



## Kundenbeziehungen

# Den Einsatz von *Chatbots* für das Bankwesen

Par Alexandre Jotterand le 22 Oktober 2024

Die jüngsten Fortschritte in der generativen künstlichen Intelligenz (KI) haben das Interesse der Finanzakteure an Konversationsrobotern oder *Chatbots* für das Management von Kundenbeziehungen neu entfacht. Laut einem 2023 veröffentlichten [Bericht](#) des US-amerikanischen *Consumer Financial Protection Bureau* (CFPB) interagierten 2022 rund 37 % der Amerikaner mit einem *Bank-Chatbot*, und alle großen US-Banken setzen sie ein.

Ihr Einsatz wirft jedoch viele Fragen auf. Einige davon sind nicht neu, insbesondere in Bezug auf den Umgang mit Daten und Subunternehmern ; andere sind eher spezifisch für die eingesetzte Technologie : automatisierte Entscheidungen, Fehler- und Diskriminierungsrisiken etc. Wir konzentrieren uns in diesem Beitrag auf die zweite Kategorie von Fragen und insbesondere auf die Aspekte, die die Kontrolle der *Chatbot-Antworten* und die Konsequenzen im Falle von Fehlern betreffen.

## Unterschiede zwischen deterministischen und statistischen Systemen

Es ist heute allgemein bekannt, dass KI-Systeme Fehler machen und halluzinieren können. Es ist jedoch nicht überflüssig, daran zu erinnern, dass dies nicht immer der Fall war : Frühere Generationen von *Chatbots* basierten auf Wissensdatenbanken, die von Experten generiert wurden (deterministische algorithmische Systeme). Diese deterministischen Systeme liefern vorhersehbare, aber manchmal wenig hilfreiche Antworten.

Die neuen Generationen von *Chatbots* verwenden generative KI-Modelle, die auf *Large Language Models* (LLM) basieren. Diese Systeme können aufgrund ihrer statistischen Natur unberechenbar sein und sachlich falsche oder verzerrte Antworten liefern, was für die Banken, die sie einsetzen, ein Risiko darstellt. Im Übrigen äußert sich das CFPB *in* seinem oben erwähnten Bericht sehr kritisch über ihren Einsatz und kommt zu dem Schluss, dass „*the use of conversational chatbots trained on LLMs in banking [is] an unreliable source for responding to customers*“.

## Vertragliche Aspekte

Dieses Merkmal wirft die Frage nach den vertraglichen Risiken auf, wenn unrichtige Informationen bereitgestellt werden, die zu finanziellen Schäden führen. In der Rechtssache [Moffatt v. Air Canada](#), 2024 BCCRT 149, urteilte ein kanadisches Gericht zum ersten Mal, dass ein Unternehmen für die von seinem *Chatbot* bereitgestellten Informationen haftet, und zwar auf

die gleiche Weise wie für alle „statischen“ Informationen auf seiner Website. Das Gericht stellte im Übrigen fest, dass das Unternehmen nicht die vernünftigerweise erforderlichen Maßnahmen ergriffen hatte, um sicherzustellen, dass sein *Chatbot* korrekte Informationen lieferte.

Übertragen auf den Bankensektor in der Schweiz würde dieser Fall unserer Meinung nach die Frage nach Haftungsausschlüssen aufwerfen, die in den Allgemeinen Geschäftsbedingungen des Dienstes festgelegt werden müssten. Solche Ausschlüsse wären nur in dem Maße gültig, wie es das Gesetz zulässt, insbesondere [Art. 100 OR](#) oder die Regeln über den unlauteren Wettbewerb (insbesondere die Regeln über ungewöhnliche Klauseln). Der Handlungsspielraum der Banken wird eingeschränkt, da die in Art. 100 Abs. 2 OR für lizenzierte Industrien vorgesehenen Beschränkungen grundsätzlich auch für sie gelten werden. So könnte ein Richter eine Klausel für nichtig halten, die leichtes Verschulden der Bank ausschließt. Nach [Art. 101 Abs. 3 OR](#) kann die Bank jedoch das leichte Verschulden ihrer Hilfsperson ausschließen. Es wird sich dann die Frage stellen, ob die am Prozess der Bereitstellung des *Chatbots* beteiligten Drittanbieter Erfüllungsgehilfen sind oder nicht. Angesichts der potenziellen Anzahl der neben der Bank beteiligten Akteure (Anbieter des LLM, der Datenbanken oder des KI-Systems, Entwickler, Integrator oder Betreiber usw.) und der Komplexität der Beziehungen wird diese Frage eine konkrete Analyse der Rollen und Verantwortlichkeiten jedes Einzelnen erfordern.

## Regulatorische Aspekte und Empfehlung

Die FINMA hat keine spezifische Stellungnahme zu *Chatbots* abgegeben. In ihrem „[Risikomonitoring 2023](#)“ nahm sie eine pragmatische und offene Haltung gegenüber dem Einsatz von KI ein. Wie die Prozesse, die sie ersetzen, müssen auch KI-Systeme allen anwendbaren Gesetzen sowie den bestehenden FINMA-Rundschreiben entsprechen. Die FINMA identifiziert jedoch vier Bereiche, auf die speziell bei KI geachtet werden muss: „Governance und Rechenschaftspflicht“, „Robustheit und Zuverlässigkeit“, „Transparenz und Erklärbarkeit“ sowie „Gleichbehandlung“.

Die FINMA erklärt nicht, wie diese vier Bereiche konkret angegangen werden sollen. Glücklicherweise gibt es zahlreiche *Frameworks* zur Etablierung eines vertrauenswürdigen KI-Managements (*trustworthy AI*), wie die „[AI Principles](#)“, der OECD oder das „[AI Risk Management Framework](#)“ des NIST.

Generell sollte der Einsatz von KI in eine multidisziplinäre Governance eingebettet sein und einer klaren Strategie folgen, um sicherzustellen, dass die geplante technologische Lösung sowohl notwendig als auch geeignet ist, um den ermittelten Bedarf zu decken. Robustheit und Erklärbarkeit werden dann besonders kritisch für LLM-basierte *Chatbots* sein. Es gibt verschiedene technische Maßnahmen zur Verbesserung dieser Aspekte – z. B. in Bezug auf die Wahl des Modells und der Trainingsalgorithmen, die Techniken der RAG (*Retrieval Augmented Generation*) und des *Fine Tuning* sowie Tests und Validierungen -, die während des gesamten Lebenszyklus des KI-Systems umgesetzt werden müssen. Wir betonen hier die *Überwachung* des Systems während des Einsatzes, die unserer Meinung nach ein wichtiges Element bei der Beurteilung der Einhaltung gesetzlicher Vorschriften und der Haftung (insbesondere unter dem Gesichtspunkt des Verschuldens) darstellen wird.

Schließlich muss sichergestellt werden, dass die Nutzer angemessen über den Einsatz von KI und die Fähigkeiten und Grenzen von *Chatbots* informiert werden und dass die Nutzungsbedingungen für die Dienste entsprechend gestaltet werden.

---

Reproduction autorisée avec la référence suivante: Alexandre Jotterand, Den Einsatz von *Chatbots* für das Bankwesen, publié le 22 Oktober 2024 par le Centre de droit bancaire et financier, <https://cdbf.ch/de/1377/>