

Cyberwindykator musi mieć nadzór człowieka

Przedsiębiorcy coraz częściej korzystają ze sztucznej inteligencji, np. do rozmów z dłużnikami. Może to być ryzykowne, zwłaszcza gdy przetwarzane są dane biometryczne

Jakub Styczyński

jakub.styczynski@infor.pl
@JakubStyczynski

Program wykorzystujący sztuczną inteligencję prowadzi Alior Bank. Komputerowy system już nie tylko przeprowadza ankiety, ale także bierze udział w procesie windykacji wierzytelności. Jak to działa? Otóż automat dzwoni do osoby posiadającej dług i przeprowadza z nią krótki wywiad na temat tego, kiedy zwróci pieniądze. Rozmowa jest nagrywana, a rozmówca identyfikowany na podstawie porównania próbki głosowej z tą istniejącą w bazie. Dzwoniący robot potrafi zrozumieć odpowiedzi na podstawowe pytania i nawet nawiązać prostą konwersację. Jeśli dłużnik poda datę zwrotu pieniędzy – sztuczna inteligencja zapisuje ją w bazie.

Wymierne rezultaty działania nowej technologii pozytywnie zaskoczyły nawet specjalistów ją wdrażających. Pilotażowy program wykazał, że skuteczność w odzyskiwaniu należności wzrosła o 10 proc., a koszty obsługi spadły aż pięciokrotnie (można zatrudnić mniej ludzi do wykonywania tej pracy).

Maszyna nie może mieć ostatniego słowa

Nowa technologia budzi coraz większe zainteresowanie wśród innych przedsiębiorców, którzy chcieliby w przyszłości wykorzystywać podobny system nie tylko do dochodzenia wierzytelności. Pojawia się jednak wiele wątpliwości natury prawnej. Przykładowo: czy system komputerowy może dzwonić w imieniu windykatorka bądź banku.

– Robot działa w imieniu banku i w sensie prawa cywilnego czy bankowego to tak, jakby działał bank, więc wykorzystanie go nie wymaga jeszcze żadnych zmian w regulaminie czy konkretnych postanowień w umowie – uważa dr Paweł Litwiński, adwokat w kancelarii Barta Litwiński, ekspert Instytutu Allerhanda.

Ale uwaga! Zasady działania robota, a w szczególności podejmowane przez niego decyzje, mogą wymagać oceny z punktu widzenia art. 26a ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U z 2016 r. poz. 922 ze zm.), czyli zakazu automatycznych rozstrzygnięć. Zgodnie z tym przepisem

niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

– Innymi słowy, nie można tak skonstruować systemu, by algorytm w oparciu o dane zbierane w czasie rozmowy czy też przechowywane już w systemie bankowym podejmował ostateczne decyzje dotyczące np. windykacji należności – wyjaśnia Witold Chomiczewski, radca prawny w kancelarii Lubasz i Wspólnicy. A zatem system musi uwzględniać człowieka w procesie podejmowania decyzji albo przynajmniej możliwość odwołania się od tej decyzji do realnego windykatorka.

Podobnym zagadnieniem zajmował się sąd administracyjny w Warszawie. W wyroku z 24 listopada 2005 r. (sygn. akt II SA/Wa 1335/05) orzekł on, że jeśli decyzja o odmowie pożyczki zapadła w związku z negatywną oceną scoringową podejmowaną automatycznie przez system informatyczny, to takie postępowanie jest niedopuszczalne w świetle postanowień wspomnianego wcześniej art. 26a ustawy o ochronie danych osobowych.

Weryfikacja głosu niedoskonała

Przedsiębiorcy muszą pamiętać też o tym, że to oni odpowiadają za błędy maszyny. Choć technologia rozpoznawania głosu zrobiła w ostatnich latach wielki postęp, to wciąż twórcy takich systemów napotykają problemy. Wszystko przez fakt, że głos – inaczej niż np. odcisk palca – ulega modyfikacjom. W opracowaniach czytamy, że systemy weryfikacji mogą szwankować np. w momencie, gdy rozmówca mówi zbyt cicho (albo zbyt głośno), niewyraźnie, posiada słaby mikrofon wbudowany w telefonie bądź jego głos jest zakłócony przez odgłosy w tle. Zniekształcenia mogą powodować chryпка czy katar.

Doktor Paweł Litwiński ostrzega, że pomyłki systemów, szczególnie w przypadku banków oraz działających w ich imieniu pracowników i podwykonawców, mogą skutkować surowymi karami. Wystarczy bowiem, by system zadziałał nieprawidłowo i wyjawiał informacje o długach lub inne poufne dane osobie nieuprawnio-

nej. A zgodnie z art. 171 ustawy z 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz.U z 2015 r. poz. 128 ze zm.) za złamanie tajemnicy bankowej grozi grzywna nawet do miliona złotych oraz kara pozbawienia wolności do lat 3.

Alior zapewnia jednak, że ma wszystko pod kontrolą. – Zniekształcenia powstałe w wyniku trwałych zmian głosowych nie są problemem, ponieważ próbki głosu są aktualizowane przy każdym kontakcie z contact center. Bank przechowuje jedynie macierz z matematycznym zapisem charakterystyki głosu klienta – wyjaśnia Igor Zacharjusz, menedżer zespołu współpracy z partnerami zewnętrznymi w Alior Innovation Lab.

Gdyby system został zastosowany w innym podmiocie niż instytucja finansowa i ujawniłby poufne informacje osobie nieuprawnionej, to w grę wchodziłaby również odpowiedzialność z tytułu naruszenia dóbr osobistych. A wtedy, zgodnie z art. 24 ustawy z 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U z 2016 r. poz. 380 ze zm.), osoba, której dobra zostały naruszone cudzym działaniem, może nie tylko żądać zaniechania tego działania, ale również naprawienia szkód (także majątkowych) powstałych z powodu tego działania.

Szalejące maszyny

To jednak nie wszystkie możliwe problemy. Znaną są przypadki, gdy automatyczne systemy call center w wyniku awarii wydzwaniały do losowo wybranych klientów np. przez całą noc. Taka awaria mogłaby skutkować posądzeniem o uporczywe nękanie (stalking). A zgodnie z art. 190a par. 1 ustawy z 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U z 2016 r. poz. 1137 ze zm.), kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.

Przedsiębiorcy muszą również pamiętać, by uzyskać odpowiednie zgody klientów. W przeciwnym razie mogą ponieść odpowiedzialność z tytułu braku uzyskania zgody na używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla

OPINIA EKSPERTA



MAŁGORZATA KAŁUŻYŃSKA-JASAK

rzecznik prasowy generalnego inspektora ochrony danych osobowych

Większości przypadków dane biometryczne stanowią dane osobowe, i to szczególnej kategorii. Są bowiem niezmiennymi, niepowtarzalnymi i ściśle związane z konkretną osobą fizyczną. Bo o ile dane biometryczne danej osoby można usunąć lub zmienić, to jednak źródła, z którego pochodzą, nie da się zasadniczo ani zmienić, ani usunąć. Dlatego tym bardziej należy zwrócić uwagę na potencjalne zagrożenia związane ze stosowaniem biometrii głosowej – przede wszystkim z punktu widzenia bezpieczeństwa tego rodzaju identyfikacji i ryzyka związanego z możliwością przechwycenia próbki głosu. Zatem rozwiązanie zaprojektowane jako ułatwiające kontakt z klientem powinno uwzględniać zastosowanie odpowiednich zabezpieczeń. Gdy bowiem raz udostępnimy dane biometryczne, będzie można nas zawsze automatycznie identyfikować, bez konieczności jakichkolwiek dodatkowych działań z naszej strony. Gdy dostaną się one w ręce osób niepowołanych, umożliwią kradzież naszej tożsamości, co może rodzić bardzo poważne i trudne do odwrócenia konsekwencje. Przykład konieczności spłacania niezaciągniętego kredytu przemawia do wyobraźni. GIODO nie popiera bezrefleksyjnego wykorzystywania danych biometrycznych w sytuacjach, w których dla osiągnięcia zamierzonego celu wystarczy wykorzystać inne dane, mniej ingerujące w naszą prywatność, gdyż do stopniowej jej utraty może się właśnie przyczynić powszechne i nieograniczone stosowanie biometrii.



celów marketingu bezpośredniego, o której mowa w art. 172 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U z 2016 r. poz. 1489 ze zm.). Karę za taki czyn nakłada prezes Urzędu Komunikacji Elektronicznej w wysokości do 3 proc. przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym (zgodnie z art. 209 ust. 25 prawa telekomunikacyjnego).

RODO a biometria

Wyzwaniem dla przedsiębiorców jest też odpowiednie zabezpieczenie danych biometrycznych gromadzonych dla celów weryfikacji przez maszyny. Na początku maja 2016 r. w Dzienniku Urzędowym Unii Europejskiej (nr L119) opublikowano teksty nowego rozporządzenia i dyrektywy o ochronie danych osobowych (RODO). Państwa członkowskie mają czas na implementację dyrektywy do 6 maja 2018 r. Zgodnie z regulacjami dane takie jak charakterystyka głosu zostaną uznane za dane biometryczne i będą traktowane w podobny sposób jak dziś dane wrażliwe (np. dane medyczne, poglądy polityczne czy orienta-

cja seksualna). By je przetwarzać, wymagana będzie wyraźna zgoda.

– Będzie musiała być ona jednoznaczna, świadomym i niedomniemanym oświadczeniem woli – mówi mec. Witold Chomiczewski. Tłumaczy, że w przypadku klientów, z którymi przedsiębiorca będzie miał zawartą umowę przed dniem wejścia w życie postanowień dyrektywy RODO, dla potwierdzenia zgody na wykorzystanie próbki głosowej wystarczy kontakt telefoniczny z jasnym komunikatem i informacją o jej pobraniu lub próbie weryfikacji.

W przypadku nowych klientów zalecać się będzie jednak przygotowanie nowego zapisu w umowie, który będzie zawierał wyraźną zgodę na gromadzenie i przetwarzanie danych biometrycznych. Klauzula ta musi być wyraźnie odseparowanym punktem w umowie bądź osobnym dokumentem do podpisania – a więc powinna zostać przedstawiona w podobny sposób, jak dziś wyraża się zgodę na gromadzenie i przetwarzanie zwykłych danych osobowych. Klauzula nie będzie mogła zostać ukryta między paragrafami bądź w regulaminie.

