Digitalgespräch Folge 45
Digitale Forensik

Mit Felix Freiling von der Friedrich-Alexander-Universität Erlangen-Nürnberg, 12. Dezember 2023
https://zevedi.de/digitalgespraech-045-felix-freiling/

[Der Vorspann mit Musik und Ausschnitten aus dem Gespräch beginnt.]

Marlene Görger [mg]: „Herr Freiling, Sie sind Informatiker, Professor für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. In Ihrer Arbeit befassen Sie sich intensiv mit forensischer Informatik."

Felix Freiling [Freiling]: „Das wird zunehmend spannender, weil ja überall Digitaltechnik in unsere Umgebung eingebaut sind." – „Das, was gut ist für die Forensik, äh, ist schlecht für die Privatsphäre."

Petra Gehring [pgg]: „Lässt sich das immer machen, ohne kaputt zu machen, oder müssen Sie manchmal auch den Zustand des Datenträgers zerstören?"

[Freiling]: „Wir haben Experimente gemacht mit Studierenden, die mussten fälschen. Die haben eine Festplatte gekriegt und sie sollten mal den korrupten Beamten spielen." – „Typische Einsatzgebiete von KI: Immer da, wo KI auch von den Straftätern eingesetzt wird, wird auch von den Ermittlungsbehörden [lacht] KI eingesetzt." – „Eine richtige Untersuchung der Wirksamkeit von KI auf Echtfällen kenne ich nicht." – „Es gibt einen Zweig der digitalen Literaturkritik. - Also es ist wirklich eine ganz, ganz faszinierende Anwendung von diesen Methoden, die wir hier entwickeln." – „Man braucht so eine intelligente Digitalisierung – das impliziert jetzt auch ein bisschen, dass manche Sachen vielleicht nicht digitalisiert werden dürfen, weil sie vielleicht für die Gesellschaft so wichtig sind."

[Der Vorspann endet, das Gespräch beginnt.]

[mg]: „Wenn Verbrechen geschehen, fordert die Gesellschaft Aufklärung. So alt wie die Idee des Gesetzes ist wohl auch die Erwartung von Strafe bei Verfehlung. Was als Verbrechen gilt und welche Verfahren zu einem gerechten Urteil führen, das hat sich über die Jahrtausende freilich dramatisch verändert. Heute, in einer von Rationalität und humanistischen Werten geprägten Demokratie, fordern wir, dass Gerichte auf Basis von belastbaren Beweisen und sorgfältiger Abwägung entscheiden. Dazu gehört die Erwartung, dass Ermittlungsbehörden kriminelle Handlungen mit wissenschaftlich-technischen Mitteln untersuchen. Ein hoher Stellenwert kommt dabei der Sicherung und Auswertung von Beweismitteln zu. Denn diese stummen Zeugen haben besondere Überzeugungskraft, versprechen Objektivität und Verlässlichkeit. Technischer wie wissenschaftlicher Fortschritt schlägt sich dabei auch in der Welt der Verbrechen und

ihrer Aufklärung nieder. Verräterische Korrespondenz, Blutspuren oder Fußabdrücke haben schon in der Antike Mörder:innen und Dieb:innen entlarvt. Fingerabdrücke und DNA-Spuren wurden für Kriminelle erst im 19. und 20. Jahrhundert zum Problem. Und noch neuer ist nicht nur das Konzept des Cybercrime, sondern sind auch die Spuren, die wir im digitalen Raum hinterlassen. Mit ihnen befasst sich die digitale Forensik. Was genau steckt hinter diesem Begriff? Was sind das für Spuren, die wir auf unseren Endgeräten oder im Netz hinterlassen, mit denen sich Ermittler wie auch Kriminelle auseinandersetzen? Und: In welchen ganz anderen Szenarien abseits der Polizeiarbeit sind die Techniken der digitalen Forensik nützlich? Das ist unser Thema heute im *Digitalgespräch*. Mein Name ist Marlene Görger. Ich bin Physikerin und Technikphilosophin und arbeite am Zentrum verantwortungsbewusste Digitalisierung."

[pgg]: „Und ich bin Petra Gehring, Professorin für Philosophie an der Technischen Universität Darmstadt. Wir begrüßen als Gast im *Digitalgespräch* – wie stets – einen Experten für unser Thema. Wir dürfen mit Professor Dr. Felix Freiling sprechen. Er ist über Videokonferenz zugeschaltet aus Erlangen. Hallo und herzlich willkommen im ZEVEDI-Podcast, Herr Freiling! Wir freuen uns sehr auf das Gespräch mit Ihnen."

[Freiling]: Ja, hallo Frau Gehring und hallo Frau Görger."

[mg]: „Herr Freiling, Sie sind Informatiker und Professor für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Zudem sind Sie Mitglied im Direktorium des bidt, dem *Bayerischen Forschungsinstitut für Digitale Transformation*. In Ihrer Arbeit befassen Sie sich intensiv mit forensischer Informatik und IT-Sicherheit und sind hierzu ein gefragter Experte, zum Beispiel für das Bundesverfassungsgericht. Neben der Weiterentwicklung der technischen Möglichkeiten in diesem Feld ist Ihnen aber auch die Ausbildung von qualifizierten Fachleuten ein Anliegen. Sie haben die ersten dezidierten Studiengänge für forensische Informatik in Deutschland mitkonzipiert und bieten an verschiedenen Hochschulen Lehrveranstaltungen zu digitaler Forensik an. Was genau lernen Studierende da?"

[Freiling]: „Das ist zunächst mal natürlich eine informatische Ausbildung, die die da mitmachen. Das heißt erst mal, die Technik zu verstehen, die ausgewertet wird. Aber im Wesentlichen lernt man da so ein bisschen so die, dieses forensische Mindset, sage ich immer: Das, was wichtig ist bei der forensischen Arbeit, nämlich präzise zu sein, genau, äh, zu gucken, wie Sachen funktionieren, und die Mechanismen dahinter zu verstehen, damit die Schlüsse, die man aus den Spuren zieht, die auf den digitalen Asservaten enthalten sind, dass die auch möglichst, ja, richtig sind, damit man möglichst wenige Fehler macht bei der Interpretation dieser Daten."

[pgg]: „Gehören dazu auch juristische Kenntnisse der Polizeiarbeit?"

[Freiling]: „Genau. Also in den Studiengängen zur digitalen Forensik, äh, ist es so, dass die Studierenden natürlich technische Sachen lernen, die informatischen Grundlagen usw. und auch die technischen Methoden der Datenauswertung, aber das ist auch ganz

wichtig, und das ist, glaube ich, immer eine wichtige Säule in der forensischen Ausbildung, dass da auch die juristische Begleitausbildung noch stattfindet. Ähm, Begleitausbildung ist wahrscheinlich zu wenig gesagt. Also jede forensische Arbeit muss immer, egal ob es bei der Polizei ist oder im privaten Bereich, jede forensische Arbeit muss immer, ja… in, in einen prozeduralen Kontext eingebettet sein. Äh, und bei der Polizei ist das im Wesentlichen die Strafprozessordnung, die beschreibt, was die Polizei machen darf und was nicht machen darf. Und im Privaten sind es so Datenschutzregelungen, arbeitsrechtliche Regelungen zum Beispiel, Regelungen des Zivilrechts. Und da muss man natürlich sich auch auskennen. Die Informatik sagt immer, was man machen kann, und die [lacht] Rechtswissenschaften sagen, was man machen darf. Und das ist immer ein ganz guter, ganz guter Ausgleich miteinander."

[mg]: „Sie haben jetzt einen Ausdruck gesagt im ersten Satz, da müssen wir, glaube ich, erstens einhaken, zweitens können wir da, glaube ich, gut einsteigen: digitale Asservaten. Das ist sozusagen das, mit dem man dann zu tun hat. Was umfasst das alles?"

[Freiling]: „Also es gibt ja diese zwei großen Bereiche der digitalen Forensik. Das ist einmal dieser strafrechtliche, strafprozessuale Forensikbereich, wo im Wesentlichen die Polizei agiert und die Strafverfolgungsbehörden agieren. Und dann gibt es noch so einen großen Bereich, äh, den man auch als digitale Forensik bezeichnet, der so im Unternehmen stattfindet. Also im Grunde ist es so, dass immer wenn irgendwo was Böses passiert [lacht], irgendwie eine Straftat oder halt ein IT-Sicherheitsvorfall oder sowas, dann muss natürlich rausgekriegt werden, was da passiert ist, und am Ende natürlich auch, wer es war. Wenn es im öffentlichen Bereich passiert, wo die Polizei aktiv ist, dann ist es halt so diese, ich sage mal, klassische kriminaltechnische Arbeit, äh, die bei den Strafverfolgungsbehörden, bei der Kriminaltechnik immer angesiedelt ist. Wenn's im privaten Bereich passiert, da sind dann natürlich erst mal die Unternehmen gefragt. Also, was ist es für eine Straftat? Was ist es für ein Delikt, der stattgefunden hat? Ist es irgendwie ein arbeitsrechtliches Delikt, weil irgendwie ein Systemadministrator, äh, seine Kompetenzen überschritten hat? Oder ist man tatsächlich von außen angegriffen worden? Das wird erst mal sozusagen intern, äh, durch die IT-Sicherheitsabteilung, wo auch Forensiker dann dazu gehören, herausgekriegt, ne? Und dann unter Umständen dann auch in diesen öffentlichen, in diesen Polizeiforensikbereich dann eingestiegen. Und, äh, die Asservate, das ist jetzt eher so ein Begriff aus dem Polizeiforensikbereich. Das sind halt die Beweismittel, die gesichert werden. Also das ist im Wesentlichen schon Datenträger, wenn man so will. Also, alles das, was man, dessen man sich physisch habhaft machen lassen kann, und Asservat ist halt dieser Begriff aus dem polizeilichen Bereich, da gibt es die Asservatenkammer. Asservate sind dann halt die, die Beweismittel, die dann im schlimmsten Fall oder im besten Fall dann auch vor Gericht, äh, eine Rolle spielen. Und die muss man natürlich dann gut behandeln. Das ist aber auch der zentrale Untersuchungsgegenstand dann von, äh, Forensikern."

[mg]: „Das heißt, wenn man dann von digitalen Asservaten spricht, das sind dann Geräte, die dann ausgewertet werden?“

[Freiling]: „Genau. Das ist immer so die Idee, die auch immer ganz plakativ ist, die ich auch immer in so Vorträgen versuche deutlich zu machen: Ich zeig den Leuten ein, ein Büro, wo ganz normale Sachen stehen – also es könnte auch bei Ihnen oder bei mir das Büro sein – da stehen Computer, da stehen, da steht ein Telefon, da steht ein Laptop, äh, eine Digitalkamera, CDs liegen da rum und ich frag die Leute dann: ‚Ja, wenn, wenn es jetzt eine digitale Straftat gegeben hat, wie zum Beispiel Steuerhinterziehung oder sowas oder sagen wir Unternehmensuntreue oder sowas, ja? Und Sie kommen hierhin, was würden Sie denn alles mitnehmen, ja?‘ Und das, was man dann mitnimmt, das sind die Asservate. Wenn es auch drum geht, bei… ob da Fingerabdrücke drauf sind, kommen die natürlich in so Tüten rein, um, äh, die Authentizität und Integrität zu sichern. Genauso wie man es aus dem Fernsehen kennt, so vom Tatort. Aber im Wesentlichen: Wenn es nur um die digitalen Daten geht, äh, werden dir die Computer einfach abgestöpselt, rausgetragen [lacht] und, äh… zur Polizei geschafft. Das sind dann die Asservate, die kriegen alle eine Nummer, äh, damit man sie genau referenzieren kann und nachvollziehen kann, was mit ihnen passiert ist. Und dann werden im Wesentlichen im nächsten Schritt dann die, die Datenträger, äh, die da drin eingebaut sind, ja, ausgewertet, ausgeschraubt, normalerweise. Bei Handys ist das bisschen schwieriger, aber da gibt's andere Methoden, an die Daten ranzukommen. Äh, das sind die, die Asservate, die man da betrachtet.“

[pgg]: „Lässt sich das immer machen, ohne die kaputt zu machen, oder müssen Sie manchmal auch den Zustand des Datenträgers zerstören, um dranzukommen?“

[Freiling]: „Standardmäßig… Also es kommt immer auf das Asservat an, was man untersucht, ne? Und das wird zunehmend spannender, sagen wir es mal so, ja? Also, weil ja überall Digitaltechnik in unsere Umgebung eingebaut sind. Das heißt, äh, klassisch waren es natürlich dann die PCs, äh, die man mitgenommen hat, ne? Wo dann die Festplatten drinne waren, die man tatsächlich noch ausschrauben konnte, und die waren auch alle unverschlüsselt usw., ne? Heutzutage ist natürlich… ein großer Teil der digitalen Asservate sind Smartphones, die kann man nicht mehr aufschrauben, jedenfalls nicht mehr so einfach aufschrauben. Äh, im Prinzip: Wenn man sie aufmacht, macht man sie kaputt. Was, was es auch noch gibt, sind natürlich diese ganzen Smartwatches jetzt mittlerweile, die sind ja so hochintegriert, äh, da kann man ja nicht mal mehr den Akku wechseln. Was es auch noch alles gibt, sind so, was weiß ich, intelligente Kühlschränke, Waschmaschinen haben ja jetzt mittlerweile auch irgendwie Internetanschluss, intelligente Thermostate, diese ganze Smart-Home-Thematik, das ist dann zunehmend so ein bisschen esoterisch, da kann man auch nicht so richtig von vornherein sagen: Wie kommt man da eigentlich an die Daten dran? Vielleicht kann ich ein Beispiel bringen, was wir jetzt neulich, äh, mal analysiert hatten. Also da ging es um die Spuren, die auf so einem digitalen Fahrradcomputer gespeichert sind. Also die E-Bikes haben ja mittlerweile alle so einen Steuerrechner dran, und wenn man den aufmacht, da gibt es dann entsprechende, äh, Speicherbausteine, die man erstmal

identifizieren muss, und bei einem neueren System, was wir da analysiert haben: Da ging es nicht anders, da musste man tatsächlich den Speicherchip von der Platine runterlöten und selber in, in so eine Fassung einlöten, um den auszulesen. Und das ist sozusagen der letzte… das letzte Mittel der Wahl, ne? Also auch die Polizei zum Beispiel, wenn es darum geht, hochwichtige Smartphones zum Beispiel auszuwerten, da geht es auch manchmal nicht anders, als dass man die tatsächlich kaputt macht, äh, um an die Speicherbausteine zu kommen, um sie auszulesen."

[mg]: „Wie ist das denn mit, ähm… Geräten, die schon zerstört sind? Also wo jemand versucht hat, zum Beispiel auch digitale Spuren zu vernichten. Wie weit kommen Sie denn da in der Rekonstruktion?"

[Freiling]: „Also das passiert gar nicht so selten, dass die Straftäter versuchen, die digitalen Spuren zu vernichten. Dadurch, dass sie entweder Festplatten in den Fluss schmeißen oder versuchen, in der Mikrowelle die Festplatten kaputt zu machen [lacht] oder zu verbrennen oder mit einem Hammer draufschlagen oder so, ja? Manche Leute, die versuchen dann auch, was weiß ich, so Chipkarten zu zerschneiden, damit die Polizei nicht drankommt. Aber gerade bei Chipkarten zum Beispiel ist es so, dass der eingebaute Chip, der ist wirklich winzig, also da muss man sehr, sehr genau schneiden, [lacht] um den zu treffen. Und auch wenn der Chip teilweise beschädigt ist, kann man dann immer noch tatsächlich unterm Mikroskop halt, äh, Drähte anlöten und dann, äh, die Daten auslesen. Und bei Festplatten da ist es noch viel schwieriger, äh, auch wenn die korrodiert sind oder sowas. Es gibt ja dieses Beispiel von einer Festplatte, die im, im Space Shuttle *Columbia* drinne war, was ja beim Eintritt in die Erdatmosphäre Anfang der 2000er ja verglüht ist. Und da ist dann tatsächlich auf so einem Acker in Texas [lacht] so eine Festplatte aufgeschlagen, aus diesem, äh, aus diesem Space Shuttle, und da hat man tatsächlich noch einen Großteil der Daten rauskitzeln können. Das waren so Forschungsdaten, und die Physiker, die damals mit den Daten gearbeitet, die Experimente gemacht haben, haben sogar noch ein Papier publiziert, äh, auf Basis dieser Daten. Also es ist wahnsinnig schwierig, Daten aus solchen Speichermedien tatsächlich vollständig zu zerstören. Bei rotierenden Festplatten ist das vielleicht noch einfacher. Es gibt ja auch so, so Festplattenhäcksler. Also im Prinzip, wie wenn man Papier häckselt, gibt es auch so Geräte, wo man eine Festplatte reinmachen kann, und die wird dann so zerstört, dass sie im Prinzip nicht mehr rekonstruierbar ist. Aber bei so Speicherbausteinen ist das dann schon wieder noch ein Tick schwerer."

[pgg]: „Aber ganz normale Haushaltsgeräte können dann auch zum stummen Zeugen werden, unter Umständen, je nach Ablauf? Was weiß ich, wenn die Waschmaschine beim Tathergang eine Rolle gespielt haben könnte – wird die dann auch?"

[Freiling]: „Genau. Ja. Ich glaube, das, das sind noch so, so Spurenquellen, die zum großen Teil einfach noch so ungenutzt rumliegen, ne? Also, äh, man weiß ja manchmal gar nicht, was diese intelligenten Systeme da alles so speichern. Ähm. Also der Fahrradcomputer ist jetzt nur das eine Beispiel. Da sieht man natürlich, wann gefahren wurde, wohin gefahren wurde und auch wann angehalten wurde, wann das Fahrrad

mal stand, wann irgendwelche Knöpfe gedrückt worden sind. Analog gibt es halt auch entsprechende Spuren in Autos, ne? Also, Autos speichern ja im Prinzip alles, äh, was da vor sich geht. Also das Beispiel, was ich mal aus, aus der Praxis gehört hab, war, dass, äh, die Polizei ein Auto verfolgt hat und es kam darauf an, wer der Fahrer tatsächlich war. Und als sie das Auto dann erreicht haben, dann stieg der Fahrer aus, war auch ein Beifahrer dabei. Der Fahrer war, äh, nüchtern und der Beifahrer [lacht] war stockbetrunken. Als dann später die Auto-Telematik ausgewertet wurde, hat man gesehen, dass tatsächlich nach der Entdeckung des Fahrzeugs und der kurzen Verfolgung das Fahrzeug angehalten hat. Die Sitzsensoren von Fahrer- und Beifahrersitz haben angezeigt, dass hier mal kurz niemand gesessen hat. Also die Türen sind aufgegangen, niemand saß, dann saßen wieder beide, ne? Und dann wurde weitergefahren. Und das war – da war natürlich der Verdacht, lag der Verdacht sehr nahe, dass die tatsächlich die Plätze getauscht haben. In dem Bereich war es, glaube ich, sogar so, dass die Sitzsensoren das Gewicht gemessen haben, der Leute, das ist ja heutzutage auch wichtig, um sozusagen die Sitzdämpfung usw. einzustellen. Da hätte da ja noch jeder behaupten können: Ja, wir sind mal ausgestiegen, sind wieder eingestiegen, aber da war tatsächlich auch das Gewicht vertauscht, ne? Also das ist dann – wenn man den Daten dann trauen kann, das ist ja immer die Frage – dann ist natürlich eindeutig, was passiert ist. Also solche Sachen findet man dann, ne? Und, äh, das ist natürlich für die Polizei sehr, sehr aufschlussreich."

[mg]: „Das kann ich mir vorstellen. Merkt man natürlich auch, wie interessant dann auch diese ganzen Aufzeichnungen sind, die Geräte von uns den ganzen Tag machen."

[Freiling]: „Also diese ganze Instrumentierung des privaten Haushaltes mit diesen intelligenten Lautsprechern, intelligente Bilderrahmen zum Beispiel, das sind ja diese Dinger, die kann man sich an die Wand hängen und die laden sich aus dem Internet dann Bilder und zeigen die an oder das Wetter oder sowas, ne? Das sind ja alles Sachen, wenn man mit denen interagieren kann, ne, dann speichern die auch Daten intern ab. Das ist natürlich dann auch eine reichhaltige Quelle, ne? Also da kann man fragen: War jemand zu Hause zu der Zeit, ne? Oder die schneiden ja dann teilweise auch Ton mit: Hat jemand gerufen oder was ist da passiert in der Zeit, wo tatsächlich fraglich eine Straftat stattgefunden hat? Aber natürlich auch solche Sachen: Wurde da irgendwie ein Küchengerät bedient zu der Zeit, ne? Oder hat jemand was an- oder ausgeschaltet? Das sind alles Daten, die heutzutage in diesen Geräten gespeichert sind. Da ist es gar nicht mehr so sehr das Problem, ob solche Daten tatsächlich am Tatort vorliegen, sondern einfach, wo die sind und wie man die rauskriegt aus den Geräten. Und das ist natürlich auch ein ganz deutlicher Fingerzeig darauf, dass digitale Forensik auch sehr viel zu tun hat mit Privatsphäre oder mit der digitalen Privatsphäre. Das, was gut ist für die Forensik, äh, ist schlecht für die Privatsphäre, wenn man so will, ne? Und das, finde ich, ist auch ein sehr schöner Gegensatz, sozusagen in der Arbeit, den ich sehe, weil ich ja auch prinzipiell jemand bin, der für Privatsphäre ist und Privatsphäreschutz, und deswegen ist auch dieser Bezug zu den juristischen oder den rechtlichen Gegebenheiten wichtig, dass man auch Einschränkungen dahingehend hat, was man darf, ne? Und nicht nur, was man kann."

[mg]: „Bei welcher Art von Verbrechen sind denn diese alltäglich anfallenden Daten wirklich besonders hilfreich? Also ich kann mir vorstellen, ich muss immer so ein bisschen denken an eine Analogie zu Fingerabdruck und dem Handschuh. Also jemand, der wirklich, der weiß, dass er einen Einbruch plant, der wird sich vielleicht Handschuhe anziehen."

[Freiling]: „Hmhm."

[mg]: „Und, äh, ein Haarnetz oder so, also einfach die Spuren, von denen man weiß, dass man die wahrscheinlich hinterlässt, vermeiden. Das würde man dann ja auch versuchen, in diesem digitalen Feld zu machen. Also ist das irgendwie, dass man solche Spuren findet, ist das eher was, was so in so einem etwas weniger technisch versierten Umfeld anfällt? Also ist es noch mal sozusagen, wenn man es mit, mit Profis zu tun hat, die sich auch im Digitalen auskennen, schwieriger?"

[Freiling]: „Ja, das ist so, äh, aber das ist wie mit jedem Verbrechen. Die Erfolge der Polizei basieren immer auf Fehlern, die die Straftäter machen – immer. Ja, wenn die Straftäter keine Fehler machen, dann kann man sie auch nicht kriegen. Die Erfahrung zeigt aber natürlich, dass es wahnsinnig schwierig ist, keine Fehler zu machen, als Straftäter. Insbesondere wenn man vielleicht ein Ding gedreht hat und keinen Fehler gemacht hat. Da hat man vielleicht Glück gehabt, ne? Aber sozusagen fortgesetzt Kriminalität durchzuführen und dabei keine Fehler zu machen, das ist das Problem [lacht] , glaube ich. Deswegen empfehle ich auch niemandem, sozusagen eine kriminelle Karriere zu starten, weil irgendwann macht man halt den Fehler, ne? Und dann kriegt einen die Polizei. Das ist der, der lange Atem des Gesetzes, ne? Also was man in der Praxis halt sieht: Es gibt diesen, diesen großen Phänomenbereich der illegalen Inhalte, ne? Also der Kinderpornographie, Propaganda und Extremismus natürlich. Das ist eigentlich ein sehr gut verstandener Bereich in der digitalen Forensik, wenn es drum geht, den Nachweis zu führen, dass, äh, dass der Besitz vorliegt, ne? Das heißt, wenn man irgendwo durchsucht, zum Beispiel, dann, ähm, findet man halt Datenträger, wo solche Dateien drauf sind. Was viele Leute nicht verstehen, ist, dass der reine Besitz juristisch interpretiert was anderes ist als die Existenz von Dateien strafbaren Inhalts auf der Festplatte. Man muss auch noch sozusagen den Vorsatz nachweisen, ne? Den, den subjektiven Tatbestand, heißt es dann bei den Juristen. Also man muss nachweisen, dass die Leute das auch haben wollten, ja? Also, dass eine Intention da lag. Und da weiß man heutzutage eigentlich auch relativ gut, wie das geht. Das heißt, irgendwo Vorschaubilder in irgendeinem Cache zu finden, ist was anderes, als wenn man halt zehntausende Bilder fein sortiert in irgendeiner selbstgewählten Begriffshierarchie bei den persönlichen Daten findet, ne?"

[mg]: „HmHm."

[Freiling]: „Aber natürlich auch solche Spuren, wo es um den Austausch von Daten geht, ne? Also File-Sharing-Plattformen, äh, zum Beispiel, da entstehen ja auch immer Spuren.

Und der Großteil der Straftäter da ist, ja… sagen wir mal, relativ unbedarft. Da ist der Nachweis relativ einfach. Was anderes ist es, äh, wenn man es halt mit, ähm, ja, Professionellen zu tun hat, ne? Also die dann tatsächlich, äh, Handel treiben, auch gegen Bezahlung mit solchen Inhalten. Die haben natürlich dann etwas höhere Sicherheitspraktiken, die sie an den Tag legen. Die schulen sich auch gegenseitig immer. Die benutzen das Tor-Netzwerk zum Beispiel und, äh, verschlüsseln ihre Dateien. Da ist es dann schon ein bisschen schwieriger und da ist es dann auch weniger ergiebig, einfach nur eine offene Durchsuchung zu machen, äh, und dann zuzugreifen und an die Daten ranzukommen. Da reichts im Prinzip schon, wenn, äh, die Straftäter dann den Strom abstellen von ihren Rechnern, dann fährt der halt noch nicht mal runter. Der ist dann einfach aus, ne? Und wenn er aus ist, dann ist die Festplatte wieder zu, dann ist sie verschlüsselt, und dann kann die Polizei machen, was sie will, und kommt an die Daten nicht ran. Das heißt, in solchen Fällen muss man halt sehr aufwendig bei der Polizei die Infrastrukturen vorab aufklären, das heißt also verdeckt arbeiten. Das kann man auch teilweise unter Forensik, äh, auch noch fassen, ne? Also solche, solche verdeckten Maßnahmen. Das ist dann so, diese TKÜ-Maßnahmen, also Telekommunikationsüberwachung, oder die, das, was ja, was man als Onlinedurchsuchung kennt, ne? Aber das muss man dann halt auch einsetzen gegen solche professionelleren Täter. Aber der Großteil, äh, der Leute, die Cyberkriminalität begehen, ist tatsächlich noch in diesem Bereich, wo relativ wenig Vorsichtsmaßnahmen getroffen werden."

[pgg]: „Das klingt sehr speziell, auch was Sie im ganz konkreten Fall dann einbringen an Ideen und Wissen, wie man noch Spuren finden könnte, wo welche sein könnten usw. Sind Sie oder sind ihre Leute dann da mit vor Ort? Oder können da, äh, vor Ort, sage ich mal, die handfesten Ermittler schon entscheiden, was mitgenommen werden muss und wo noch Spuren wären?"

[Freiling]: „Ja, das ist ein großes Problem, heutzutage noch, in der digitalen Forensik. Man hat einfach so viele Daten und man weiß nicht, wo man zuerst hinschauen soll – sagen wir es mal so, ne? Also in der klassischen Kriminaltechnik, da gibt es mittlerweile eigentlich ein sehr gutes Verständnis dafür. Es gibt ein paar wenige gut untersuchte Spurenklassen. Das ist halt Fingerabdrücke, DNA, Faserspuren zum Beispiel. Man weiß sozusagen als Kriminaltechniker oder auch, auch schon so als normaler Streifenbeamter, wenn man halt an den Tatort kommt, was,… wo man aufpassen muss, ja? Was darf man nicht verunreinigen oder sowas, und was sind die Spuren, die tatsächlich einen besonders hohen Beweiswert haben. Dieses Verständnis, das hat man in der digitalen Forensik noch nicht. Das gibt es vielleicht in Ansätzen, äh, in gut verstandenen Bereichen, wie zum Beispiel halt, äh, illegale Schriften, ne, was ich eben gesagt hab. Ähm, aber so generell: Es gibt einfach so viele Spuren [lacht], ne? Und, äh, wo man zuerst hinschaut, das ist unklar. Das steckt momentan noch in den Köpfen von so den erfahrenen Cyberermittlern drinne, ne, die vielleicht schon viele Fälle gesehen haben. Aber das ist auch schwer irgendwie zu fassen. Und das ist auch ein aktiver Forschungsgegenstand bei uns, dass wir einfach Wege und Methoden entwickeln wollen, wie man diese, diese Erfahrungen, also welche Spuren sind für welche

Deliktarten relevant und wo findet man die, tatsächlich aus den Köpfen von den Ermittlern rauskriegt und so irgendwie fassen kann, dass das in die Ausbildung mit einfließen kann, so dass die neuen Generationen von Forensikern dann auch besser werden. Das Problem ist dabei natürlich, dass, äh, die Technologien einfach so voranschreiten. Und wenn man heutzutage sagt: Man muss in der Registry von *Windows* an der und der Stelle gucken und da steht das und das drinne. Bei der nächsten Version von *Windows* ist es dann wieder anders, ne? Das heißt, man muss auch so den richtigen Abstraktionsgrad der Spurenarten finden, ne? Also es gibt so eine, so eine grobe Klassifizierung von, von Spurenarten. Das eine sind so Kommunikationsspuren, die sind relativ wichtig: Wer hat mit wem wann was ausgetauscht, ne? Und das andere sind so Spuren, wo man sozusagen die Existenz von Sachen nachweisen kann und die, die bewusste Existenz von Sachen auf Festplatten, ne? Also sowas, was ich eben gesagt habe: Man findet strafbare Inhalte und man möchte gerne nachweisen, dass die intendiert, sozusagen, beschafft worden sind. Also, das sind so zwei generelle Spurenarten, die sich so ein bisschen abzeichnen. Da braucht man halt auf diesem Abstraktionsgrad auch noch weitere Verfeinerungen, damit man irgendwann mal zu sowas kommt wie so einem digitalem Fingerabdruck – was immer das auch ist, dann im digitalen Bereich, weil so diesen Bezug zur Person gibt es ja eigentlich nicht, weil das ist ja alles digitale Daten, das kann auch beliebig manipuliert werden. Obwohl wir jetzt sehen, dass durch diese Smartwatches, äh, oder diese Fitnesstracker eine neue Klasse von Spuren Einzug hält in die digitale Forensik, weil die ja die ganze Zeit und Körperfunktionen aufzeichnen, ne? Das geht so in die Biometrie rein, ne? Die Körperfunktionen sind schon erstens mal charakteristisch für eine individuelle Person und zweitens mal auch schwer zu manipulieren, ne, so ohne dass man es merkt, ne? Das könnte so ein Ansatz dafür sein, dass es so eine Art digitale DNA gibt, ne? Aber das ist auch noch aktuelle Forschung [lacht] aktuell."

[pgg]: „Da hätte ich jetzt auch im Grunde noch mal gefragt, ob das Unterschieben von digitalen Spuren oder Hinweisen leicht möglich ist oder schwer möglich. Also, dass es mit den Smartwatches ziemlich schwierig ist, weil da ja so eine Art physische Signatur der Person drinsteckt, das kann ich mir gut vorstellen. Aber wie ist es jetzt mit so einem PC oder so?"

[Freiling]: „Hmhm. Ja, das dachte man früher. Also früher, in den Anfängen der digitalen Forensik, also vor bis vor zehn Jahren vielleicht, war eigentlich so die allgemeine Ansicht, dass es leicht ist, digitale Spuren zu fälschen, ne? Und dass es leicht ist, jemandem da Daten unterzuschieben, ne? Natürlich ist es weiterhin leicht am Tatort – ja, das ist so das Analogon zu, äh, der korrupte Polizist lässt einfach ein Päckchen Drogen fallen am Tatort und ‚findet' das dann in Anführungsstrichen – das gilt natürlich weiterhin, ne? Also man kann auch am Tatort einfach eine Speicherkarte fallen lassen, ne? Aber wo man immer Angst hatte, war der Umstand, dass wenn die Polizei die, die Festplatte jetzt mitnimmt, ist es dann nicht möglich, nachträglich, ohne dass man es merkt, digitale Spuren, ne, – also im Prinzip, Bits auf der Festplatte – so zu verändern, dass es irgendwie ganz anders aussieht, äh, als wie es wirklich war? Das ist eine Befürchtung, die haben wir tatsächlich auch mal experimentell untersucht, ne? Das heißt, wir haben Experimente gemacht mit

Studierenden, äh, die mussten fälschen, ja? Also das heißt, das Szenario war: Die haben eine Festplatte gekriegt und sie sollten mal den korrupten Beamten spielen, der zum Beispiel auf einer Festplatte so tun sollte, als wenn tatsächlich jemand auf einer Website gesurft, ohne dass er es tatsächlich gemacht hat, ne? Das heißt, sie mussten die Festplatte dahingehend fälschen und dann anschließend haben wir die Fälschungen genommen und wir hatten tatsächlich auch Originale, das heißt Festplatten, wo tatsächlich zu der Zeit auch jemand auf dieser Seite gesurft war. Und dann haben wir die sozusagen gemischt und den Leuten wieder zur Untersuchung gegeben und die mussten dann unterscheiden: Ist das jetzt eine Fälschung oder Original? Und die Erkenntnis davon ist, dass eigentlich alle Fälschungen entdeckt wurden und alle Originale auch korrekt klassifiziert wurden. Das heißt, das ist so ein Indiz dafür, dass das Fälschen doch schwieriger ist, als es, äh, vielleicht den Anschein hat. Aber da gibt es auch Unterschiede, ne? Also wir haben das Experiment dann in verschiedenen Varianten mal wiederholt. Ähm… das heißt, das Hinzufügen von Material ist schwieriger als das Löschen von Material, also das Überschreiben von Material, ne? Also so, dass es noch konsistent bleibt. Aber das ist auch Gegenstand aktueller Forschung, wie schwierig es eigentlich ist, digitale Spuren zu fälschen. Aber so von, von der Grunderkenntnis her ist es dann noch schwieriger als man denkt."

[mg]: „Ähm, in Ihrem experimentellen Setup war es jetzt, wenn ich das richtig verstanden habe, so, dass man schon wusste, man soll überprüfen, ob es sich um eine Fälschung handelt oder nicht, ne? Ist das was, was man routinemäßig dann immer macht, oder ist es dann so offensichtlich, dass das eigentlich jeder Fachmann sofort erkennt?"

[Freiling]: „Ja, in dem Experiment war es halt so, dass wir im Prinzip für die Ergebnisse, äh, bestmögliche Umstände haben sollten, ne? Das heißt, wenn man den Studierenden nicht gesagt hätte: Hier könnte gefälscht worden sein, dann hätten sie vielleicht eher das übersehen. Also ich habe auch immer die Praktiker gefragt, mit denen ich spreche: Habt ihr Beispiele für echte Fälschungen, ja? Fälle, wo das tatsächlich aufgetaucht ist? Und da gibt es so gut wie keine, ja? Jedenfalls die, die mir untergekommen sind, sind ganz, ganz wenige, ne? Insofern die erfahrenen Leute in der Praxis wissen zwar, dass man im Prinzip fälschen kann, aber das ist jetzt nicht so die erste Hypothese, mit der sie an den Fall rangehen. Aber es ist natürlich so: Wenn Ungereimtheiten auftauchen in Daten, die sie analysieren, dann wird natürlich genauer hingeschaut, ne? Und dann kann da tatsächlich auch diese Hypothese im Raum stehen: Ist da was manipuliert worden? Aber das ist zunächst mal nicht so der – jedenfalls, was ich aus der Praxis kenne – nicht so der erste Gedanke an den man,… den man hat."

[pgg]: „Setzen Sie auch KI ein oder spielt das irgendwie eine Rolle? Oder sind Sie so nah dran an der Hardware, dass das nicht naheliegt?"

[Freiling]: „Ja, es gibt so verschiedene typische Einsatzgebiete von KI. Immer da, wo KI auch von den Straftätern eingesetzt wird [lacht], wird auch von den Ermittlungsbehörden eigentlich KI eingesetzt. Also so beim Erstellen von Deep Fakes

zum Beispiel. Da wird ja, wird ja KI eingesetzt oft, andererseits gibt es dann auch KI, die dann versucht zu erkennen, ob ein Deep Fake, äh, gemacht worden sind. Also dieser ganze Bereich der, der Multimediasicherheit, Multimediaforensik oder Sprachaufzeichnungen, die vielleicht erzeugt worden sind mit KI, die synthetisch jemanden imitieren, ne? Da wird auch mit KI gearbeitet. KI ist halt immer dann gut, wenn man es tatsächlich mit Massendaten zu tun hat, ne? Diese Vorsortierung von Spuren, das heißt, wenn man 2 Millionen Bilder hat auf der Platte, man will die entscheidenden Missbrauchs-Bilderserien identifizieren, um die Opfer zu schützen, dann ist es natürlich gut – auch von, von der psychischen Beanspruchung der Beamten natürlich –, wenn man da irgendwie eine sehr, sehr gute Vorsortierung hat, ähm, von der Maschine. Aber es ist halt immer die Frage: Was sind sozusagen die Falschnegative? Was übersieht die KI? Das ist im Kontext von der Strafverfolgung halt die viel wichtigere Frage. Man möchte nichts übersehen und den Missbrauch sozusagen unterbinden, der vielleicht noch stattfindet. Und da scheiden sich so ein bisschen die Geister. Also da gibt es auch keine verlässlichen Zahlen. Die Zahlen, die die Hersteller von diesen KI-Programmen angeben, die sind natürlich immer positiv für die Hersteller. Und wir wissen ja, dass aus KI… also bei der Bewertung von KI ist es immer so, dass man da irgendwelche Testdatensätze braucht und dann fragt man sich: Wie repräsentativ sind die Testdatensätze? Aber so eine richtige Untersuchung der Wirksamkeit von KI, gerade zum Beispiel bei der Bildersortierung, auf Echtfällen kenne ich nicht, ne? Das müsste auch zum Beispiel mal gemacht werden, um so ein bisschen besseres Gefühl dafür zu kriegen, wie gut und wie wirksam diese Programme sind. Insbesondere vor dem Hintergrund, dass die Kriminalpolitik immer Druck macht, KI einzusetzen, aber die natürlich auch leicht den, den Versprechungen der Toolanbieter folgen, die dann natürlich ihre Tools anbieten wollen, die einen horrendes Geld kosten."

[mg]: „Wie kommen denn solche Toolanbieter dann auch an Trainingsdaten? Also gerade in dem Bereich ist das ja eine naheliegende Frage."

[Freiling]: "Hm, ja. Ich kann mir es nur vorstellen, dass sie halt kooperieren, äh, mit Strafverfolgungsbehörden, um die Trainingsdaten zu erzeugen. Aber wie sie es machen, ob die das synthetisch machen, das weiß ich nicht, ja? Das ist natürlich genau das entscheidende Problem, ne?"

[mg]: „Es gibt ja auch noch einen anderen Bereich von, äh, Cybercrime, der viel in der Öffentlichkeit auch diskutiert wird und große wirtschaftliche Schäden verursacht. Das sind so Hackerangriffe im Allgemeinen auf zum Beispiel Unternehmen, ja? Ransomware-Attacken, ne? So was in der Art. Wie oft ist die Polizei denn dann mit sowas tatsächlich befasst?"

[Freiling]: „Also, äh, immer wenn dem Unternehmen was passiert, ist erst mal das Unternehmen am Zug. Die Unternehmen sind immer so ein bisschen in dem Dilemma: Die Unternehmen möchten ja gerne möglichst schnell wieder operativ werden, ne? Auf der anderen Seite ist es natürlich auch wichtig, dass man die kriminellen Infrastrukturen, die hinter diesen Angriffen stecken, auch verfolgt. Viele Unternehmen versuchen das

erst mal selber, äh, in den Griff zu bekommen, ja haben da ihre eigenen Abteilungen, die, äh, damit befasst sind. Aber gerade kleinere Unternehmen haben halt auch nicht die Manpower, um mit diesen Angriffen zurechtzukommen. Dann wird natürlich Anzeige erstattet, die Polizei kommt. Bei den großen Unternehmen ist es mittlerweile so: Wenn die Polizei das Gefühl hat, die kommen schon alleine damit zurecht, ne, dann versuchen sie, auch diesen Prozess nicht zu stark zu behindern, und sichern einfach nur die Beweise, die sie brauchen, um Belege zu haben für den Bezug zu bestimmten Infrastrukturen, die im Hintergrund laufen. Das sind ja meistens irgendwelche Botnetze, die von kriminellen Gruppen betrieben werden. Und diese Erkenntnisse sind dann wieder wichtig für solche Zentralstellen, die es bei der Polizei mittlerweile gibt, ne? Also in, in Hessen gibt es das, das ZIT, dann in Nordrhein-Westfalen das ZAC und hier in Bayern ist es dieses ZCB, ne, die *Zentralstelle Cybercrime Bayern*. Das sind dann so Schwerpunktstaatsanwaltschaften, die diese verstreuten Indizien für die Aktivität von diesen kriminellen Banden dann in ein Verfahren integrieren und dann mit geballter Schlagkraft die kriminellen Infrastrukturen dahinter versuchen aufzuarbeiten. Das ist teilweise dann auch so ein bisschen entkoppelt von den konkreten Straftaten vor Ort, ne? Äh, aber nur so ist es dann tatsächlich möglich, die Ursache für, äh, Ransomware-Angriffe zum Beispiel dann auch systematisch zu bekämpfen. Und diese Zentralstellen, die diese Großverfahren dann so an sich ziehen, das ist in gewisser Weise auch so eine Erfolgsgeschichte der Polizeibehörden in der Bekämpfung von Cyberkriminalität."

[pgg]: „Das heißt, das sind dann eher ihre Partner, dass sie im Grunde versuchen, diesen Kriminellen das Handwerk zu legen, und so die, die schiere Datenrettung im Unternehmen, das kriegen dann wahrscheinlich die Sicherheitsexperten selber hin?"

[Freiling]: „Genau. Also da ist sozusagen die Selbstverantwortung der, der Unternehmen dann auch, äh, gefragt, ne? Selbstverantwortung ist natürlich vor allem auch Prävention. Das heißt also, dass man sich gut aufstellt für einen möglichen Hackervorfall. Die Grundannahme muss heutzutage eigentlich immer sein: Nicht ob ich Opfer eines Angriffs werde, sondern wann ich Opfer eines Angriffs werde, ne. Das heißt, man muss darauf vorbereitet sein, und nur wer vorbereitet ist, äh, hat dann auch sozusagen Chancen, einigermaßen konsequenzfrei aus so einem Vorfall rauszukommen. Das ist ein Punkt, wo man vielleicht auch sagen kann: Da könnte die Polizei auch noch ein bisschen mehr machen. So im Bereich der, der Cyberprävention, äh, bei Unternehmen. Das ist natürlich auch immer eine Ressourcenfrage. Aber im Wesentlichen ist auch die, der Schutz vor Cyberkriminalität sehr, sehr stark eine Präventionsaufgabe, ne? Also sowohl im Unternehmen wie auch im privaten Bereich."

[pgg]: „Es gibt noch ein ganz anderes Feld, in dem digitale Forensik helfen kann. Das ist die Auswertung von Festplatten aus Forschungsgründen jetzt gar nicht unter polizeilichem Blickwinkel, sondern einfach, um zu erforschen: Wie ist die benutzt worden? Beispielsweise habe ich mal erfahren, dass im *Deutschen Literaturarchiv* in Marbach Dichternachlässe, also, äh, die Arbeitsgeräte von Schriftstellerinnen, Schriftstellern, die heute auch eingeliefert werden, in solche Archive dann untersucht

werden, um zu rekonstruieren: Wie sind Texte entstanden, wie hat jemand gearbeitet? Stimmt das?“

[Freiling]: „Genau. Also das ist wirklich einer der faszinierenden Aspekte von der digitalen Forensik, ne? Also in digitaler Forensik steckt natürlich immer Datenrettung drinne, ne? Das heißt also, wenn Leute in meinem Umfeld mitkriegen, dass ich digitale Forensik machen, mache, dann kommen die teilweise zu mir und sagen: Ich habe hier eine Speicherkarte, da sind meine Urlaubsfotos drauf, die kann ich nicht mehr lesen, kannst du was machen? Äh, also das ist so eine der, der netten Vorteile, wenn man digitale Forensik macht, dass man auch noch mit Festplatten umgehen kann, die andere Leute nicht mehr lesen können, ne? Oder Speicherkarten. Aber natürlich geht das noch weiter. Alles das, was an Methodik entwickelt wird, äh, um rauszukriegen, was auf der Festplatte passiert ist, kann man natürlich auch für andere Zwecke einsetzen, ne? Und, äh, das ist tatsächlich so, also es gibt, äh, so einen Zweig, äh, der digitalen Literaturkritik, wenn man so will. Heutzutage arbeiten Dichter und Literaten ja nicht mehr nur auf Papier, sondern haben alle auch irgendwie Computer, mit denen sie ihre Lyrik oder ihre Romane schreiben. Und natürlich entstehen da, äh, nicht nur Dateien, die Endprodukte, sondern auch Zwischenprodukte, ne? Also, Sicherheitskopien zum Beispiel oder früher in *Word*-Dateien, äh, wurden ja auch so Änderungsmarkierungen zum Beispiel mitgespeichert, ne? *Google Docs*, ne? Wer *Google Docs* benutzt: *Google Docs* speichert die Dokumente nicht als eine Datei ab, sondern im Prinzip als Historie von Tastendrücken, ne? Das heißt, man kann im Prinzip ein *Google Docs*-Dokument vor- und zurückspulen mit exakten Zeitstempeln, ne, wann welche Taste gedrückt worden ist. Und das ist natürlich ein wahnsinniger Schatz für Literaturwissenschaftler, die rauskriegen wollen: Was hat sich jemand dabei gedacht, als er vielleicht irgendwie eine Variante, äh, gemacht hat? Früher hat man dann die Markierungen und die, die händischen Notizen am Manuskript dann versucht zu interpretieren. Und heute ist es so, dass man dann so Vorversionen vergleicht mit den Endversionen, ne? Oder Zwischenversionen und daraus versucht, irgendwie Interpretationsansätze zu liefern.“

[pgg]: „Ganz neue Perspektiven für die Editionswissenschaft.“

[Freiling]: „Ja.“

[pgg]: „Sich zu überlegen, wie man das dann tatsächlich auch edieren kann.“

[Freiling]: „Ja. Also das ist, äh, wirklich ein ganz, ganz faszinierende, äh, faszinierende Anwendung von diesen, äh, Methoden, die wir hier entwickeln.“

[mg]: „Wie funktioniert dann die Anwendung? Werden dann dieselben Experten dazugeholt, die auch ansonsten in der, also der Kriminalitätsbekämpfung unterwegs sind, oder entwickeln sich da auch eigene Fachlichkeiten?“

[Freiling]: „Die Leute, die das in der Forschung machen, die belegen halt die gleichen Kurse bei uns [lacht] wie dann auch die Polizisten. Also wir hatten jetzt auch kürzlich

einen Kollegen da aus den digitalen Literaturwissenschaften, der, der sich dafür interessiert hat, wie man Speicherkarten oder wie man Speicherchips ablötet, ne? Weil er den Fall tatsächlich auch hatte in einer Forschungsarbeit. Die lernen dann den Umgang mit den Tools. Ja, machen im Prinzip die Anwendung oder variieren, sagen wir mal so, variieren die Anwendung der Werkzeuge für einen Zweck, der bisschen anders ist als das, was die Polizei macht, ne? Aber im Prinzip die gleichen Methoden benötigt."

[mg]: „Die Forschung in dem Feld mal so allgemein gefragt, ähm: Ist die sehr bedarfsgetrieben, sage ich mal? Also: Es gibt einen Fall und es gibt noch nicht die technische Lösung, um an die Daten zu kommen? Oder gibt es irgendwie eine eigene, gibt es eigene Zielsetzungen, die jetzt unabhängig sind von dem, was die Polizei konkret tut, gerade."

[Freiling]: „Ja, das ist so ein bisschen die Entwicklung des Feldes. Das Feld selber der digitalen Forensik ist sehr, sehr stark… entstammt sehr, sehr stark praktischen Bedürfnissen. Äh. Und so ist das auch zu großen Teilen noch gestrickt. Das heißt, man hat einen Fall, äh, und man baut sich sozusagen die Methoden um diesen Fall herum, den man zu lösen hat. Erst seit vielleicht 15 Jahren oder sowas, äh, wo tatsächlich auch verstärkt eine akademische Forschung in dem Bereich gemacht wird, guckt man so allgemeinere Fragestellungen an, ne? Also die für auch mehrere Fälle, äh, sinnvoll sind. Also es geht um so generelle Fragen: Wie stellt man Integrität sicher, von Beweismitteln zum Beispiel, ne? Wie analysiert man Dateisysteme auf eine Art und Weise, dass es nicht so ad hoc ist, äh, wie das früher mal war? Aber dann auch Fragen nach Fälschbarkeit von Spuren oder sowas. Das sind alles so Sachen, die jetzt ja so erst in den letzten zehn Jahren aufgekommen sind und die versuchen, das Feld ein bisschen wissenschaftlicher zu machen – sagen wir es mal so, ne? Also die Forensik, äh, auch die klassische Forensik, Kriminaltechnik, ist ja eigentlich der Einsatz von wissenschaftlichen Methoden aus unterschiedlichen Fächern zur Beantwortung gerichtlicher Fragen. Das heißt, da steckt Wissenschaftlichkeit eigentlich drinne, ne? Deswegen müssen eigentlich die Methoden, die man in der digitalen Forensik auch anwendet, eigentlich wissenschaftliche Methoden sein. Das ist ja auch so ein bisschen der Kontext, weswegen wir hier in Erlangen dieses Graduiertenkolleg haben, „Cyberkriminalität und forensische Informatik", wo man zusammen mit den Juristen versuchen, einfach so eine wissenschaftliche Grundlage unter die digitale Forensik, wie sie momentan existiert, zu legen. Weil da gibt es noch viele Defizite, wenn man in die Praxis schaut, und das ist, denke ich, eine Entwicklung, die bestimmt noch, sagen wir mal, fünfzig bis hundert Jahre dauern wird. Erstens mal, bis sich die Technik ein bisschen stabilisiert hat, äh, und dann auch methodisches Verständnis für die digitale Forensik dann auch stabilisiert hat. Dann wird man vielleicht auch eher wissen, ob es so eine digitale DNA gibt oder nicht. Vielleicht haben wir die ja entdeckt, dann."

[pgg]: „Auf jeden Fall vermutlich auf Dauer ein sehr interdisziplinäres Gebiet, nicht nur wegen der rechtlichen Fragen, sondern Sie kommen ja, je tiefer Sie blicken, auch in die Verhaltensmuster der Leute hinein und damit in sozialwissenschaftliche Felder. Und so,

diese digitale DNA ist ja auch in hohem Maße, ja, so eine Art Sozialdaten oder Verhaltensdatenkörper?“

[Freiling]: „Genau. Es ist also wirklich sehr, sehr multidisziplinär. Also KI haben wir schon angesprochen, ne? Da ist diese ganze Biometrie-Geschichte Signalverarbeitung drinne, das ist so aus dem technischen Bereich, ne? Aber natürlich aus dem sozialwissenschaftlichen Bereich, äh, oder an der Grenze zur Rechtswissenschaft: Die Kriminologie, ne? Also die… ja, Verhaltensmuster von, äh, von Straftätern, äh, oder die Motivation von Straftätern, kriminell zu werden, kriminelle Handlungen zu vollziehen, die Ursachen dafür zu untersuchen, ne, die dann auch in diesen digitalen Daten drinne stecken… ist also ein sehr, sehr breites und interessantes Feld, ne? Und ja, da ist auch noch sehr, sehr viel Potenzial, weil auch die Kriminalitätsphänomene im digitalen Bereich sich auch stetig verändern und weiterentwickeln. Also, diese ganzen Ransomware-Sachen, die scheinen uns so normal heutzutage. Die sind aber relativ neue Phänomene, ne? Und man kann sich vorstellen, dass irgendwann, wenn das Auto mal total digital vernetzt ist, dann auch [lacht]… man fährt an die Tankstelle, das Auto ist vielleicht infiziert, ne? Ähm, man tankt, ne? Man will weiterfahren, und da sagt dann so einem das Auto: ‚Nee, äh, bevor du weiterfahren darfst, musst du erst mal 50 € bezahlen‘ und ‚kannst du direkt an der Tankstelle dann mit entsprechenden anonymen Zahlungsmitteln dann auch bezahlen‘. Und dann tankt man halt für 50 €, legt noch 50 € drauf, äh, um weiterfahren zu dürfen. Und, äh, ja, das könnte auch noch so ein schönes Kriminalitätsphänomen sein, was in der Zukunft passiert. Diese ganzen Onlinebetrugssachen, die auch auftreten, ne? Also, wo man dann auf der Grenze ist, wieder zur klassischen Kriminalität, äh, was man heutzutage auch hat: diese ganzen Schockanrufe zum Beispiel, die man auch jetzt zunehmend mit, äh, synthetisierten Stimmen machen kann. Das sind alles so Phänomene, die noch kommen werden. Und Aufgabe der Forschung ist es, sowas auch zu antizipieren, ne? Und, äh, den Straftätern so ein bisschen voraus zu sein, ne? Deswegen ist es aus meiner Sicht auch immer wichtig, diese offensive Forschung, die wir ja auch, auch viel machen, voranzutreiben. Also versuchen, Sachen anzugreifen, also auch forensische Tools anzugreifen, ne? Äh, und zu gucken, wo deren Schwachstellen sind. Umso dieses, dieses Katz-und-Maus-Spiel, was es so im Bereich IT-Security ja häufig gibt, einfach zu beschleunigen, äh, und dadurch die Qualität insgesamt der Werkzeuge, der Personen, der Prozesse zu erhöhen, so dass es einfach für die Kriminellen immer schwieriger wird, solche Straftaten zu begehen.“

[mg]: „Wie wichtig ist aus Ihrer Sicht das Verhalten der einzelnen Personen? Also muss sich jetzt jeder und jede ein Stück weit damit befassen und auskennen, auch im persönlichen Raum? Oder denken Sie, das sollte auf einer gesamtgesellschaftlichen politischen Ebene, wie auch immer, von Experten gelöst werden?“

[Freiling]: „Das ist eine, eine sehr schwierige Frage. Das, was ich vorhin gesagt habe, also Prävention, ist, denke ich so, das Schlagwort, was man im digitalen Bereich auch braucht, im physischen Bereich: Also, wenn Sie auf der Straße unterwegs sind, da lernt man präventive Verhaltensweisen quasi von Kindesbeinen an, ne? Also wenn man an

der Hand der Eltern durch die Straßen geht, äh, dann weiß man, dass man nicht schnell auf die Straße rennt, ne? Oder wenn man am Bahnhof vorbeigeht und da gibt es irgendwelche schummrigen Ecken, da merkt man auch: Die Eltern gehen vielleicht schneller vorbei oder so was, oder die sagen einem: ‚Oh, guck mal da, da darfst du nicht hingehen' oder sowas, ja? Also präventives Verhalten, ne? Und sowas braucht man eigentlich auch im Netz oder bei der Benutzung, äh, digitaler Medien. Da zeichnen sich so ein paar Sachen ab, was präventives Verhalten ist, ne? Also… gibts ja diesen Satz: Nicht auf alles klicken, was blinkt. Aber das ist auch viel zu einfach gesagt, ne? Was so ein gutes, äh, präventives Verhalten ist in der heutigen Zeit, ist nicht so richtig klar. Das liegt natürlich daran, dass die Medien sich dauernd verändern, ne? Aber so was muss sich erst mal entwickeln, äh, und das wäre, glaube ich, vermessen, wenn man im Prinzip jetzt, sagen wir fünzig Jahre nach Erfindung des Internet schon vollkommen wüsste, was so ein präventives Verhalten ist, äh, in der digitalisierten Welt, ne? Äh, das wird sicherlich auch noch ein bisschen dauern. Da braucht man als Gesellschaft auch ein bisschen Geduld. Aber es ist natürlich trotzdem wichtig, das Thema weiter zu beforschen, äh, und zu überlegen, was an Kompetenzen man eigentlich braucht, um sich dann genauso sicher und unversehrt durch den digitalen Raum oder in der digitalisierten Welt zu bewegen, äh, wie man es gewohnt war, sozusagen in der physischen Welt sich zu bewegen. Wenn man einigermaßen gut präventives Verhalten an den Tag legt, war es ja eigentlich relativ unwahrscheinlich, dass man Opfer von Kriminalität wird. Das ist im Internet ein bisschen anders, ne? Wir müssen dahin die Gesellschaft bringen, dass es genauso unwahrscheinlich ist, Opfer von Kriminalität zu werden im Internet, in der digitalisierten Welt, wie in der nicht digitalisierten Welt."

[pgg]: „Das heißt, so ein bisschen müssen wir das Sorgenmachen bejahen und uns da auch, auch wenn es unbequem ist, mit diesen ganzen möglichen Gefahren konfrontieren?" [MG: „Hmhm."]

[Freiling]: „Ja, genau. Ähm, man muss aber auf der anderen Seite auch sagen, dass ein Nicht-Partizipieren im Digitalen nicht schlimm ist [lacht]. Das ist sogar ein superpräventives Verhalten, wenn man halt nicht überall, in allen sozialen Netzwerken oder auf allen Messengern unterwegs ist, sogar auch nicht im Darknet oder was weiß ich. [lacht] Das ist super präventives Verhalten. Das heißt, Leute, die sich dazu entscheiden, ohne Smartphone zum Beispiel zu leben, sondern nur mit [lacht], mit einem Computer vielleicht – die muss man nicht bemitleiden. In gewisser Weise sind das so die neuen Ökos, die so hochkommen, ne? Und genauso muss man auf der gesamtgesellschaftlichen Ebene auch aufpassen, dass man nicht Digitalisierung um jeden Preis vorantreibt, ne? Weil Digitalisierung bedeutet nicht einfach überall Computer reinzustecken, sondern man braucht so eine intelligente Digitalisierung und das digitalisieren und in Computerprozesse übertragen, wo es tatsächlich Sinn macht. Und das impliziert jetzt auch ein bisschen, dass manche Sachen vielleicht nicht digitalisiert werden brauchen, ne? Vielleicht sogar nicht digitalisiert werden dürfen, weil sie vielleicht für die Gesellschaft so wichtig sind. Ne? Ich glaube, diese Dimension der Diskussion der Digitalisierung, äh, hat noch gar nicht begonnen. Und, äh, das sind sicherlich Sachen, die momentan auch bei ZEVEDI oder auch beim bidt diskutiert

werden: Also verantwortungsvolle Digitalisierung, ne? Diese Diskussion muss, denke ich, auch noch weitergeführt werden und auch gesellschaftlich breite Akzeptanz gewinnen. Ist natürlich immer das Problem, weil mit Digitalisierung natürlich Unternehmen auch Geld verdienen. Äh, die Lobbyarbeit in Richtung Digitalisierung ist natürlich auch sehr stark, ne, und man braucht im Prinzip auch sozusagen die Gegenlobby, äh, die sagt, man muss genau hinschauen, wo man digitalisiert, und nicht einfach den Glauben haben, dass Digitalisierung alleine irgendwie gesellschaftliche Vorteile bringt. Das schlägt immer zurück, ne? Wenn man zu viel digitalisiert und nicht aufpasst dabei, dann erzeugt das vielleicht noch mehr gesellschaftliche Kosten, viel mehr gesellschaftliche Kosten, als man durch, vermeintlich durch Digitalisierung eingespart hat, ne? Also da schlägt das alles wieder zurück."

[Der Abspann mit Musik beginnt.]

[mg]: „Und damit ist dieses *Digitalgespräch* zu Ende und wir bedanken uns bei Felix Freiling von der Friedrich-Alexander-Universität Erlangen-Nürnberg für dieses spannende Gespräch und die faszinierenden Einblicke. Viele Grüße! Und natürlich auch besten Dank an Sie, liebe Zuhörerinnen und Zuhörer, dass Sie uns Ihr Interesse und Ihre Aufmerksamkeit geschenkt haben. Wenn Sie mögen, hören wir uns im nächsten Jahr wieder, am 23. Januar 2024, zur nächsten Folge des *Digitalgesprächs*, einem Podcast von ZEVEDI, dem *Zentrum verantwortungsbewusste Digitalisierung*."