Wenn die KI zum verdeckten Ermittler wird

Drei Professoren der Universität Bayreuth erforschen, was täuschend echte KI-Fälschungen bewirken können. Ermittler haben dadurch einst ungeahnte Möglichkeiten – Kriminelle ebenso.

Von Johannes Pittroff

BAYREUTH. Inwiefern kann und darf der Staat Künstliche Intelligenz (KI) bei der Verbrechensbekämpfung einsetzen? Und was ist technisch möglich – sowohl für Ermittler als auch für Kriminelle? Das sind zwei zentrale Fragen des Forschungsprojekts „For The Greater Good? Deepfakes in der Strafverfolgung", an dem Wissenschaftler der Universität Bayreuth seit dem Frühjahr arbeiten.

Es geht um Deepfakes – also von der KI erzeugte, täuschend echt wirkende Fälschungen. So können Verbrecher mithilfe von Deepfakes beispielsweise Stimmen imitieren und damit Opfer in ihre Falle locken – etwa bei einem Schock-Anruf. Aber auch Ermittler könnten die Technik nutzen, um etwa kriminelle Netzwerke zu infiltrieren.

Professor Christian Rückert (links) und Professor Niklas Kühl arbeiten an der Universität Bayreuth an dem Forschungsprojekt „For The Greater Good?", kurz: „FoGG". Foto: Johannes Pittroff

Identitätsdiebstahl leichter möglich

Die Forscher gehen das Thema an der Universität Bayreuth aus drei Richtungen an: aus der juristischen, der technischen und der philosophischen. Es soll dabei nicht um abstrakte Forschung gehen, sondern darum, Erkenntnisse für die Praxis zu gewinnen. Der Praxispartner des Projekts ist die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, die bei Computerkriminalitäts-Fällen ermittelt sowie Staatsanwaltschaften, Polizei und den Bund berät.

Die Ermittler hätten mit Deepfakes die Möglichkeit, „staatlichen Identitätsdiebstahl" zu begehen, sagt Professor Christian Rückert, Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und IT-Strafrecht. Beispielsweise könnten Ermittler sich in den Video-Chat einer kriminellen Bande einschleichen und sich dort mithilfe der KI als ein Bandenmitglied ausgeben. Indem sie die KI die Gesichtszüge und die Stimme eines tatsächlich existierenden Bandenmitglieds nachahmen lassen – die KI könnte das Gesicht des Nachgeahmten wie eine lebendige Maske über das Gesicht des Ermittlers legen. „Was verdeckte Ermittler schon immer getan haben, ist, das Gegenüber zu täuschen", sagt der Professor – wie es von Undercover-Agenten aus Kinofilmen bekannt sei. Neu sei die Frage, ob sie das Recht haben, die Identität eines anderen per KI nachzuahmen, sei dies doch ein Eingriff in das Persönlichkeitsrecht des Betroffenen.

Professor Rückert betrachtet die juristische Seite: Ist das Strafrecht dafür gewappnet, wenn Kriminelle mit KI arbeiten? Was erlaubt die Gesetzgebung den Behörden? Und wie müssen Gerichte angesichts von Deepfakes mit Beweisen umgehen? „Früher oder später werden Fälle kommen, bei denen Angeklagte sagen: ‚Das bin ich nicht'", sagt der Professor. Bisher hätten mediale Beweise – etwa Video- und Fotoaufnahmen – als relativ sicher gegolten. Nun könne es zumindest bei bestimmten Fällen fraglich werden. Aber nicht in allen: Wenn ein Angeklagter, von dem weder Foto- noch Videomaterial im Internet existiere, behaupte, jemand habe von ihm einen Deepfake erstellt, sei das eher unglaubwürdig.

Den juristischen Problemen müsse sich der Gesetzgeber stellen, sagt Rückert. Bis jetzt zeigt die Politik hier aus seiner Sicht zu wenig Initiative. Es seien aber nicht nur juristische, sondern auch ethische Fragen – es gehe nicht nur darum, was möglich sei, sondern auch darum, was möglich sein soll. Mit dem ethischen Bereich beschäftigt sich Professorin Lena Kästner, Inhaberin des Lehrstuhls für Philosophie, Informatik und Künstliche Intelligenz.

Was technisch möglich ist, will Professor Niklas Kühl, Inhaber des Lehrstuhls für Wirtschaftsinformatik und humanzentrische Künstliche Intelligenz, aufzeigen. Er wolle einen auf die Ermittler zugeschnittenen „Demonstrator" entwickeln, der den aktuellen Stand der KI-Technik zeige. Wobei dieser sich schnell weiterentwickle. Schon jetzt könne jemand, wenn er etwas Geld auszugeben bereit sei, ein Deepfake-Video einer Person erstellen lassen. Vorausgesetzt, dass von der Person, die imitiert werden soll, genügend Videomaterial im Internet zu finden ist. Stimmenimitation sei in Echtzeit noch schwieriger zu bewältigen, aber prinzipiell auch möglich.

Professor Kühl erklärt, wie schnell die Entwicklung vorangeht: Als das Forschungsprojekt im April begonnen habe, hätte jemand, der einen Echtzeit-Deepfake erstellen wollte, noch grundlegende Programmierkenntnisse haben müssen. Jetzt sei das schon nicht mehr nötig. Die Programme operierten auf „Open-Source"-Basis. Das heißt, dass eine Gemeinschaft an Programmierern und Nutzern sie entwickelt, häufig ohne Beteiligung von großen Softwarefirmen. Er könne sich vorstellen, dass es im nächsten Schritt eine App gebe, mit der der Nutzer ohne große Vorkenntnisse Deepfakes erstellen kann, sagt der Professor.

Bald erste Ergebnisse

Das Forschungsprojekt soll drei Jahre lang dauern, die Forscher wollen aber nicht so lange warten, bis sie erste Ergebnisse veröffentlichen. Rückert und Kühl rechnen damit, dass sie und Professorin Lena Kästner spätestens im kommenden Jahr die ersten Ergebnisse bekannt machen können – durch wissenschaftliche Artikel in Fachzeitschriften und Vorträge etwa.

Wichtig sei, sagen Rückert und Kühl, dass die Lösungen, die sie aufzeigen, auch in der Praxis anwendbar seien: Sie sollten juristisch durchführbar, ethisch vertretbar und technisch möglich sein – und das nicht nur auf Hochleistungscomputern. Am Projekt arbeiten zusammen mit den drei Professoren mehrere wissenschaftliche Mitarbeiter und studentische Hilfskräfte, zwei Staatsanwälte und ein IT-Forensiker. Das Interesse aus der Praxis an dieser Forschung, sagt Rückert, sei enorm.