Elektronische Beweissicherung

(die Praxis)

Deutscher EDV-Gerichtstag 2019

Ulrike Meising Rechtsanwältin @RAinUMeising

Mein Vortrag befasst sich mit:

- dem Alltag bei Justiz und Anwaltskanzleien bei dem Umgang mit digitalen Dokumenten und Beweisstücken;
- der aktuellen Rechtslage zum Thema Beweis;
- der aktuellen Rechtslage zur Sicherung von digitalen Dokumenten;
- exemplarische Beispiele von SW-Einsatz im Rahmen der Beweisführung

Alltag digitaler Beweissicherung ist oft, dass aus unbestimmten Quellen (z.B. Parteien, Gegner, Beteiligten oder eigenen Ermittlungen) erlangte digitale Dokumente in ein eigenes digitales System (Justiz / Behörden / Kanzleien) übernommen werden:

Dies ist bequem, stellt nur keine Beweissicherung dar, sondern lediglich die Speicherung eines Dokuments im Dateisystem der Anwendenden. Mit der schlichten Speicherung von Dokumenten in einem Dateisystem fehlt jeder dauerhafte Nachweis der Herkunft eines Dokuments, der Person, welche es gespeichert hat, das genaue Aussehen des Dokuments und wer wann welche Änderungen an dem Dokument vorgenommen hat. M.a.W.: Eine Sammlung von Beliebigkeiten, die leicht durch entsprechende Anträge (schlichtes Bestreiten) erschüttert werden kann. Selbstverständlich sind derartige Dokumente auch ohne jeden Schutz vor Manipulationen oder Löschung.

Beweissicherung erfolgt um präzise juristisch definierte Aufgaben zu erfüllen, nämlich:

Beweisführung
Beweisverwertung
Beweiswürdigung
Beweislast

Fraglich ist, was dies für den Gesetzgeber und den juristischen Alltag bedeutet

Die Welt ist digital

… und bald auch die deutsche Justiz

ANALOG -> DIGITAL

Kennzeichnend für die gegenwärtige Zeit ist, dass es eine Zeit des Umbruchs, der Transformation, ist: Analoges wird digital. Und zwar alles! (Nicht nur einzelne Schriftstücke)

Ein solcher Zustand fordert Gesellschaft, Unternehmen und jeden einzelnen Menschen. Ein Mehr an Toleranz, Phantasie, Neugierde, Angstfreiheit und Energie sind erforderlich.
Comfort-Zonen müssen verlassen werden; was schon immer gemacht wurde wird bedeutungslos; die *Alten* können kein Wissen und Erfahrung an die *Jungen* weitergeben; bekannte Regeln der Organisation des Zusammenlebens bis hinein ins private lösen sich auf.
Ab einer gewissen Dichte dieser Änderungen verschliessen sich einzelne Personen, aber auch ganze Organisationen, diesen Entwicklungen, versuchen sich aggressiv an Vergangenem zu orientieren - oder leugnen ganz die Veränderungen.

Die Justiz in Deutschland befindet sich mitten im Prozess der Transformation, wird jedoch zunehmend von aussen (über den Inhalt der gerichtlichen Verfahren, Möglichkeiten der Technik, z.B. für Verhandlungen oder Ermittlungen) getrieben. Wirtschaft und privates Leben befinden sich in einem viel weiter fortgeschrittenen Zustand der Digitalisierung als die Justiz.

Eine ablehnende Haltung seitens der Justiz, oder präziser der Menschen, die dort arbeiten, gegenüber digitaler Transformation ist derzeit häufiger anzutreffen.
Dies ist problematisch, da so Potential für Verbesserungen verschenkt und auch Fehler gemacht werden, die zu erheblichen Nachteilen von Verfahrensbeteiligten führen können - oder wenigstens falschen Urteilen. Dies gilt besonders dann, wenn es um elektronische Beweismittel und -sicherung geht.

Analog und digital sind in drei Varianten möglich.
Variante drei sollte unbedingt vermieden werden, ist jedoch Alltag in Justiz, Verwaltung und Kanzleien, wenn ohne eAkte gearbeitet wird:

analoge Dokumente werden digitalisiert und digital weiterverarbeitet

👇

digitale Dokumente werden digital verarbeitet

👇

digitale Dokumente werden analogisiert und analog weiterverarbeitet

👇

DMS

Dokumenten Management System

Die Entsprechung einer Geschäftsstelle, Asservatenkammer, Anwaltskanzlei im digitalen Alltag ist wenigstens ein DMS.
Dort werden nach eigenen Vorgaben Strukturen vorgehalten, innerhalb derer Anwendende Arbeit organisieren, also Informationen (Dokumente, Daten) vorhalten, verbinden, verteilen, bearbeiten, erstellen.

Es ist hilfreich sich zu vergegenwärtigen, dass digitale Dokumente reiner Programm-Code bzw. Informationen sind, welcher (nur) in Objekte umgesetzt wird, damit diese menschlicher Wahrnehmung zugänglich sind. Zunächst optische und akustische Wahrnehmung, zunehmend jedoch auch haptische, z.B. im Rahmen von VR-Anwendungen.

Die Manipulation eines digitalen Dokumentes findet immer an der menschlicher Wahrnehmung NICHT zugänglichen Ausgestaltung statt, so dass deshalb auch die Manipulation an sich nicht auffällt. Problematisch ist, dass heute Manipulation digitaler Dokumente sehr einfach ist: Zeit- und Ortseinträge lassen sich ändern, Farben, Personen, Hintergründe können in Fotos (und Filmen) auf Knopfdruck verändert und neu komponiert werden. Nicht nur Papier ist geduldig, auch Code …

Aus diesem Grund gibt es verschiedene Regeln ein digitales Dokument derart zu sichern, dass Veränderungen entweder ganz unmöglich gemacht werden oder wenigstens leicht festgestellt werden können. Der Umfang insoweit bestehender Regelungen kann unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html nachgelesen werden.

Im wesentlichen lassen sich diese Richtlinien derart zusammenfassen, dass Dokumente, welche nicht mit wenigstens einer Form von digitaler Signatur (ausgestellt von anerkannten Vertrauensdiensten oder TrustCentern), sowie mit digitalem Siegel und Zeitstempeln versehen sind, keinerlei beweisrelevante Aussage haben.

DMS ≠ Archivierung

Archivierung meint die Entfernung eines Vorgangs (Akte, Geschäftsvorfall, Ermittlung) aus einem DMS. Voraussetzung ist, dass der Vorgang an sich abgeschossen ist. Dies entspricht einer Archivierung bzw. Aktenablage in der analogen Welt. Die Archivierung wird in der Wirtschaft am qualifiziertesten und konsequentesten schon sehr lange betrieben, da verschiedene gesetzliche Verpflichtungen entstehen, wenn Vorgänge abgeschlossen sind: z.B. Verjährungs-, Steuer-, Haftungsfristen, deren Missachtung zu empfindlichen wirtschaftlichen Folgen führen können.

Einer standardmässigen digitalen Archivierung ist eigen, dass:
- der Vorgang an sich verschlüsselt wird (Stand der Technik);
- mit einer digitalen Signatur der verantwortlichen Person(en) versehen wird;
- mit einem digitalen Zeitstempel versehen wird;
- rechtzeitig an Migrationsbedarf erinnert wird.

Problematisch ist, dass derzeit Zertifikate für digitale Signaturen nur für ca. 24 Monate ausgestellt werden. Da durchschnittliche gesetzliche Fristen wenigstens fünf Jahren betragen, bedeutet dies, dass digitale Signaturen regelmässig erneuert werden müssen, bis ein Vorgang endgültig vernichtet werden kann. Archivierungssysteme managen daher die rechtzeitige Erinnerung an den Ablauf eines Zertifikats, damit dieses rechtzeitig erneuert werden kann.

Die Nicht-Erneuerung eines abgelaufenen Zertifikats bedeutet, dass die Beweiswirkung der digitalen Signatur genau bis zu dem Tag des Ablaufes reicht. Danach könnte dann nur noch im Anscheins- und Zeugenbeweis versucht werden nachzuweisen, dass keine Veränderung an den Daten stattgefunden hat, was - je nach Qualität der Verschlüsselung - möglich sein kann.

Zusammengefasst: Alle, die digitale Archive verwenden, sind mit dem Stand der Technik digitaler Beweissicherungen in Deutschland vertraut.

Problem: DMS ≠ Archivierung: Die Regeln der digitalen (Beweis)Sicherung werden so gut wie gar nicht, bzw. sehr unstrukturiert in einem DMS, also in laufenden Vorgängen verwendet.

Legal Tech
Legal Design

Beide Begriffe bezeichnen (digitale) Anwendungen und Möglichkeiten, die über ein DMS hinaus gehen, bildet ein DMS letztlich doch nur die digitale Ausgestaltung der analogen Welt ab - und wenig darüber hinaus.

LegalTech in der Organisation:
Anwendungen, die z.B. Vorgänge organisieren, Wiederholungen vermeiden, gesetzliche Vorgaben (z.B. Berufs- oder Datenschutzrecht) einhalten, passgenaues Wissensmanagement für die jeweilige Angelegenheit sowie aktuelle Rechtsprechung vorhalten.

LegalTech in der elektronische Sicherung:
Systeme zur Automation digitaler Sicherungen, in dem z.B.
- **bestimmte Dokumententypen oder -klassen automatisch digital signiert werden,**
- **nicht elektronisch signierte Dokumente nicht elektronisch versandt werden können;**
- **nicht elektronisch signierte Dokumente nicht als Beweise vorgehalten oder verwendet werden können;**
- **automatisierte Aktenablage;**
- **automatisierte Überwachung der Gültigkeit von Zertifikaten etc.**

Für das vorher aufgezeigte Problem der Notwendigkeit mehrfacher „Nach“-Signierung bieten sich heute moderne Verfahren an, die zusätzlich das Problem der im Laufe der Zeit nicht (mehr) ausreichenden Verschlüsselung lösen:
DLT (Distributed Ledger Technologie), am bekanntesten ist die Blockchain-Technologie:
Die technischen Details dazu finden Sie im Vortag von Silvan Jongerius.

Legal Design ist nicht unbedingt digital und beschäftigt sich im Kern mit der Veränderung der Rechtsanwendung durch Digitalisierung der Gesellschaft.
Hier ist besonders für Deutschland auffällig, dass in der gegenwärtigen Gesetzgebung ein deutlicher Unterschied zwischen sog. „öffentlichen“ Urkunden oder Dokumenten und deren Beweiswirkung zu „privaten“ gemacht wird. Diese Unterscheidung ist sinnlos wenn es um digitale Dokumente geht: Entweder ist ein digitales Dokument mit einem gültigen Zertifikat signiert, oder nicht. Wer das Dokumente hergestellt hat oder welchen Beruf die signierende Person hat, ist ohne Bedeutung (jedoch noch nicht in der Gesetzgebung angekommen).

Beweis:

- **Feststellung eines Sachverhalts als Tatsache.**
- **Zu diesen Feststellungen sind nach der ZPO eine abschliessende Kategorie von Beweismitteln zugelassen.**

Zentral für das Verfahrensrecht in Deutschland ist die ZPO. Das Thema Beweismittel ist dort abschliessend geregelt:

- **Augenschein, §§ 371ff ZPO**
- **Zeugen, §§ 373ff ZPO**
- **Sachverständige, §§ 403 ff ZPO**
- **sachverständige Zeugen, § 414 ZPO**
- **öffentliche Urkunden, § 415ff ZPO**
- **private Urkunden, § 416 ZPO**
- **Echtheit von Privaturkunden, § 440 ZPO**
- **Schriftvergleichung, § 441 ZPO**
- **Parteivernehmung, § 445 ff ZPO**
- **Vernehmung von Amts wegen, § 448 ZPO**

Hinterfragt werden muss, ob diese Regelungen ausreichend sind, digitale Beweise zu erfassen. Tatsächlich erlebt z.B. der *Augenschein* - lange ein Mauerblümchen im Beweisrecht - im Zuge der Digitalisierung sein Revival. Ist dies ausreichend oder vielleicht Ausdruck von Hilflosigkeit gegenüber dem, was da in Augenschein genommen wird?

Es mag überraschen: V.a. Zeugen (und Parteien) werden maximal digitalisiert (dazu später); der Umgang mit digitalen *Dokumenten -> Urkunden* scheint noch am einfachsten.

Ein Beispiel der wenig schönen Realität in der Justiz:
Ein Gericht erklärt mir, dass es reine URL-Links nicht als Beweis akzeptiere.
Begründung: Findet sich nicht in der ZPO! Allenfalls würde es einen Ausdruck der Seite akzeptieren. Hingewiesen darauf, dass so eine sehr hohe Wahrscheinlichkeit für nicht authentische Dokumente (aka Fälschungen) bestehe, erklärt es: Mag sein, ich kann nur nicht anders: Nahe zu alle Links seien justizverwaltungsseitig aus Sicherheitsgründen gesperrt, so dass reinen Links im Parteivortrag (sollte irgendwann die eAkte verwendet werden) nicht nachgegangen werden könne.

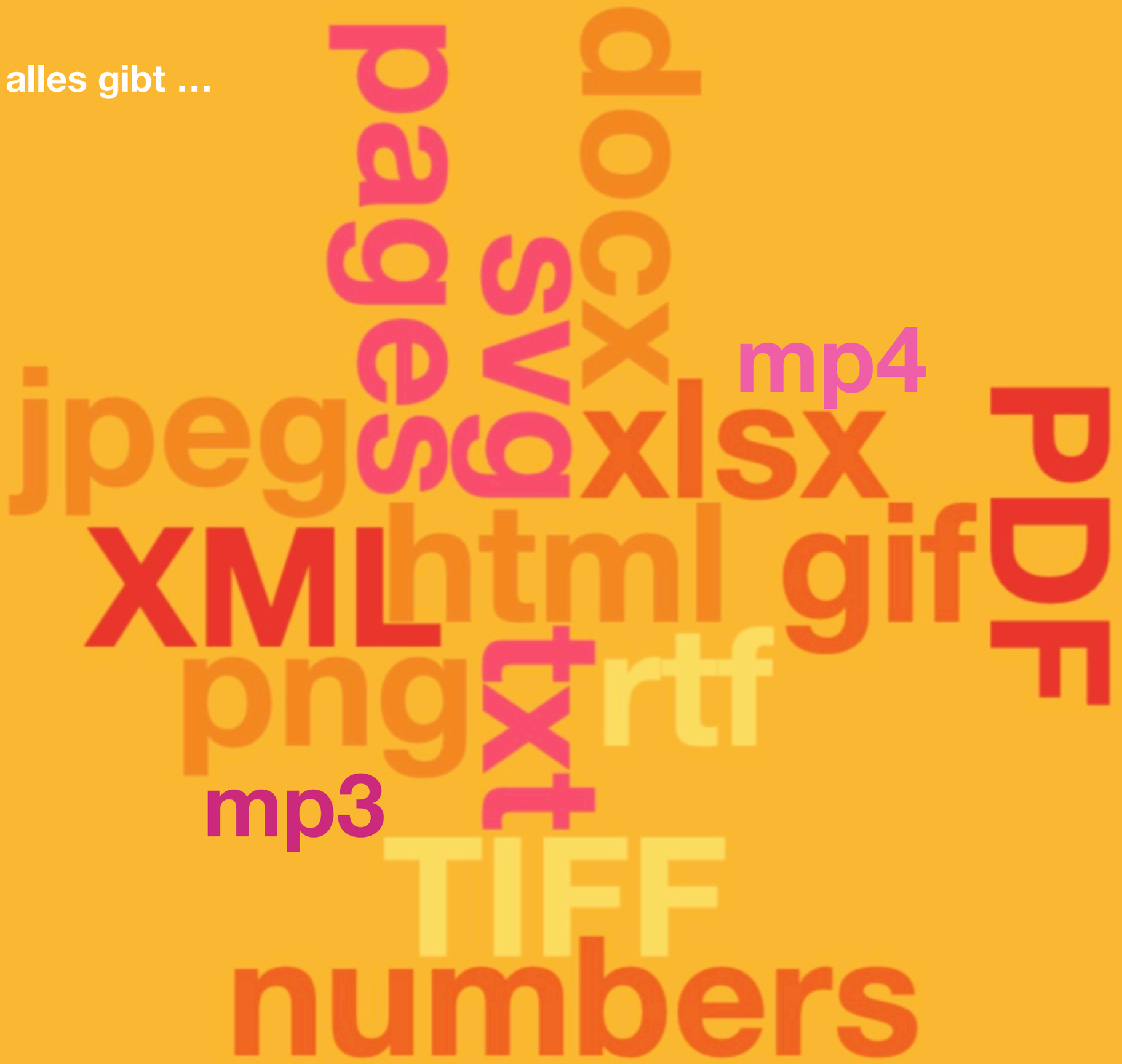
… zu elektronischen Beweismitteln ist dem Gesetzgeber bisher dies eingefallen:

- § 371a ZPO (Beweiskraft elektronischer Dokumente)
- § 371b ZPO (Beweiskraft gescannter öffentlicher Urkunden) -> ResiScan -> § 437 ZPO

- Transit: Ausdruck öffentliches elektronisches Dokument, § 416a ZPO

Bei Lektüre dieser Vorschriften wird schnell klar, dass sie relativ alt sind, ausschliesslich digitalisierte Schriftstücke regeln - und damit dem heutigen Alltag kaum noch gerecht werden.

Was es so alles gibt …



Anforderungen an digitale Dokumente

- Integrität
-Authentizität
-Vollständigkeit
-Nachvollziehbarkeit
-Verfügbarkeit
-Lesbarkeit
-Verkehrsfähigkeit
-Vertraulichkeit
-Löschbarkeit

Integrität:
Die Daten oder Systeme wurden nicht verändert.
Bei wirksamem Integritätsschutz werden zudem zumindest Veränderungen erkannt:

Authentizität:
Die Quelle der Daten ist eindeutig bestimmbar.

Vollständigkeit:
Der gegenseitige Bezug mehrerer aufgrund eines inneren Zusammenhangs zusammengehörigen Datenobjekte ist sichergestellt.

Nachvollziehbarkeit:
Alle wesentlichen Schritte des Vorgangs können von einer unabhängigen Stelle nachvollzogen werden.

Verfügbarkeit:
Wenn Daten, Dienste, IT-Systeme, IT-Anwendungen oder IT-Netze den Benutzern innerhalb akzeptabler Wartezeiten in der benötigten Form zur Verfügung stehen.

Lesbarkeit:
Die in den Daten enthaltenen Informationen können erkannt werden:
Ein elektronisches Dokument ist „lesbar“, wenn die notwendige Hard- und Software die Daten verarbeiten, ihre Informationen interpretieren und dem menschlichen Betrachter in lesbarer Weise präsentieren kann.

Verkehrsfähigkeit:
Die Möglichkeit, Dokumente und Akten von einem System zu einem anderen übertragen zu können, bei der die „Qualität“ des Dokuments sowie seine Integrität und Authentizität nachweisbar bleiben.

Vertraulichkeit:
Die Verhinderung einer unbefugten Kenntnisnahme.

Löschbarkeit:
Das Unkenntlichmachen der gespeicherten Daten:
Wenn Daten unwiderruflich so behandelt worden sind, dass eigene Informationen nicht aus gespeicherten Daten gewonnen werden können, wenn also Rückgriff auf diese Daten nicht mehr möglich ist.

… und was ist an Zeugen digital?

- Online-Verhandlungen / Vernehmungen;
- Einsatz von Facial- oder Emotional-Recognition-SW, also Software, die aus Bild-, Film- und Tonaufnahmen Personen und / oder deren Emotionen erkennt - im Rahmen von Verhandlungen oder auch Ermittlungen;
- Ein Beispiel der aktuellen Qualität dieser Anwendungen ist die App „Seeing AI“ von microsoft (nur unter iOS);
- Profiling, Tracking und Scoring aufgrund vom (personenbezogenen) Daten

Software ist neutral

Von technikbegeistert bis -ablehnend - für alle gilt:
Software und Technik sind (bisher) immer nur Werkzeuge, die unterstützen und daher an sich weder gut oder schlecht, gar kriminell sind.

Jede Software oder Technik kann positiv oder negativ eingesetzt werden:
- **Sachverhalte aufklären oder fake news schaffen;**
- **Straftaten ermöglichen oder aufklären;**
- **Sicherheit herstellen oder Überwachung;**
- **Informationen verbreiten oder Chilling-Effekte auslösen;**
- **etc.**

Software macht es andererseits leicht möglich, digitale Daten zu verändern.

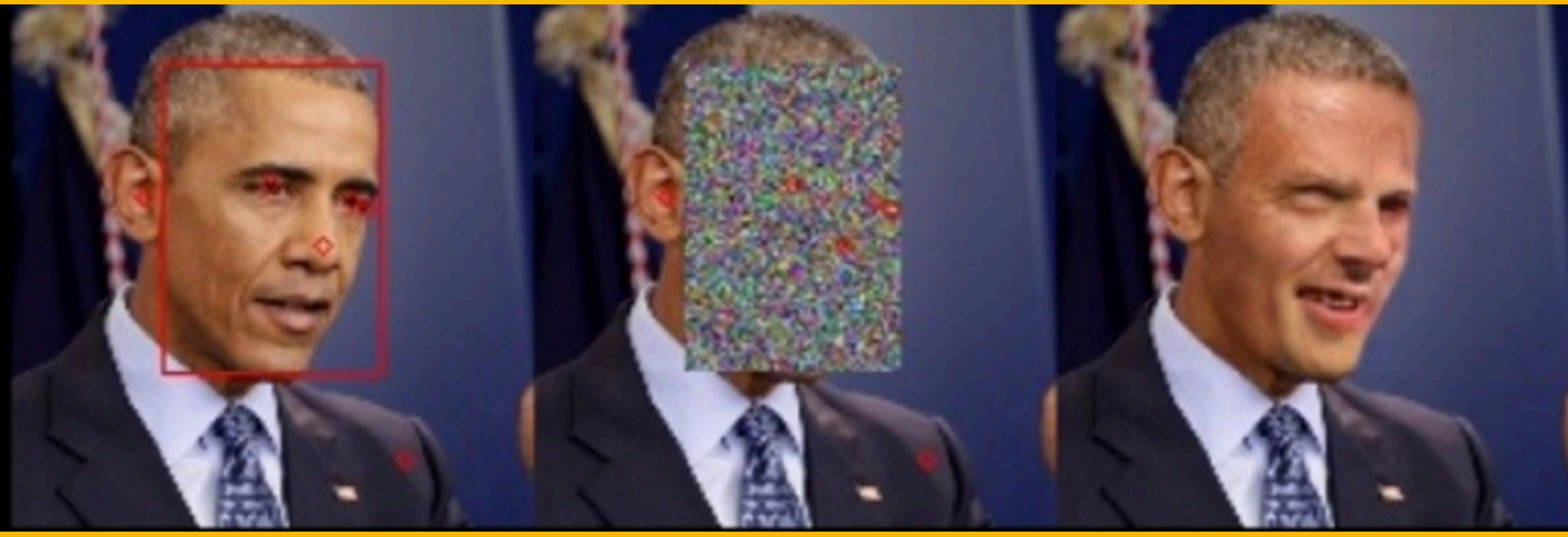
Es ist ein Trugschluss deshalb davon auszugehen, dass digitale Dokumente häufiger gefälscht seien als analoge; die Qualität der Fälschung ist nur einerseits besser und andererseits leichter festzustellen.

Versicherung setzen schon lange Software ein, um Manipulationen an Fotos aufzudecken, die zur Begründung eines Anspruchs eingereicht werden: Wenigstens 20 % der eingereichten Fotos sind „optimiert“.

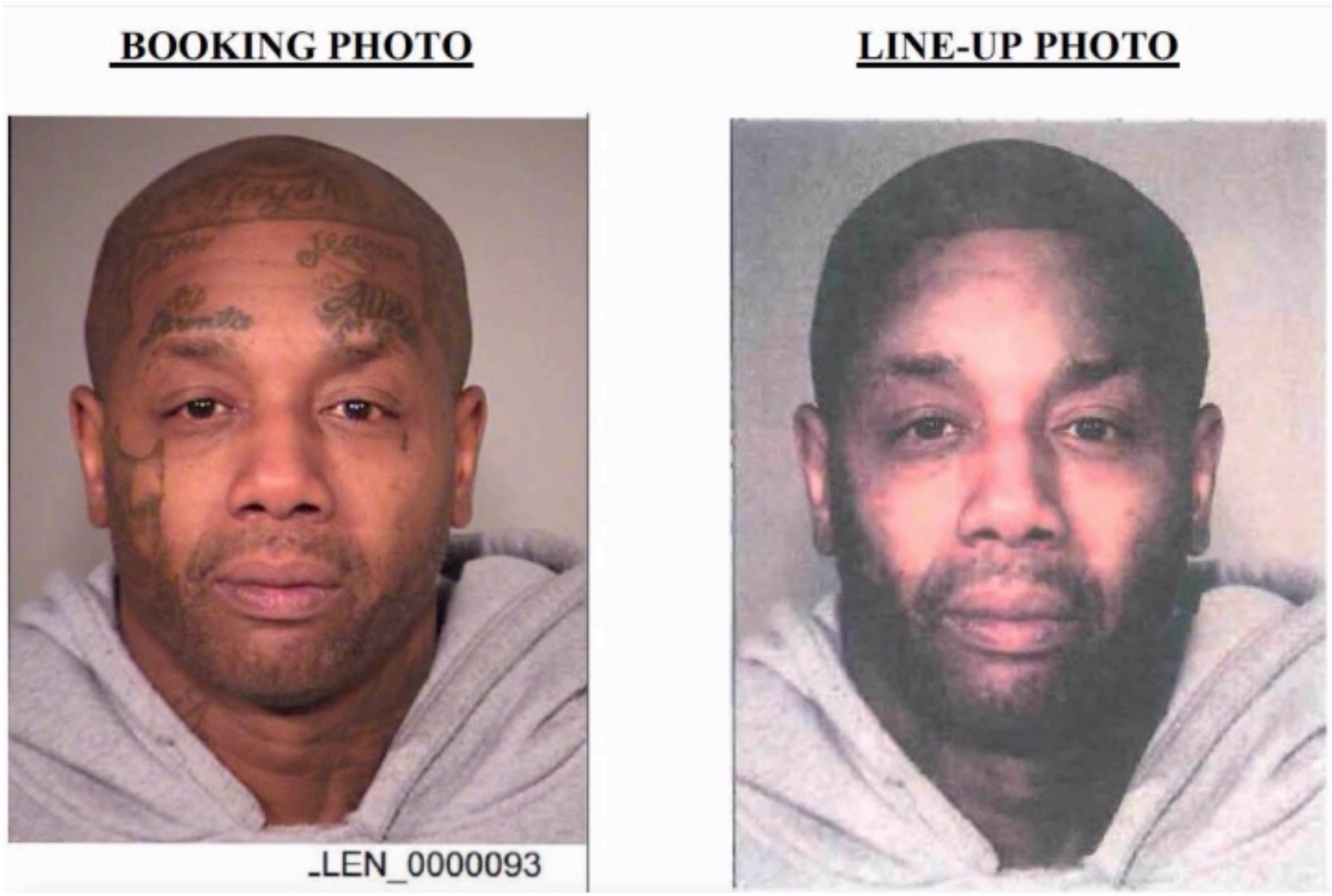
Nachfolgend daher einige relativ aktuelle Beispiele, wie mit den Möglichkeiten von Software und der Realitätsmanipulation umgegangen wird.

Deepprivacy

Software, die per Zufalls aus einem riesigen, ständig wachsenden Datenpool Gesichtsaufnahmen auswählt und mit denen vorhandener Fotos austauscht.

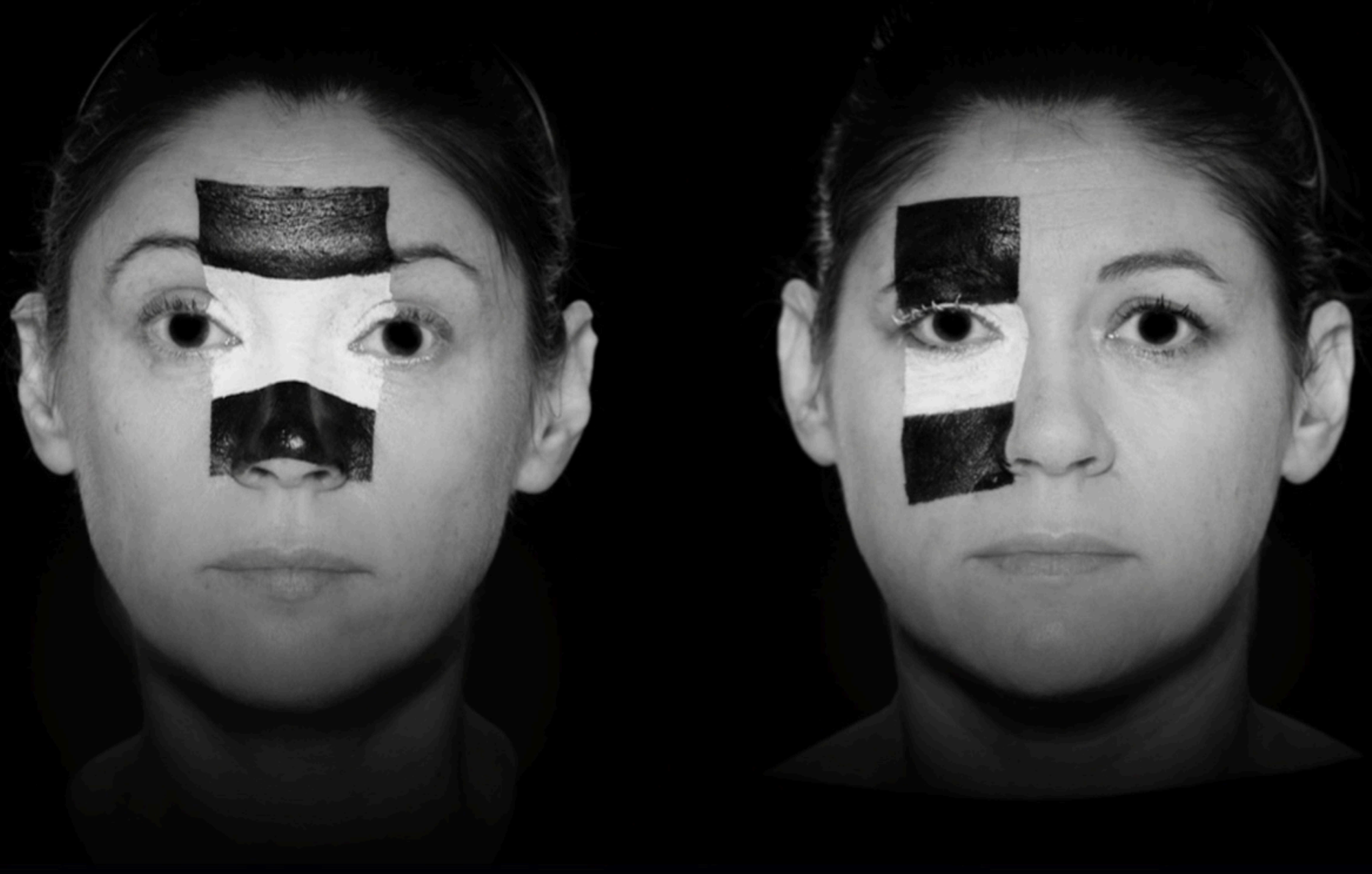


Fahnungsfoto (US Polizei) eines Verdächtigen:
links: Original, rechts nachbearbeitetes Fahndungsfoto



Tyrone Allen's facial tattoos were removed in a photograph shown to four bank tellers in a robbery case.

Dazzle Camouflage:
Gesichtsmarkierungen / Make-Up, wodurch Facial-Recognition-SW ausser Kraft gesetzt wird.



JANE & LOUISE WILSON

Take Aways:

- **Kenntnis digitaler Dokumente, Daten und Dateien UND deren Manipulationsmöglichkeiten sind unerlässlich für juristisches Arbeiten;**
- **gesetzliche Regeln welche Sicherungsmechanismen, Zertifikate etc. mit welchen Wirkungen verwendet werden können fehlen bzw. sind lückenhaft oder veraltet;**
- **digitale Signaturen, Siegel, Zeitstempel etc. sind kompliziert in der Anwendung und daher automatisiert am besten zu verwalten;**
- **DLT bietet Lösungen für Probleme der Verschlüsselung und Sicherung;**
- **Die Beweisregeln der ZPO sind teilweise nicht auf digitale Dokumente anwendbar;**
- **Differenzierung zwischen öffentlichen und privaten Dokumenten (Dateien) ist nicht mehr zeitgemäss und hilfreich.**