Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Glaser, Severin

Künstliche Intelligenz im Strafrecht

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1/2024), 10-21.

doi: 10.7396/2024_1_B

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Glaser, Severin (2024). Künstliche Intelligenz im Strafrecht, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 10-21, Online: https://dx.doi.org/10.7396/2024_1_B.

Online publiziert: 5/2024

Künstliche Intelligenz im Strafrecht

SEVERIN GLASER,
Lehrstuhl für Finanz- und Wirtschaftsstrafrecht, Institut für Strafrecht, Strafprozessrecht und Kriminologie, Leopold-Franzens-Universität Innsbruck.

Künstliche Intelligenz stellt aus strafrechtlicher Sicht eine vielfältige Herausforderung dar: Neu eröffnete Verhaltensweisen, die wie der Hochfrequenzhandel früher gar nicht denkbar waren, fordern den Strafgesetzgeber; materiell-rechtliche Fragestellungen im Zusammenhang mit täterseitiger und opferseitiger Verwendung künstlicher Intelligenz führen nicht nur in grundsätzliche Probleme des allgemeinen Teils des Strafrechts (insbesondere bei autonom fahrenden Autos), sondern auch in zunehmende Unzulänglichkeiten von Delikten wie Betrug und Erpressung, die sich interpretativ nur über eine verstärkte Anwendung des betrügerischen Datenverarbeitungsmissbrauchs sowie eine diesen umfassende Auslegung des § 22 Abs 2 Finanzstrafgesetz (FinStrG) lösen lassen dürften. Strafprozessual ergeben sich theoretisch vielfältige Einsatzmöglichkeiten insbesondere für entscheidungsunterstützende künstliche Intelligenz, zB im Bereich der Zeugeneinvernahme. Für eine entscheidungstreffende künstliche Intelligenz besteht hingegen kaum Bedarf.

1. EINFÜHRUNG

Der vorliegende Beitrag ist an meinen gleichnamigen Vortrag bei der Salzburger Juristischen Gesellschaft angelehnt, den ich am 25.05.2023 in den Räumen der Universität Salzburg gehalten habe. Er denkt Fragestellungen an, die sich durch die rasant fortschreitenden Einsatzmöglichkeiten künstlicher Intelligenz im materiellen Strafrecht sowie im Strafprozessrecht stellen. Es kann angesichts der teils noch sehr schlecht abschätzbaren Lage und der andauernden technischen Entwicklung dabei kein Anspruch auf letztgültige Beantwortung der aufgeworfenen Fragen erhoben werden; der Beitrag soll jedoch zumindest eine Diskussion in Wissenschaft und Praxis anstoßen.

2. HAUPTTEIL

2.1 Was ist künstliche Intelligenz aus rechtlicher Sicht?

Das allgemeine Begriffsverständnis künstlicher Intelligenz ist – zumindest derzeit noch – eher unklar, was in starkem Ausmaß daran liegen mag, dass schon die genaue Bedeutung des Begriffs der Intelligenz Schwierigkeiten bereitet. Unter diesen Umständen ist der Versuch, eine brauchbare Legaldefinition für künstliche Intelligenz zu entwickeln, ein besonders herausforderndes und verdienstvolles Unterfangen. Wenngleich es bislang noch keine Legaldefinition für diesen Begriff gibt, ist die Europäische Kommission in ihrer Annäherung daran zumindest schon weit fortgeschritten. In ihrer Mitteilung „Künstliche Intelligenz für Europa“ aus dem Jahr

2018 definiert sie künstliche Intelligenz als „Systeme mit einem ‚intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen"[1], und unterscheidet des Weiteren rein softwaregestützte Anwendungen künstlicher Intelligenz in einer virtuellen Umgebung (wie etwa Sprachassistenten, Suchmaschinen oder Bildanalysesoftware) von künstlicher Intelligenz, die in Hardware eingebettet ist (zB moderne Roboter, autonom fahrende Autos, Drohnen oder das „Internet der Dinge"). Eine echte Legaldefinition wird es geben, wenn das derzeit im Verhandlungsprozess des europäischen Gesetzgebers stehende „Gesetz über Künstliche Intelligenz"[2] verabschiedet wird. Der Kommissionsvorschlag für diese Verordnung definiert in Art 3 Z 1 ein „System der künstlichen Intelligenz (KI-System)" als „eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren". Die in Anhang I des Verordnungs-Vorschlags (VO-Vorschlags) genannten „Techniken und Konzepte", auf die Art 3 Z 1 Bezug nimmt, umfassen zum ersten „Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning)", zum zweiten „Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme", sowie zum dritten statistische „Ansätze und Bayessche Schätz-, Such- und Optimierungsmethoden". Etwas kürzer, aber inhaltlich ähnlich liest sich die Definition des Systems künstlicher Intelligenz nach Art 3 Z 1 in der Fassung der allgemeinen Ausrichtung des Rates als „System, das so konzipiert ist, dass es mit Elementen der Autonomie arbeitet, und das auf der Grundlage maschineller und/oder vom Menschen erzeugter Daten und Eingaben durch maschinelles Lernen und/oder logik- und wissensgestützte Konzepte ableitet, wie eine Reihe von Zielen erreicht wird, und systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld beeinflussen, mit dem die KI-Systeme interagieren"[3]. Beide Fassungen der geplanten Legaldefinition für künstliche Intelligenz umfassen sohin kumulativ ein technisches Element (im Hinblick auf die Entwicklung), bestimmte Einsatzmöglichkeiten sowie ein dadurch eröffnetes Beeinflussungspotenzial gegenüber dem Umfeld, mit dem interagiert wird.

2.2 Bedeutung der künstlichen Intelligenz

Die äußerst vielfältigen Einsatzmöglichkeiten künstlicher Intelligenz in so gut wie allen Bereichen des Wirtschafts- und Gesellschaftslebens – etwa von Medizin über Landwirtschaft bis hin zum Straßenverkehr – und die damit wahrscheinlich einhergehenden gesellschaftlichen Wandlungen[4] machen eine juristische Auseinandersetzung mit dem Phänomen unumgänglich. Auch aus strafrechtlicher Sicht stellen sich viele neue Fragen: Zunächst bietet der Einsatz künstlicher Intelligenz kriminelle Möglichkeiten, die bis vor kurzem nicht bestanden haben; zu denken ist dabei nicht notwendigerweise an ganz neue Kriminalitätsformen, sondern eher an neue Begehungsmethoden „herkömm-

licher“ Kriminalität. Darüber hinaus ist aber auch die Strafrechtswissenschaft berufen, neu eröffnete Fragestellungen im Bereich des materiellen Strafrechts wie auch des Strafprozessrechts zu diskutieren.

2.3 Künstliche Intelligenz und Kriminalität

Es kann nicht überraschen, dass die zahlreichen Einsatzmöglichkeiten künstlicher Intelligenz auch bei kriminellen Vorhaben nützlich sein können und deshalb auch zum Einsatz kommen. Allerdings ist nicht jede Form computergestützter Kriminalität auch stets mit künstlicher Intelligenz verbunden: Typische Computerstraftaten wie etwa Hackerdelikte, Straftaten in Zusammenhang mit virtuellen Währungen bzw Kryptowerten (zB Betrug oder Geldwäscherei), der Einsatz von Ransomware, Cybermobbing oder Hass im Netz können auch ohne künstliche Intelligenz erfolgen.

Bei bestimmten schon zuvor existierenden Phänomenen eröffnen sich durch künstliche Intelligenz hingegen neue Methoden der Begehung. Beispielhaft sei hier der sogenannte Hochfrequenzhandel erwähnt, ein Verhalten an der Börse, das nicht immer nur Ausdruck des schon davor existierenden Marktmissbrauchs sein muss, sondern durchaus auch legale Anwendungsbereiche hat, aber ohne Einsatz künstlicher Intelligenz nicht denkbar wäre.

Da Börsen mittlerweile rein elektronisch geführte Handelssysteme sind, wird ein algorithmischer Handel möglich, bei dem die Entscheidung über die konkrete Vornahme und Durchführung einer Transaktion nicht von einem Menschen, sondern von einer Computersoftware getroffen wird. Die hier eingesetzte künstliche Intelligenz ist in der Lage, Entscheidungen sehr viel schneller zu treffen und zu übermitteln, als ein Mensch das könnte. Das ist die Grundlage des Hochfrequenzhandels: Hier entscheidet die künstliche Intelligenz über die Einleitung, das Erzeugen, Weiterleiten und die Ausführung eines Auftrags ohne menschliche Intervention für einzelne Geschäfte oder Aufträge. Dadurch minimiert sich die Latenzzeit, also die Zeit, die zwischen dem Absenden eines Signals (einer Order) und der Bearbeitung des Signals beim Empfänger vergeht. Zwischen dem Kauf und dem Verkauf eines Finanzinstruments vergehen so nur Sekundenbruchteile (im Mikrosekundenbereich). Diese enorme Geschwindigkeit kann auf verschiedene Weise genützt werden.

Vollkommen legal sind Arbitrage-Strategien, bei denen es darum geht, Kursdifferenzen an unterschiedlichen Handelsplätzen auszunützen.[5] In der kurzen Zeitspanne, die vergeht, bis sich Kurse an verschiedenen Börsen aneinander angeglichen haben, können Hochfrequenzhändler an den langsamer reagierenden Handelsplätzen Orders platzieren und Papiere so noch zu einem eigentlich bereits durch den Markt überholten Preis kaufen, um sie dann umgehend zum aktualisierten Preis wieder abzustoßen.

Klar illegal ist hingegen die Benützung des Hochfrequenzhandels zu Zwecken der (handelsgestützten) Marktmanipulation: Die aktive Beeinflussung der Preisbildung durch rasche Einspeisung unzähliger Orders in ein elektronisches Handelssystem in kürzester Zeit, zB durch das sogenannte „Spam and Cancel“ (dh die umgehende Stornierung von über 90 % der Orders) oder das „Quote Stuffing“ (dh die Überforderung der Börsen-EDV durch Spam-Orders und Ausnützung der eintretenden Verzögerung des Handels, dh der künstlich herbeigeführten Latenzzeit im Vergleich zu anderen Handelsplätzen). Marktmanipulation ist auch ohne Anwendung künstlicher Intelligenz als Verwaltungsübertretung (§ 154 Abs 1 Z 3 Börsegesetz [BörseG] iVm Art 15 Marktmissbrauchs-VO[6]) oder gerichtlich (§ 164 BörseG)

strafbar, aber derartige Begehungsweisen sind nur im Hochfrequenzhandel möglich.

Elektronisches Frontrunning ist schließlich eine Anwendung des Hochfrequenzhandels, die sich insofern in einem rechtlichen Graubereich befindet, als nur unter bestimmten Umständen verwaltungsrechtliche (§ 154 Abs 1 Z 1 BörseG iVm Art 14 lit a Marktmissbrauchs-VO) oder gerichtliche (§ 163 Abs 1 Z 1 BörseG) Strafbarkeit vorliegen kann, ansonsten aber kein Straftatbestand erfüllt wird. Von elektronischem Frontrunning spricht man, wenn der Algorithmus von der Abgabe einer Order durch eine andere Händlerin oder einen anderen Händler erfährt, noch bevor diese ausgeführt werden kann, und sich daraufhin noch schnell selbst durch eine eigene Order günstig eindeckt und die ursprüngliche Order der anderen Händlerin bzw des anderen Händlers bedient.[7] Eine Strafbarkeit könnte nur dann vorliegen, wenn die Information über die Orderabgabe durch die andere Händlerin bzw den anderen Händler kurserheblich wäre. Darunter versteht man nach Art 7 Abs 1 lit a Marktmissbrauchs-VO die Eignung der Information, den Kurs des betroffenen Finanzinstruments oder den Kurs damit verbundener derivativer Finanzinstrumente erheblich zu beeinflussen, wobei Art 7 Abs 4 Marktmissbrauchs-VO ausführt, dass dies Informationen betrifft, die ein verständiger Anleger wahrscheinlich als Teil der Grundlage seiner Anlageentscheidungen nutzen würde. Erheblich ist eine Kursbeeinflussung ab einer Änderung von rund 5 %.[8] Meistens werden die dem elektronischen Frontrunning zugrunde liegenden Informationen nicht kurserheblich im genannten Sinn sein, wodurch auch der Tatbestand eines Insidergeschäftes nicht erfüllt wird, und die Vorgangsweise als legal zu qualifizieren ist. Sollte man elektronisches Frontrunning dennoch als durchwegs unerwünscht und strafwürdig erachten, müsste der Gesetzgeber die Rechtslage insofern nachschärfen.

2.4 Materiell-rechtliche Fragen hinsichtlich künstlicher Intelligenz

Abgesehen von der angesprochenen kriminalpolitischen Frage stellen sich auch bei der Auslegung des geltenden materiellen Strafrechts schwierige Fragen, von denen einige wenige in der Folge angesprochen werden sollen. Dabei scheint es sinnvoll, Konstellationen, in denen künstliche Intelligenz täterseitig zum Einsatz kommt, von jenen Fällen zu unterscheiden, bei denen auf Seiten des Opfers künstliche Intelligenz agiert.

2.4.1 Täterseitige Verwendung künstlicher Intelligenz

Robotor, die Menschen angreifen, sind ein Thema, das in Romanen und Filmen (zB I, Robot; Terminator etc) aus dem Bereich der Science-Fiction schon lange und wiederholt behandelt wird und offenbar auf ein breiteres Interesse stößt. Es verwundert daher nicht, dass sich auch die strafrechtliche Diskussion bisher auf eine Thematik fokussiert, die den Delikten gegen Leib und Leben entspricht, letztlich aber auch zentrale Fragen des allgemeinen Teils des Strafrechts betrifft. Dies betrifft vor allem autonom fahrende Autos, und hierbei insbesondere die sogenannte „Leben-gegen-Leben"-Programmierung. Vorauszuschicken ist dabei, dass eine Verwendung vollautomatisiert fahrender Autos in Österreich kraftfahrrechtlich derzeit nicht zulässig ist: Nach § 102 Abs 3a Kraftfahrgesetz (KFG) „darf der Lenker bestimmte Fahraufgaben im Fahrzeug vorhandenen Assistenzsystemen oder automatisierten oder vernetzten Fahrsystemen übertragen". Erlaubt ist – abgesehen von Testfahrten – de lege lata also nur eine Teilautomatisierung (zB eine Einparkhilfe), und auch für diesen Fall gebietet § 102 Abs 3b KFG, dass der Lenker stets verantwort-

lich bleibt, seine Fahraufgaben wieder zu übernehmen.[9] Die Strafrechtswissenschaft kann sich jedoch nicht damit zufrieden geben, dass der reguläre Einsatz autonom fahrender Autos in Österreich (noch) nicht zulässig ist, sondern muss in ihren Überlegungen von dem Faktum ausgehen, dass künstliche Intelligenz durchaus in der Lage ist, vollautonom, also ohne Eingriff durch eine menschliche Lenkerin oder einen menschlichen Lenker, ein Auto zu steuern. Wie wäre strafrechtlich mit Unfällen mit Personenschaden umzugehen, die durch ein autonom fahrendes Auto verursacht werden? Der Fahrzeugnutzerin bzw dem Fahrzeugnutzer (also der „Lenkerin" bzw dem „Lenker", die bzw der konkret gar nicht lenkt) kann ein Vorwurf wegen eines (idR wohl nur fahrlässigen) Deliktes gegen Leib und Leben nur im Fall einer objektiven Sorgfaltswidrigkeit gemacht werden, wenn sie bzw er also zB durch den Einsatz des autonom fahrenden Autos gegen ein Schutzgesetz verstoßen hat (also etwa gegen die derzeitigen kraftfahrrechtlichen Einschränkungen), oder auch, weil sie bzw er es in sorgfaltswidriger Weise unterlässt, in einer bestimmten Situation selbst die Steuerung wieder an sich zu ziehen, in der es eine Maßfigur (also ein einsichtiger und besonnener Mensch aus dem Verkehrskreis des Täters) sehr wohl getan hätte. Auch der Herstellerin/dem Hersteller bzw der Programmiererin/dem Programmierer des autonom fahrenden Fahrzeugs kann nur bei sorgfaltswidrigem Verhalten (etwa bei durch Nachlässigkeit hervorgerufenen Produktionsmängeln oder Programmierfehlern) ein strafrechtlicher Vorwurf gemacht werden. In der Literatur diskutiert wurde auch, ob das autonom fahrende Auto, also die künstliche Intelligenz selbst, einer Strafbarkeit unterliegen könnte.[10] Freilich sieht das Strafrecht derzeit keine Verantwortung einer solchen „E-Person" vor, sondern wendet sich mit seinen Normbefehlen nur an natürliche Personen, also Menschen. Dies bedeutet jedoch nicht, dass eine strafrechtliche Verantwortlichkeit nichtmenschlicher Rechtsträger de lege ferenda völlig ausgeschlossen wäre: Ansonsten dürfte es auch keine Verbandsverantwortlichkeit, also strafrechtliche Verantwortung juristischer Personen und Personengesellschaften, geben, wie sie 2006 durch das Verbandsverantwortlichkeitsgesetz (VbVG) eingeführt wurde.

Beliebtes Beispiel in der wissenschaftlichen Diskussion um autonom fahrende Autos ist die angesprochene Leben-gegen-Leben-Programmierung.[11] Sie knüpft an einen „Klassiker" der Strafrechtsdogmatik an: Ausgangslage ist, dass autonom fahrende Autos darauf programmiert sind, Unfälle zu vermeiden, und, soweit dies nicht mehr möglich ist, Menschenleben zu schützen (dh im Zweifelsfall eher einen Sachschaden als einen Personenschaden in Kauf zu nehmen). Es sind allerdings auch Situationen denkbar, in denen nicht nur ein Unfall an sich unvermeidbar wird, sondern auch ein damit verbundener Personenschaden; hier stellt sich der das Auto steuernden künstlichen Intelligenz nicht mehr die Frage, ob das Fahrzeug einen Menschen überfahren (und damit verletzen oder töten) wird, sondern, falls kein Anhalten, aber zumindest ein Fahrtrichtungswechsel möglich ist, nur noch, welche(n) Menschen es in Mitleidenschaft ziehen soll. Erhält das autonom fahrende Auto eine Programmierung für diesen Fall, die eine Richtungsänderung vorsieht, um möglichst wenige Menschen zu überfahren, auch wenn es sich dabei um andere Personen handelt als jene, die ohne Richtungswechsel überfahren würden?

Bsp: Das Auto rast auf die Fußgänger A, B und C zu, ein rechtzeitiges Abbremsen ist nicht mehr möglich. Durch das einzig mögliche Ausweichmanöver wird stattdessen der Fußgänger D überfahren.

In einem solchen Richtungswechsel könnte ein vorsätzliches Delikt gegen Leib und Leben liegen, insbesondere ein Mord (§ 75 Strafgesetzbuch [StGB]), allenfalls auch ein Körperverletzungsdelikt nach §§ 83–85 StGB. Da eine Leben-gegen-Leben-Programmierung vorsätzlich vorgenommen wird, stellt sich die Frage objektiver Sorgfaltswidrigkeit kaum; der jeweilige Tatbestand wird zumindest bei der Programmiererin bzw dem Programmierer erfüllt sein. Letztlich liegt in einer solchen Programmierung das Grundproblem des bekannten „Weichensteller-Falles".[12] Einen Rechtfertigungsgrund für das tatbestandsmäßige Verhalten wird es nicht geben: Weder kommt ein rechtfertigender Notstand zum Tragen, da menschliches Leben nicht quantifizierbar ist, und somit eine Notstandshandlung – das bedrohte Rechtsgut muss eindeutig höherwertiger sein als das beeinträchtigte Rechtsgut – ausgeschlossen ist: Das Leben eines einzigen Menschen ist nicht weniger wert als das Leben eines anderen oder mehrerer anderer. Noch kommt eine Rechtfertigung durch Pflichtenkollision in Betracht, da sich bei einer Kollision aus einer Verbotsnorm (Programmiere keinen Fahrtrichtungswechsel, bei dem jemand überfahren wird!) und einer Gebotsnorm (Programmiere einen Fahrtrichtungswechsel, um zu vermeiden, dass jemand überfahren wird!) die Verbotsnorm gegenüber der Gebotsnorm durchsetzt;[13] aus diesem Grund ist vielmehr das Unterlassen einer Leben-gegen-Leben-Programmierung gerechtfertigt. Eine Strafbarkeit (nicht jedoch das Unrecht der Tat!) der Leben-gegen-Leben-Programmierung könnte erst auf Schuldebene vermieden werden, durch Anwendung eines entschuldigenden Notstandes: Insoweit genügt es, dass „der aus der Tat drohende Schaden nicht unverhältnismäßig schwerer wiegt als der Nachteil, den sie abwenden soll" (§ 10 Abs 1 StGB). Standfest will der Programmiererin bzw dem Programmierer einer Leben-gegen-Leben-Programmierung den entschuldigenden Notstand nicht zubilligen, da sie bzw er zum Zeitpunkt des Programmierens keiner Druck- und Zwangssituation ausgesetzt war, womit die ausdrückliche Voraussetzung des subjektiven Notstandselements nach § 10 Abs 1 StGB, dass „in der Lage des Täters von einem mit den rechtlich geschützten Werten verbundenen Menschen kein anderes Verhalten zu erwarten war", nicht erfüllt sei.[14] Diese mE allzu strenge Auffassung übersieht, dass eine Druck- und Zwangssituation nicht nur aus unmittelbarer Zeitnot entstehen kann, sondern gerade bei einem ungelösten ethischen Dilemma wie dem hier vorliegenden auch in ansonsten vollkommen ruhigen Lebenslagen (wie eben auch dem Arbeitsalltag einer Programmiererin bzw eines Programmierers) vorstellbar ist.

2.4.2 Opferseitige Verwendung künstlicher Intelligenz

Materiell-rechtliche Fragestellungen iZm opferseitiger Verwendung künstlicher Intelligenz könnten sich daraus ergeben, dass manche Straftatbestände – tatsächlich oder vielleicht auch nur scheinbar – menschliches Verhalten beim Opfer voraussetzen. Fehlt es opferseitig an einem Menschen, könnten deshalb Strafbarkeitslücken entstehen. Beispielhaft seien der Betrug und die Erpressung genannt, die auch als „Selbstschädigungsdelikte" bezeichnet werden, weil sie ein durch Täuschung (Betrug) oder gefährliche Drohung bzw Gewalt (Erpressung) hervorgerufenes Verhalten des Opfers erfordern, mit dem dieses entweder sich selbst oder einen Dritten am Vermögen schädigt. Beide Delikte erfordern, dass die Täterin bzw der Täter „jemanden" täuscht bzw nötigt: Jemand ist nach dem allgemeinen Sprachgebrauch wohl ein Mensch, zumindest

jedoch eine Person; es überstiege den äußersten Wortsinn, unter „jemanden" auch künstliche Intelligenz zu verstehen. Eine Anwendung des Betrugs oder der Erpressung auf Konstellationen, in denen kein Mensch, sondern künstliche Intelligenz getäuscht oder genötigt wird, verstieße somit gegen das Analogieverbot.[15]

Eine Konsequenz zeigt sich etwa bei sogenannten Fehlbuchungen. Weist das Bankkonto einer Kontoinhaberin oder eines Kontoinhabers ein unerwartetes (und unberechtigtes) Guthaben aus, kann dies zum einen daran liegen, dass ihr bzw ihm eine andere Kontoinhaberin bzw ein anderer Kontoinhaber irrtümlicherweise Geld überwiesen hat (sogenannte Fehlüberweisung); verwendet die bereicherte Kontoinhaberin bzw der bereicherte Kontoinhaber dieses Guthaben, indem sie bzw er es abhebt oder weitertransferiert, kann dies bei entsprechendem Vorsatz eine Unterschlagung (§ 134 Abs 1 StGB) darstellen: Niemand wird über das Guthaben getäuscht, das tatsächlich am Bankkonto vorliegt (da es durch einen unmotivierten Irrtum des Dritten überwiesen wurde), und die Verwendung dieses fremden Gutes stellt eine Irrtumsunterschlagung dar.[16] Zum anderen kann der unberechtigt hohe Guthabenstand aber auch auf einen Darstellungsfehler der Bank zurückzuführen sein. Bei einer solchen Fehlbuchung gab es keine Überweisung eines Dritten, und das dargestellte Guthaben besteht gar nicht in der angezeigten Höhe. Nützt die Kontoinhaberin oder der Kontoinhaber nur diesen bankseitigen Irrtum aus, indem sie bzw er eine Überweisung des scheinbaren Guthabens unternimmt, täuscht sie bzw er letztlich eine Bankangestellte oder einen Bankangestellten, die bzw der die Überweisung freigibt. Die Anwendbarkeit des Betrugstatbestandes beruht allerdings darauf, dass seitens der Bank ein Mensch in die Freigabe der Überweisung involviert ist, also „jemand", der iSd § 146 StGB getäuscht werden kann und in der Folge (einem themengleichen Irrtum unterliegend) die – in diesem Fall die Bank – schädigende Vermögensverfügung vornimmt. Bedient sich die Bank dazu keiner Menschen mehr, sondern greift sie auf künstliche Intelligenz zurück – wie etwa bei Echtzeitüberweisungen –, kann die Ausnützung einer Fehlbuchung durch die Kontoinhaberin oder durch den Kontoinhaber keinen Betrug darstellen. Freilich entsteht insoweit keine Strafbarkeitslücke, da sich insoweit § 148a StGB, betrügerischer Datenverarbeitungsmissbrauch, als bereits bestehender Ausweichtatbestand anbietet.

An anderer Stelle könnte die Unanwendbarkeit des Betrugstatbestandes problematischer werden bzw zumindest eine Änderung der höchstgerichtlichen Judikatur erzwingen: § 22 Abs 2 FinStrG bestimmt, dass ein auf betrügerische Weise oder durch Täuschung begangenes Finanzvergehen gleichwohl nur nach dem FinStrG zu ahnden ist. Diese durch die Finanzstrafgesetznovelle 1975[17] eingeführte Subsidiaritätsbestimmung sollte den bis dahin vorherrschenden Zustand abschaffen, nachdem Finanzvergehen, die auf betrügerische Weise begangen worden waren, zusätzlich zum jeweiligen finanzstrafrechtlichen Tatbestand auch noch als Betrug verfolgt wurden.[18] Letztlich kann eine solche betrügerische Vorgangsweise bei allen vorsätzlichen Finanzvergehen festgestellt werden, bei denen es um bescheidmäßig vorzuschreibende Abgaben geht.

Bsp: A gibt vorsätzlich eine unvollständige Einkommensteuer-Erklärung ab, um Einkommensteuer (ESt) zu verkürzen. Er erfüllt dadurch einerseits eine Abgabenhinterziehung nach § 33 Abs 1 FinStrG. Andererseits ließe sich sein Verhalten problemlos unter den Betrugstatbestand subsumieren, denn A täuscht eine Finanzbeamtin oder einen Finanzbeamten über

Tatsachen (nämlich sein wahres Einkommen), führt bei dieser oder diesem kausal einen themengleichen Irrtum herbei, der wiederum die Finanzbeamtin bzw den Finanzbeamten zu einer Handlung veranlasst (Erlass eines ESt-Bescheids), die einen Dritten, nämlich den Fiskus, am Vermögen schädigt (weil ihm weniger ESt zukommt, als ihm zukommen sollte).

§ 22 Abs 2 FinStrG ist Ausdruck der Abkehr des Gesetzgebers von einer derart zwangsläufigen, regelmäßigen Doppelgleisigkeit der Verfolgung von Finanzvergehen. Obwohl der Wortlaut des § 22 Abs 2 FinStrG den Tatbestand des Betrugs nicht ausdrücklich verwendet, sondern von „betrügerischer Weise" spricht, hat der Oberste Gerichtshof (OGH) den Anwendungsbereich der Bestimmung stets auf den Betrug (und seine Qualifikationen sowie das praktisch nicht relevante Delikt der Täuschung) beschränkt.[19] Eine weitergehende Interpretation, die durchaus auch mit dem Wortlaut vereinbar wäre und nach der etwa auch der betrügerische Datenverarbeitungsmissbrauch durch ein Finanzvergehen verdrängt würde, hat der OGH bislang abgelehnt.

Dies könnte problematisch werden, sobald statt dem bereits jetzt teilautomatisierten Abgabenverfahren künstliche Intelligenz in einem vollautomatisierten Verfahren Abgabenbescheide erstellt: Wird kein Mensch über steuerrelevante Tatsachen getäuscht, sondern nur das Ergebnis einer automationsunterstützten Datenverarbeitung beeinflusst, wäre nicht der Betrugstatbestand erfüllt, sondern der Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs. Würde § 22 Abs 2 FinStrG auch dann in seinem Anwendungsbereich weiterhin auf den Betrug beschränkt, liefe er vollkommen ins Leere; wie vor 1975 würde dann so gut wie jedes vorsätzliche Finanzvergehen, das eine bescheidmäßig vorzuschreibende Abgabe betrifft, zusätzlich zur finanzstrafrechtlichen Verfolgung auch kernstrafrechtlich verfolgt, diesmal nach § 148a StGB. Will man eine solche Entwicklung vermeiden, müsste entweder der OGH seine Rechtsprechung im Hinblick auf die Erfassung des § 148a StGB durch die Subsidiaritätsbestimmung nach § 22 Abs 2 FinStrG ändern[20], oder der Gesetzgeber den Anwendungsbereich des § 22 Abs 2 FinStrG explizit auch auf § 148a StGB erstrecken.

Auch die Erpressung, die ganz auf die Nötigung eines Menschen zu einer vermögensschädigenden Handlung, Duldung oder Unterlassung zugeschnitten ist, ist unanwendbar auf vergleichbare Verhaltensweisen gegenüber künstlicher Intelligenz. Gleichwohl ist es schon für die nahe Zukunft zumindest technisch denkbar, dass ein Unternehmen gewisse Entscheidungen in der Geschäftsführung künstlicher Intelligenz überträgt. Auch ein solches Unternehmen könnte Opfer gewisser erpressungsähnlicher Machenschaften werden.

Bsp: B droht der geschäftsführenden künstlichen Intelligenz eines lebensmittelerzeugenden Unternehmens, dessen Produkte in Supermärkten zu vergiften, wenn ihm keine Geldsumme bezahlt wird. Die künstliche Intelligenz wägt Chancen und Risiken ab und bezahlt dann den geforderten Betrag.

Auf eine solche Konstellation kann der Tatbestand der Erpressung nicht angewendet werden: Zwar wäre es durchaus im Einklang mit dem Erpressungstatbestand, dass sich das angedrohte Übel (ebenso wie die als alternatives Nötigungsmittel eingesetzte Gewalt) auch gegen einen Dritten (und nicht gegen den Bedrohten selbst) richten kann, und auch das – neben dem fremden Vermögen – mitgeschützte Rechtsgut der Willensbildungs- und Willensbetätigungsfreiheit schließt nicht automatisch den Willen künstlicher Intelligenz aus; doch verlangt die Erpressung jedenfalls, dass die Genötigte bzw der Genötigte eine Person („jemand") ist, was (zu-

mindest derzeit rechtlich) bei künstlicher Intelligenz nicht zutrifft. Um für eine solche Konstellation vermögensschädigenden Verhaltens keine Strafbarkeitslücke entstehen zu lassen, könnte der Gesetzgeber entweder die Erpressung nach § 144 StGB erweitern, oder man müsste – ohne Bedarf einer Gesetzesverschärfung – den betrügerischen Datenverarbeitungsmissbrauch auch auf „Nötigungen" künstlicher Intelligenz zur Anwendung bringen, was zumindest vom Wortlaut des § 148a Abs 1 StGB her nicht ausgeschlossen ist.

2.5 Strafprozessuale Fragen hinsichtlich künstlicher Intelligenz

Schon jetzt kommen digitale Instrumente im Strafverfahren in verschiedener Weise zum Einsatz, so etwa der elektronische Rechtsverkehr[21], Videokonferenzen[22] oder auch der „Bundes-Trojaner"[23]. Es steht außer Frage, dass auch die Anwendung künstlicher Intelligenz im Strafverfahren nutzbringend sein kann. Aus heutiger Sicht lassen sich ihre Einsatzgebiete allerdings nur erahnen. Dabei kann man jedoch bereits jetzt zumindest zwei Bereiche unterscheiden: Zum ersten kann künstliche Intelligenz im Vorfeld der Strafverfolgung zum Einsatz kommen, um strafbare Handlungen als solche überhaupt erst zu entdecken, zum anderen im Strafprozess selbst. Im Hinblick auf die Art des Einsatzes lässt sich darüber hinaus zwischen Entscheidungsunterstützung und Entscheidungsfindung durch künstliche Intelligenz unterscheiden.

Zur Aufdeckung strafbarer Handlungen wird (entscheidungsunterstützende) künstliche Intelligenz bereits jetzt angewendet, wie etwa bei der Erkennung von Geldwäscherei bzw Geldwäscherei begründenden Vortaten und Terrorismusfinanzierung: § 7a Finanzmarkt-Geldwäschegesetz (FM-GwG) erlaubt ausdrücklich, dass die Verpflichteten des FM-GwG, wie zB Banken und Versicherungen, der sie treffenden Sorgfaltspflicht der kontinuierlichen Überwachung der Geschäftsbeziehung (§ 6 Abs 1 Z 6 FM-GwG) auch „unter Verwendung eines auf künstlicher Intelligenz oder anderen fortschrittlichen Technologien basierenden Ansatzes" (§ 7a Abs 1 FM-GwG) nachkommen können. Auch die Finanzmarktaufsichtsbehörde (FMA) bedient sich im Rahmen der risikobasierten Aufsicht (§ 25 Abs 2 FM-GwG) eines „Risk Scoring Tools", um das Geldwäschemissbrauchsrisiko der von ihr überwachten Unternehmen einzustufen. Auch bei der Aufdeckung von Marktmissbrauch verwendet die FMA ein „Alert Surveillance Tool", das Auffälligkeiten im Handel erkennt und Alarm auslöst, sowie ein Tool zur Orderbuchrekonstruktion, mit dem abnormales Handelsverhalten analysiert werden kann. Gewisse Anwendungsmöglichkeiten, vor allem die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, wird Art 5 des künftigen Gesetzes über künstliche Intelligenz aber wohl stark einschränken.

Auch im Strafverfahren selbst kann der Einsatz künstlicher Intelligenz nützlich sein. Dabei ist zunächst an entscheidungsunterstützende künstliche Intelligenz zu denken, deren potenzielle Einsatzgebiete wohl weit mehr umfassen als „nur" Profiling. Denkbar sind für die Zukunft viele weitere Anwendungen. So zeigt schon die jetzige Fähigkeit künstlicher Intelligenz, Gespräche zu führen (wie etwa ChatGPT), dass sie grundsätzlich (zumindest technisch) in allen Situationen zum Einsatz kommen könnte, bei denen es letztlich um Gespräche geht, insbesondere bei Vernehmungen von Zeugen oder sogar Beschuldigten. Der Begriff der Vernehmung nach § 151 Z 2 Strafprozessordnung (StPO) („das Befragen von Personen nach förmlicher Information über ihre Stellung und ihre Rechte im Verfahren") setzt

zumindest nach seinem Wortlaut nicht voraus, dass die Vernehmende bzw der Vernehmende ein Mensch sein muss; ob die Vernehmung eines Menschen durch künstliche Intelligenz mit der Menschenwürde und damit der Europäischen Menschenrechtskonvention (EMRK) vereinbar wäre, muss jedoch vorerst dahingestellt bleiben. Von praktischem Interesse könnte eine solche Vernehmung jedenfalls sein, wenn es gilt, eine Vielzahl potenzieller Zeugen zu hören. Da künstliche Intelligenz wohl – insbesondere nach einem Lernprozess – gut in der Lage wäre, Lügen als solche zu erkennen, wäre bei ihrem Einsatz aber wohl jedenfalls die restriktive Haltung des OGH zu Lügendetektortests zu beachten.[24] Eine verdeckte Ermittlung (§ 129 Z 2 StPO) setzt nach derzeitiger Rechtslage jedenfalls ein Organ der Kriminalpolizei oder eine Person im Auftrag der Kriminalpolizei voraus, dürfte demnach also nicht durch künstliche Intelligenz durchgeführt werden; technisch gesehen wäre ein solcher Einsatz im Internet jedoch durchaus denkbar. Dies gilt ebenso für ein Scheingeschäft (§ 129 Z 3 StPO) im Internet, wobei insoweit schon die aktuelle Legaldefinition nicht unbedingt auf menschliches Handeln auf Seiten der Strafverfolgungsbehörden hindeutet. Mit fortschreitender Technologie könnten auch andere Ermittlungsmaßnahmen durch künstliche Intelligenz unterstützt werden, wie etwa durch Heranziehung von (bisher nur hypothetischen) Nanobots bei der Leichenbeschau und Obduktion (§ 128 StPO).

Könnte künstliche Intelligenz über eine entscheidungsunterstützende Funktion hinaus in zukünftigen Strafverfahren auch selbst Entscheidungen treffen? Denkbar erscheint dies überall dort, wo Entscheidungen direkt aus Rechtstexten übernommen werden können, ohne Fakten/Konsequenzen abwägen zu müssen, dh keinerlei Ermessen erforderlich ist. Unter solchen Umständen ermöglicht etwa das deutsche Verwaltungsverfahrensrecht (§ 35a dVwVfG[25]) automatisierte Entscheidungsfindungen: „Ein Verwaltungsakt kann vollständig durch automatische Einrichtungen erlassen werden, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht." In Österreich hat der Verfassungsgerichtshof (VfGH) schon vor über 35 Jahren strenge verfassungsrechtliche Anforderungen an den sogenannten „Computerbescheid" gestellt, zu denen etwa Veranlassung und Einflussmöglichkeit durch die Behörde gehören.[26] Im Einklang mit diesen Anforderungen steht etwa die Regelung des österreichischen Abgabenverfahrensrechts zu „Ausfertigungen, die mittels automationsunterstützter Datenverarbeitung erstellt werden", nach § 96 Abs 2 Bundesabgabenordung (BAO).

Obwohl Köck mittlerweile auch für das Finanzstrafrecht bei Finanzvergehen mit „einfachem Tatbestand" vorschlägt, auf Basis eines entsprechend zu ändernden § 143 FinStrG vollautomatisierte Strafverfügungen zuzulassen,[27] ist mE festzustellen, dass es im Strafverfahren – auch bei (scheinbar) einfachen Tatbeständen – kaum Entscheidungen geben wird, die ohne Ermessen direkt aus Rechtstexten zu übernehmen wären. Gerade verfahrensbeendende Entscheidungen wie Urteile, Einstellungsbeschlüsse, Rücktritte von der Anklage etc erfordern stets Abwägungen, etwa zur inneren Tatseite, zu Rechtfertigungsgründen, Irrtümern oder der Schuld. In ähnlicher Weise gilt dies aber auch für wesentliche Entscheidungen des laufenden Strafverfahrens, wie zB Verhängung und Verlängerung der Untersuchungshaft, Bewilligung von Durchsuchungen, Beschlagnahmen etc: Auch insoweit werden stets Umstände des Einzelfalls gegeneinander abzuwägen sein. Am ehesten vorstellbar sind strafprozessuale Entschei-

dungen künstlicher Intelligenz mE bei zwischenbehördlichen Vorgängen, wenn im zweiten Schritt ein Mensch entscheidet, zB bei der Beantragung von bestimmten Ermittlungsmaßnahmen oder der Erstattung einer Anzeige nach § 78 StPO (oder § 81 FinStrG). Auch dafür fehlt es jedoch derzeit an der Rechtsgrundlage sowie mE wohl auch an Bedarf.

3. CONCLUSIO

Eine Legaldefinition für künstliche Intelligenz besteht derzeit noch nicht, steht aber knapp bevor. Dies ist angesichts der Bedeutung, die künstliche Intelligenz für unsere Gesellschaft und Wirtschaft haben wird, sehr zu begrüßen. Auch aus strafrechtlicher Sicht wirft die künstliche Intelligenz viele Themen auf, die sich derzeit teilweise erst abzuzeichnen beginnen. Neben neuen Verhaltensweisen diesseits und jenseits der Strafbarkeitsgrenze wie beim Hochfrequenzhandel werden auch grundsätzliche Fragen sowohl im materiellen Strafrecht als auch im Strafprozessrecht aufgeworfen. Im materiellen Recht hat sich die bisherige Debatte bislang auf die täterseitige Verwendung künstlicher Intelligenz konzentriert, insbesondere auf autonom fahrende Autos, die Unfälle mit Personenschäden verursachen. Da eine strafrechtliche Haftung für E-Personen derzeit nicht in Betracht kommt, kann es insoweit nur um die strafrechtliche Haftung von Menschen gehen, die sich gegebenenfalls das Verhalten des autonom fahrenden Autos zurechnen lassen müssen, allen voran die Programmiererinnen und Programmierer. In diesem Zusammenhang hat auch die sogenannte Leben-gegen-Leben-Programmierung Aufmerksamkeit erhalten, die einerseits eine strafrechtliche Verantwortung wegen vorsätzlicher Delikte gegen Leib und Leben (insb Mord) begründen kann, andererseits unter dem Aspekt des entschuldigenden Notstandes relevant sein könnte. Nicht minder interessant sind die Probleme, die opferseitig eingesetzte künstliche Intelligenz mit Blick auf die Wortlautgrenzen einzelner Straftatbestände wie Betrug und Erpressung auslöst. Vielleicht wird dieser Umstand dem bisher nur selten judizierten Tatbestand des betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) zu größerer Bedeutung verhelfen und auch die Erstreckung der Subsidiaritätsregelung des § 22 Abs 2 FinStrG auf den § 148a StGB bewirken. Die denkbaren Einsatzgebiete künstlicher Intelligenz zu Strafverfolgungszwecken schreiten mit der technischen Entwicklung immer weiter voran. Entscheidungsunterstützende Einsätze künstlicher Intelligenz werden bereits jetzt zur Aufdeckung von Straftaten, also im Vorfeld von Strafverfahren, durchgeführt. Im eigentlichen Strafverfahren ist entscheidungsunterstützende künstliche Intelligenz ebenfalls denkbar, wie etwa im Bereich der Zeugenvernehmung. Für eine Entscheidungsfindung im Strafverfahren besteht mE hingegen allenfalls nur bei zwischenbehördlichen Vorgängen eine Einsatzmöglichkeit, wenn im zweiten Schritt ein Mensch entscheidet, zB bei der Beantragung von bestimmten Ermittlungsmaßnahmen oder der Erstattung einer Anzeige nach § 78 StPO.

[1] *Europäische Kommission, Mitteilung „Künstliche Intelligenz für Europa", 25.04.2018, COM(2018) 237 final, 1.*

[2] *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.04.2021, COM(2021) 206 final.*

[3] *Rat der Europäischen Union, Generalsekreta-*

riat des Rates, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union – Allgemeine Ausrichtung (6. Dezember 2022), 06.12.2022, 15698/22.

[4] *Die Europäische Kommission, Mitteilung „Künstliche Intelligenz für Europa", 25.04.2018, COM(2018) 237 final, 2, vergleicht die künstliche Intelligenz im Hinblick auf die Auswirkungen auf die Gesellschaft mit der Dampfmaschine oder dem elektrischen Strom.*

[5] *Vgl dazu etwa Kasiske, Marktmissbräuchliche Strategien im Hochfrequenzhandel, WM 2014, 1933 (1933f).*

[6] *Verordnung (EU) Nr 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission, ABl L 173 vom 12.06.2014, 1.*

[7] *Vgl zu dieser Vorgangsweise schon Lewis, Flashboys (2014) 114ff.*

[8] *BT-Drucksache 12/6679, 47, 27.01.1994.*

[9] *Vgl insoweit auch § 3 Abs 2 Verordnung des Bundesministers für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie über Rahmenbedingungen für automatisiertes Fahren (Automatisiertes Fahren Verordnung – AutomatFahrV), BGBl II 402/2016.*

[10] *Hilgendorf, Können Roboter schuldhaft handeln? Zur Übertragbarkeit unseres normativen Grundvokabulars auf Maschinen, in Gless/Seelmann (Hrsg), Intelligente Agenten und das Recht (2016) 119ff.*

[11] *Vgl etwa schon Rohregger, Strafrechtsfragen um autonome Fahrzeuge, Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2017 (2017) 119 (129ff).*

[12] *Vgl dazu Welzel, Zum Notstandsproblem, ZStW 1951, 47.*

[13] *Vgl Fuchs/Zerbes, Strafrecht Allgemeiner Teil I11 (2021) Kap 18 Rz 4.*

[14] *Standfest, Autonomes und automatisiertes Fahren im Strafrecht, Diss Uni Innsbruck 2020, 198f; auch Rohregger, Strafrechtsfragen um autonome Fahrzeuge, Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2017 (2017) 119 (131) ist gegen die Anwendung des entschuldigenden Notstandes.*

[15] *OGH 14.07.2011, 13 Os 61/11m; vgl etwa auch (zum Betrug) Kienapfel/Schmoller, Studienbuch Strafrecht Besonderer Teil II[2] (2017) § 146 Rz 94; Kirchbacher/Sadoghi in Höpfel/Ratz, WK[2] StGB § 146 (Stand 01.03.2019, rdb.at) Rz 47; Kert in SbgK-StGB § 146 StGB, 26. Lfg (Mai 2012) Rz 135f; Fuchs/Reindl-Krauskopf, Strafrecht BT I[7] (2020) 209; Expliziter Ausschluss von Täuschungen künstlicher Intelligenz aus dem Betrugstatbestand bei Glaser, Betrug und Erschleichung einer Leistung (§§ 146–148, 149–150), in Glaser (Hrsg), Handbuch Vermögensdelikte (2023) Rz 9/89.*

[16] *Vgl dazu etwa Glaser, Betrug und Erschleichung einer Leistung (§§ 146–148, 149–150), in Glaser (Hrsg), Handbuch Vermögensdelikte (2023) Rz 9/37.*

[17] *BGBl 335/1975.*

[18] *ErlRV 1130 BlgNR 13. GP 55.*

[19] *RS0118271.*

[20] *In diesem Sinne zuletzt Kahl/Kert, Abgabenhinterziehung oder betrügerischer Datenverarbeitungsmissbrauch?, in Leitner/Brandl (Hrsg), Finanzstrafrecht 2021 (2022) 13 (32).*

[21] *Verordnung der Bundesministerin für Justiz über den elektronischen Rechtsverkehr (ERV 2021), BGBl II 587/2021.*

[22] *So etwa bei der Vernehmung von Zeugen oder Beschuldigten nach § 153 Abs 4 StPO.*

[23] *Diesem deutliche Grenzen setzend: VfGH 11.12.2019, G72/2019.*

[24] *Vgl zuletzt OGH 15.01.2020, 15 Os 125/19z.*

[25] *Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl I S 102), das zuletzt durch Artikel 24 Absatz 3 des Gesetzes vom 25. Juni 2021 (BGBl I S 2154) geändert worden ist, dBGBl 2003 I 102.*

[26] *VfGH 16.12.1987, G110/87 ua.*

[27] *Vgl Köck, Vollautomatisierte Entscheidungen im Finanzstrafrecht?, ZWF 2022, 260.*