Samstag, 04. Oktober 2025, 13:00 Uhr
~7 Minuten Lesezeit

Die Big-Brother-Banker

KI-gestützte Überwachungssysteme der Geldinstitute stellen Kunden unter Generalverdacht — für manche von ihnen kann das schwerwiegende Folgen haben.

von Michael Brückner
Foto: TPCX/Shutterstock.com

Offiziell geht es um hehre Ziele: die Bekämpfung von Geldwäsche, Steuerhinterziehung, Terrorfinanzierung

und anderen Formen der Finanzkriminalität. Doch die künstliche Intelligenz hat die Compliance der Banken — also sozusagen die interne „Polizei“ der Geldinstitute — mit Überwachungs- und Kontrollsystemen ausgestattet, die dystopisch anmuten. Betroffen davon sind auch viele unbescholtene Menschen, die unversehens in Generalverdacht geraten. Wenn die Algorithmen es so wollen, werden Bankkunden unter verschärfte Kontrolle gestellt, oder aber man kündigt ihnen gleich das Konto. Wer lückenlos die Finanzdaten eines Menschen kontrolliert, kontrolliert dessen Leben. „Nichts zu verbergen“ zu haben, stellt keinen Schutzschild gegen einen übergriffigen Staat und Banken dar, die nicht selten in vorauseilendem Gehorsam agieren.

Wie sich George Orwell den totalitären Überwachungsstaat vorstellte, beschrieb er in seinem Roman „1984“: Alle Menschen sind im Visier von „Big Brother“, Wahrheit und Privatsphäre sind ausgelöscht, es herrscht totale Sprach- und Gedankenkontrolle, und die Menschen werden unter anderem mithilfe des „Doppeldenk“ manipuliert.

Weniger bekannt als der Brite George Orwell ist der Franzose Michel Foucault. Der 1984 verstorbene Philosoph veröffentlichte in seinem Buch „Überwachen und Strafen“ einen Kontrollmechanismus, der wesentlich subtiler ist und effizienter zu funktionieren scheint als das fiktive Überwachungssystem in Orwells Roman. Foucault nannte es das „Prinzip der panoptischen Macht“. Er nahm damit Bezug auf das von Jeremy Bentham, einem britischen Juristen und Philosophen, entwickelte Konzept des

Panoptikums. Es besteht aus einem im Rundbau angelegten Gefängnis mit einem zentralen Wachturm. Die Aufseher können daraus stichprobenartig die Gefangenen kontrollieren, ohne dass diese es bemerken. Aus Angst, die Wärter blickten gerade in ihre Zelle, verhalten sich alle vorbildlich. Kurzum: Die ständige Möglichkeit der Beobachtung führt zu einer Selbstdisziplinierung der Individuen.

Digitales Panoptikum

> ***Die Methoden, mit denen Banken und andere Finanzdienstleister ihre Kunden überwachen — oder besser: auf staatlichen Druck überwachen müssen —, gleichen tatsächlich einem Mix aus dem „Big Brother"-Konzept von Überwachung und dem digitalen Panoptikum zur Selbstdisziplinierung. In letzterem Fall treten Algorithmen an die Stelle der diskret beobachtenden Wärter.***

Die Überwachung von Bankkunden, seien es nun Privat- oder Geschäftskunden, vollzieht sich weitgehend durch den Einsatz von Anti-Financial-Crime-Technologien nach dem Blackbox-Prinzip. Das heißt, der Kunde wird größtenteils von künstlicher Intelligenz (KI) durchleuchtet, ohne dass er davon weiß oder etwas bemerkt. Dass er ins Visier der Überwachungssoftware geraten ist, ahnt der Kunde in der Regel erst, wenn er schlechtere Konditionen erhält, ihm bestimmte Finanzprodukte nicht mehr zugänglich sind oder sogar seine Konten gekündigt werden. Er „ahnt" es nur, denn das Geldinstitut muss keine Gründe nennen. Auch in der Geschäftsbeziehung zwischen Banken und Kunden besteht Vertragsfreiheit. Sprich: Das Institut kann entscheiden, mit wem es zusammenarbeiten will und mit wem nicht.

Was läuft also hinter den Kulissen ab, mit welchen Kontrollsystemen

arbeiten die Anti-Financial-Crime-Technologien? Vorgeblich geht es immer um hehre Ziele, im konkreten Fall also um die Verhinderung von Finanzcrashs und darum, Finanzkriminellen wie Geldwäschern und Steuerhinterziehern das Handwerk zu legen. Ganz gleich, ob Bargeldrestriktionen umgesetzt werden, der digitale Euro mit allen damit verbundenen Kontroll- und Steuerungsmöglichkeiten konkrete Formen annimmt oder mit der Antigeldwäschebehörde AMLA ein neues EU-Bürokratiemonster entsteht, das eigentlich niemand braucht — in all diesen Fällen werden die vermeintlichen Vorteile in den Vordergrund gestellt. Noch mehr Kontrolle, noch mehr Schnüffeleien in den Bankkonten? Viele Betroffene agieren mit erstaunlicher Arglosigkeit: „Sollen die doch gucken, ich habe nichts zu verbergen“, so lautet das Standardargument.

> ***Dabei geht es nicht darum, ob jemand etwas zu verbergen hat. Es geht um nicht mehr und nicht weniger als um die Privatsphäre der Menschen. Und gerade die finanzielle Privatsphäre gilt es zu schützen.***

Denn wer über die Finanzdaten eines Menschen verfügt, hat gleichsam ein Röntgenbild des Betreffenden vor Augen: Ist er oder sie verheiratet, haben sie Kinder, was verdienen sie, wie hoch sind die Konsumausgaben, wie hoch ist ihre Steuerlast, wie steht es um ihre Bonität, sind sie Mitglied einer Partei oder einer anderen Institution, für welche Organisationen spenden sie, welche Medien haben sie abonniert, mussten sie in der Vergangenheit Geldstrafen entrichten? Über diese und viele andere Fragen gibt das Girokonto als finanzielle Drehscheibe Auskunft. Wer die Finanzen eines Menschen lückenlos kontrolliert, kontrolliert auch dessen Leben.

Von der Nischensoftware zum Überwachungsinstrument

Diese Daten lieferten schon in der Vergangenheit den Banken wichtige Informationen für ihr Cross-Selling-Geschäft. Sie konnten also zum Beispiel herausfiltern, wer noch Miete zahlt, und dem Betreffenden dann eine Baufinanzierung anbieten. Inzwischen geht es aber um sehr viel mehr. Nach der Finanzkrise 2008 entwickelten sich die Anti-Financial-Crime-Technologien von einer Nischensoftware zu einem zentralen Bestandteil des globalen Bankensystems.

Anti-Financial-Crime-Technologien stehen für alle Systeme und Tools, mit deren Hilfe Banken Finanzkriminalität erkennen, verhindern und bekämpfen können. Also zum Beispiel Geldwäsche, Betrug, Terrorismusfinanzierung und Insiderhandel. Die KI wird dabei eingesetzt, um Muster zu identifizieren, die einem Banker vermutlich nie auffallen würden. Eigentlich doch eine gute Sache, sollte man meinen. Auf den ersten Blick vielleicht. Auf den zweiten Blick indessen erkennt man die Gefahr von erheblichen Kollateralschäden, welche die erwähnte finanzielle Privatsphäre immer löchriger werden lassen. Die Anti-Financial-Crime-Technologien machen es möglich, größere Datenmengen in Bezug auf suspekte Geldwäsche-Transaktionen zu untersuchen. Dabei verarbeiten die KI-Systeme jedoch auch personenbezogene Daten von unbescholtenen Bürgern. Jede Art von Kundentransaktionsdaten wird dadurch gläsern gemacht und von KI-Systemen in Echtzeit durchleuchtet.

Besonders problematisch erscheint das sogenannte Customer Risk Rating (CRR, Kundenrisikorating), ein integraler Bestandteil der Anti-Financial-Crime-Technologien. Hier könnte eine Art von algorithmischer Sozialkontrolle drohen. Vor allem dann, wenn die gewonnenen Daten nicht nur zur Bonitäts- und Risikoeinschätzung der betreffenden Kunden genutzt werden, sondern auch zur Beurteilung ihres „politisch korrekten“ Verhaltens. Nachhaltige Kreditmodelle und entsprechende Formen der Geldanlage sind längst üblich. „Gute“ Menschen werden mit günstigen Konditionen

belohnt, „schlechte“ Kunden sanktioniert — nicht durch Gesetze, sondern durch finanzielle Mechanismen.

Intransparente Risikokategorien

Das Customer Risk Rating teilt die Bankkunden in drei Kategorien ein: geringes Risiko (Low Risk), mittleres Risiko (Medium Risk) und hohes Risiko (High Risk). Schon gelegentliche Auslandsüberweisungen können negativ bewertet werden und zum Beispiel dazu führen, dass der Kunde in die Kategorie „mittleres Risiko“ eingeordnet wird, was eine verstärkte Beobachtung durch die Bank zur Folge hat. Auch häufige Bargeldtransaktionen, negative Presseberichte und die Zusammenarbeit mit Firmen in einem Risikoland, das sich zum Beispiel nicht an Sanktionen beteiligt, können negative Konsequenzen für die betreffende Person oder das Unternehmen haben. Ein als „hochriskant“ eingestufter Firmenkunde dürfte erhebliche Probleme haben, bei einem anderen Geldinstitut ein Konto zu eröffnen oder aber einen Kredit zu bekommen. Die Konsequenzen können mithin existenzbedrohend sein.

> ***Die Bewertungskriterien für die automatisierte Risikoeinstufung sind für die Kunden insgesamt wenig transparent. Das hat zur Folge, dass es schwierig ist, eine als ungerecht empfundene Einstufung anzufechten.***

Die Banken sind nicht zimperlich, wenn es gilt, Restriktionen gegen ihre Kunden durchzusetzen. Da werden Konten eingefroren oder aufgelöst, weil die Banker einen Verdacht und Angst vor hohen Bußgeldern haben. Meist führen die Geldinstitute dann angebliche Reputationsrisiken ins Feld. Das sogenannte Debanking (Sperren oder Kündigen von Bankkonten durch die Bank) gehört nicht zum klassischen Bankgeschäft, sondern wird mehr und mehr zum

Instrument der Ausgrenzung.

Staatsbank als Kontenkiller

Wie massiver Druck auf die Bürger ausgeübt werden kann, zeigt das Beispiel Vietnam, wo im Spätsommer 2025 sage und schreibe 86 Millionen Bankkonten gelöscht wurden. Die Staatsbank von Vietnam (SBV) bezeichnete dies als Teil des Regierungsplans zur „digitalen Transformation“. Künftig müssen alle Bankkonten, geschäftlich wie privat, biometrisch verifiziert werden. Diese Maßnahme dient wohl auch der Einführung der vietnamesischen Zentralbankwährung (Central Bank Digital Currency, kurz CBDC).

So etwas wäre in Europa unvorstellbar, mag da mancher denken. Doch Vorsicht: Ferne Länder mit einer überschaubaren Wirtschaftsstärke waren gerade auch für die Einführung von CBDCs regelrechte „Versuchslabore“, Jamaika etwa oder Nigeria. Wobei in Nigeria der sogenannte eNaira krachend gescheitert ist.

Wie lassen sich in einem von zunehmender Kontrolle und Überwachung geprägten wirtschaftlichen und gesellschaftlichen Umfeld die so wichtige finanzielle Privatsphäre und die Selbstbestimmung wahren? Wie bei der Kapitalanlage lautet auch bei der Sicherung des Zahlungsverkehrs und bei der Erhaltung einer größtmöglichen finanziellen Privatsphäre die Lösung „Diversifikation“. Konkret bedeutet dies, nach Möglichkeit zwei Konten in unterschiedlichen Banksystemen zu unterhalten, also nicht etwa Haupt- und Zweitkonto bei verschiedenen Sparkassen, sondern zum Beispiel eines bei einer Sparkasse und das andere bei einer Genossenschaftsbank oder einer Direktbank. Dadurch entstehen zwar zusätzliche Kosten, wenn aber eines der Konten gesperrt wird, kann das — finanzielle — Leben über die Zweitbankverbindung weiterlaufen.

Klumpenrisiken vermeiden

Alle elektronischen Zahlungsmittel, wie etwa Kreditkarten, Debitkarten und Zahlungs-Apps, hinterlassen Spuren.

> ***Bargeldzahlungen sind zwar wegen der Möglichkeiten des Bargeld-Trackings auch nicht zu 100 Prozent anonym, die Bezahlprozesse laufen dennoch sehr viel diskreter ab als beim Einsatz von Karten oder Smartphones.***

Kryptos, also etwa Bitcoin, Ethereum oder Stablecoins, können alternative Zahlungswege öffnen. Kryptowährungen erlauben Transaktionen außerhalb der klassischen Banksysteme. Empfehlenswert ist ein Mix unterschiedlicher Zahlungsarten. Also nicht nur auf Kartenzahlungen, Bargeld oder Kryptos setzen. Sonst entsteht nämlich genau das, was Risk-Manager als „Klumpenrisiken“ bezeichnen. Und die machen „Big Brother“ das Leben leichter.

Michael Brückner, Jahrgang 1958, war nach seinem Volontariat bei der Mainzer Allgemeinen Zeitung dort acht Jahre Redakteur. Danach übernahm er die Chefredaktion des in Stuttgart erscheinenden Wirtschaftsmagazins Europa und anschließend des Immobilien-Fachmagazins Monumente. Brückner machte sich 1995 selbstständig, schrieb mehrere Dutzend Sachbücher zu den Themen Europa, Wirtschaft und Finanzen und war als Freiberufler Ghostwriter und Redenschreiber für die Vorstände einer der größten deutschen Banken und einer führenden Sparkasse. Er lebt und arbeitet in Mainz und in Lindau/Bodensee.