



# Ausweis bitte! Rechtliche Lage ...wer hat Recht?

RA Lukas Bühlmann, LL.M.  
Partner, Meyerlustenberger Lachenal Froriep (MLL), Zürich

8.9.2021



# Agenda

- **Einführung**
- **Pflichten zur Identifizierung**
- **Rechtliche Problemfelder**
- **Pflichten bei der Identifizierung**
- **Gesetzgebung**



# Einführung

# Begrifflichkeiten

- **Ausweise**

- «[amtliches] Dokument, das als Bestätigung, Legitimation für etwas ausgestellt worden ist, Angaben zur Person enthält [und zu etwas berechtigt]» (Duden)
- Art. 2 Bundesgesetz über die Ausweise für Schweizer Staatsangehörige
- «Ausweise im Sinne dieses Gesetzes dienen der Inhaberin oder dem Inhaber zum **Nachweis** der Schweizer Staatsangehörigkeit und der eigenen **Identität**.»

- **Elektronische Identität**

- Keine einheitliche Verwendung und Definition des Begriffs
- «Jeder digitale Identitätsnachweis von Bürgern, Personen oder Organisationen» (Wikipedia)
- Digitale Identitäts*nachweis*
- Probleme der elektronischen Identität bestehen vor allem hinsichtlich der **Authentizität** des elektronischen Nachweises

# Welche elektronischen Identitätsnachweise gibt es in der Praxis?

- **Gar keine Identifizierung**
  - ungeprüftes Log-in
- **"Identifizierung" der Adressangaben**
  - Versenden eines Bestätigungslink zur Aktivierung an eine E-Mailadresse (häufig)
- **(Schwache) Identifikation über Verknüpfung mit anderer elektronischer Identität**
  - Log-In von Google/Facebook
- **Abgleich der Angaben mit Scan von Pass/ID**
- **Qualifizierte elektronische Signatur**
  - Gleichgestellt der handschriftlichen Unterschrift (Art. 14 Abs. 2bis OR)
- **Videoidentifizierung**
  - Durch Mensch oder Software-Tools



# **(Rechtliche) Pflichten zur Identifizierung**

# Gibt es rechtliche Pflichten zur Identifizierung oder gar zur Verwendung eines digitalen Identitätsnachweises?

- **Keine allgemeine Pflicht** seine Vertragspartner zu identifizieren
  - Grundsätzlich ist die Person des Vertragspartners irrelevant, ausser es kommt bei der Leistung auf die Persönlichkeit an (vgl. Art. 68 OR)
  - Mit der falschen Person einen Vertrag zu schliessen, führt aber zu Problemen (siehe hinten)
- **Spezifische Sorgfaltspflichten** zur Identifizierung des Vertragspartners
  - **Finanzmarkt**
    - Art. 3 GWG: "Finanzintermediär muss bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines **beweiskräftigen Dokumentes** identifizieren." (Verhinderung von Geldwäscherei)
    - FINMA-Rundschreiben 2016/7: Video- und Online-Identifizierung
  - **Telekommunikation**
    - Prüfung des Alters von Minderjährigen mit ID für Telekomdienste (Art. 41 FDV)
  - **Datenschutzrecht**
    - Bevor ein Auskunftsbegehren elektronisch beantwortet wird, muss der Gesuchsteller identifiziert werden (Art. 1 Abs. 1 und 2 VDSG)
  - **Behördengänge**
    - Notariate müssen z.B. Personen identifizieren und dürfen nicht jedes Dokument akzeptieren
      - z.B. § 13 NotariatsVO ZH: «Der Notar prüft die Identität der am Rechtsgeschäft beteiligten Personen. Von Personen, die ihm nicht persönlich bekannt sind, verlangt er die Vorlegung amtlicher Identitätsausweise. Dabei muss er Schriftenempfangsscheine, Führerbewilligungen und ähnliche Ausweise nicht als genügend annehmen. Die Verwendung des Dienstbüchleins als Ausweisschrift ist untersagt»
  - **Weitere...**

# Neuere Erlasse mit Vorschriften zur elektronischen Identifizierung

- Art. 7 Abs. 1 EPDG (Gesetz über das **elektronische Patientendossier**)
  - «Für die Bearbeitung von Daten im elektronischen Patientendossier müssen über sichere **elektronische Identitäten verfügen**: a) Patientinnen und Patienten sowie b) Gesundheitsfachpersonal»
  - Wahrscheinlich nicht von Ablehnung E-ID Gesetz betroffen, weil kein direkter Verweis auf E-ID Gesetz
- Art. 19 Abs. 2 des Vorentwurf des Gesetz über die Plattformen für **elektr. Kommunikation der Justiz (VE-BEKJ)**
  - Regeln zur **Authentifizierung** der Benutzerinnen und Benutzer
  - «Sie benötigen dazu **eine elektronische Einheit**, die zur Identifizierung natürlicher Personen verwendet wird (**E-ID**), auf dem Sicherheitsniveau «substanziell» oder «hoch» nach Art. 4 Abs. 1 Bst. B & c des E-ID Gesetzes vom 27.09.2019»
  - Nach Ablehnung des E-ID Gesetzes wird von der Projektleitung zusammen mit dem Bundesamt für Informatik und Telekommunikation (BIT) abgeklärt, ob auf etablierte Identitätsservices gesetzt werden kann



# Rechtliche Problemfelder

# Gültigkeit der Verträge

- **Beispiel: Deepfakes**
  - **Deepfakes** = realistisch wirkende **Fotos, Audioaufnahmen** oder **Videos**, die mit Techniken der künstlichen Intelligenz abgeändert und verfälscht worden sind
- **Verträge** brauchen **übereinstimmende Willenserklärung** (Art. 1 OR)
  - **Irrtum**
    - Wenn der Vertrag mit Rücksicht auf eine bestimmte Person abgeschlossen wurde und der Wille des Irrenden auf eine andere Person gerichtet war, liegt ein wesentlicher Irrtum vor (Art. 24 Abs. 1 Ziff. 2 OR)
  - **Täuschung**
    - Wer absichtlich über Identität getäuscht wurde, für den ist ein Vertrag nicht verbindlich (Art. 28 OR)
  - **Rechtsfolgen**
    - Vertrag mit Deepfake ist **anfechtbar** und zwar innert eines Jahres ab Kenntnis des Irrtums (Art. 31 OR)
  - **Nichtigkeit?**
    - Vertrag der unmöglichen oder widerrechtlichen **Inhalt** hat oder gegen die guten Sitten verstösst
    - Deepfake betrifft Zustandekommen, nicht Inhalt



# Gültigkeit der Verträge

- Verträge mit **Minderjährigen** insbesondere
  - Minderjährige können nur Verträge über **geringfügige Leistungen** selber schliessen (siehe Art. 18 ZGB)
  - Schliessen Minderjährige komplexe Geschäfte oder teure Verträge Online ab, sind die Verträge nicht gültig zustande gekommen.
  - Im E-Commerce müsste man Personen identifizieren, um sicherzustellen, dass man keine Verträge mit Minderjährigen schliesst
  - Problem wird im E-Commerce oft ignoriert
- **Datenschutzrechtliche Einwilligung** von Kindern unter 16 in der EU
  - Explizit nur gültig, wenn **Eltern zustimmen** (Art. 8 DSGVO)
  - Pflicht "angemessene Anstrengungen" zu unternehmen, um festzustellen, dass Eltern einverstanden sind (Art. 8 Abs. 2 DSGVO)
    - In Praxis wird oft Bestätigung in den AGB verlangt, was kaum genügt
  - Schweiz: Gültigkeit nach allg. privatrechtlichen Grundsätzen betr. Handlungsfähigkeit (Art. 11 ff. ZGB)

# Zivilrechtliche Haftungsfragen

- Wer haftet, wenn keine (korrekte) Identifizierung stattfindet?
- Es kommt drauf an (**einzelfallabhängig**)
- Risiko Identitätsmissbrauch für gewisse Konstellationen **vertraglich regelbar**
  - Enthält Vertrag eine Pflicht bezgl. Identifizierung?
  - Wenn ja, trifft Vertragspartner bei Pflichtverletzung Schadenersatzpflicht (Art. 97 OR)
- Problem: Oft bestehen **keine Verträge** mit Schadensverursachern (Person, die sich falsch identifiziert hat) bzw. diese lauten auf andere Personen
  - Versand von Sachen an falsche Adresse: Evtl. Besitzschutz (Art. 926 ff. ZGB) und Eigentumsherausgabe (Art. 641 ZGB)
  - Schadenersatz?
    - Vermögensschäden werden nur ersetzt, wenn gegen Schutznorm verstossen wurde
      - Schutznormen oft im StGB: vgl. nachfolgend strafrechtlicher Schutz
  - Klage wegen ungerechtfertigte Bereicherung aus dem Vermögen eines anderen (Art. 62 OR)

Risk

Safety



**Beispiel vertraglicher Regelung von Identifikationspflichten in Bank  
AGB (BGE 146 II 32)**

# Zivilrechtliche Haftungsfragen

- **BGE 146 II 326 «Freizeichnung; Risikotransferklauseln»**

## Sachverhalt

- Kunde schloss mit Bank einen Vertrag, welcher es ermöglichte, Überweisungsaufträge per E-Mail aufzugeben. Zu einem späteren Zeitpunkt wurde das E-Mail-Konto des Kunden gehackt und mittels verschiedener per E-Mail versandter Aufträge mehrere hunderttausend Franken vom Konto abgehoben.
- Bank bestritt Haftung für Überweisungsaufträge. Vertrag sah vor, Korrespondenz banklagernd zu lagern und enthielt eine **Entlastungsklausel für Kommunikation per Telefon, Fax und E-Mail**.
- Kunde ermächtigte damit die Bank per E-Mail erteilte Aufträge **sofort und unter allen Umständen** auszuführen; er **übernahm sämtliche daraus erwachsenden Risiken**, auch bei Irrtum der Bank über seine **Identität**, und stellte die Bank von jeder diesbezüglichen Haftung frei.

## Bundesgericht

- Bestätigt **rechtliche Gültigkeit** dieser Klausel
  - *«Wenn die Parteien vereinbart haben, dass der Kunde seine Überweisungsaufträge per E-Mail übermitteln kann, muss die Bank ebenfalls **keine ausserordentlichen Prüfmassnahmen ergreifen**, zumal dies einer raschen Abwicklung der Geschäfte entgegenstehen würde; sie darf vielmehr davon ausgehen, dass der von der E-Mail-Adresse des Kunden abgesandte Auftrag rechtmässig ist.»*

# Strafrechtliche Fragen

## Dürfen IDs für die Identifizierung fotokopiert oder gescannt werden?

- Bei vielen (digitalen und analogen) Geschäftsvorgängen, wird eine Kopie der ID verlangt
- Kopieren einer ID an sich ist **keine Urkundenfälschung** (Art. 251 StGB)
  - Keine Schädigungsabsicht (kein Schaden) und keine Verschaffung eines unrechtmässigen Vorteils
- Achtung: In **Deutschland** ist dies teilweise strafbar (Art. 20 Abs. 2 D-PersAuswG)
  - Ausgenommen: Ausweisinhaber darf Ablichtung vornehmen, diese muss eindeutig und dauerhaft als Kopie erkennbar sein
  - Risiko der Strafbarkeit bei grenzüberschreitenden Dienstleistungen abklären



# Strafrechtliche Fragen

## ID Fälschung mit Deepfakes

- Noch keine konkreten Fälle von ID Fälschungen mittels Deepfakes
- Sicherheit von Ausweisen und Identitätskarten momentan noch sehr hoch, aber es besteht Risiko für die Zukunft
- **Beispielfall** aus Deutschland:
  - **Stimmimitation** mittels Deep Fakes:
    - Der Leiter der britischen Niederlassung eines deutschen Energiekonzerns fiel 2019 einem Betrüger zum Opfer, welcher dank Stimmenimitationssoftware wie sein Chef klang.
    - Der Manager liess sich dazu hinreissen, 220'000.- Euro auf ein Konto in Ungarn zu überweisen. Dieses Geld wurde umgehend von den Betrügern abgeräumt.
    - Siehe: <https://www.boersen-zeitung.de/deep-fakes-erleichtern-betrug-e5a43b80-9933-11eb-bf5d-0b6bc58d3fae>



# Strafrechtliche Fragen

## Strafbarkeit Deepfakes

- Wenn **Computer getäuscht** werden: Werden mit Verwendung des Deepfakes Vermögensvorteile angestrebt, ist dies u.E. **betrügerischer Missbrauch einer Datenverarbeitungsanlage** (Art.147 StGB), da auch «**unrichtige**, unvollständige oder unbefugte **Verwendung von Daten**» tatbestandsmässig,
- Wird ein Mensch getäuscht: **Betrug** wahrscheinlich, weil für Menschen nicht nachprüfbar und damit eine «arglistige Irreführung»

-  **Betrug**

-  **Art. 146**

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen andern am Vermögen schädigt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

-  **Betrügerischer Missbrauch einer Datenverarbeitungsanlage**

-  **Art. 147**

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

# Strafrechtliche Fragen

## Gebrauch einer fremden ID

- **Betrug (Art. 146 StGB)**
  - Wenn Täuschung des Geschädigten mittels ID einen unrechtmässigen Vorteil verschafft
  - Muss «**arglistig**» sein: Nicht immer gegeben in Praxis
    - Darunter fällt bspw. strafbares Phishing (Vermögensvorteil erlangen)
    - Arglist scheidet aus, wenn der Getäuschte den Irrtum mit einem Mindestmass an Aufmerksamkeit hätte vermeiden können. Wenn eine Privatperson z.B. einen leistungsstarken Drucker der Mittelklasse für rund Fr. 2'200.- bestellt, kann nicht mehr von einem Alltagsgeschäft gesprochen werden. Wenn Online-Händler diesen Drucker ohne Vorkasse an unbekannte Privatperson liefert, geht er bewusst ein gewisses Risiko ein. Der Händler hätte ohne erheblichen zusätzlichen Aufwand die Bonität des Beschwerdeführers zumindest rudimentär prüfen können. Daher keine Arglist gegeben (so die Bundesgerichtsrechtsprechung: BGE 142 IV 153). Umkehrschluss: Bei Identität- und Bonitätsprüfung wäre Betrug wohl gegeben wesen.
- **Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)**
  - Siehe dazu hinten (Urteil des Obergerichts Zürich vom 28. September 2020)
- **Fälschen von Ausweisschriften (Art. 252 StGB)**
  - Gebrauch eines unechten oder Missbrauch eines echten Ausweises
- **Hacking (Art. 143bis StGB)**
  - Täter dringt im Zusammenhang mit den persönlichen Daten in ein Computersystem ein
- **Unbefugte Datenbeschaffung (Art. 143 StGB)**
  - Täter gelangt mittels ID unrechtmässig an fremde, nicht für ihn bestimmte Daten

# Strafrechtliche Fragen

## Fälschen von Ausweisen

- Tatbestand schützt **das öffentliche Vertrauen**, das Ausweisschriften, Zeugnissen und Bescheinigungen im Rechtsverkehr entgegengebracht wird
- **Ausweisschrift**
  - tendenziell nur offizielle Dokument
  - Begriff aber offen
- Absicht sich das **Fortkommen zu erleichtern**
  - Nicht nur Vermögensvorteile, sondern jede Verbesserung der persönlichen Lage reicht

### - **Fälschung von Ausweisen**

### - **Art. 252<sup>266</sup>**

Wer in der Absicht, sich oder einem andern das Fortkommen zu erleichtern, Ausweisschriften, Zeugnisse, Bescheinigungen fälscht oder verfälscht, eine Schrift dieser Art zur Täuschung gebraucht, echte, nicht für ihn bestimmte Schriften dieser Art zur Täuschung missbraucht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

# Strafrechtliche Fragen

## OGer Zürich: Online-Bestellungen unter falscher Identität

- Beschuldigte **bestellte in fremden Namen Waren an eigene Adresse** (Bestellbetrug)
- Verteidiger machte geltend, dies müsse als **Betrug** (Art. 146 StGB) geprüft werden
  - Beim Betrug muss Täter **«Arglist»** nachgewiesen werden
  - Regelmässig schwierig (Stichwort «Opfermitverantwortung»; siehe oben)
- Gemäss **OGer Zürich** erfüllten die Bestellungen bereits den Tatbestand **Missbrauch einer Datenverarbeitungsanlage** (Art. 147 StGB)
  - Arglistige Täuschung einer Person hier nicht notwendig
  - Erhöht für Online-Händler Erfolgchancen für ein strafrechtliches Vorgehen gegen betrügerischen Bestellungen
- **Detaillierte Besprechung:** [MLL-News vom 14. Juni 2021](#)



# Strafrechtliche Fragen

## Neuer Tatbestand des Identitätsmissbrauchs (Art. 179<sup>decies</sup> revStGB)

- Im Zuge der Revision des DSG geschaffen
- *«Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird auf Antrag mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.»*
- **Verwenden einer (fremden) Identität** → sich als fremde Person ausgeben
  - Identität: *«Echtheit einer Person oder Sache; völlige Übereinstimmung mit dem, was sie ist oder als was sie bezeichnet wird»*
  - Beispiele
    - Erstellen eines Social-Media-Profiles
    - Eingeben von Daten bei einer Online-Bestellung
    - Sich als eine andere Person vorstellen
  - Strafbarkeit nur wenn dem «Original» geschadet wird
    - Beispiel: In einem Online-Shop auf Rechnung auf Name und Adresse einer anderen Person etwas bestellen

# **Datenschutzrechtliche Pflichten bei der Identifizierung**

# Pflichten bei der Online Identifizierung

## Datenschutzrecht

- **Datenminimierung / Speicherbegrenzung**
  - Keine Speicherung von Daten, nachdem diese nicht mehr benötigt werden
  - Keine grundlose Speicherung von ID-Kopien
  - Problem: Zulässigkeit der Speicherung von Bildern oder Stimmufnahmen zum Training der KI (Machine-Learning)
    - Europäischer Datenschutzausschuss Guidelines 02/2021 on virtual voice assistants: *“The processing activities (...) should not be considered as (strictly) “necessary for the performance of a contract” within the meaning of Article 6(1)(b) GDPR, and therefore require another legal basis from Article 6 GDPR.”*
- **Datenrichtigkeit**
  - Pflicht zur Ergreifung von Massnahmen, damit Richtigkeit der Daten sichergestellt wird
  - Umsetzung in der Praxis?




# Pflichten bei Online Identifizierung

## Datensicherheit

- Privacy by Design (Art. 6 nDSG)
  - Sicherstellen von angemessenen technischen und organisatorischen Massnahmen zum Schutz von Personendaten bei der **Planung** neuer Bearbeitungsvorgängen
  - Insb. Verschlüsselung von heiklen Daten *at rest*
- Privacy by Default (Art. 6 nDSG)
  - Sicherstellen, dass Bearbeitungsvorgänge durch **geeignete Voreinstellungen** auf das Mindestmass beschränkt sind
- Zusammenarbeit mit Dienstleistern
  - Verträge prüfen (Auftragsdatenbearbeitungsverträge)
  - Wer den Dienstleister einsetzt, muss sicherstellen, dass dieser eine angemessene Datensicherheit gewährleistet (Art. 10a DSG)
  - Dienstleister im Ausland: Besondere Sorgfaltspflichten (insb. wenn dieser Sitz in Land das kein angemessenes Datenschutzniveau bietet (z.B. USA))





# **Entwicklung Gesetzgebung (Schweiz)**

# Bundesgesetz über die E-ID

- **Ziel**

- Vertrauenswürdige Legitimationsmittel (E-ID) schaffen, um Personen online zuverlässig identifizieren zu können
- Rahmenbedingungen für die Anerkennung der Anbieter und die Bereitstellung von Identitätsdaten durch den Bund

- **Kernpunkte Gesetzesprojekt**

- **Anerkennung und Aufsicht** der privaten Aussteller einer E-ID (Identity Provider)
  - Detaillierte **Pflichten** für die anbietenden Unternehmen, welche durch das EIDCOM (neue Aufsichtsbehörde) überwacht werden
- Bereitstellung von **Identitätsdaten** für eine E-ID durch den Bund
- **Kein Zwang** der Unternehmen, E-ID zu akzeptieren
- **Kein Zwang** der **Privatpersonen**, sich eine E-ID ausstellen zu lassen



# Bundesgesetz über die E-ID

- **Ablehnung des Bundesgesetzes über die E-ID**

- Das E-ID Gesetz wurde am 7. März 2021 von 64% der Stimmberechtigten **abgelehnt**
- Hauptgrund: **Keine privaten Aussteller** der E-ID gewollt

- **Weiteres Vorgehen?**

- EJPD wurde beauftragt bis Ende Jahr ein neues Grobkonzept zu erarbeiten
  - ETH, EPFL und Kantone sollen stärker miteinbezogen werden
  - 6 parlamentarische Motionen mit dem Titel «vertrauenswürdige, staatliche E-ID → Annahme empfohlen
- Vernehmlassung neues Gesetz Anfang 2022

→ neue Vorlage: **staatliche Institution** wird E-ID herausgeben, ansonsten keine grossen Änderungen zu erwarten



Lukas Bühlmann, LL.M.

Partner, ICT, Zürich

[lukas.buehlmann@mll-legal.com](mailto:lukas.buehlmann@mll-legal.com)

[www.mll-legal.com](http://www.mll-legal.com)

---

**Vielen Dank für Ihre Aufmerksamkeit**

Wir freuen uns auf Ihre Kontaktaufnahme

**MLL**