobowych i prywatnością

Wykorzystanie systemów rozpoznawania głosu wiąże się z kilkoma kluczowymi wyzwaniami dotyczącymi prywatności:

• Zbieranie danych dźwiękowych

Systemy rozpoznawania głosu często wymagają stałego nasłuchu, aby mogły reagować na komendy użytkowników. Taki ciągły nasłuch wiąże się z ryzykiem rejestrowania prywatnych rozmów bez zgody użytkowników. Przykłady takich sytuacji pojawiały się już w przeszłości, gdy urządzenia nagrywały dźwięk, mimo że użytkownicy nie wydali żadnej komendy.

• Przechowywanie danych

Nagrania głosowe są często przechowywane przez firmy świadczące usługi rozpoznawania głosu. Przechowywanie tych danych niesie ze sobą ryzyko ich niewłaściwego wykorzystania, na przykład do celów analitycznych, marketingowych lub w przypadku wycieku danych.

Brak odpowiednich zabezpieczeń może prowadzić do poważnych naruszeń prywatności.

• Analiza biometryczna

Głos jest unikalny dla każdej osoby i może być wykorzystywany do identyfikacji tożsamości. Wykorzystanie takich danych wiąże się z ryzykiem ich nieuprawnionego dostępu lub użycia. Przykładowo, w przypadku ich wycieku, osoba trzecia mogłaby uzyskać dostęp do zabezpieczonych systemów lub dokonać podszywania się pod daną osobę.

• Brak transparentności

Użytkownicy systemów rozpoznawania głosu często nie są w pełni świadomi, jakie dane są zbierane, w jaki sposób są one przetwarzane i do jakich celów mogą być wykorzystywane. Brak jasnych i przejrzystych polityk prywatności oraz brak informacji o tym, co dzieje się z ich danymi, może prowadzić do naruszeń praw użytkowników.

RODO a systemy rozpoznawania głosu RODO, wprowadza ścisłe regulacje dotyczące ochrony danych osobowych, do których

zaliczany jest również głos:

- Jak wspomniano wcześniej systemy rozpoznawania głosu mają dostęp do informacji o charakterze prywatnym, które mogą być chronione na mocy art. 9 RODO, takich jak dane biometryczne. Dlatego projektanci i twórcy takich systemów muszą dokładnie określić, w jakich przypadkach przetwarzanie wiąże się ze specjalnymi kategoriami danych.
- Zgodnie z RODO, przed zbieraniem danych osobowych konieczne jest uzyskanie wyraźnej zgody użytkownika. Użytkownicy muszą być w pełni informowani o celu zbierania danych i sposobie ich przetwarzania.
- Użytkownicy mają prawo wiedzieć, jakie dane są zbierane, w jakim celu i jak długo będą przechowywane.
- • Użytkownicy mogą zażądać usunięcia swoich danych osobowych, co ma szczególne znaczenie w przypadku danych biometrycznych.
- • Twórcy aplikacji i systemów rozpoznawania głosu powinni wdrożyć odpowiednie zabezpieczenia, które mogą znacząco zmniejszyć ryzyko naruszeń prywatności np.:
    - o Szyfrowanie danych end-to-end
    - o Lokalne przetwarzanie danych głosowych bez przesyłania ich do chmury
    - o Techniki federated learning: pozwalające na trenowanie modeli bez konieczności centralizacji danych użytkowników
    - o Differential privacy: metoda dodawania kontrolowanego szumu do danych, aby chronić prywatność jednostek przy zachowaniu użyteczności danych zbiorczych
    - o Regularne audyty bezpieczeństwa
    - o Implementacja zasady privacy by design w procesie tworzenia systemów rozpoznawania głosu

Systemy rozpoznawania głosu a ich wpływ na ochronę danych i prywatność

Technologia rozpoznawania głosu, mimo licznych korzyści, budzi istotne obawy związane z prywatnością użytkowników. Głos ludzki stanowi cenne źródło informacji o jednostce, a jego nieuprawnione wykorzystanie może prowadzić do poważnych naruszeń prywatności. Choć przypadki nadużyć są szeroko dyskutowane, wciąż brakuje kompleksowych rozwiązań, które w pełni zabezpieczyłyby dane głosowe. Dlatego niezwykle ważne jest połączenie zaawansowanych technologii zabezpieczeń z odpowiednimi regulacjami prawnymi, aby zapewnić, że rozwój technologii rozpoznawania głosu będzie się odbywał z poszanowaniem fundamentalnych praw człowieka.