Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

Seria poradników z przymrużeniem oka ;)

Mam AI na Każdym Spotkaniu i Nie Wiem, Co Ono Zapamiętuje

Jak ustalać zasady nagrywania, transkrypcji i użycia firmowych danych przez asystentów AI bez zamieniania każdego calla w przesłuchanie RODO



Mamy problem. Ale spokojnie.
Da się go rozwiązać i jeszcze będzie z czego się pośmiać.

Mam AI na Każdym Spotkaniu i Nie Wiem, Co Ono Zapamiętuje

Jak ustalać zasady nagrywania, transkrypcji i użycia firmowych danych przez asystentów AI bez zamieniania każdego calla w przesłuchanie RODO

Max Paradox

PROBLEM? WYLUZUJ. OGARNIESZ TO!

ISBN: 978-83-8483-561-6

SPIS TREŚCI

INTRO 5

Rozdział 1 - Kto właściwie zaprosił AI na spotkanie? 11

Rozdział 2 - Nagranie, transkrypcja i notatka nie są tym samym 20

Rozdział 3 - RODO nie jest zaklęciem, które rozwiązuje wszystko 30

Rozdział 4 - Zakazaliśmy botów, więc teraz wszyscy używają ich po cichu 41

Rozdział 5 - Kalendarz zaprosił bota, zanim zdążyłeś powiedzieć dzień dobry 52

Rozdział 6 - Udostępniasz jeden slajd, a pokazujesz pół firmy 62

Rozdział 7 - Link do notatek dostał własne życie i teraz zwiedza firmę 72

Rozdział 8 - AI miało robić notatki, a zaczęło wystawiać ludziom oceny 82

Rozdział 9 - Zanim włączysz nagrywanie, ustal, po co właściwie to robisz 92

Rozdział 10 - Jak powiedzieć o AI w minutę i nie zepsuć spotkania 101

Rozdział 11 - Kiedy AI ma zapomnieć, czyli porządki w cyfrowej pamięci 112

Rozdział 12 - Nie karm kolejnego AI wszystkim, co powiedzieliście na spotkaniu 123

Rozdział 13 - AI napisało, że ustaliliśmy. Szkoda, że nikt o tym nie wie 134

Rozdział 14 - Dostawca mówi, że AI jest bezpieczne. Świetnie, ale co to właściwie znaczy?.....145

Rozdział 15 - Co zrobić, kiedy AI narobiło bałaganu i wszyscy patrzą na ciebie 157

Rozdział 16 - Kiedy wszystkie zasady są słuszne, ale nie da się ich zastosować naraz.....167

Rozdział 17 - Połowa zespołu kocha AI, druga połowa chce wyrzucić je przez okno.....178

Rozdział 18 - Zasady działały świetnie, dopóki ktoś nie zaktualizował aplikacji 189

Rozdział 19 - Wszystko działało, dopóki nie przestaliśmy zwracać uwagi 201

Rozdział 20 - Nie musisz kontrolować każdego bota, żeby odzyskać kontrolę nad spotkaniami 211

INTRO

Jest 9:07. Spotkanie trwa od siedmiu minut, ale właśnie dołącza kolejny uczestnik. Nazywa się Meeting Assistant, nie ma twarzy, nie pije kawy i prawdopodobnie jako jedyny naprawdę uważnie słucha. Ktoś rzuca: „To mój bot, robi notatki". Wszyscy kiwają głowami, bo przecież jesteśmy nowoczesną organizacją, a nie klubem przeciwników elektryczności. Pięć minut później padają informacje o marży, problemach z klientem i planowanej zmianie personalnej. Dopiero wtedy pojawia się myśl: zaraz, gdzie właściwie trafiają te notatki? Kto je zobaczy? Czy można je usunąć? I dlaczego nikt nie zadał tych pytań, zanim cyfrowy stenograf rozsiadł się przy naszym wirtualnym stole?

Najbardziej fascynujące jest to, jak szybko zaakceptowaliśmy obecność dodatkowego słuchacza. Gdyby na spotkanie wszedł nieznajomy człowiek, usiadł w kącie i oznajmił, że będzie zapisywał wszystko, co mówimy, zapewne ktoś poprosiłby go o przedstawienie się. Gdy robi to oprogramowanie, wystarcza sympatyczna ikonka i zapewnienie, że dzięki niemu będziemy bardziej produktywni. Być może będziemy. Problem zaczyna się wtedy, gdy produktywność staje się odpowiedzią na pytania, których jeszcze nie zadaliśmy. Automatyczny protokół może oszczędzić godzinę pracy, ale nie wyjaśnia automatycznie, czy wolno było zebrać wszystkie zawarte w nim informacje.

Samo słowo „zapamiętuje" również potrafi wprowadzić niezłe zamieszanie. Jeden asystent przetwarza dźwięk i przygotowuje podsumowanie. Inny tworzy pełną transkrypcję, przechowuje nagranie albo pozwala później przeszukiwać wypowiedzi uczestników. Jeszcze inny łączy

informacje ze spotkania z dokumentami dostępnymi w firmowym środowisku. Zakres działania zależy od konkretnego narzędzia, konfiguracji, uprawnień i zasad dostawcy. Nie można zakładać, że każdy system działa identycznie. Pytanie „czy AI to pamięta?" jest więc trochę jak pytanie „czy biuro ma klucze?". Owszem, ale rozsądnie byłoby ustalić, do których drzwi, kto je posiada i czy przypadkiem jeden komplet nie leży pod wycieraczką.

W organizacjach próbuje się zwykle rozwiązać ten problem na dwa sposoby. Pierwszy polega na całkowitym zaufaniu technologii. Skoro narzędzie zostało kupione przez firmę, zapewne ktoś wszystko sprawdził. Być może rzeczywiście sprawdził, ale zakup licencji nie oznacza, że każdy użytkownik automatycznie zna wszystkie ograniczenia. Drugi sposób to reakcja obronna: zakazać wszystkiego, wyłączyć wszystkie funkcje i traktować każdy nowy przycisk jak podejrzaną przesyłkę pozostawioną przed siedzibą zarządu. W efekcie pracownicy wracają do ręcznych notatek albo szukają wygodniejszych narzędzi na własną rękę. Żadna skrajność nie daje szczególnie dobrego poczucia kontroli.

Istnieje też trzecia droga, znacznie mniej widowiskowa, ale bardziej użyteczna: ustalić jasne zasady, zanim pojawi się kłopot. Nie wymaga to, żeby każdy prowadzący spotkanie posiadał dyplom z prawa, certyfikat cyberbezpieczeństwa i umiejętność recytowania RODO z pamięci. Wymaga natomiast rozpoznania kilku istotnych różnic. Nagrywanie nie jest tym samym co sporządzanie notatek. Dostęp do podsumowania nie oznacza automatycznie dostępu do nagrania. Usunięcie widocznej transkrypcji nie musi oznaczać natychmiastowego zniknięcia wszystkich kopii danych. A zgoda wypowiedziana

mimochodem przez jednego uczestnika nie rozstrzyga wszystkich obowiązków organizacji.

To ostatnie jest szczególnie ważne, ponieważ kwestie prywatności i bezpieczeństwa nie sprowadzają się do magicznego zdania „wszyscy się zgadzają?". To, jakie zasady prawne mają zastosowanie, zależy między innymi od rodzaju danych, celu ich wykorzystania, relacji między uczestnikami i sposobu działania organizacji. W niektórych sytuacjach potrzebna będzie ocena specjalistów od ochrony danych, bezpieczeństwa albo prawa. Ta książka nie zastąpi ich pracy. Pomoże jednak zadawać właściwe pytania i rozpoznawać sytuacje, w których sympatyczny komunikat „bot tylko pomaga" jest zdecydowanie zbyt skromnym opisem rzeczywistości.

Nie zamierzam przekonywać cię, że asystenci AI są z definicji zagrożeniem. Ich zalety potrafią być bardzo konkretne. Dobrze przygotowane podsumowanie pozwala wrócić do ustaleń bez organizowania kolejnego spotkania pod tytułem „Przypomnijmy, co ustaliliśmy na poprzednim". Transkrypcja może ułatwić odnalezienie ważnego fragmentu rozmowy, a lista zadań ograniczyć sytuacje, w których pięć osób wychodzi z identycznym przekonaniem, że zadanie wykona ktoś inny. Technologia rzeczywiście potrafi zmniejszyć administracyjny ciężar spotkań. Tylko że jej korzyści nie zwalniają nas z odpowiedzialności za to, jakie informacje jej powierzamy i jak później wykorzystujemy rezultaty.

W dodatku AI nie jest bezbłędnym kronikarzem. Potrafi pomylić rozmówców, nie uchwycić ironii, zgubić zastrzeżenie albo przedstawić luźną propozycję jako podjętą decyzję. To szczególnie nieprzyjemne, gdy w automatycznym podsumowaniu pojawia się zdanie: „Zespół

uzgodnił redukcję budżetu", chociaż zespół uzgodnił jedynie, że warto porozmawiać o możliwościach oszczędzania. Między tymi sformułowaniami mieści się całkiem spory kawałek firmowej rzeczywistości, niekiedy razem z premią roczną. Dlatego oprócz zasad zbierania informacji potrzebujemy również zasad sprawdzania, poprawiania i zatwierdzania tego, co sztuczna inteligencja stworzyła.

Najtrudniejsze bywają jednak nie ustawienia techniczne, lecz ludzie. Jak poprosić przełożonego o wyłączenie nagrywania, nie brzmiąc jak osoba mająca coś do ukrycia? Co zrobić, gdy klient zaprasza własnego asystenta, a twoja firma ma inne zasady? Jak poinformować uczestników o transkrypcji, żeby pierwsze dziesięć minut spotkania nie przypominało rozprawy sądowej? I kto właściwie powinien podjąć decyzję: organizator, właściciel narzędzia, dział IT, osoba odpowiedzialna za bezpieczeństwo czy ktoś jeszcze? Odpowiedzi nie zawsze będą identyczne. Tym bardziej potrzebujemy procesu, który nie wymaga każdorazowego zwoływania komisji do spraw obecności robota na Teamsach.

Będziemy więc przyglądać się nie tylko technologii, lecz również codziennym decyzjom. Dowiesz się, jak rozróżniać informacje, które można bezpiecznie wykorzystać w zatwierdzonym środowisku, od tych wymagających dodatkowej ostrożności. Jak ustalać cel nagrywania, zakres dostępu, okres przechowywania i zasady usuwania danych. Jak traktować spotkania z osobami spoza organizacji oraz jak reagować, gdy asystent pojawia się bez wcześniejszego uzgodnienia. Ważne będzie także to, czego nie robić: nie kopiować poufnej transkrypcji do przypadkowej aplikacji tylko dlatego, że potrafi ona przygotować ładniejszą tabelkę,

i nie traktować wygenerowanego streszczenia jak niepodważalnego protokołu.

Nie będziemy przy tym zakładać, że dysponujesz nieograniczonym budżetem, własnym działem prawnym i wolnym piątkiem przeznaczonym wyłącznie na analizę ustawień. Być może zarządzasz zespołem, który ma zbyt wiele spotkań i zbyt mało czasu. Być może jesteś pracownikiem, który nie wybiera firmowych narzędzi, ale odpowiada za informacje przekazywane podczas rozmów. A może właśnie próbujesz stworzyć rozsądne standardy dla całej organizacji, w której jedni używają AI do wszystkiego, a inni nadal podejrzliwie obserwują funkcję automatycznych napisów. Dobre zasady muszą działać również w takich warunkach, a nie wyłącznie na idealnym schemacie przygotowanym do prezentacji dla zarządu.

Wyobraź sobie teraz spotkanie, na którego początku organizator spokojnie wyjaśnia, czy asystent będzie używany, co zostanie zapisane i kto otrzyma wynik. Uczestnicy wiedzą, kiedy mogą poprosić o wyłączenie określonych funkcji, a informacje poufne mają właściwie ustaloną ścieżkę postępowania. Po spotkaniu ktoś sprawdza podsumowanie, zanim zacznie ono żyć własnym życiem. Nikt nie wygłasza dwudziestominutowego wykładu o ochronie danych. Nikt również nie musi udawać, że temat nie istnieje. Brzmi mało spektakularnie? Doskonale. Właśnie o to chodzi. Rozsądne korzystanie z AI powinno być normalną częścią pracy, a nie wydarzeniem wymagającym specjalnej oprawy.

Celem nie jest doprowadzenie do sytuacji, w której przestaniesz ufać wszystkim urządzeniom wyposażonym w mikrofon. Chodzi o odzyskanie wpływu na to, co dzieje się z informacjami ze spotkań. Możesz korzystać z wygody

automatycznych notatek, a jednocześnie wiedzieć, gdzie przebiegają granice. Możesz zapytać o prywatność bez oskarżania współpracownika o szpiegostwo przemysłowe. I możesz zaakceptować obecność cyfrowego asystenta, nie przyznając mu automatycznie nieograniczonego dostępu do firmowej pamięci.

Bo jeśli AI ma siedzieć z nami przy stole, wypada przynajmniej wiedzieć, kto je zaprosił, co zapisuje i kiedy wreszcie wychodzi.

Rozdział 1 - Kto właściwie zaprosił AI na spotkanie?

Piątek, godzina 14:46. Zespół omawia kwartalne wyniki, a prowadząca spotkanie próbuje ustalić, dlaczego prognoza sprzedaży wygląda tak, jakby ktoś przygotował ją po trzech kawach i jednej osobistej tragedii. W pewnym momencie na liście uczestników pojawia się tajemnicza nazwa. Nie jest to człowiek, którego ktokolwiek kojarzy. Nie ma stanowiska, działu ani nawet zdjęcia z firmowego wyjazdu integracyjnego. Ktoś pyta, kto to. Odpowiedź brzmi: „Spokojnie, to tylko asystent AI". Sprawa zostaje uznana za wyjaśnioną, chociaż w rzeczywistości wyjaśniono mniej więcej tyle, ile wyjaśnia odpowiedź „to tylko samochód" na pytanie, kto zaparkował ciężarówkę w sali konferencyjnej.

Słowo „asystent" brzmi niewinnie. Kojarzy się z kimś, kto pomaga, organizuje i przypomina o terminach. Tymczasem określenie to obejmuje bardzo różne rozwiązania techniczne. Jedne działają jako osobni uczestnicy spotkania, inne są funkcją platformy komunikacyjnej, kolejne pracują w przeglądarce albo na urządzeniu użytkownika. Niektóre wymagają wyraźnego uruchomienia, inne można skonfigurować tak, aby aktywowały się automatycznie. Sam wygląd ikonki czy nazwa wyświetlana obok uczestników niewiele mówi o rzeczywistym sposobie przetwarzania informacji. Dlatego pierwsza rzecz, którą warto zrozumieć, jest zaskakująco prosta: obecność AI na spotkaniu nie oznacza jednej, zawsze takiej samej czynności.

Można to porównać do tradycyjnego zebrania. Jedna osoba robi krótkie notatki w zeszycie. Druga nagrywa dźwięk telefonem. Trzecia filmuje salę, a czwarta sporządza

szczegółowy protokół, który następnie wysyła całemu przedsiębiorstwu. Wszyscy mogliby powiedzieć, że dokumentują spotkanie, ale trudno uznać, że robią dokładnie to samo. W świecie AI różnice bywają jeszcze mniej widoczne, ponieważ kilka funkcji może kryć się za jednym przyciskiem. Użytkownik widzi wygodne „Utwórz podsumowanie", a za kulisami mogą zachodzić różne operacje, których zakres trzeba ustalić dla konkretnego produktu i jego konfiguracji.

Niewidzialny uczestnik nie zawsze ma własną ikonkę

Pierwszym błędem jest zakładanie, że jeśli na liście uczestników nie widać żadnego dodatkowego bota, to spotkanie nie korzysta ze sztucznej inteligencji. Część funkcji jest wbudowana bezpośrednio w platformę. Inne rozwiązania mogą przetwarzać dźwięk dostępny na urządzeniu użytkownika, niezależnie od tego, czy do rozmowy dołączył osobny uczestnik. Bywają też narzędzia, które otrzymują dopiero gotowy materiał po zakończeniu spotkania. W takich sytuacjach sprawdzenie listy obecności jest przydatne, lecz nie wystarcza do ustalenia, jakie dane trafiają do systemów AI.

Wyobraź sobie pracownika, który podczas rozmowy z klientem korzysta z zatwierdzonej firmowej platformy. Nie uruchamia nagrywania i nie zaprasza dodatkowego uczestnika. Po spotkaniu kopiuje jednak historię czatu oraz własne notatki do zewnętrznego asystenta, prosząc o przygotowanie profesjonalnego podsumowania. Z punktu widzenia pozostałych osób spotkanie odbyło się bez udziału AI. Z punktu widzenia danych sprawa wygląda inaczej: informacje zostały później przekazane do kolejnego systemu. To nie dowód, że automatycznie doszło do

naruszenia zasad. To dowód, że kontrolowanie samego momentu nagrywania nie obejmuje całej rzeczywistości.

Warto więc przestać myśleć o sztucznej inteligencji wyłącznie jak o gościu, który wchodzi na spotkanie, i zacząć patrzeć na nią jak na element procesu. Informacje mogą zostać zebrane przed rozmową, podczas niej albo po jej zakończeniu. Zaproszenie z agendą może zawierać dane o klientach. Udostępniony ekran może ujawnić dokumenty, których nikt nie planował omawiać. Historia czatu może zostać zachowana niezależnie od dźwięku. A wygenerowane podsumowanie może później trafić do systemu zarządzania zadaniami, gdzie zobaczą je osoby nieobecne na spotkaniu. Każdy z tych kroków zasługuje na oddzielne pytanie o cel, uprawnienia i odpowiedzialność.

Nie oznacza to oczywiście, że należy przed każdym połączeniem prowadzić techniczne śledztwo. Gdybyśmy szczegółowo analizowali wszystkie procesy informatyczne przed każdym cotygodniowym statusem, zabrakłoby nam czasu nawet na omawianie opóźnień. Rozsądniejszym podejściem jest poznanie narzędzi używanych w organizacji i ustalenie podstawowych reguł ich działania. Wtedy uczestnik spotkania nie musi od początku badać całego systemu. Powinien wiedzieć, jakie rozwiązanie jest dopuszczone, do czego może zostać użyte i kiedy trzeba się zatrzymać.

Cztery pytania, które oszczędzają czterdzieści nieporozumień

Gdy podczas spotkania pojawia się asystent AI, dobrze jest umieć odpowiedzieć na cztery pytania: kto go uruchomił, z jakiej usługi korzysta, jakie informacje przetwarza oraz kto otrzyma rezultaty. Nie są to pytania o wewnętrzną architekturę modeli językowych. Nie wymagają

znajomości procesorów, serwerowni ani umiejętności wyjaśniania, dlaczego chatbot czasami odpowiada z pewnością siebie godną prezesa, mimo że właśnie pomylił miesiące. Chodzi o podstawową wiedzę operacyjną.

Pierwsze pytanie dotyczy odpowiedzialności. Jeżeli ktoś uruchamia narzędzie, powinien rozumieć przynajmniej zakres jego działania i obowiązujące zasady. Drugie pozwala ustalić, czy wykorzystywana jest usługa zaakceptowana przez organizację. Trzecie rozstrzyga, czy system ma dostęp wyłącznie do wypowiedzi, czy również do innych elementów spotkania. Czwarte jest szczególnie istotne, ponieważ rezultaty pracy asystenta często żyją znacznie dłużej niż sama rozmowa. Nawet bez nagrania dźwięku podsumowanie może zawierać informacje, których nie należy swobodnie rozpowszechniać.

Przyjrzyjmy się przykładowej sytuacji. Kierowniczka projektu organizuje cotygodniowe spotkanie dotyczące wdrożenia nowego produktu. Jeden z uczestników ma własne narzędzie automatycznie dołączające do wszystkich wydarzeń w kalendarzu. Dzisiaj oprócz zwykłego omówienia terminów pojawi się temat opóźnienia dostawcy i możliwej kary umownej. Gdy asystent próbuje wejść do rozmowy, prowadząca pyta spokojnie, z jakiej usługi korzysta pracownik i czy jest ona zatwierdzona dla tego rodzaju informacji. Okazuje się, że pracownik nie zna odpowiedzi. Asystent nie zostaje wpuszczony, a spotkanie odbywa się normalnie. Decyzja nie wynika z przekonania, że każde AI jest niebezpieczne. Wynika z braku informacji potrzebnych do świadomego użycia konkretnego rozwiązania.

Właśnie tutaj pojawia się istotna różnica między ostrożnością a podejrzliwością. Ostrożność polega na weryfikowaniu warunków, które mają znaczenie.

Podejrzliwość próbuje zgadywać intencje innych. Pracownik, który zaprosił niezidentyfikowanego asystenta, nie musi być nieodpowiedzialny ani działać w złej wierze. Mógł po prostu włączyć funkcję poleconą przez znajomego lub zaznaczyć opcję automatycznego dołączania, nie rozumiejąc wszystkich konsekwencji. Zamiast urządzać mu publiczny proces o zdradę tajemnic handlowych, lepiej wskazać konkretną niejasność i sposób jej wyjaśnienia.

Firmowe konto nie jest magiczną tarczą

Często słyszymy argument: „Przecież loguję się służbowym adresem, więc wszystko jest firmowe". Niestety adres e-mail nie jest certyfikatem bezpieczeństwa. Może służyć do utworzenia konta w usłudze, której organizacja wcale nie zatwierdziła. Może też umożliwiać korzystanie z narzędzia na warunkach innych niż te ustalone w ramach firmowej umowy. Sam fakt, że aplikacja pozwoliła na rejestrację, nie oznacza, że sprawdziła politykę bezpieczeństwa przedsiębiorstwa, jego zobowiązania wobec klientów i wewnętrzne ograniczenia dotyczące danych.

Z drugiej strony również hasło „narzędzie zatwierdzone przez IT" wymaga odpowiedniego rozumienia. Zatwierdzenie niekoniecznie oznacza pozwolenie na przetwarzanie każdego rodzaju informacji w każdej sytuacji. Firma może dopuszczać automatyczne notatki podczas rutynowych spotkań, ale ograniczać nagrywanie rozmów o wynagrodzeniach, negocjacjach handlowych czy niepublicznych planach strategicznych. Decydujące znaczenie mają rzeczywisty zakres akceptacji, konfiguracja narzędzia oraz klasyfikacja informacji. Innymi słowy, przepustka do biura nie upoważnia jeszcze do otwierania wszystkich sejfów.

Pomocne jest stworzenie prostego, aktualizowanego wykazu dopuszczonych rozwiązań. Nie musi przypominać encyklopedii podzielonej na siedem tomów. Powinien jednak wskazywać nazwę usługi, odpowiedzialny zespół, zatwierdzone zastosowania, istotne ograniczenia i miejsce, w którym użytkownik może sprawdzić aktualne zasady. Dla pracownika informacja „możesz używać tego narzędzia do podsumowania wewnętrznego statusu, ale nie wprowadzaj do niego danych spoza zatwierdzonego zakresu" jest znacznie bardziej przydatna niż dwudziestostronicowy dokument zaczynający się od definicji systemu teleinformatycznego.

Sam wykaz nie zastępuje oceny bezpieczeństwa ani zgodności z przepisami. Tę pracę muszą wykonać osoby mające odpowiednie kompetencje i dostęp do szczegółów technicznych oraz umownych. Może natomiast przełożyć wynik ich ustaleń na codzienne decyzje. Inaczej powstaje osobliwa sytuacja: dział bezpieczeństwa uważa, że wszystko zostało opisane, pracownicy nie rozumieją dokumentacji, a asystenci AI korzystają z wolności większej niż większość członków zarządu.

Kto odpowiada za gościa przyprowadzonego przez klienta?

W firmowych spotkaniach sytuacja zwykle jest prostsza, ponieważ organizacja może określić własne zasady. Komplikacje zaczynają się wtedy, gdy do rozmowy dołączają kontrahenci, partnerzy lub dostawcy. Każda ze stron może używać innych platform, mieć odmienne ograniczenia i uważać własne rozwiązanie za całkowicie standardowe. Jeżeli klient mówi „u nas nagrywamy wszystkie spotkania", nie oznacza to automatycznie, że

druga strona musi zaakceptować każdy sposób dokumentowania rozmowy.

Załóżmy, że rozpoczynają się negocjacje dotyczące warunków współpracy. Po stronie kontrahenta pojawia się automatyczny asystent. Prowadzący może powiedzieć: „Zanim zaczniemy omawiać warunki handlowe, ustalmy, czy spotkanie będzie nagrywane lub transkrybowane i gdzie trafią materiały. Musimy działać zgodnie z zasadami obu organizacji". Jest to komunikat rzeczowy, niewymagający oskarżeń ani teatralnego wyłączania kamery. Jeżeli warunków nie da się ustalić od razu, można odroczyć omawianie wrażliwych szczegółów do momentu wyjaśnienia sprawy. Warto pamiętać, że samo wyproszenie widocznego bota nie potwierdza jeszcze, iż żadna inna funkcja nie przetwarza rozmowy.

Podobna odpowiedzialność pojawia się po stronie gospodarza spotkania. Organizator nie musi osobiście konfigurować wszystkich systemów, ale powinien znać przyjęte reguły i sposób uzyskania pomocy. Jeśli firmowa polityka wskazuje, kto może uruchomić transkrypcję, dobrze, aby ta informacja była dostępna przed rozpoczęciem rozmowy. Jeżeli potrzebna jest wcześniejsza ocena lub odpowiednie poinformowanie uczestników, warto zadbać o to na etapie planowania. Improwizowanie zasad w chwili, gdy ktoś właśnie zaczyna przedstawiać poufne wyniki, przypomina montowanie pasów bezpieczeństwa podczas hamowania awaryjnego. Teoretycznie można próbować, ale moment jest wyjątkowo niekorzystny.

Nie należy również traktować pytania o nagrywanie jako bezwarunkowego referendum, w którym jedno „tak" rozwiązuje całą sprawę. Obowiązki prawne dotyczące przetwarzania danych osobowych mogą zależeć od celu,

podstawy prawnej, relacji między stronami i wielu innych okoliczności. Zgoda w rozumieniu przepisów ma własne wymagania i nie zawsze jest właściwą podstawą działania. W relacjach pracowniczych pojawiają się dodatkowe kwestie związane z zależnością służbową. Dlatego praktyczne zasady uczestnictwa w spotkaniu powinny wynikać z odpowiednio ocenionego procesu, a nie wyłącznie z odruchowego pytania „czy wszystkim pasuje?".

Jak odzyskać kontrolę bez otwierania wydziału śledczego

Dobrym początkiem jest przyjrzenie się jednemu rzeczywistemu, powtarzalnemu spotkaniu w swojej organizacji. Sprawdź, jakie narzędzia mogą w nim uczestniczyć, skąd są uruchamiane i jakie ustawienia obowiązują. Ustal, kto zatwierdził dane rozwiązanie, kto odpowiada za jego konfigurację i gdzie znajdują się instrukcje dla użytkowników. Jeżeli nie da się znaleźć tych informacji, problem nie musi tkwić w samym asystencie. Być może organizacja wprowadziła technologię szybciej, niż przygotowała zasady jej użytkowania. Zdarza się to nawet bardzo dobrze zarządzanym firmom, szczególnie gdy nowe funkcje pojawiają się w usługach, które pracownicy wykorzystują od lat.

Warto też odróżniać wiedzę użytkownika od wiedzy administratora. Zwykły pracownik może zobaczyć informację o aktywnym nagrywaniu i sprawdzić, gdzie udostępniono podsumowanie. Nie zawsze zobaczy ustawienia retencji, szczegółową konfigurację integracji czy warunki umowne dostawcy. Nie powinien więc udawać, że potwierdził coś, czego nie jest w stanie zweryfikować. Znacznie rozsądniej zgłosić konkretną lukę osobie odpowiedzialnej. „Nie wiem, czy podsumowania są dostępne poza zespołem" jest pytaniem, na które można

znaleźć odpowiedź. „Czy nasze AI jest w stu procentach bezpieczne?" brzmi poważniej, ale niewiele pomaga.

Na koniec pozostaje jeszcze element, o którym łatwo zapomnieć: komfort uczestników. Świadomość, że każda wypowiedź może zostać zapisana i wykorzystana poza pierwotnym kontekstem, potrafi zmienić sposób prowadzenia rozmowy. Ludzie mogą ostrożniej formułować pomysły, rzadziej zgłaszać wątpliwości albo unikać szczerej dyskusji nad niedopracowanymi propozycjami. Nie oznacza to, że należy rezygnować z automatycznej dokumentacji. Oznacza, że decyzja o jej zastosowaniu powinna uwzględniać nie tylko wygodę organizatora, lecz również charakter spotkania i uzasadnione oczekiwania uczestników.

Pierwszym krokiem do rozsądnego korzystania ze sztucznej inteligencji nie jest zatem zakup kolejnej aplikacji ani napisanie kolejnego regulaminu. Jest nim zdobycie elementarnej wiedzy o narzędziach, które już działają. Kto je uruchamia, co mogą przetwarzać, w jakim celu i kto za nie odpowiada. Dopiero wtedy można podejmować decyzje zamiast zgadywać. Bo największym problemem nie jest to, że AI pojawia się na spotkaniu. Największym problemem jest sytuacja, w której nikt nie wie, co właściwie robi, a wszyscy zgodnie uznają, że skoro nie prosi o podwyżkę, to zapewne nie ma powodów do niepokoju.

Rozdział 2 - Nagranie, transkrypcja i notatka nie są tym samym

Sześć tygodni po spotkaniu projektowym ktoś otwiera automatyczne podsumowanie i znajduje zdanie: „Dział zakupów zaakceptował nowe warunki cenowe". Problem polega na tym, że dział zakupów niczego jeszcze nie zaakceptował. Podczas rozmowy padło jedynie: „Jeżeli dostawca zmieni termin płatności, możemy rozważyć te warunki". Dla człowieka różnica jest dość oczywista. Dla systemu przygotowującego zwięzłe podsumowanie najwyraźniej stanowiła zbędny szczegół. Dokument został już przekazany do kilku osób, ktoś wpisał nowe ceny do planu, a kierownik próbuje teraz ustalić, dlaczego firma realizuje decyzję, której nikt formalnie nie podjął. Witamy w świecie, w którym automatyczne notatki potrafią zdobyć większy autorytet niż uczestnicy spotkania.

Problem nie polega wyłącznie na tym, że sztuczna inteligencja może popełnić błąd. Ludzie również zapisują nieprawidłowe informacje, pomijają kontekst i mylą nazwiska. Różnica polega na skali i sposobie rozpowszechniania rezultatów. Elegancko sformatowane podsumowanie, wyposażone w nagłówki, zadania i przypisanych właścicieli, wygląda na dokument przygotowany z dużą starannością. Łatwo zapomnieć, że jego treść może powstać automatycznie, bez rzeczywistego potwierdzenia ustaleń. Im bardziej profesjonalny wygląd, tym większa pokusa, aby przestać sprawdzać szczegóły. Tymczasem AI potrafi nadać niepewnej informacji ton oficjalnego komunikatu z taką łatwością, jakby od początku pracowało w dziale komunikacji korporacyjnej.

Zanim jednak zajmiemy się jakością takich dokumentów, trzeba uporządkować podstawowe pojęcia. Nagranie, transkrypcja, automatyczne napisy i podsumowanie to różne formy przetwarzania informacji. Mogą powstawać razem, ale nie muszą. Mogą być przechowywane w tym samym systemie albo w różnych miejscach. Mogą mieć odmienne ustawienia dostępu i okresy przechowywania. Jeśli organizacja traktuje wszystkie te elementy jako jedną funkcję o nazwie „AI robi notatki", prędzej czy później odkryje, że jej zasady pozostawiają więcej luk niż kalendarz dyrektora w ostatni piątek przed urlopem.

Cztery rezultaty jednej rozmowy

Nagranie jest zapisem określonych elementów przebiegu spotkania, najczęściej dźwięku, obrazu lub obu tych elementów, zależnie od wybranej funkcji. Może zachowywać głosy rozmówców, sposób wypowiedzi, pauzy, ton, a w przypadku obrazu również gesty i to, co było widoczne na ekranie. Stanowi bogate źródło informacji, lecz właśnie dlatego może zawierać znacznie więcej, niż rzeczywiście potrzeba do udokumentowania ustaleń. Ktoś może przypadkowo udostępnić niewłaściwe okno. Na ekranie mogą pojawić się dane klienta, wewnętrzna wiadomość albo fragment dokumentu niezwiązany z rozmową. Nagranie nie odróżnia automatycznie informacji potrzebnych od tych, które znalazły się w kadrze przypadkiem.

Transkrypcja jest tekstowym odwzorowaniem wypowiedzi. Może umożliwiać szybkie wyszukiwanie konkretnych sformułowań i odnajdywanie fragmentów rozmowy bez ponownego odsłuchiwania całego materiału. Nie jest jednak idealnym stenogramem. Rozpoznawanie mowy bywa zawodne przy kilku mówiących jednocześnie

osobach, specjalistycznym słownictwie, słabym połączeniu lub nazwach własnych. System może nieprawidłowo przypisać wypowiedź uczestnikowi albo zgubić krótkie słowo zmieniające sens zdania. W negocjacjach różnica między „możemy zaakceptować" a „nie możemy zaakceptować" bywa warta więcej niż roczna subskrypcja całego pakietu narzędzi.

Automatyczne napisy mogą wyglądać podobnie do transkrypcji, ale nie należy zakładać, że zawsze powstaje z nich trwały dokument. W niektórych rozwiązaniach służą przede wszystkim bieżącemu wyświetlaniu wypowiedzi. W innych mogą być powiązane z funkcją zachowywania tekstu. Trzeba sprawdzić konkretne ustawienia i sposób działania platformy. Jest to również ważne z perspektywy dostępności. Dla części uczestników napisy stanowią istotne ułatwienie komunikacji, dlatego mechaniczny zakaz wszystkich funkcji przetwarzających mowę może przynieść niezamierzone konsekwencje. Dobrze zaprojektowane zasady powinny uwzględniać takie potrzeby bez automatycznego uznawania każdej funkcji za nieszkodliwą.

Podsumowanie AI to jeszcze inna kategoria. Nie jest po prostu krótszą transkrypcją. System wybiera informacje, nadaje im strukturę i formułuje wnioski na podstawie przetworzonego materiału. Może wyróżniać decyzje, zadania, terminy i kwestie wymagające dalszych działań. W praktyce wykonuje więc operację interpretacji, nawet jeśli użytkownik oczekuje tylko uporządkowanych notatek. Im więcej swobody ma w tworzeniu dokumentu, tym istotniejsze staje się jego sprawdzenie. Uczestnik, który powiedział „może warto zbadać ten wariant", niekoniecznie chciał zostać właścicielem zadania „Wdrożyć wariant do końca miesiąca".

Dlaczego krótszy dokument nie zawsze oznacza mniejsze ryzyko

Na pierwszy rzut oka podsumowanie wydaje się bezpieczniejsze niż pełne nagranie. Zawiera mniej szczegółów, zajmuje mniej miejsca i zwykle pomija nieistotne dygresje. Czasami rzeczywiście może lepiej realizować zasadę ograniczania zakresu przechowywanych informacji. Nie należy jednak automatycznie przyjmować, że krótsza forma oznacza brak problemów. Kilkuzdaniowa notatka potrafi zawierać najbardziej poufny element całego spotkania: plan przejęcia firmy, wysokość proponowanego wynagrodzenia albo informację o przyszłej zmianie strategii handlowej. O znaczeniu danych nie decyduje ich objętość. Hasło do systemu również jest krótkie, a jednak nikt rozsądny nie traktuje go jak nieszkodliwego haiku.

Dobrym przykładem jest spotkanie dotyczące oceny potencjalnego dostawcy. Przez czterdzieści minut uczestnicy omawiają terminy, jakość obsługi, możliwości techniczne i historię współpracy. Na koniec ktoś wspomina, że jeden z kandydatów może wkrótce stracić ważnego klienta, ale informacja nie została potwierdzona. Automatyczne podsumowanie może wyróżnić właśnie tę uwagę jako istotny czynnik ryzyka. Jeśli dokument zostanie szeroko udostępniony, niezweryfikowana sugestia zacznie funkcjonować jako element oficjalnej oceny. Problem dotyczy jednocześnie poufności, dokładności informacji i sposobu podejmowania decyzji.

To pokazuje, dlaczego należy oddzielić pytanie „co zostało zarejestrowane?" od pytania „co z tego powstało?". Pierwsze dotyczy zakresu zbieranych informacji. Drugie dotyczy rezultatu ich przetwarzania oraz jego późniejszego wykorzystania. Można ograniczyć nagrywanie, a mimo to