

Ausgabe
Nr°3

WOB

World of Business Law

Angelina Rau

Gen-Revolution unter Anwendung der CRISPR/Cas9- Methode

- S. 14

Stefan Hegyi

Der Weg zum wissenschaftlichen Mitarbeiter

- S. 22

Jacqueline Panzeri

Kapstadt – das schönste Ende der Welt

- S. 26



Editorial

Geschätzte Leserin, Geschätzter Leser,

Die Digitalisierung ist heute in aller Munde und doch stehen wir erst am Anfang dieses bedeutenden Gesellschaftswandels. Technisch ist bereits vieles möglich, doch die effektive Umsetzung und die Adaption digitaler Technologien auf den Alltag erfordern Starthilfe in Form von Finanzierungen und rechtlichen Grundlagen. Um die Effizienz und Sicherheit von Geschäftsfeldern wie dem Gesundheitssektor, der Banken- und Versicherungsbranche oder der Industrie zu verbessern, müssen wir die Art und das Ausmass des digitalen Wandels antizipieren, um essentielle Rahmenbedingungen zur regulierten Weiterentwicklung der dadurch möglichen Innovationsvielfalt zu schaffen.

In dieser Ausgabe von World of Business Law erfahren Sie unter anderem, welche rechtlichen Herausforderungen sich bei der Regulierung neuer Biotechnologien stellen, welcher Optimierungsbedarf bei Versicherungsbrokerportalen angesichts der Digitalisierung und des Datenschutzes besteht und wie die Schweizer Gesetzgebung und die Strafverfolgungsbehörden Cyberkriminalität bekämpfen. Wir möchten anhand dieser spannenden Beispiele aufzeigen, in welchen Bereichen das Recht vermehrt auf den technischen und gesellschaftlichen Wandel reagiert. Am Ende blicken wir jeweils auf Herausforderungen, die es noch zu bewältigen gibt.

Welche vielfältigen Berufsbilder sich daraus ergeben, zeigen wir in Porträts und Interviews mit Absolventinnen und Absolventen des Wirtschaftsrechtsstudiums: vom Weg zum Rechtsanwalt, wissenschaftlichen Mitarbeitenden oder Dozierenden bis hin zur Karriere im Rechtsdienst einer Grossbank. Ausserdem erwartet Sie ein eindrücklicher und mutiger Bericht der chinesischen Studentin Ying Song, die ihr Wirtschaftsrechtsstudium komplett an der ZHAW absolviert hat. Umgekehrt zeigen Erfahrungsberichte aus dem atemberaubenden Kapstadt und der Summer School in der Metropole London, was Schweizer Studierende in Ausland erlebt haben.

Unser Verein hat im Frühjahr einen neuen Vorstand gewählt, welcher die Vielfalt laufender und neuer Projekte mit viel Energie und Elan weiterträgt. Dies freut mich ausserordentlich, stimmt mich zuversichtlich für die kontinuierliche Weiterentwicklung der World of Business Law und erleichtert mir den Abschied, denn mit dieser Zeitschrift ist viel Herzblut verbunden. Ich möchte mich an dieser Stelle für die tatkräftige Unterstützung der Studiengangleitung Wirtschaftsrecht an der ZHAW bedanken, welche der Verein und die World of Business Law ununterbrochen erfahren darf.

Bleiben Sie gespannt. Wir wünschen Ihnen eine interessante Lektüre.

Angelina Rau
Chefredaktorin World of Business Law



Inhaltsverzeichnis

	Intern
3	Editorial
33	Das sind Wir!
51	Impressum
	Interviews
16	Der Weg ins Legal einer Grossbank
22	Der Weg zum wissenschaftlichen Mitarbeiter
30	From China to Switzerland – an intercultural path to success
46	Der Weg zum Rechtsanwalt
	Themenartikel
5	Der Kampf gegen Cyberkriminelle
	Gründe für das Scheitern der Schweizer Strafverfolger
14	Gen-Revolution unter Anwendung der CRISPR/Cas9-Methode: Rechtliche Herausforderungen bei der Regulierung neuer Biotechnologien
20	Das Internet der Dinge als Herausforderung für das Schweizer Haftpflichtrecht
34	Digitalisierung und Datenschutz
	Auslandberichte
26	Kapstadt – das schönste Ende der Welt
42	The London experience – UCL Summer School

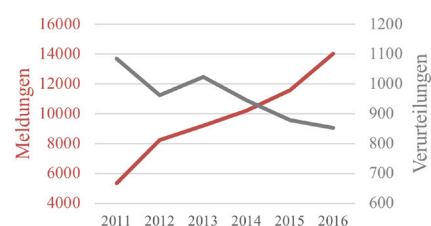
Der Kampf gegen Cyberkriminelle: Gründe für das Scheitern der Schweizer Strafverfolger

° Text von Lea Stühlinger

Trotz steigender Anzahl Meldungen zu Computerdelikten ist die Anzahl Verurteilungen von Cyberkriminellen in der Schweiz rückläufig. Wie dieser Artikel zeigt, sind die Ursachen vielfältig. Fehlende Meldungen zu Delikten, unscharf formulierte Strafnormen, Ressourcenmangel, aber auch Probleme des internationalen Strafrechts tragen zur Problematik bei.

Der Einsatz von digitalen Technologien bei Schweizer Unternehmen ist in den letzten zwei Jahrzehnten exponentiell gestiegen. Die Schweizer Wirtschaft ist daher stark abhängig von einer funktionierenden IT-Infrastruktur. Nicht nur Schweizer Unternehmen, sondern auch Privatpersonen sind auf den Zug der Digitalisierung aufgesprungen. Fast 90 Prozent aller Schweizerinnen und Schweizer zwischen 16 und 76 Jahren nutzen mindestens einmal pro Woche das Internet. Zum Vergleich: Vor zehn Jahren waren es ungefähr 60 Prozent. Diese Entwicklung bringt einerseits viele Chancen mit sich, andererseits wird dadurch eine enorme Angriffsfläche für Cyberkriminalität geschaffen. Die Anzahl der Meldungen zu Cyberkriminalität, die beim Fedpol eingingen, stieg von 2011 bis 2016 von 5530 auf 14033. Cyberkriminelle scheinen die geschaffenen Angriffsflächen vermehrt

zu nutzen. Betrachtet man in der Kriminalstatistik die Verurteilungen aufgrund von Computerdelikten im gleichen Zeitraum, zeigt sich ein etwas anderes Bild: Die Anzahl der Verurteilungen ist von 1085 auf 853 gesunken. Abbildung¹ verdeutlicht die gegenläufige Entwicklung graphisch:



1 | Anzahl Meldungen und Verurteilungen zu Computerdelikten 2011-2016.

Wie kommt es zu dieser gegenläufigen Entwicklung?

Der Kampf der Schweizer Strafverfolgung gegen Cyberkriminelle wird in einer 360-Grad Analyse genau unter die Lupe genommen, um diese Frage beantworten zu können. Durch die Auswertung von wissenschaftlicher Literatur, Publikationen des Bundes und politischen Vorstössen werden mögliche Schwachstellen beziehungsweise Herausforderungen ans Tageslicht gebracht. Die Analyse wird durch Einschätzungen der Thematik von der Abteilung für Cybercrime der Kantonspolizei Zürich ergänzt.

Die Analyse beleuchtet insgesamt sechs Aspekte der Strafverfolgung von Cyberkriminellen in der Schweiz. Sie startet bei den Tätern: Es soll zunächst herausgearbeitet werden, wer überhaupt hinter Cyberangriffen in der Schweiz steckt und worin sich verschiedene Typen von Tätern in Bezug auf Ressourcen und Motivation unterscheiden. Nach den Tätern wird der Fokus auf die Opfer von Cyberangriffen und deren Verhalten nach einem Angriff gelegt. Erst nachdem Täter und Opfer genau untersucht wurden, werden die Tatbestände der Computerdelikte im Schweizer Strafrecht sowie die Strafverfolgung analysiert und mögliche Schwachstellen aufgedeckt. Zuletzt wird der Horizont über die Landesgrenzen hinaus erweitert, um mögliche Ursachen für die fehlenden Verurteilungen von Cyberkriminellen im Kontext des internationalen Strafrechts aufzudecken.

Bevor mit der eigentlichen Analyse der Thematik begonnen werden kann, muss jedoch das Phänomen „Cyberkriminalität“ zuerst begrifflich abgegrenzt werden: Grundsätzlich werden durch den Begriff alle Delikte erfasst, bei denen der Computer Werkzeug oder Ziel einer Tathandlung ist. Bei Cyberkriminalität im Strafrecht wird zwischen zwei Kategorien von Delikten unterschieden: Computerdelikte im engeren und Computerdelikte im weiteren Sinne. Bei Computerdelikten im engeren Sinne werden Daten oder andere Elemente der Informationstechnik geschädigt. Computerdelikte im weiteren Sinne sind „traditionelle“ Delikte, die durch Mittel der Informations- und Kommunikationstechnologie, respektive durch das Internet, begangen werden. Diese Analyse fokussiert insbesondere auf Computerdelikte im engeren Sinne.

Wie bereits erläutert wurde, gilt der Fokus im ersten Teil der Analyse den Cyberkriminellen selbst.

Das Bild des klassischen Hackers muss begraben werden.

Ist die Rede von Cyberkriminellen, fällt schnell einmal der Begriff „Hacker“. Mit diesem Begriff wird meistens die „Gewinnung eines nicht autorisierten Zugangs zu Computersystemen durch eine Einzelperson“ in Verbindung gebracht. Heute steckt hinter Cyberkriminalität jedoch in den meisten Fällen ein gewisses Mass an Organisation und Spezialisierung, sodass das Täterbild des „klassischen Hackers“ begraben werden muss.

Typologie der Täterschaft



2 | Typologie der Täterschaft.

Die Melde- und Analysestelle des Bundes, MELANI, unterscheidet zwischen vier verschiedenen Arten von Cyberkriminellen (Vgl. Abbildung 2): Staatliche Akteure, Cyberkriminelle Organisationen, Cyberaktivisten und Einzel Täter. Die Unterschiede zwischen den verschiedenen Arten von Cyberkriminellen beschreibt MELANI wie folgt: Staatliche Akteure oder staatlich finanzierte Akteure verfügen in der Regel über ein hohes Mass an finanziellen, technischen und personellen Mitteln sowie einen hohen Organisationsgrad.

Bei staatlichen Akteuren muss daher von einem hohen Schadenspotential ausgegangen werden. Ein vergleichbar hoher Ressourceneinsatz und Organisationsgrad kann auch cyberkriminellen Organisationen zugeschrieben werden: Diese können beispielsweise durch gezielte Angriffe Industriespionage betreiben und Daten weiterverkaufen. Sie führen aber auch klassische ungezielte Cyberattacken in Form von DDoS, Spam oder Bots durch. Cyberaktivisten, auch „Hacktivist“ genannt, wollen durch die Angriffe in erster Linie Aufmerksamkeit erhalten, ein Statement abgeben oder an Daten gelangen, die sie anschliessend an die Öffentlichkeit bringen können. Über wesentlich weniger Ressourcen als die bisher aufgezählten Arten von Cyberkriminellen verfügen Einzel Täter.

Alle Tätertypen haben insbesondere eine für Cyberkriminelle typische Gemeinsamkeit: Sie geben ihre Identität aus der realen Welt durch Angriffe in der virtuellen Welt nicht preis. Diese Eigenschaft ist auch einer der wichtigsten Unterscheide zu „klassischen Kriminellen“. Hinzukommt, dass Cyberkriminelle gerade bei ungezielten Angriffen mit wenig Ressourceneinsatz eine Vielzahl von Opfern schädigen können. Dabei nimmt die genutzte Technologie eine Art „Multiplikator-Rolle“ ein. Somit sind grundsätzlich alle Computernutzer potentielle Opfer von Cyberkriminellen – Privatpersonen und Unternehmen. Diese Tatsache unterstreicht die am Anfang des Artikels erläuterte Relevanz der Problematik für die gesamte Schweiz. Gezielte Angriffe werden jedoch als effektiver eingestuft als ungezielte.

Im Zusammenhang mit gezielten Angriffen muss an dieser Stelle der Begriff der kritischen Infrastruktur eingeführt werden: Dabei handelt es sich um „eine Anlage, die für Aufrechterhaltung von unerlässlichen gesellschaftlichen Funktionen verantwortlich ist“. Ein Betreiber von kritischer Infrastruktur ist ein entsprechend beliebtes Angriffsziel für Cyberkriminelle. In der Schweiz geniessen die Betreiber von nationalen, kritischen Infrastrukturen wie Energieversorger, Telekommunikationsunternehmen oder Banken darum erweiterten Schutz durch MELANI.

Herausforderungen

Wie nun deutlich gezeigt wurde, unterscheiden sich die verschiedenen Arten von Cyberkriminellen in Bezug auf Motivation und Ressourcen. Ein erhöhter Organisations- und Spezialisierungsgrad der Täterschaft erschwert die Aufgabe der Strafverfolgung. Zudem ist grundsätzlich jeder Computernutzer ein potentielles Opfer, aber vor allem kritische Infrastruktur ein beliebtes Angriffsziel. Diese Tatsachen führen dazu, dass Strafverfolgungsbehörden ihrerseits mehr Ressourcen aufwenden müssen, um Täter zu fassen und Opfer zu schützen.

Die Opfer beziehungsweise deren Meldeverhalten stehen sogleich im Fokus des nächsten Abschnitts.

Die Opfer sind vielmals mitschuldig an den fehlenden Verurteilungen.

Wird eine Privatperson oder eine Unternehmung Opfer eines Cyberangriffs, so kann entweder an das Bundesamt für Polizei beziehungsweise deren Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) oder an die Melde- und Analysestelle Informationssicherung (MELANI) gemeldet werden. Wie die aufgeführten Zahlen in der Einleitung des Artikels zeigen, sind die Anzahl der Meldungen an die Behörden in den letzten Jahren deutlich gestiegen. Umso erstaunlicher ist die Tatsache, dass bei den meisten Cyberangriffen gar keine Meldung erstattet wird. In einer Studie der ETH Zürich wurden insgesamt 562 Unternehmen befragt. Nur 34 (6 Prozent) gaben an, dass sie wegen eines Vorfalls betreffend Informationssicherheit schon einmal die Polizei eingeschaltet hatten. Ein Teil der nicht gemeldeten Angriffe ist darauf zurückzuführen, dass diese schon im Versuchsstadium durch moderne technische Sicherheitseinrichtungen abgewehrt werden.

Die Gründe für das Nicht-Melden von Angriffen, die nicht abgewehrt werden, sind unterschiedlich. Als Hauptgrund für das Nicht-Melden nannten die meisten Teilnehmer der ETH-Studie, dass sie die Vorfälle für zu wenig gravierend hielten, um die Polizei zu benachrichtigen. Zudem befanden viele der befragten Unternehmen ihre eigenen Massnahmen für effizienter als diejenigen der Polizei. Überraschendes Resultat der Umfrage ist, dass die Angst vor Imageschäden fast von keinem Unternehmen als Grund für die Nicht-Meldung von Vorfällen genannt wurde. Dies muss angesichts einer neueren Schweizer Studie, die von gfs-zürich 2017 durchgeführt wurde, jedoch angezweifelt werden. Denn bei dieser Studie sagten 52 Prozent der Befragten, dass sie Cyberangriffe aus Angst vor Reputationschäden nicht melden möchten.

Nebst einem Reputationsverlust führt eine Cyberattacke auch in vielen Fällen zum Verlust von vertraulichen Daten von Kunden oder Partner. Dies wiederum kann unter Umständen zu Schadenersatzansprüchen auf Grundlage von Gesetz oder Vertrag führen. Insbesondere die Verletzung von Geheimhaltungs- oder Datenschutzvereinbarungen mit Kunden oder Partnern durch eine Datenpanne könnte zu Schadenersatzforderungen führen. Durch entsprechende Spezialversicherungen kann sich ein Unternehmen bis zu einem gewissen Grad absichern. Ein Restrisiko bleibt jedoch. Drohende Schadenersatzklagen können ebenfalls ein Grund sein, einen Cyberangriff nicht zu melden.

Schliesslich ist auch zu betonen, dass das Strafverfahren bei Computerdelikten, welches noch genauer erläutert wird, beziehungsweise Strafverfahren im Allgemeinen nicht in erster Linie auf eine Wiedergutmachung des entstandenen Schadens bei den Opfern abzielen. Viel eher steht die Wiederherstellung des rechtmässigen Zustands im Vordergrund: Durch die Bestrafung muss ein Täter für die Folgen seines normwidrigen Verhaltens einstehen. Ein geschädigtes Unternehmen oder eine geschädigte natürliche Person hat entsprechend wenig intrinsische Motivation, Vorfälle zu melden. Strafverfahren können aber unter Umständen auch bei der Durchsetzung von zivilrechtlichen Ansprüchen helfen, den entstandenen Schaden festzustellen.

Dass eine Zurückhaltung beim Melden von Vorfällen gerade bei Banken, Versicherungen und Grosskonzernen spürbar ist, bestätigte auch die Abteilung Cybercrime der Kantonspolizei Zürich auf Anfrage: „Oftmals wird erst gemeldet, nachdem schon Lösegeld bezahlt wurde oder schon an die Öffentlichkeit durchgesickert ist, dass ein Angriff stattfand.“

Zurzeit wird im Parlament über eine Meldepflicht für schwerwiegende Sicherheitsvorfälle bei Betreibern von kritischer Infrastruktur diskutiert. Die Schweiz wäre nicht das erste Land, welches eine Meldepflicht gesetzlich regelt: Deutschland hat bereits 2016 durch das IT-Sicherheitsgesetz eine solche Meldepflicht eingeführt.

Herausforderungen

Wie dargelegt werden konnte, werden Computerdelikte in der Schweiz nur in den seltensten Fällen oder zu spät an die Behörden gemeldet. Die Ursachen dafür scheinen vielfältiger Art zu sein. Wie in den folgenden Abschnitten noch gezeigt wird, werden die meisten Computerdelikte von Amtes wegen verfolgt. Die Strafverfolgungsbehörden benötigen nichtsdestotrotz so schnell wie möglich Informationen über einen Cyberangriff. Ansonsten ist die Identifizierung der Täterschaft schwierig. Wird also gar nicht oder zu spät gemeldet, kommt es mit grosser Wahrscheinlichkeit nie zu einer Verurteilung.

Im nächsten Schritt, werden die Straftatbestände der Computerdelikte auf den Prüfstand gestellt.

Die Straftatbestände der Computerdelikte hinken der technologischen Entwicklung hinterher.

Wie in den vorherigen Abschnitten bereits dargelegt wurde, kennt Cyberkriminalität viele Gesichter. Die Schaffung von strafrechtlichen Bestimmungen, die alle Arten von Cyberkriminalität abdecken, ist ein entsprechend schwieriges Vorhaben. Im Schweizer Strafrecht sind Cyber-Angriffe im engeren Sinne durch die sogenannten Computerstraftatbestände geregelt. Zu den Computerstraftatbeständen zählen die unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die Datenbeschädigung (Art. 144bis StGB) und der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB). Die Straftatbestände der Computerdelikte wurden 1994 ins Schweizer Strafrecht eingeführt und sind im Prinzip Abwandlungen von traditionellen Vermögensstraftatbeständen. Da Computerdelikte in nur vier Artikeln des Strafgesetzbuches abgehandelt werden, stellt sich die Frage, ob das Schweizer Strafrecht die Angriffsflächen abdeckt, die durch die Digitalisierung geschaffen wurden. Entsprechend der geltenden Lehrmeinung sind die Tatbestände unscharf formuliert worden, was zu zahlreichen Abgrenzungs- und Interpretationsproblemen führt. Zu den Computertatbeständen hat sich auch die Abteilung Cybercrime der Kantonspolizei Zürich auf Anfrage geäußert: „Da viele Straftatbestände im Zusammenhang mit Cybercrime nicht explizit festgelegt sind, werden sie versuchsweise über die üblichen Straftatbestände abgehandelt, dies funktioniert aber nicht immer gut“. Es würden dadurch zu viele Analogien nötig, die nicht immer mit der digitalen Welt zusammenpassen und schliesslich zu Strafbarkeitslücken im Gesetz führten. Getreu dem Grundsatz „Keine Strafe ohne Gesetz“ (Art. 1 StGB und Art. 7 EMRK), kann niemand für Delikte bestraft werden, die das Gesetz nicht ausdrücklich unter Strafe stellt. Ergo können für begangene Computerdelikte nur dann Strafen ausgesprochen werden, wenn das strafbare Verhalten, sowie dessen Folgen, gesetzlich eindeutig festgehalten sind. Die explizit festgelegten Straftatbestände werden nachfolgend beschrieben und hinsichtlich möglicher Unklarheiten oder Lücken kritisch beurteilt.

Art. 143 StGB Unbefugte Datenbeschaffung

1 Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

2 Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Durch die Einführung von Art. 143 StGB hat der Gesetzgeber versucht, die Strafbarkeitslücke bei diebstahlsähnlichen Handlungen zu schliessen. Dies erklärt die Bezeichnung „Datendiebstahl“, welche für Art. 143 StGB ebenfalls zur Anwendung kommt.

Tatobjekt der unbefugten Datenbeschaffung sind unkörperliche Daten, welche für den Täter fremd, also nicht für ihn bestimmt sind. Tathandlung ist das Beschaffen der Daten: Jede Verhaltensweise, durch die der Täter die Verfügungsgewalt über die Daten erlangt. Subjektiv ist nur vorsätzliches Handeln strafbar. Zudem wird eine Bereicherungsabsicht des Täters vorausgesetzt. Eine Tat qualifiziert nur dann als unbefugte Datenbeschaffung, wenn die Daten gegen den unbefugten Zugriff des Täters besonders geschützt waren. Die Abteilung Cybercrime der Kantonspolizei Zürich machte darauf aufmerksam, dass dieses Tatbestandsmerkmal dazu führt, dass Art. 143 StGB bei „Hausfriedensbruch“ einer Datenverarbeitungsanlage nicht einschlägig ist. Auch kein anderer Gesetzesartikel deckt diese Straftat ab, womit dieser fehlende Tatbestand eine Lücke im Gesetz darstellt. Eine weitere Gesetzeslücke besteht hinsichtlich „Datenhehlerei“: Wenn Daten gemäss Art. 143 StGB unbefugt beschafft wurden und dann durch einen Dritten in Kenntnis ihrer unbefugten Beschaffung genutzt werden. Ein entsprechender Tatbestand ist im Schweizer Strafgesetzbuch nicht zu finden. Wie dem Gesetzestext zu entnehmen ist, werden tatbestandsmässige Delikte zum Nachteil eines Angehörigen oder Familiengenossen nur auf Antrag verfolgt. Die Deliktvariante gemäss Abs. 1 ist jedoch ein Offizialdelikt und wird daher von Amtes wegen verfolgt.

Art. 143bis StGB Unbefugtes Eindringen in ein Datenverarbeitungssystem

1 Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

2 Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Dieser Tatbestand soll ein Datenverarbeitungssystem vor Hackern schützen. Im Gegensatz zum vorher erläuterten Tatbestand sind hier nicht Daten selber, sondern ein Datenverarbeitungssystem Tatobjekt, welches für den Täter wiederum fremd ist. Die Tathandlung von Art. 143bis Abs. 1 StGB stellt das Eindringen in das Datenverarbeitungssystem auf dem Wege von Datenübertragungseinrichtungen dar. Das Eindringen ist vollendet, wenn alle Zugangsschranken zur Datenverarbeitung überwunden sind. Vom Tatbestand wird auch eine Überwindung der Zugangsschranken durch Täuschung, Kniffe, List und dergleichen erfasst, wie zum Beispiel durch sogenannte Phishing-Mails. Wie bei Art. 143 StGB bildet auch beim Hackertatbestand Vorsatz das subjektive Tatbestandselement. Handelt ein Hacker mit Bereicherungsabsicht, so ist nicht Art. 143bis, sondern Art. 143 StGB einschlägig. Entsprechend kommen bei Delikten nach Art. 143bis StGB nur nicht-wirtschaftliche Beweggründe für das Eindringen in Frage. Grundsätzlich findet Art. 143bis StGB im Verhältnis zu allen anderen Computerdelikten nur subsidiär Anwendung. Abs. 2 des gerade erläuterten Tatbestandes sanktioniert das Inverkehrbringen oder Zugänglichmachen von Passwörtern, Programmen oder anderen Daten, welche zur Begehung einer strafbaren Handlung nach Ziffer 1 verwendet werden

können. Die Tatbestandsvariante nach Abs. 1 ist ein Antragsdelikt. Diejenige nach Ziff. 2 stellt jedoch ein Offizialdelikt dar.

Art. 144^{bis} Datenbeschädigung

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Hat der Täter einen grossen Schaden verursacht, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Handelt der Täter gewerbsmässig, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden.

Durch den Tatbestand der Datenbeschädigung soll verhindert werden, dass Programme in Umlauf gebracht werden, die Daten beschädigen. Bei diesen Programmen kann es sich um jede Form von Malware handeln, also z.B. Viren oder Trojaner. Aber auch bei einem sogenannten Denial of Service Angriff (DoS) oder einer Distributed Denial of Service Attacke (DDoS) ist dieser Artikel einschlägig. Tatobjekt sind Daten, an denen der Täter nicht oder nicht ausschliesslich berechtigt ist, wobei es bei diesem Tatbestand keines besonderen Schutzes der Daten bedarf. In der Lehre wird kritisiert, dass Ton- und Bilddokumente, die ebenfalls elektronisch gespeichert werden und von grossem Wert sein können, nicht vor Beschädigung geschützt sind. Die Tathandlung besteht gemäss Gesetzestext aus einem Löschen, Verändern oder Unbrauchbarmachen der Daten. Der Taterfolg tritt dann ein, wenn der Datenberechtigte nicht mehr in gewünschter Weise über die beschädigten Daten verfügen kann. Der Wortlaut des Artikels besagt, dass nur Delikte von Amtes wegen verfolgt werden, wenn der Täter grossen Schaden verursacht hat (Ziff. 1 Satz 2).

Durch Ziffer 2 ist auch das Zugänglichmachen von datenschädigenden Programmen strafrechtlich erfasst. Dies entspricht dem sogenannten „Virentatbestand“, der als abstraktes Gefährdungsdelikt eingeführt wurde, um dem grossen Schädigungspotential von Viren Rechnung zu tragen. Datenbeschädigung nach Ziff. 1 und 2 ist nur bei vorsätzlichem Handeln durch den Täter strafbar. Es besteht echte Konkurrenz zwischen dem Tatbestand von Art. 144bis StGB und dem Tatbestand der unbefugten Datenbeschaffung (Art. 143 StGB).

Art. 147 Betrügerischer Missbrauch einer Datenverarbeitungsanlage

1 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.

2 Handelt der Täter gewerbsmässig, so wird er mit Freiheitsstrafe bis zu zehn Jahren oder Geldstrafe nicht unter 90 Tagessätzen bestraft.

3 Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Diese Strafnorm wurde eingeführt, um die Lücke zu schliessen, die dadurch entstanden ist, dass Betrug nach Art. 146 StGB nur dann vorliegt, wenn ein Mensch getäuscht und nicht wenn ein Computer manipuliert wurde. Daher besteht die Tathandlung bei Art. 147 StGB aus einer Manipulation der Datenverarbeitung. Diese kann in der Verwendung unrichtiger oder unvollständiger Daten oder in der unbefugten Verwendung von Daten bestehen. Hinzukommt eine Generalklausel der „vergleichbaren Einwirkung“, die in der Lehre kritisiert wird, da sie die Analogie direkt im Gesetz festschreibt und so dem Bestimmtheitsgebot nicht standhalten dürfte. Den Taterfolg bildet eine Vermögensverschiebung. Das heisst, die Datenmanipulation muss geeignet sein, das Vermögen des Betroffenen unmittelbar zu vermindern. In subjektiver Sicht ist Vorsatz und Bereicherungsabsicht des Täters notwendig. Echte Konkurrenz ist denkbar zu Art. 143 StGB. Wenn jedoch Art. 143^{bis} oder Art. 144^{bis} gleichzeitig anwendbar ist, geht in der Regel Art. 147 StGB vor.

Dieser Tatbestand hat sich mit Blick auf die Urteile seit der Einführung 1994 als wirksam erwiesen: Pro Jahr werden rund 600 Urteile gefällt – so viele wie bei keinem anderen Computerdelikt.

Herausforderungen

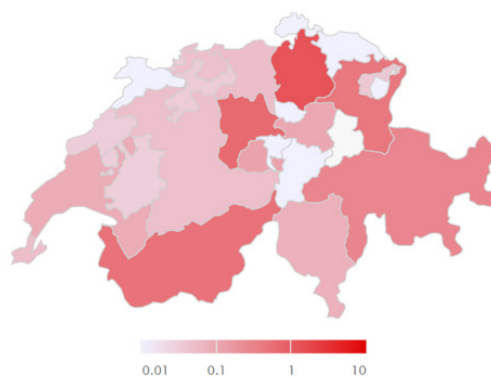
Die gerade beschriebenen Strafnormen der Computerdelikte wurden in den Neunzigerjahren eingeführt und 2012 leicht angepasst. Gleichzeitig konnte in den letzten zwei Jahrzehnten eine rasante Weiterentwicklung der technologischen Möglichkeiten beobachtet werden. Für die Strafverfolgung führt dies zu Schwierigkeiten, denn Cyberkriminelle gehören in vielen Fällen zu den ersten Anwendern von neuen Technologien. Darum muss auch das materielle Strafrecht einer fortwährenden Weiterentwicklung unterzogen werden.

Nur so kann die Nutzung von neuen Technologien durch Cyberkriminelle eingeschränkt beziehungsweise bestraft werden. Wie zudem herausgearbeitet wurde, gibt es in Bezug auf die Straftatbestände der Computerdelikte Lücken und Unklarheiten im Gesetz. Diese sind unter anderem entstanden, weil die Straftatbestände in Anlehnung an die klassischen Vermögensdelikte eingeführt wurden. Die Lücken müssen geschlossen und Unklarheiten verbessert werden. Dabei gilt es die Eigenheiten der Informations- und Kommunikationstechnologie und deren Weiterentwicklungen genau zu berücksichtigen. Nachdem nun analysiert wurde, wie Computerdelikte strafrechtlich erfasst sind, liegt der Fokus im nächsten Abschnitt auf den Zuständigkeiten im Strafverfahren.

Die Kantone sind mit der Strafverfolgung von Cyberkriminellen überfordert.

In der föderalistischen Schweiz sind grundsätzlich die Kantone für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung auf ihrem Hoheitsgebiet verantwortlich. Einzelne Aufgaben sind im begrenzten Rahmen dem Bund zugeteilt (Art. 24 StPO).

Da Computerdelikte zu den Vermögensdelikten des Strafgesetzbuches gezählt werden (zweiter Teil StGB), kann die Staatsanwaltschaft des Bundes selber eine Strafuntersuchung eröffnen, wenn folgende Voraussetzungen erfüllt sind (Art. 24 Abs. 2 StPO): Es muss sich bei der Täterschaft um eine kriminelle Organisation handeln (lit. a) und keine kantonale Strafverfolgungsbehörde darf mit der Sache befasst sein oder die zuständige kantonale Behörde ersucht die Staatsanwaltschaft des Bundes um Übernahme des Verfahrens (lit. b). In der Praxis sind folglich in den meisten Fällen die kantonalen Strafverfolgungsbehörden für Computerdelikte zuständig. Die Schweizer Kantone sind geprägt von starker Heterogenität. Entsprechend verfügen sie auch über unterschiedlich grosse Polizeikorps. In der „Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken“ wurde darum klar betont, dass nur Kantone mit grossen Polizeikorps und enger Zusammenarbeit mit der Wirtschaft und im Sicherheitsbereich tätigen Organisationen fähig sind, umfangreiche Ermittlungen im Bereich der Cyberkriminalität durchzuführen. Abbildung 3 zeigt, dass die Kantone unterschiedlich stark von Cyberkriminalität betroffen sind. Je stärker rot eingefärbt ein Kanton erscheint, desto mehr mit Schadsoftware infizierte Systeme sind in diesem Gebiet zu finden.



3 | Anzahl mit Schadsoftware infizierte Systeme.

Es ist erkennbar, dass der Kanton Zürich sehr stark von Cyberkriminalität betroffen ist. Der Regierungsrat des Kantons Zürich hat im Februar 2015 informiert, dass der Kanton eine Führungsrolle in der Schweiz wahrnimmt und sein national einzigartiges Kompetenzzentrum für Cybercrime noch mehr ausbauen wird. Nach eigenen Aussagen verfügt die Abteilung Cybercrime der Kantonspolizei Zürich über genügend Ressourcen, um die Cyberkriminalität im Kanton bekämpfen zu können.

Die Politik hat jedoch erkannt, dass die restlichen Kantone mit der Bekämpfung von Cyberkriminalität überfordert sind und entsprechende Massnahmen zur Zuständigkeitsverlagerung hin zum Bund lanciert. 2017 hat das Parlament zudem beschlossen, ein Cybersecurity-Kompetenzzentrum auf Stufe des Bundes zu schaffen. Darüber hinaus informierte Bundesanwalt Michael Lauber im November 2017 über eine andere Massnahme, die sich in Planung befindet: Schweizer Staatsanwälte, das Bundesamt für Polizei, die Vereinigung der Polizeikommandanten und die Bundesanwaltschaft setzen sich gemeinsam für die Schaffung von regionalen Kompetenzzentren

zur Bekämpfung von Cyberkriminalität auf kantonaler Ebene ein. Diese Massnahme würde die Zuständigkeit nicht verlagern, sondern die Zusammenarbeit der Kantone stärken.

Herausforderungen

Grundsätzlich sind die Kantone für die Strafverfolgung von Cyberkriminellen zuständig. Viele Kantone verfügen aber nicht über die nötigen Kompetenzen, um die Herausforderungen zu meistern. Ob die Lösung des Problems in der Verlagerung der Zuständigkeit hin zum Bund oder in einer Stärkung der Strafverfolgung auf kantonaler Ebene liegt, werden die politischen Entwicklungen in naher Zukunft zeigen.

Nach den Zuständigkeiten in der Strafverfolgung werden nachfolgend auch die verschiedenen Möglichkeiten der Ermittlungen sowie die vorhandenen personellen Ressourcen kritisch betrachtet.

Nicht fehlende gesetzliche Grundlagen, sondern mangelnde Ressourcen erschweren die Ermittlungen.

Wie schon erläutert wurde, begehen Cyberkriminelle Verbrechen in den meisten Fällen unter Wahrung ihrer Anonymität. Primäres Ziel der Strafverfolgung ist deshalb zunächst die Identifikation und Lokalisierung der Täterschaft. Dabei versagen klassische Ermittlungs- und Beweissicherungsansätze oftmals und müssen auf die Umstände der Internetnutzung übertragen werden.

Schweizer Strafverfolgungsbehörden können bei der Beweissammlung im Internet auf verschiedene Ermächtigungsgrundlagen der Strafprozessordnung (StPO) zurückgreifen. Diese ermächtigen unter anderem zur Beschlagnahme und Durchsuchung von Datenträgern (Art. 246 ff. und 263 ff. StPO), zur Überwachung des Post- und Fernmeldeverkehrs (Art. 269 ff. StPO), zur Observation (Art. 282 f. StPO) oder zum Abruf von Randdaten (Art. 273 StPO). Randdaten sind beispielsweise die IP-Adresse oder die Telefonnummer. Gemäss Art. 273 Abs. 3 StPO können Randdaten rückwirkend maximal sechs Monate verlangt werden. Die Abteilung Cybercrime der Kantonspolizei Zürich vertritt die Meinung, dass gerade diese sechsmonatige Frist eine grosse Herausforderung bei der Strafverfolgung von Cyberkriminellen darstellt: Denn je nachdem wie schnell eine Anzeige erfolgt und wie schnell die Behörden arbeiten, sind die Daten bei den Access-Providern unter Umständen schon nicht mehr verfügbar. Mit der Revision des Bundesgesetzes betreffend Überwachung des Post- und Fernmeldeverkehrs wurde im Parlament eine Vorratsdatenspeicherung von zwölf Monaten diskutiert. In der finalen Fassung sind jedoch wiederum sechs Monate festgelegt worden. Die Revision schuf aber eine gesetzliche Grundlage für den Einsatz von neuen Überwachungstechnologien: Durch die Einführung von Art. 269bis StPO dürfen sogenannte IMSI-Catcher für Überwachungen eingesetzt werden und mit Art. 269ter StPO ist die Verwendung von Staatstrojanern „GovWare“ gesetzlich geregelt. Staatstrojaner dürfen aber nur unter Einhaltung von technischen Auflagen (Art. 269quater StPO) genutzt werden. Dies wird den praktischen Einsatz wohl stark beschränken.

Der Einsatz von Zwangsmassnahmen, wie Durchsuchungen oder Überwachungen, hat immer innerhalb der rechtsstaatlichen Schranken zu erfolgen. Der Schutz der Privatsphäre muss in jedem Fall gewahrt werden (Art. 8 EMRK und Art. 8 BV). Einschränkungen sind gemäss Art. 36 BV nur zulässig, wenn sie auf einer gesetzlichen Grundlage beruhen, im öffentlichen Interesse liegen, verhältnismässig sind und den Kerngehalt der Grundrechte nicht verletzen. Art. 197 StPO konkretisiert diese verfassungsrechtliche Schranke in Bezug auf Zwangsmassnahmen bei Ermittlungen: Es muss eine gesetzliche Grundlage vorhanden sein (lit. a), hinreichender Tatverdacht vorliegen (lit. b), die damit angestrebten Ziele können nicht durch eine mildere Massnahme erreicht werden (lit. c) und die Bedeutung der Straftat rechtfertigt die Zwangsmassnahme (lit. d).

Wie nun verdeutlicht wurde, verfügen die Strafverfolgungsbehörden in der Schweiz über diverse gesetzliche Ermächtigungsgrundlagen, um Cyberkriminelle zu identifizieren und Beweise über die materielle Wahrheit der Delikte zu sammeln. Deshalb stellt sich die Frage, ob die Schweizer Strafverfolgungsbehörden über genügend personelle Ressourcen verfügen, um Ermittlungen durchzuführen und die vorhandenen Mittel in der Praxis zu nutzen. Wie schon erwähnt wurde, sind die meisten Kantone durch kleine Polizeikorps nicht in der Lage, Cyberkriminalität effektiv zu bekämpfen. Zur personellen Situation auf der Ebene des Bundes hat sich der Bundesrat Anfang 2017 geäussert: Der Bund verfüge insgesamt über 86 Stellen zur Bekämpfung von Cyberberrisiken, die sich auf verschiedene Abteilungen verteilen. Bis 2020 soll ein deutlicher personeller Ausbau folgen. Des Weiteren vertritt der Bundesrat klar die Meinung, dass nachrichtendienstliche und forensische Fähigkeiten für das Erkennen, die Verfolgung und den Nachweis von Cyber-Angriffen in Zukunft weiterentwickelt werden müssen. Eine Knappheit an personellen Ressourcen zur Bekämpfung von Cyberkriminalität ist folglich auch beim Bund feststellbar.

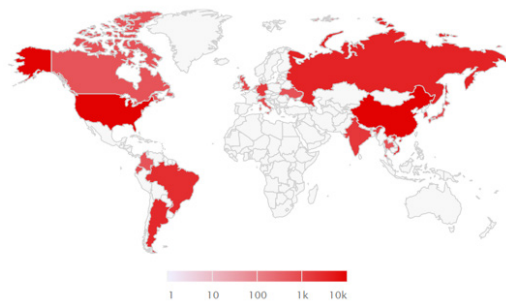
Herausforderungen

Schweizer Strafverfolgungsbehörden können auf diverse gesetzliche Ermächtigungsgrundlagen für die Beweissammlung bei Cyberangriffen zurückgreifen. Wenn durch Zwangsmassnahmen Grundrechte eingeschränkt werden, muss dies zwingend innerhalb des gesetzlich zulässigen Rahmens erfolgen. Unter Umständen kann das die technischen Möglichkeiten eingrenzen oder Verfahren verzögern. Auch die relativ kurze Speicherfrist von Randdaten kann Ermittlungen behindern. Grundsätzlich liegen die Probleme jedoch eher bei mangelnden personellen Ressourcen. Es scheint eindeutig Bedarf für mehr qualifiziertes Ermittlungspersonal zu geben – beim Bund und den Kantonen.

Ein letzter Aspekt der Strafverfolgung von Cyberkriminellen, die Internationalität, soll im folgenden Abschnitt genauer untersucht werden.

Ein globales Problem wie Cyberkriminalität kann die Schweiz nicht im Alleingang bekämpfen.

Ein die Ermittlungen im Bereich Cyberkriminalität erschwerender Faktor wurde bisher noch nicht erwähnt: Cyberkriminalität macht nicht Halt an den Grenzen des Nationalstaates, sondern ist ein internationales Problem. Gemäss einer Studie, welche vom Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung durchgeführt wurde, sind über 50 Prozent aller Fälle von Cyberkriminalität transnational, betreffen also mindestens zwei verschiedene nationale Rechtssysteme. Abbildung 4 zeigt durch die rote Einfärbung, von welchen Ländern aus, die meisten Cyberangriffe auf die Schweiz lanciert werden. Die Abbildung verdeutlicht, den globalen Umfang von Cyberangriffen in der Schweiz klar.



4 | Die Schweiz angreifende Systeme pro Land.

In welchen Fällen sind Schweizer Gerichte überhaupt zuständig? Die Anknüpfung der staatlichen Strafgewalt wird nach dem Territorialitätsprinzip (Art. 3 Abs. 1 StGB) an den Begehungsort eines Delikts geknüpft. Der Begehungsort kann nach dem Ubiquitätsprinzip mit dem Ort der Tathandlung oder mit dem Ort des Erfolgeintrittes identisch sein. Grundsätzlich liegt bei den Computerdelikten der Begehungsort an dem Ort, von welchem aus Programmbefehle eingegeben und abgesendet worden sind. Dieser Ort ergibt sich in erster Linie aus der IP-Adresse. Subsidiär ist auch eine Anknüpfung an den Ort des Erfolgeintrittes möglich. Zusätzlich besteht die Möglichkeit der Zuständigkeit Schweizer Gerichte gemäss staatsvertraglicher Verpflichtung nach Art. 6 StGB. Bei Computerdelikten ist insbesondere an eine Verpflichtung der Schweiz durch die Bestimmungen des Übereinkommens über die Cyberkriminalität (CCC) möglich. In einem Pilotverfahren kam es 2016 erstmals zu einer Anklage gestützt auf Art. 6 StGB: Bis 2016 erfasste die Bundesanwaltschaft 255 internationale Phishing-Fälle. Die Beschuldigten wurden des gewerbsmässigen betrügerischen Missbrauchs einer Datenverarbeitungsanlage (Art. 147 Abs. 1 und Abs. 2 StGB), sowie des mehrfachen Versuches desselben Delikts im verkürzten Verfahren angeklagt. Die Bundesanwaltschaft vertrat bei der Anklage die Meinung, dass die Schweiz auch für die Beurteilung der im Ausland durch ausländische Personen gegen ausländische Opfer begangenen Straftaten zuständig ist. Das Bundesstrafgericht hingegen verweigerte die Anklage aufgrund mangelnder Zuständigkeit. Das Beispiel des Pilotverfahrens verdeutlicht, dass die Zuständigkeit von Schweizer Gerichten bei grenzüberschreitenden Computerdelikten nicht immer eindeutig bestimmbar ist.

Auch bei grenzüberschreitenden Ermittlungen im Zusammenhang mit Computerdelikten treten vermehrt Schwierigkeiten auf. Um die Ermittlungen zu erleichtern, wurde zu Beginn der Jahrtausendwende das Übereinkommen über die Cyberkriminalität (CCC) verabschiedet. Für die Schweiz ist es am 1. Januar 2012 in Kraft getreten. Das Übereinkommen haben fast alle europäischen Staaten und auch Staaten, wie USA, Kanada, Australien und Japan unterzeichnet. Ziel des Übereinkommens ist insbesondere eine gut funktionierende Zusammenarbeit der Staaten in Strafsachen. Mit Artikel 32 enthält das Übereinkommen die Grundlage für den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten ohne Einhaltung des Rechtshilfverfahrens. Die Zugriffsbefugnis bezieht sich einerseits auf öffentlich zugängliche Daten (lit. a) und andererseits auf nicht öffentliche Daten (lit. b). Auf letztere Daten kann gemäss Gesetzeswortlaut mit freiwilliger Zustimmung der Person, die rechtmässig zur Herausgabe der Daten befugt ist, zugegriffen werden. Diese freiwillige Herausgabe der Daten auf Basis des Abkommens funktioniert gemäss Aussagen der Abteilung Cybercrime der Kantonspolizei Zürich grundsätzlich relativ gut. Mit einigen wenigen Ländern gäbe es jedoch immer wieder Probleme. Nicht alle Staaten sind gewillt, zum Schutz des Cyberspace einen Teil beizutragen. Wenn die Voraussetzungen für die freiwillige Herausgabe der Daten nicht erfüllt sind, muss der ordentliche Rechtshilfeweg beschritten werden. In diesem Fall sind in der Schweiz die Vorschriften des Bundesgesetzes über internationale Rechtshilfe in Strafsachen (IRSG) anwendbar. Der Nachteil eines ordentlichen Rechtshilfverfahrens ist der zeitliche Aspekt: Ein solches Verfahren kann sich über mehrere Monate hinziehen. Dies ist insbesondere im Zusammenhang mit den erwähnten Speicherfristen von Randdaten problematisch.

Herausforderungen

Cyberkriminalität ist keine rein nationale, sondern eine internationale Herausforderung für die Strafverfolgungsbehörden. Die Zuständigkeit der Schweizer Gerichte bei internationalen Fällen von Cyberkriminalität ist teilweise umstritten, wie der Phishing-Pilotfall deutlich machte. Zudem profitiert die Schweiz zwar vom grenzüberschreitenden Zugriff auf gespeicherte Computerdaten durch das Übereinkommen über die Cyberkriminalität, es scheint trotzdem immer wieder zu Problemen in der internationalen Strafverfolgung zu kommen. Dies ist vor allem der Fall, wenn die Voraussetzungen für die Herausgabe von Daten via CCC nicht erfüllt sind und darum der ordentliche Rechtshilfeweg bestritten werden muss.

Fünf Verbesserungsvorschläge, um Cyberkriminelle zukünftig das Handwerk legen zu können.

Die Strafverfolgung von Computerdelikten in der Schweiz wurde kritisch analysiert und Herausforderungen in allen Bereichen herausgearbeitet. Diese Herausforderungen sind mögliche Erklärungen dafür, dass es in der Schweiz trotz steigender Anzahl Cyberangriffe nicht zu mehr Verurteilungen von Cyberkriminellen kommt. Die dargelegten Herausforderungen sind aber in keiner Weise eine abschlies-

sende Ursachenauflistung. Dies würde den Rahmen dieses Fachartikels sprengen. Abschliessend werden die Herausforderungen zusammengefasst und zuletzt in Verbesserungsvorschläge umgewandelt.

Zu Beginn wurde verdeutlicht, dass moderne Cyberkriminelle oftmals in organisierter Form agieren und bei Angriffen verstärkt Ressourcen einsetzen. Dies führt dazu, dass auch Strafverfolgungsbehörden stärker gefordert sind, um die Täter zu identifizieren und verurteilen zu können. Nebst den Herausforderungen durch die Täter, wurde ersichtlich, dass auch das Verhalten der Opfer nach einem Angriff zu den fehlenden Verurteilungen beiträgt: Viele Cyberangriffe in der Schweiz werden gar nicht gemeldet. Die Rechtsnormen der Computerdelikte wurden ebenfalls geprüft. Dabei konnten Lücken und Unklarheiten aufgedeckt werden, welche einem Strafverfahren unter Umständen die gesetzliche Grundlage entziehen. Ausserdem stellte sich heraus, dass materielles Strafrecht gerade bei Computerdelikten stets weiterentwickelt werden muss, um mit dem technologischen Wandel Schritt halten zu können. Grundsätzlich verfügen die Strafverfolgungsbehörden in der Schweiz jedoch über eine Vielzahl von Möglichkeiten in den Ermittlungen, die dem technologischen Stand unserer Zeit entsprechen. An der Beantwortung der Frage, ob diese durch genügend ausgebildetes Personal genutzt werden können, bestehen begründete Zweifel. Vor allem die Kantone scheinen mit der Bekämpfung von Cyberkriminalität stark gefordert oder gar überfordert zu sein. Eine Zuständigkeitsverlagerung hin zum Bund oder eine Stärkung der Zusammenarbeit der Kantone in dieser Hinsicht muss auf jeden Fall in Erwägung gezogen werden. Zuletzt wurde erörtert, dass Cyberkriminalität eine grenzüberschreitende Problematik ist. Dies führt dazu, dass die Zuständigkeit der Schweizer Gerichte nicht in allen Fällen eindeutig bestimmbar ist. Hinzukommt, dass Ermittlungen durch die Internationalität der Delikte erschwert werden, auch wenn durch das CCC eine erleichterte Herausgabe von Daten ermöglicht wird.

Die Herausforderungen für die Schweizer Strafverfolgungsbehörden, welche sich in dieser Analyse herauskristallisiert haben, können mit hoher Wahrscheinlichkeit nicht von heute auf morgen gemeistert werden. Wichtig scheint jedoch, dass in allen aufgezeigten Bereichen schon in absehbarer Zukunft Verbesserungen angestrebt werden:

- I. Opfer müssen stärker dazu ermutigt werden, Cyberangriffe zu melden.
- II. Das materielle Strafrecht muss fortlaufend an technologische Entwicklungen angepasst werden.
- III. Die Strafverfolgungsbehörden benötigen genügend qualifiziertes Personal, um Ermittlungen durchführen zu können.
- IV. Es braucht eine Stärkung der Kantone bei der Bekämpfung von Cyberkriminalität oder eine Zuständigkeitsverlagerung hin zum Bund.
- V. Die internationale Kooperation in der Strafverfolgung ist weiter zu pflegen und auszubauen.

**INTERESSEN-
VERTRETUNG**



TECHSHOP



techshop.vszhaw.ch

MITSPRACHE



vszhaw.ch

BRAINSTORM



brainstorm.vszhaw.ch

CAMPUS.FM



campusfm.vszhaw.ch

**STUDITREFF
FREIFACH
SEMESTERPARTYS**



**THEATER-
GRUPPE**



Gen-Revolution unter Anwendung der CRISPR/Cas9-Methode: Rechtliche Herausforderungen bei der Regulierung neuer Biotechnologien

° Text von Angelina Rau

Die CRISPR/Cas9-Technologie ermöglicht gezielte Eingriffe in das Erbgut (Genomeditierung). Man kann damit Krankheiten heilen, aber auch bestimmte Merkmale verändern, ohne einen therapeutischen Ansatz zu verfolgen (sog. Enhancement). Im Gegensatz zu herkömmlichen Methoden für Eingriffe in das Erbgut ist CRISPR/Cas9 vielseitig anwendbar – bei Menschen, Tieren oder Pflanzen. Selten wurden mit einer Entdeckung gleichzeitig derart viele neue Schnittstellen geschaffen, die Bereiche wie die Digitalisierung (Big Data, Biobanks), synthetische Biologie etc. in einem solchen Ausmass tangieren. Seit der Publikation von JINEK et al. im Jahr 2012, die zeigt, wie diese neue Technologie als Werkzeug in der Gentechnik eingesetzt werden kann, ist die Zahl wissenschaftlicher Publikationen dazu exponentiell gestiegen.

Stand der Forschung

Rund um den Globus wird Forschung mit CRISPR/Cas9 betrieben, die vielversprechende Ergebnisse zutage fördert. Auch Versuche an nicht lebensfähigen Embryonen wurden bereits unternommen, was die Forderung nach einem weltweiten Moratorium der neuen Technologie für gewisse Anwendungen im Humanbereich auf den Plan rief. Damit ist die Frage nach einer gesetzlichen Regulierung dieser neuen Biotechnologie in der Humanmedizin und Humanforschung in den Vordergrund gerückt.

Aktuelle Gesetzgebung im Humanbereich

Während die somatische Gentherapie weitestgehend unumstritten ist, und die geltende Rechtsordnung deren Anwendungsmöglichkeiten angemessen reguliert, sind Keimbahneingriffe unter der geltenden Rechtsordnung ausnahmslos verboten. Die Schweiz weist damit eine der restriktivsten Rechtsordnungen in Europa in der Fortpflanzungsmedizin auf. Der internationale Vergleich zeigt, dass ausländische Gesetzgeber für die Regulierung am häufigsten einen Mittelweg einschlagen. Keimbahneingriffe an Embryonen, die ausgetragen und geboren werden sollen, sind überall verboten. Damit die Forschung nicht gänzlich verunmöglicht wird, bleiben Keimbahneingriffe zu blossen Forschungszwecken an Embryonen (die nicht ausgetragen werden dürfen) unter restriktiven Voraussetzungen zugelassen. Dabei haben China und Grossbritannien die liberalsten Gesetzgebungen. Jüngst wurde in Grossbritannien der erste Eingriff in das Genom eines Embryos von der Human Fertilisation and Embryology Authority (HFEA) bewilligt. In der Schweiz sind die Präimplantationsdiagnostik (PID) und die Gewinnung von embryonalen Stammzellen (ES) aus überzähligen Embryonen vom Verbot des Art. 119 Abs. 2 lit. a BV ausgenommen. Bis dato wurde der Umgang mit überzähligen Embryonen lediglich in Bezug auf die Stammzellenforschung gesetzlich geregelt. Die als Folge einer PID überzähligen Embryonen dürfen sonst nicht für die Forschung genutzt werden. Eben-

so dürfen Embryonen hierzulande auch nicht eigens für die Forschung hergestellt werden. Darüber hinaus ist die Rechtsstellung des Embryos in der Schweiz nicht hinreichend geklärt, was weiter zur inkohärenten Regelung für die Embryonenforschung beiträgt. Daraus resultiert eine unbefriedigende Situation für die Grundlagenforschung. Eine Ausweichmöglichkeit bieten induzierte pluripotente Stammzellen (iPS), die anstelle von ES für die Forschung im Zusammenhang mit CRISPR herangezogen werden können und als ethisch und rechtlich unbedenklich gelten. Die diesbezügliche Forschung ist jedoch zum jetzigen Zeitpunkt noch nicht dahingehend ausgereift, dass iPS in der Praxis ausnahmslos als Ersatz für ES zur Anwendung kommen. Somit erübrigt sich derzeit eine Diskussion der aktuellen Gesetzeslage bezüglich Embryonenforschung noch nicht.

Angesichts der zu erwartenden Weiterentwicklung von CRISPR/Cas9 wird die Wissenschaft bezüglich verbrauchender Embryonenforschung weiterhin Druck ausüben. Entschiede sich die Schweiz dereinst, Keimbahneingriffe zuzulassen, setzte dies Revisionen auf diversen gesetzgeberischen Stufen voraus: Teilrevision BV und/oder Streichung Art. 119 Abs. 2 BV, allenfalls Kündigung BMK, Revision Embryonenforschungsgesetzgebung. Insgesamt lässt sich feststellen, dass neue Biotechnologien in der Humanmedizin und Humangenetik den Gesetzgeber bereits zu Revisionen in tangierten Bereichen veranlasst haben. Das Interesse der Schweiz an der Thematik wird nicht zuletzt auch durch die Partizipation am International Bioethics Committee verdeutlicht. Aktuell lassen die fehlende technische Reife und gesellschaftliche Auseinandersetzung und die damit verbundene Frage, ob Keimbahneingriffe das Selbstbestimmungsrecht verletzen, eine Gesetzesänderung in weiter Ferne erscheinen.

Liberalisierungstendenz in der Bevölkerung?

Neben den technischen Entwicklungen lassen die Ergebnisse der vergangenen Volksabstimmungen über die Revision der Artikel 118b und 119 BV sowie die Änderung des FMedG und des StFG eine Liberalisierungstendenz in der gesellschaftlichen Haltung erkennen. Unter Fachpersonen herrscht Konsens bezüglich der Notwendigkeit einer transparenten, öffentlichen Debatte. Daneben verdeutlicht der Anstieg der Finanzierungsmittel für Forschung und Entwicklung an neuen Biotechnologien das ökonomische Interesse an CRISPR/Cas9. Ein Unsicherheitsfaktor besteht bis auf Weiteres wegen der weltweit anhängigen Patentstreitigkeiten, deren Ausgang die praktischen Anwendungen und mithin die Bedeutung der neuen Technologie für den Innovationsprozess mitprägen werden.

Ausblick

Der Regulierungsdruck, den CRISPR/Cas9 als neue Querschnittstechnologie mit zunehmender Anwendungsreife auslöst, wird auch auf den schweizerischen Gesetzgeber wirken. Daher sollte die öffentliche Debatte in Bezug auf Keimbahneingriffe bereits jetzt initiiert werden. Dies bietet der Bevölkerung die Gelegenheit, einen ethischen Reflexionsprozess zu durchlaufen – vorbereitend zur Debatte einer möglichen Gesetzesänderung.

Der Weg ins Legal einer Grossbank

° Ein Interview mit Tobias Burger, M Law, Rechtsdienst Credit Suisse

- Das Interview wurde schriftlich geführt von Amina Ouakrim.



Tobias Burger

Guten Tag Herr Burger, bitte stellen Sie sich dem Leser vor.

Mein Name ist Tobias Burger, ich bin 28 Jahre alt und komme aus Baden. Heute arbeite ich im Rechtsdienst einer Schweizer Grossbank. Vor meinem Studium an der ZHAW habe ich eine Banklehre mit Berufsmaturität absolviert und danach den MLaw an der Universität Luzern erworben.

Warum haben Sie sich damals für ein Wirtschaftsrechtsstudium entschieden?

Während dem KV habe ich erste Erfahrungen mit „rechtlichen Fragestellungen“ sammeln können. Eine richtige Vorstellung über die Tragweite dieses Fachgebietes hatte ich damals aber ehrlich gesagt noch nicht. Für das Wirtschaftsrechts Studium habe ich mich dann u.a. deshalb entschieden, weil es im Vergleich zum Betriebsökonomiestudium in der Schweiz einmalig ist und damit auch ein gewisses Alleinstellungsmerkmal bietet. Bereits nach kurzer Zeit an der ZHAW wurde mein Interesse für die Wissenschaft Recht geweckt und mir wurde klar, dass ich die richtige Entscheidung getroffen hatte.

Würden Sie sich nochmals für den Studiengang Wirtschaftsrecht entscheiden?

Wenn ja, warum?

Ja, auf jeden Fall. Das Wirtschaftsrechtsstudium ist m.E. eine hervorragende Grundlage für die spätere Berufstätigkeit im Schnittpunkt zwischen Wirtschaft und Recht. Der Studiengang vermittelt ein solides und breites Grundlagenwissen sowohl im juristischen als auch im ökonomischen Bereich.

Haben Sie während des Studiums gearbeitet? Wenn ja, was war Ihre Tätigkeit und wie viel Stellenprozente haben Sie gearbeitet?

Ja, trotz Vollzeitstudium habe ich während der meisten Zeit nebenbei gearbeitet. Im ersten Studienjahr habe ich nur während den Semesterferien gearbeitet, im Winter als Lagerleiter in einem Schneesportlager, im Sommer auf der Bank bei welcher ich bereits vor dem Studium angestellt war. Im zweiten Studienjahr habe ich dann ca. 20-30% in der Buchhaltung bei einem Start-Up gearbeitet. Für das dritte Studienjahr habe ich durch den Absolvententag der ZHAW eine Stelle bei einer Versicherung gefunden, wo ich dann in einem 40% Pensum arbeiten konnte.

Welchen Nutzen haben Sie daraus gezogen?

Je nach Tätigkeit konnte ich mein Wissen aus dem Studium einbringen und teilweise sogar vertiefen. In erster Linie hat mir die Arbeit allerdings ermöglicht das Studium zu finanzieren. Trotzdem war es mir wichtig einen Job zu haben, von dem ich für die spätere Berufstätigkeit etwas profitieren konnte.

Wie verliefen die Vorbereitungen für die Passarellenprüfungen an der Unilu?

Gut, ich habe alle Prüfungen im ersten Anlauf bestanden. Im Wesentlichen habe ich die Passarellenfächer als Vertiefung der an der ZHAW erworbenen Grundkenntnisse empfunden. Der Aufwand darf sicher nicht unterschätzt werden, er ist mit dem in etwa gleichen Einsatz wie für die ZHAW aber gut zu bewältigen.

In wie vielen Semestern haben Sie diese absolviert? Haben Sie die damaligen Empfehlungen der Studienberatung berücksichtigt?

Da ich auch während dem Studium an der Uni Luzern weiterhin 40% gearbeitet habe, verteilte ich die Prüfungen auf 4 Semester. Mir war wichtig, dass ich genügend Zeit für die Passarellenfächer zur Verfügung habe und nebenbei trotzdem bereits einige Masterfächer absolvieren kann. Ich bin deshalb nicht einer spezifischen Empfehlung gefolgt, sondern habe den Stundenplan so gelegt, dass er für mich persönlich passt. Diese Flexibilität habe ich sehr geschätzt, was sicher auch ein grosser Vorteil des Masterstudiums an der Universität Luzern ist.

Hatten Sie die Möglichkeit in Luzern Anschluss zu anderen Studierenden, als diejenigen, die Sie bereits von der ZHAW kannten, zu finden?

Ich denke das ist – wie auch in anderen Lebenssituationen – eine Frage der eigenen Persönlichkeit. Wenn man neue Bekanntschaften machen und sich integrieren möchte, sollte man auf die anderen Leute zugehen und sich aktiv am Studienleben beteiligen. An der Universität Luzern werden den Studierenden dazu reichlich Gelegenheiten geboten, sei es durch die meist angenehme Klassengrösse in den Masterfächern oder durch verschiedene Anlässe und Parties der verschiedenen Studentenvereine.

Haben Sie während den Passarellenprüfungen bereits Fächer aus dem regulären Masterprogramm belegt?

Ja, ich habe jeweils ein bis zwei Masterfächer pro Semester besucht. Für mich persönlich hat das so gepasst, da es eine gewisse Abwechslung zu den Grundlagenfächern bot und man auch mit Leuten aus höheren Semestern in Kontakt kam. Ich denke es ist aber wichtig, dass man die Passarellenfächer dadurch nicht vernachlässigt.

Welche Vorlesungen aus dem regulären MA haben Sie hauptsächlich besucht? Welche können Sie besonders empfehlen?

Mir haben insb. die Seminare sehr gut gefallen. Ein grosser Vorteil ist, dass man i.d.R. keine regelmässigen Vorlesungen hat, sondern meist als Gruppe ein Themengebiet aufarbeitet und dann an einem zwei- bis dreitägigen Seminar präsentiert. Ausserdem steht dann die Note bereits während dem Semester fest und man kann sich in der Prüfungszeit voll und ganz auf die Passarellenfächer konzentrieren. Thematisch habe ich Vorlesungen aus verschiedensten Rechtsgebieten besucht. Am meisten interessiert haben mich aber privatrechtliche Themen und insb. das Finanzmarktrecht.

Haben Sie ein Semester an einer anderen Universität besucht? Wenn ja, würden Sie dies weiterempfehlen?

Ja, ich habe tatsächlich ein „Austauschsemester“ an der Universität Zürich gemacht. Ich fand es sehr interessant, die Gemeinsamkeiten und Unterschiede der beiden Universitäten persönlich zu erleben. Allen, die aus persönlichen oder beruflichen Gründen keine Universität im Ausland besuchen können oder möchten, kann ich diese Alternative sehr empfehlen.

Wie verlief Ihr Einstieg in die Berufswelt nach dem Studium, was waren die Schwierigkeiten?

Genau gesagt erfolgte mein Einstieg in die Berufswelt bereits während dem Studium, denn nach einem Sommerpraktikum im Rechtsdienst einer Grossbank wurde mir ein Teilzeitarbeitsvertrag offeriert, den ich dann nach Abschluss des Studiums auf eine 100-Prozent Stelle ausweiten konnte.

War Ihnen von Anfang an klar, dass Sie den MLaw an der Universität Luzern absolvieren möchten?

Nein, das hat sich im Verlauf des Studiums so ergeben. Ich habe lange mit dem Gedanken gespielt, wie viele meiner Kommilitoninnen und Kommilitonen, eine Stelle in der Wirtschaftsprüfung oder Steuerberatung zu suchen. Letztlich habe ich mich aber doch dazu entschlossen, meine juristischen Kenntnisse weiter zu vertiefen.

„Nach meiner Erfahrung gibt es insbesondere in der Finanzindustrie einige sehr interessante Stellen in juristischen Bereichen.“

Haben Sie den Absolvententag oder Firmenworkshops während des Studiums besucht? Wenn ja, welche Erfahrungen haben sie damit gemacht?

Ja, den Absolvententag habe ich besucht und dort auch erfolgreich eine Teilzeitstelle gefunden. Ich fand es sehr interessant, an einem Tag gleich mehrere potenzielle Arbeitgeber kennenzulernen und mit den jeweiligen HR-Vertretern zu sprechen.

Wie schätzen Sie die beruflichen Chancen (Karrieremöglichkeiten) ohne Anwaltspatent ein?

Nach meiner Erfahrung gibt es insbesondere in der Finanzindustrie einige sehr interessante Stellen in juristischen Bereichen. Es stimmt allerdings, dass im Bewerbungsprozess oftmals ein Anwaltspatent gewünscht wird. Wenn dies nicht geplant ist, ist es deshalb umso wichtiger, dass man sich bereits während des Studiums um eine Stelle beim Wunsch-Arbeitgeber bemüht. Viele Banken und Versicherungen bieten Praktika während den Semesterferien oder sogar Teilzeitarbeitsstellen für Studierende an. Wenn man sich dort beweist und engagiert arbeitet, können sich auch ohne Anwaltspatent sehr interessante Möglichkeiten ergeben.

Wie lautet Ihre Berufsbezeichnung und was sind Ihre Tätigkeiten? Können Sie uns einige Beispiele aus dem Alltag nennen?

Ich arbeite derzeit in einem spezialisierten Team innerhalb des Rechtsdienstes einer Grossbank. Unser Team kümmert sich primär um rechtliche Fragestellungen, die sich aus dem Börsenhandel ergeben (z.B. Verträge mit Kunden und Brokern). Ausserdem beraten wir interne Projekte im Zusammenhang mit der Umsetzung von regulatorischen Anforderungen.

Was hat Sie dazu bewogen, sich bei einer Grossbank zu bewerben?

Ich habe meine Lehre bei einer Regionalbank absolviert und das Bankengeschäft hat mich schon damals fasziniert. Nach einigen Erfahrungen in anderen Branchen stellte ich fest, dass ich mich in der Finanzbranche am wohlsten fühle. Im Vergleich zu einer Regionalbank bietet eine Grossbank nochmals einiges mehr an interessanten Tätigkeitsbereichen und für Studenten gibt es gute Einstiegsmöglichkeiten.

Warum ist dieser Beruf interessant (Herausforderungen)? Was gefällt Ihnen gut, was eher weniger?

Ich lerne beinahe jeden Tag etwas Neues. Unser Team interagiert mit sehr vielen Stakeholdern innerhalb der Bank und deckt ein breites Spektrum an Fragestellungen ab. Das macht die tägliche Arbeit sehr abwechslungsreich und spannend. Ausserdem gefällt mir die Internationalität in einem global tätigen Unternehmen. Man trifft hier Leute aus fast allen Teilen der Welt und lernt so auch unterschiedliche Denk- und Arbeitsweisen kennen.

Welche Fähigkeiten sind vorausgesetzt?

Ich denke das wichtigste ist, dass man gut im Team und generell mit anderen Personen zusammenarbeiten kann. Ebenfalls sehr wichtig ist eine präzise Ausdrucksweise, auf Deutsch und vor allem auch auf Englisch.

Mussten Sie sich zusätzliches Fachwissen aneignen? Wie sehen die Weiterbildungsmöglichkeiten aus?

Learning on the job ist hier das Stichwort. Mein Arbeitgeber bietet in diesem Bereich diverse Möglichkeiten, seien es Infoveranstaltungen oder sog. web based trainings. Daneben ist natürlich die Anwendung des erlernten juristischen Handwerks von grosser Bedeutung. Oftmals geht es darum, einen spezifischen Sachverhalt genau zu erfassen, die relevanten Abklärungen zu treffen und danach einen präzisen Lösungsvorschlag zu formulieren. Bei dieser Tätigkeit gewinnt man fortlaufend neues Fachwissen und wichtigen Erfahrungen.

Auch Weiterbildungsmöglichkeiten gibt es diverse. Sehr beliebt ist z.B. ein Certificate of Advanced Studies (CAS) das von verschiedenen Universitäten und Fachhochschulen in diversen Fachgebieten angeboten wird.

Vielen Dank!

„Ich denke das wichtigste ist, dass man gut im Team und generell mit anderen Personen zusammenarbeiten kann.“

Stellenbörse und CV-Datenbank online
www.absolvententag.ch

DONNERSTAG
28. FEB 2019
Eulachhallen
Winterthur



**Dein Sprungbrett
in die Karriere**

absolvententagzhaw

Das Internet der Dinge als Herausforderung für das Schweizer Haftpflichtrecht

Eine rechtliche Analyse im Rahmen von Smart Objects im B2C-Bereich

° Text von Tenzin Netsang

Das Internet der Dinge steht für die Vernetzung der physischen mit der digitalen Welt. Von der app-gesteuerten Lampe über intelligente Herzschrittmacher bis hin zu selbstfahrenden Fahrzeugen – den Anwendungsfeldern sind kaum Grenzen gesetzt. Ausgestattet mit Sensoren, Prozessoren und Netzwerktechnik werden immer mehr Gegenstände des täglichen Lebens zu sogenannten Smart Objects. Die Entwicklungen im Internet der Dinge – insbesondere die zunehmende Vernetzung – führen zu einer Änderung des haftpflichtrechtlichen Umfelds. Die Rechtsanwendung ist konfrontiert mit neuen Sachverhalten und Haftungsfragen. Die Vermischung von digitalen und physischen Wertschöpfungsstufen im Internet der Dinge ergeben komplexe Mehrebenensysteme, in denen unterschiedliche Marktteilnehmer beteiligt sind.

Wer ist Vertragspartner beim Erwerb eines Smart Objects?

Für den Kunden geht es beim Erwerb eines Smart Objects aufgrund dessen physischen und digitalen Nutzens i.d.R. um zwei vertragliche Aspekte. Der erste Aspekt ist die Übereignung des physischen Kaufgegenstandes. Der zweite Aspekt stellt die Gewährleistung der digitalen Dienstleistungen des Smart Objects dar, welche für die bestimmungsgemässe Funktionsfähigkeit vorausgesetzt sind. Die Wesensveränderung herkömmlicher Produkte wie Lampen, Kühlschränke oder Armbänder zu Smart Objects hat dazu geführt, dass mit dem Erwerb solcher Produkte neue Vertragspartner hinzutreten. Der Kunde schliesst typischerweise nicht mehr nur einen Kaufvertrag mit dem Verkäufer ab, sondern tritt abhängig von den Umständen auch in Vertragsbeziehungen mit Dritten.

Von wem kann Schadenersatz gefordert werden?

Wegen dieser neu hinzutretenden Vertragspartner und den unterschiedlichen Vertragsbeziehungen im Rahmen des Erwerbs von Smart Objects, erweist sich auf vertragsrechtlicher Ebene das Auffinden des Anspruchsgegners bei einem Schaden durch eine Fehlfunktion als problematisch. Von wem kann Schadenersatz gefordert werden, wenn zum Beispiel der intelligente Kühlschrank explodiert? In Frage kommen neben dem Verkäufer auch Dritte, wie der Softwarelieferant oder der Hersteller. Für den Kunden wird es zusätzlich komplex, wenn der Verkäufer nach einer gewissen Dauer nicht mehr für bestimmte Leistungen haftet, jedoch Dritte für ihre Leistungen einstehen müssen.

Abhängigkeit von digitalen Dienstleistungen

Eine weitere Schwierigkeit stellt die Abhängigkeit der Smart Objects von der dauerhaften Erbringung digitaler Dienstleistungen dar. Hier ist die Funktionsfähigkeit der integrierten und ausgelagerten Software eines Smart Objects von wesentlicher Bedeutung. Lässt sich die smarte LED-Lampe nicht mehr von der Ferne steuern, weil die ausgelagerte Applikationssoftware nicht mehr funktioniert oder die integrierte Standardsoftware fehlerhaft ist, so ist der bestimmungsgemässe Gebrauch dieses Produktes nicht mehr gewährleistet.

In diesem Zusammenhang werfen sich u.a. Fragen hinsichtlich der Dauer für die Gewährleistung von Software-Updates auf, da Viren, Dritteinwirkungen, aber auch ein veraltetes Betriebssystem den bestimmungsgemässen Gebrauch erheblich beeinträchtigen können. Unterschiedliche Ansichten bezüglich der Gewährleistungsdauer für Updates bestehen bei der integrierten Standardsoftware, deren Nutzungsbefugnisse i.d.R. dauerhaft überlassen werden. Es ist jedoch davon auszugehen, dass es sich bei Sicherheitsupdates von integrierten Standardsoftwares um nachwirkende Schutzpflichten handelt, die sich aus dem Vertrag ergeben und dem Schutz des Integritätsinteresses des Vertragspartners dienen. Es handelt sich um eine Nebenpflicht, die gemäss Art. 127 OR erst nach Ablauf von 10 Jahren verjährt.

Weiter ist im Zusammenhang mit der digitalen Abhängigkeit fraglich, ab wann ein Softwarevertrag für die Erbringung einer digitalen Dienstleistung gekündigt werden kann. Zu berücksichtigen ist dabei, dass das Wegfallen der genannten Dienstleistung durch Kündigung des Dauerschuldverhältnisses zu einer Einschränkung der Funktionsfähigkeit des Smart Objects führt. Die Kündigung des Softwarevertrags vor Ablauf der Lebensdauer des Smart Objects würde nicht nur den bestimmungsgemässen Gebrauch beeinträchtigen, sondern könnte zudem einen erheblichen Wertverlust des Geräts zur Folge haben.

Verantwortungszuordnung und Beweislast

Aufgrund der Zunahme der Marktteilnehmer und der komplexen Vernetzung der einzelnen Komponenten des Systems, das Daten in Echtzeit austauscht, erweist sich die rechtliche Verantwortungszuordnung als schwierig. Führt beispielsweise eine Fehlfunktion eines smarten Thermostats zu Schäden, da die Temperatur nicht mehr reguliert wurde, kann das Problem u.a. bei den Sensoren und Aktoren liegen, die keine Daten mehr gesammelt haben, bei einem Fehler in der Datenverarbeitung oder auch bei der fehlenden Vernetzung des Thermostats mit der mobilen Applikation. Die Schwierigkeit der Zuordnung der Verantwortlichkeit liegt u.a. auch an der Beweisproblematik von Datenflüssen, da diese manipulierbar, vergänglich und vom menschlichen Auge nicht wahrnehmbar sind. Besonders problematisch erweist sich die Zuordnung der rechtlichen Verantwortlichkeit bei nicht reproduzierbaren Fehlern. Dabei

handelt es sich um Fehler in Informationssystemen, die für die Funktionsfähigkeit von Smart Objects notwendig sind, deren Ursache jedoch aufgrund des komplexen Zusammenwirkens mehrerer Komponenten nicht mehr ermittelt werden kann. Die Beweislast kann bei nicht reproduzierbaren Fehlern zur faktischen Abgrenzung von Risikosphären führen, was eine rechtliche Verantwortungszuordnung verunmöglicht.

Neue Kriterien für die Fahrlässigkeit

Neue Fragen im Zusammenhang mit Smart Objects stellen sich zudem bei der Beurteilung der Fahrlässigkeit. Fraglich ist, ob in einer Mehrebenenstruktur, in der Daten in Echtzeit ausgetauscht werden und eine komplexe Vernetzung verschiedener Marktteilnehmer vorliegt, die Zurechnung der Verantwortlichkeit nach Kriterien wie leichte und grobe Fahrlässigkeit noch möglich ist. Die Beurteilung, wann gegen elementare Vorsichtsgebote verstossen wurde und wann lediglich eine geringfügige Abweichung vom Standardverhalten vorliegt, erweist sich aufgrund der technischen Komplexität als besonders schwierig. In Anbetracht der technologischen Entwicklungen, dem steigenden Automatisierungsgrad sowie fehlenden technischen Standards scheinen die bisherigen Kriterien für die Beurteilung der Fahrlässigkeit als anpassungsbedürftig.

Lösungsansätze

Grundsätzlich ist festzuhalten, dass das bestehende Recht – intelligent genutzt – in vielen Problemfällen im Zusammenhang mit Smart Objects eine Lösung bietet. Ein Beispiel dafür stellt die Beantwortung der Frage zur Dauer der Gewährleistung von Software-Updates dar. Ein Lösungsansatz für die Problematik der Kündigung von Softwareverträgen vor Ablauf der Lebensdauer des Smart Objects wäre die Einführung einer Mindestlaufdauer bzw. einer Einschränkung der Kündbarkeit für Dauerschuldverhältnisse, sofern die entsprechende Leistung für die bestimmungsgemässe Verwendung des Produktes notwendig ist. Die Fahrlässigkeit bedarf angesichts der genannten Umstände neuer Kriterien bzw. Beurteilungsansätzen. Zudem wird es unerlässlich sein, einheitliche Mindeststandards für Smart Objects festzulegen, da diese für die Beurteilung der Fahrlässigkeit von Bedeutung sind. Zur Beweisproblematik bei Smart Objects könnten Lösungsansätze der alternativen Kausalität untersucht werden. Dabei ist beispielsweise an die Beweislastumkehr oder die quotenmässige Teilhaftung zu denken.

Der Weg zum wissenschaftlichen Mitarbeiter

° Ein Interview mit Stefan Hegyi, MLaw, wissenschaftlicher Mitarbeiter am Zentrum für Sozialrecht, sowie am Zürcher Zentrum für Informationstechnologie und Datenschutz (ITPZ)

- Das Interview wurde geführt von Ivo Schnyder.



Stefan Hegyi

Guten Tag Herr Hegyi, bitte stellen Sie sich dem Leser vor.

Mein Name ist Stefan Hegyi (32). Ich bin am Greifensee aufgewachsen und wohne jetzt am Zürichsee. Meine Freizeit verbringe ich auf und im Wasser. Meine (berufliche) Ausbildung nahm mit einer KV Lehre im Immobilienbereich ihren Lauf. Vor meinem Studium war ich kurz auf meinem erlernten Beruf tätig. Nach meinem Wirtschaftsrechtstudium an der ZHAW, wechselte ich an die Universität Neuenburg und schloss dort meinen Master in Rechtswissenschaften ab. Momentan arbeite ich als wissenschaftlicher Mitarbeiter an der ZHAW.

Warum haben Sie vom Immobilienbereich auf Wirtschaftsrecht gewechselt?

Die KV Lehre war eine solide Grundausbildung und Immobilienbereich hat mir sehr gut gefallen. Für mich war jedoch klar, dass ich studieren, mich weiterbilden und damit meinen Wissenshunger stillen wollte. BWL wäre naheliegend gewesen, kam

aber nicht in Frage, da ich mich einerseits durch eine differenzierte Studienwahl von der Masse abheben wollte und andererseits eine interdisziplinäre Herausforderung suchte. Zudem hatte ich bereits während meiner Ausbildung im Immobilienbereich sehr viel mit rechtlichen Fragestellungen zu tun. Betreibungen, Ausweisungen, Kündigungen, Mietzinserhöhungen sowie Schlichtungen gehörten zum Alltag. Ich wollte verstehen was rechtens ist und wie das Recht angewendet wird. So bin ich zum Studiengang Wirtschaftsrecht gekommen.

Haben Sie zu diesem Zeitpunkt bereits geplant wieder zurück in die Immobilienbranche zu gehen?

Eigentlich wollte ich mich in die Treuhand- oder Controlling-Abteilung versetzen lassen und ein Teilzeitstudium beginnen. Da jedoch bei meinem damaligen Arbeitgeber keine Stelle frei war, habe ich mich letztlich für das Vollzeitstudium entschieden. Es war sodann völlig offen, was ich nach dem Studium machen würde.

„Persönlich wie auch beruflich war es mitunter eine der besten Ausbildungen für mich.“

Würden Sie sich nochmals für den Studiengang Wirtschaftsrecht entscheiden?

Persönlich wie auch beruflich war es mitunter eine der besten Ausbildungen für mich. Ich habe sehr viel gelernt und konnte das Gelernte im späteren Berufsalltag gut umsetzen.

Haben Sie während des Studiums gearbeitet oder Weiterbildungen besucht?

Neben dem Vollzeitstudium hatte ich immer wieder kleinere Nebenjobs: Zu Beginn in einer Liegenschaftsverwaltung, später als Aufsicht in der Bibliothek sowie im Fitnesscenter und gegen Ende des Studiums als Assistent in einer Anwaltskanzlei (40-50%). Vor allem am Ende war Organisationstalent und gutes Zeitmanagement gefragt. Neben der Anstellung hatte ich das Studium und die Bachelorarbeit. Es war eine grosse Herausforderung, aber auch eine sehr gute Erfahrung.

Fall Sie gearbeitet haben, welchen Nutzen haben Sie daraus gezogen?

Wie bereits erwähnt, lernte ich zu planen, zu koordinieren, Prioritäten zu setzen und meine Zeit einzuteilen. So war und ist es mir sehr wichtig, immer wieder Erholungsphasen einzuplanen.

Was ist Ihnen positiv oder negativ in Erinnerung geblieben, wenn Sie an Ihre Studienzeit zurückdenken?

Positiv war vor allem der interdisziplinäre Mix zwischen Sprachen, Recht und Wirtschaft. Das Studium war sehr praxisorientiert, nicht zuletzt wegen den Dozenten, die vielfach auch in der Praxis tätig waren. Der Moot Court mit den Schriftenwechseln und der anschliessenden Verhandlung vor Gericht war beispielsweise sehr lehrreich und praktisch ausgelegt. Das Austauschsemester an der Université Paris-Dauphine bildete ein weiteres Highlight. Der Austausch zwischen Studierenden aus ganz Europa sowie die sprachliche Herausforderung sind mir positiv in Erinnerung geblieben.

Als negativ beurteile ich im Nachhinein die Gewichtung gewisser Fächer, manche waren zu langatmig und für andere hatten wir wiederum zu wenig Zeit. Da der Studiengang jedoch laufend weiterentwickelt wird, wurden diese Punkte inzwischen bereinigt.

Welchen Bezug haben Sie als Alumni zur ZHAW? (Nutzung Career Services, Homecoming Day etc.)

Am Homecoming Day sowie am Wirtschaftsrechtstag nehme ich gerne teil, um alte Studienkollegen wiederzutreffen, in Erinnerungen zu schwelgen und neue Bekanntschaften zu schliessen. Von Seiten der ZHAW wird relativ viel unternommen für die Alumni. Es ist jedoch eine grosse Herausforderung die Absolventen zu erreichen und zurück an die alte Wirkungsstätte zu holen.

Hatten Sie während Ihrem Bachelor bereits eine Vorstellung, dass sie später an der ZHAW angestellt sein werden?

Wissen zu vermitteln hat mir schon immer Spass gemacht. Ich hatte jedoch damals noch keine konkrete Vorstellung darüber, wohin mich mein beruflicher Weg führen wird.

Warum haben Sie sich für einen MLaw in Neuenburg entschieden?

Viele Kolleginnen und Kollegen sind nach dem Bachelor wieder direkt ins Berufsleben eingestiegen. Ich war jedoch hungrig nach mehr Wissen und wollte mich weiter spezialisieren. Es hat mich kulturell wie auch sprachlich gereizt, mein Studium in der Romandie fortzusetzen. Da ich noch eine Anstellung in Zürich hatte, fielen Genf und Lausanne weg. In Freiburg hatte es vergleichsweise viele Deutschschweizer und so kam nur noch Neuenburg für mich in Frage. Ein entscheidender Faktor war zudem die Möglichkeit ein Austauschsemester an der Columbia Law School in New York zu absolvieren.

Wie haben sie den Unterricht in Französisch erlebt?

Zu Beginn war ich am Abend jeweils fixfertig, denn ich brauchte für alles etwa doppelt so lange wie meine Mitstudierenden. Das Gute war jedoch, dass Freunde und Familie weit weg waren und ich zunächst niemanden kannte. So konnte ich mich gänzlich auf den Unterricht fokussieren. Die Herausforderung war zu Beginn gross, jedoch ist sie machbar, wenn man zielstrebig ist, an sich glaubt und keine Angst vor dem Scheitern hat. Bei den (mündlichen) Prüfungen lief es mir jeweils sehr gut. Etwas schwieriger waren die französischen Aufsätze, wie z.B. Klageschriften beim Swiss Moot Court.

Welche Vorteile brachte ein Studium an der UNINE mit sich?

Ein grosser Vorteil war der erwähnte Austausch an die Columbia Law School. Ich konnte dort während eines Semesters dem LL.M.-Unterricht beiwohnen und viele Kontakte knüpfen, sowie neue Sichtweisen kennenlernen.

Die rechtswissenschaftliche Fakultät an der Universität Neuenburg ist im Vergleich zu anderen Universitäten/Fachhochschulen sehr klein. Dadurch war man aber immer im engen Kontakt zu seinen Mitstudierenden und den Dozierenden. Das Fächerangebot ist enorm, mittels zwei Austauschverbänden kann man praktisch alle Fächer der Universitäten Lausanne, Genf, Freiburg und Bern belegen.

Ich habe beispielsweise in Freiburg Urheberrecht und in Bern IT-Recht besucht.

Weiter kann man sich seinen Master selbst zusammenstellen ohne eine vorgefertigte Vertiefung wählen zu müssen. Das habe ich dann auch gemacht. Ich hatte schon immer eine Affinität für Technologie und war zudem während dem Studium in einer Anwaltskanzlei tätig, die sich auf IT-Recht spezialisiert hat. Folglich legte ich meinen Studienschwerpunkt auf IT-Recht. Insbesondere war es interessant zu erfahren, welche Auffassung von Privatsphäre die Amerikaner an der Columbia Law School vertreten.

Wie verlief Ihr Einstieg in die Berufswelt nach dem Studium? Was waren die Schwierigkeiten?

Nach dem Studium habe ich rund zwei Jahre in einer kleineren Anwaltskanzlei gearbeitet. Der Einstieg verlief problemlos und war ziemlich einfach. Die zu verrichtenden Arbeiten glichen überwiegend denen im Studium: Man studiert Akten und schreibt Memos. Neu hinzugekommen ist der Umgang mit Klienten, da ich jedoch bereits in der in meinem früheren Beruf viele Kundenkontakte hatte, bereitete mir dies wenig Mühe.

Warum haben sie von einer Kanzlei an eine Fachhochschule gewechselt?

Ich habe gemerkt, dass mir der Anwaltsberuf nicht zusagt. In der Kanzlei hatte ich zu wenig Zeit, um auf die Menschen einzugehen und mich mit ihnen auseinanderzusetzen. Die ausgeschriebene Stelle an der ZHAW passte zudem, zeitlich und fachlich, genau auf mein Profil. Überdies hat es mir schon immer Spass gemacht, Wissen zu vermitteln und vor Vorträge bzw. Präsentationen zu halten.

Haben Sie den Absolvententag oder Firmenworkshops während des Studiums besucht? Wenn ja, welche Erfahrungen haben sie damit gemacht?

Ich hatte immer eine Anstellung und habe daher nie an solchen Anlässen teilgenommen.

Haben Sie sich nach dem Studium weitergebildet?

Momentan plane ich meine Doktorarbeit. Ferner nehme ich laufend an Fachtagungen teil. Eine Weiterbildung im Sinne einer Ausbildung steht momentan keine an. Hätte es früher einen CAS Datenschutzverantwortliche gegeben, hätte ich diesen sicher besucht.

Wie lautet Ihre Berufsbezeichnung und was sind Ihre Tätigkeiten? Können Sie uns einige Beispiele aus dem Alltag nennen?

Ich bin wissenschaftlicher Mitarbeiter am Zentrum für Sozialrecht, sowie am Zürcher Zentrum für Informationstechnologie und Datenschutz (ITPZ). Das ITPZ ist eine Kooperation zwischen der ZHAW und dem Datenschutzbeauftragten des Kantons Zürich und setzt sich für die Förderung, Umsetzung und Weiterentwicklung des Datenschutzes ein. In meinem Berufsalltag lehre und berate ich zu technisch geprägten Rechtsfragen, insbesondere Datenschutz.

Warum ist dieser Beruf interessant (Herausforderungen)? Was gefällt Ihnen gut, was eher weniger?

Ich arbeite in diversen Leistungsbereichen. Dies ist einerseits herausfordernd, andererseits sehr abwechslungsreich. So bin ich in der Lehre (Unterricht im Bachelor Wirtschaftsrecht/Master Management and Law), in der Weiterbildung (Program Manager des CAS Datenschutzverantwortliche; Unterricht in diversen weiteren Weiterbildungen) sowie in der Forschung tätig (beispielsweise Studien zu Quantified Self, Verknüpfung von Datensätzen mit Gesundheitswesen oder Privacy Engineering). Zudem erbringen wir Dienstleistungen im Rahmen von Rechtsberatungen im Hochschulumfeld und im Rahmen des ITPZ bieten wir spezifische Datenschutzseminare für Private sowie für die Verwaltung an.

Dieses interdisziplinäre Umfeld gefällt mir besonders. Ich habe mehr Zeit mich mit den Menschen auseinanderzusetzen. Insbesondere der Kontakt zu Studierenden im Unterricht oder bei der Betreuung von Semesterarbeiten sind hier zu erwähnen.

Welche Fähigkeiten sind vorausgesetzt?

Am Ende eines Arbeitstages bin ich jeweils in fast allen Leistungsbereichen tätig gewesen. Dies ist eine Herausforderung in der Arbeitsorganisation und bedarf hoher Flexibilität. Man muss sich seine Struktur selber schaffen und Eigenverantwortung übernehmen. Aufgrund der Grösse der ZHAW muss man sich aber auch an bestehende Prozesse und Strukturen anpassen.

Mussten Sie sich zusätzliches Fachwissen aneignen?

Ich konnte sehr viel Wissen vom Studium direkt im Berufsalltag anwenden. Insbesondere die kreativen und rechtsvergleichenden Ansätze aus den Auslandssemestern waren sehr hilfreich. Da der Bereich Datenschutz jedoch eine Spezialisierung meines bisherigen Tätigkeitschwerpunktes IT-Recht war, musste ich mir in einigen Bereichen Fachwissen aneignen, so beispielsweise im öffentlichen Datenschutzrecht.

„Ich konnte sehr viel Wissen vom Studium direkt im Berufsalltag anwenden.“

Wie sehen die Weiterbildungs- und Karriere-möglichkeiten aus?

Eine Doktorarbeit ist eine Voraussetzung für die Stufe des „Dozenten“ und ist auch ein Sprungbrett für die Verwaltung oder die Privatwirtschaft. Die Tätigkeit als Dozent könnte auch gut mit einer rechtsberatenden Stelle verbunden werden. Dies wird von vielen Dozenten an der ZHAW gemacht.

Würden Sie im Vergleich eher in der Verwaltung oder Privatwirtschaft arbeiten?

Ich bin sehr neutral. Insbesondere im Datenschutzbereich gibt es in beiden Bereichen interessante Tätigkeiten. Am liebsten würde ich teilzeit arbeiten: Als Dozent und nebenbei in einer Technologiefirma als „Data Protection Officer“. Denken Sie der Bereich Datenschutz wird in Zukunft noch an Bedeutung gewinnen? Aufgrund der rasant fortschreitenden Digitalisierung werden sich weitere Problemfelder eröffnen. Die Technologie entwickelt sich schneller als das Recht und dies führt zu Spannungen. Die Frage ist, wie wir „alte“ Schutzbedürfnisse in der „neuen“ digitalen Welt umsetzen. Hierzu leiste ich gerne meinen Beitrag und sensibilisiere die Öffentlichkeit dafür.

Welche Erwartungen hatte Ihr Arbeitgeber an Sie in Bezug auf Ihren Bachelor - Abschluss?

In der Kanzlei war es einer der Gründe, warum ich die Anstellung erhalten habe. Als Absolvent des Studiengangs Wirtschaftsrecht hat man zumeist

bereits Arbeitserfahrung und wendete den Studieninhalt praktisch an. Den Entscheid zum Studium hat man bewusst gewählt. Aufgrund der Schnittstelle zu wirtschaftswissenschaftlichen Fächern ist man vielfältig einsetzbar. So habe ich beispielsweise die Buchhaltung geführt, als die Sekretärin für längere Zeit ausgefallen ist.

Gibt es etwas, was sie in ihrer Rolle als Lehrbeauftragter besser machen wollten oder wo sie speziell ihren Fokus legen?

Mir ist es wichtig, dass man den Unterricht auf die praktischen Bedürfnisse ausrichtet. Ich will auf die Studierenden und ihre Fragen eingehen und möglichst Beispiele aus dem Berufsalltag verwenden. Die Theorie kann man sich zu Hause durchlesen, hierfür muss man meines Erachtens nicht in den Unterricht kommen. Hier sehe ich den Vorteil einer Fachhochschule gegenüber einer Universität. Diesen praktischen Vorteil müssen wir an der ZHAW weiter ausbauen.

Denken Sie, es gibt Verbesserungspotenzial im Studiengang Wirtschaftsrecht?

Wenn ja, welches?

Der Studiengang entwickelt sich rasant. Die Herausforderung besteht darin, dass man einerseits praxisorientierten Unterricht bietet und andererseits einen problemlosen Übergang an die Universitäten gewährleisten. Hier besteht ein gewisses Spannungsverhältnis. Es wäre wünschenswert mittels „Law Clinics“ das Recht noch direkter anzuwenden oder in kleineren Seminaren mit den Dozenten einen engen Austausch zu pflegen.

Denken Sie die Möglichkeit zum Übergang an die Universität ist essentiell für den Studiengang?

Persönlich würde ich sagen, dass es nicht primär das Ziel einer Fachhochschule ist, diesen Übergang zu gewährleisten. Es steigert aber klar die Attraktivität des Studienganges. Primär sollte es eine praxisorientierte Ausbildung sein, um anschliessend wieder in den Beruf einzusteigen.

Was würden Sie einem zukünftigen Wirtschaftsrechtsabsolventen mit auf den Weg geben?

Nach dem Bachelor stehen einem alle Türen offen, dessen sollte man sich bewusst sein. Es gibt nicht nur den Weg nach Luzern und die Universität und den Anwaltsberuf. Es gibt sehr viele andere Berufe, in denen man sein Wissen anwenden kann. Man kann sich von Universitätsstudenten abheben, indem man betont, dass man über gewisse Arbeitserfahrung verfügt und in den Genuss einer praxisorientierten Ausbildung gekommen ist.

Vielen Dank!

„Die Herausforderung besteht darin, dass man einerseits praxisorientierten Unterricht bietet und andererseits einen problemlosen Übergang an die Universitäten gewährleisten.“

Kapstadt - das schönste Ende der Welt

° Ein Bericht von Jacqueline Panzeri

Jacqueline Panzeri ist Vollzeitstudentin an der ZHAW. Das vierte Semester hat sie in Kapstadt verbracht. Sie schildert uns ihre Erfahrung und berichtet über ihre Erlebnisse in der südafrikanischen Stadt.



Vorbereitung und Anmeldung

Der Anmeldeprozess an der Universität Kapstadt ist relativ zeitaufwändig und zum Teil auch sehr unübersichtlich, aber definitiv machbar. Als mühsam habe ich den Visumprozess empfunden: Man muss relativ früh einen Termin bei der Botschaft vereinbaren und dann mit allen erforderlichen Unterlagen nach Bern, um in der Botschaft das Formular auszufüllen. Die Sache ist in 20 Minuten erledigt und dann kann man auch schon wieder gehen. Zusätzlich braucht man noch eine südafrikanische Krankenversicherung und zwar unabhängig davon, ob die Schweizer Versicherung die Kosten in Südafrika übernehmen würde. Bevor ich nach Kapstadt aufgebrochen bin, war ich etwas verunsichert wegen der Wasserknappheit und dem berühmten DayZero von dem überall in den Medien die Rede war. Ich kann nur sagen, dass ich eigentlich extra Credits für mein dazugewonnenes Wissen über die unzähligen Möglichkeiten Wasser zu sparen verdient hätte und Trockenschampoo und hand-sanitizer in dieser Zeit meine treuesten Begleiter waren. Im Endeffekt ist DayZero nicht eingetreten und die Limite von 50 Liter pro Person ist absolut aushaltbar, während dem ganzen Semester hatten wir in unserem Haus nur dreimal kein Wasser mehr.

Unterkunft

Da ich niemanden kannte und auf keinen Fall Gefahr laufen wollte in Kapstadt zu vereinsamen, habe ich mich entschieden über Edubed, eine Seite für Studentenunterkünfte, die mir von der Uni Kapstadt angegeben wurde, eine Unterkunft zu suchen. Das kann ich nur bedingt empfehlen: Positiv ist, dass man gleich andere internationale Studenten kennenlernt, andererseits hatten wir 3 Monate kein warmes Wasser (was sich allerdings wiederum positiv auf den Wasserverbrauch ausgewirkt hat), das Wifi hat nur unzuverlässig funktioniert (was mühsam ist, wenn man Essays online einreichen muss und um 07:30 Uhr morgens wie eine Irre in ein Café rennen muss, um die Frist nicht zu verpassen) und Kakerlaken waren so normal, dass wir diesen schon bald Namen gegeben haben. Für den gleichen Preis findet man deutlich besseres. Ich habe einige Studenten kennengelernt, die sich zu zweit oder dritt ein Airbnb für diese Zeit genommen haben und es gibt zu Beginn des Semesters immer einige Studenten, die noch Mitbewohner suchen.



Sicherheit

Kriminalität ist definitiv ein Thema und das hohe Sicherheitsgefühl war etwas, das ich in Südafrika (nebst anständigem Brot und Käse) von Schweiz vermisst habe. Angst hatte ich nie, aber Kapstadt lernt einen immer aufmerksam zu sein und man sollte auch im Haus immer alles wegschliessen. Wir hatten einen Einbruch mit dem Resultat, dass alle Laptops weg waren und ich mir für den Rest des Semesters einen Computer mieten musste, der eine Akkuzeit von unglaublichen 2h hatte und mit seiner Grösse und seinem Gewicht auch als potentielle Mordwaffe durchgegangen wäre. Am Abend sollte man sich am besten in Gruppen bewegen, und lieber einmal mehr als weniger ein Uber nehmen. Paranoid muss man dennoch nicht sein.

Uni und Vorlesungen

Die erste Woche ist etwas hektisch, weil man sich in alle Kurse manuell einschreiben muss und Unterschriften von verschiedenen Personen, die grundsätzlich über Tage nirgends auffindbar sind, benötigt. Kursänderungen sind nur während der ersten Woche möglich. Randnote: Kapstadt ist sehr entspannt, die Menschen hier lassen sich auch nicht stressen und

so kann "now" auch in 2h heissen. Man erspart sich also den Stress, wenn man einfach allem seine Zeit lässt, irgendwie funktioniert dann am Ende doch immer noch alles. Nicht umsonst sagt ein afrikanisches Sprichwort: Das Gras wächst nicht schneller, wenn man daran zieht.

Ich habe die gleichen Kurse, wie die einheimischen Studenten besucht und die Vorlesungen sind wesentlich unstrukturierter und lockerer von der Atmosphäre her als in der Schweiz. Ebenso sind die Studenten hier zum Teil sehr diskussionsfreudig. Am Anfang habe ich kaum etwas verstanden, nicht unbedingt wegen der Sprache, sondern weil ich mit der Geschichte, dem politischen System und dem Rechtssystem zu wenig vertraut war. Aber auch das geht vorbei, man sollte sich einfach ein bisschen einlesen, damit man den Argumenten und Diskussionen folgen kann. Ansonsten ist der Workload ziemlich gross, in einigen Fächern muss man Essays schreiben und/oder hat Midterm-Tests, die zur Endnote zählen.

Das Leben in Kapstadt

Als ich in Kapstadt angekommen bin, war ich gleich überwältigt von den Farben, dem Licht, all den verschiedenen und freundlichen Menschen und der



wunderschönen und vielfältigen Natur. Kapstadt und seine Umgebung bieten einfach alles was man sich nur wünschen könnte: Das Meer um zu surfen, Traumstrände, Berge für kurze und lange Wanderungen, Weingüter und verträumte Fischerdörfer, endlose Ausgehmöglichkeiten, super Essen und unzählige Festivals und Konzerte. Und für Schweizer ist das Leben, insbesondere das Essen, sehr günstig. Dies zusammen mit der freundlichen und herzlichen Art der Menschen hier, macht Kapstadt zu einer absoluten Traumdestination und es wird einem hier definitiv nie langweilig. Wer sich entscheidet nach Kapstadt zu gehen, sollte sich das Afrika Burn (wie das Burning man in den USA) auf keinen Fall entgehen lassen! Kapstadt hat aber auch seine Kehrseite: Ich bin in dem Glauben nach Kapstadt gekommen, dass all die verschiedenen Volksgruppen hier miteinander in Harmonie leben. Das miteinander ist in der Realität aber vielmehr ein nebeneinander und der Unterschied zwischen den hauptsächlich reichen, weissen Kapstädtern und der armen, mehrheitlich schwarzen südafrikanischen Bevölkerung springt einem einfach überall ins Auge. Viele Menschen verkehren nicht wirklich mit Menschen anderer Hautfarbe, was man auch an der Uni beobachten kann.

Auch hat die Armut in Kapstadt eine ganz andere Dimension als in der Schweiz. Nicht einmal 15 Minuten mit dem Auto vom Stadtzentrum entfernt, wohnen zehntausende Menschen in Wellblechhütten und haben weder Strom noch einen Trinkwasseranschluss. Auch sind die Menschen hier froh, wenn man ihnen einfach etwas zu essen oder zu trinken gibt. Das kann ziemlich bedrückend sein. Trotz dieser anhaltenden Probleme sind die Kapstädter freundlich, offen, lebensbejahend und haben auch für prekäre Situationen, wie akuten Wassermangel, immer einen Witz auf Lager.

Fazit

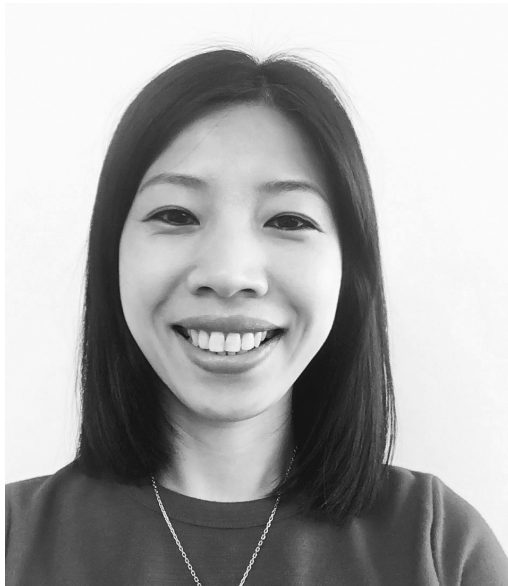
Das Austauschsemester in Kapstadt war eine grossartige und prägende Erfahrung für mich und war nicht nur aus einer akademischen Perspektive interessant, sondern auch auf einer persönlichen Ebene wertvoll. Südafrika ist historisch, kulturell und landschaftlich einzigartig und bietet für absolut jeden etwas. Selbst nach einem Semester habe ich noch längst nicht alles gesehen und ich hätte locker noch ein bisschen länger bleiben können. Ich kann Kapstadt somit jedem nur wärmstens empfehlen.



From China to Switzerland - an intercultural path to success

°Interview with Ying Song, Business Law student ZHAW

- Das Interview wurde geführt von Lynn Riethmann



Ying Song

Who are You Ying?

I am Chinese, 33 years old and I am currently enrolled at ZHAW.

I am a person who likes to take on new challenges. I am also a person who is very critical of myself and of the whole world.

I am not a person who just believes everything I hear or see in life. I always try to scrutinize the information I got and to see it in my own way.

I think this originates from my education in China. In China the parents and the school very often tell us what is right, what is wrong. It is more like black or white. But once we grow up, there are a lot of things, which we cannot only see as right or wrong, it is more about the way we deal with people and different opinions. Especially after I came to Switzerland, I experienced the so called cultural shock, the different mindsets make me go further on this road, I mean figure out my own opinion about everything.

How comes you study in Switzerland?

Most students in China want to go to the US or Canada. But I always wanted to go to Europe to pursue my studies because to my understanding Europe is a place of freedom, liberty, romance and a place of literature and art. The other reason was that I thought it would be nice to learn another language than English. I had been choosing between French and German. In the end I chose German because there are at least three countries which use German as their national language. First I intended to go to Germany because the living costs are much lower than they are in Switzerland. But due to my job at that time I visited Switzerland in 2011 and I really liked the country.

Why did you choose to study at ZHAW?

I did not know ZHAW until I met a mate at the Goethe Institute (Language School) in Shanghai at the time when I was learning German. He already had applied to study at ZHAW. He introduced me to ZHAW. That is when I started considering the idea of studying in Switzerland.

Why Business Law?

Even before I decided where to study I knew that I want to pursue Law.

I applied to UZH as well, but when I saw that ZHAW offers Business Law I preferred to do this course instead because it gives you two possibilities instead of one. You can either get into Business or Law.

What requirements did you have to fulfill to be able to study in Switzerland?

I had to hand in my college qualifications, my German and English language certificates on a level of C1 and B2 as well as a my criminal record. Afterwards the process was pretty smooth and I got an invitation letter from ZHAW.

With that I was able to apply for a student visa in the Swiss Embassy Guangzhou. The visa I was granted allows me to study in Switzerland and to work for up to 15 hours per week.

What requirement did you have to fulfill to study at ZHAW specifically?

The only difference to other universities was that I had to have some working experience, which was quite new for me as this is something not being asked when applying for a study at a university in China.

Are there big differences between studying in China and Switzerland?

I had a college diploma (Internet Technic) in China. The college I attended does not speak for the highest level of education in China. But if I have to name some differences, I would say the way the professors and students communicate and also the attitude to the exams and to the study. Back at that time in college (10 years ago) we had less discussions in the lecture. China is more of a hierarchy society, even between professors and students. We always have highest respect for the professors. We don't really express our opinions if they are not main stream. I am not saying in Switzerland we don't respect the professors, we do. But here at ZHAW I feel students are able to ask all kinds of critical questions, professors are more open-minded, we even openly said the federal courts could be wrong sometimes. So maybe it has also something to do with the free speech. Anyway, I suppose there is much more deep communication going on between students and professors.

What did you do before starting to study in Switzerland?

I actually did many things before I started my studies in Switzerland.

After high school I went to a college in Fuzhou (capital of Fujian Province) for three years, I studied IT there. Afterwards I did another two years at that college with a major in English.

After finishing my studies I started my first job in a trading company. I was an international business consultant. I was basically responsible for the enquiries of English speaking clients. After two years I started to work for a travel agency for another three years. During that time I met a lot of people who wanted to do an abroad study or just came back to China after studying abroad. That is when I started to have the desire to take on a new challenge. Even though I was promoted to a project manager I did not feel like I wanted to do that job forever.

What were the biggest challenges in your studies and also in your private life?

The biggest challenge was definitely the language, as for me it is really depending on the professors and their accents whether I do understand everything or not. So the most important thing for me was to always prepare the lectures beforehand.

One of the small problems I had was that I was unable to find a room before I came to Switzerland, because all the student homes were full at that point

(my visa was granted shortly before the semester started). But I was lucky and found a room in a shared apartment with a German guy.

But I realized quickly that the chemistry between us was not right. So after two weeks I left the apartment and stayed with a friend of mine and afterwards in a hostel for several days until I found a room where I felt comfortable.

But the troubles with the guy were not out of the world yet, as he had kept my deposit which he did not want to return to me even though he already had a new subtenant. After several unsuccessful communication attempts with him I filed a lawsuit against him. So basically only after being in Switzerland for a couple of months I had already filed my first lawsuit in life. Eventually, I won the case and got my deposit. He did not show up in the court room though.

What are your plans after receiving your Bachelor's degree?

I plan to pursue my studies at the University of Lucerne where I would like to do the Passarelle and then doing my MLaw.

„I am open to any opportunity which crosses my path.“

What are your plans after finishing your studies in Switzerland?

I do not know yet. I think of trying to become a lawyer but I am not sure yet. Right now I am really fascinated by Criminal Law and European Law and it would be really nice to be able to find a job in these areas of Law.

I feel quite comfortable here in Switzerland and Europe so I am not sure yet if I will go back to China or if I am going to stay here in Switzerland or somewhere in Europe. I am open to any opportunity which crosses my path.

And at the end of this interview, I would like to use this chance to thank ZHAW, whoever made that decision to accept me as a normal student, definitely gave me a second chance in my life, which not everyone can have, which I also cherish as the most important chance in my life. I am so so so lucky to have studied at ZHAW. I really benefit a lot from it. Whatever I may achieve in the future, it is based on the effort and experience I made at ZHAW. I will keep it in my mind as the most valuable memory.

Thank you!



Studentenverein
Wirtschaftsrecht

ALTE PRÜFUNGEN?!

Zusammenfassungen **Bücherlisten**

Bachelorarbeit

Leistungsnachweise

Berufsaussichten

Informationsaustausch

Masterstudiengang ?

Infoveranstaltungen

Bewerbungstipps

Das sind Wir!

° Das ist der Studentenverein
Wirtschaftsrecht

Studentenverein Wirtschaftsrecht

Der Studentenverein Wirtschaftsrecht wurde 2015 gegründet und ist der Erste seiner Art in der ganzen Schweiz. Unser Zweck: Die Studierenden während ihrem Studium aktiv unterstützen. Aktuell haben wir über 500 Mitglieder, Vollzeit und Teilzeit. Wir sind das Sprachrohr der WR Studenten! Der Verein und die Studiengangleitung der ZHAW arbeiten eng zusammen. Dadurch wird ein gegenseitiger Austausch zwischen Studierenden und der Hochschule ermöglicht.

Informationen

Als Mitglied hast du Zugriff auf unsere Informations-Plattform. Dort findest du alte Prüfungen, Leistungsnachweise und Zusammenfassungen. Wir geben dir Tipps zum Bücherkauf, informieren über aktuelle Anlässe im Wirtschaftsrecht und beantworten Fragen zum Studium.

Netzwerk

Wir organisieren regelmässig Events für die Studierenden. Hierzu gehören Informationsveranstaltungen mit Berufsleuten, Mitgliederevents sowie Unternehmensbesichtigungen. Dort hast du die einmalige Gelegenheit mit ehemaligen Absolventen über die Zukunft zu sprechen, dein Wissen zu erweitern und die Studierenden ausserhalb der Vorlesungsräume zu treffen.

Das wollen wir:

Dich als Mitglied! Die Mitgliedschaft kostet einmalig 20 CHF, ohne Verpflichtungen und ermöglicht dir einen exklusiven Zugang zum Mitgliederportal.

Ein Klick, deine Angaben und du bist dabei!

www.wr-studenten.ch



Digitalisierung und Datenschutz

Optimierungsbedarf bei Brokerportalen

° Text von Nadja Werren

- Quellennachweis online verfügbar unter www.wr-studenten.ch.

Ausgangslage

Die Digitalisierung breitet sich durch alle Branchen und Unternehmensebenen aus. Unternehmen integrieren das Ziel „Digitalisierung“ kontinuierlich in ihrer Unternehmensstrategie, passen die internen Systeme an und entwickeln neue Portale, um den Kunden das Abrufen und die Bearbeitung der eigenen Daten zu ermöglichen. Der vorherrschende Tenor lautet „wer nicht mit der Zeit geht, geht mit der Zeit“. Etliche Unternehmen mit renommierten Marken, wie Nokia und Kodak gaben Beispiele ab, dass ein Stehenbleiben im Untergang der Unternehmung endet. Ebenso rückt mit der fortschreitenden Digitalisierung auch das Thema Datenschutz stetig weiter in den Vordergrund. Täglich fließen Unmengen an Daten ins Internet. Dass bei einer solchen Masse an Daten auch stärkerer Schutz benötigt wird, als früher, ist unbestritten.

Dieser Fachartikel setzt sich mit der Digitalisierung in der Versicherungsbranche auseinander. Die Versicherungsgesellschaften haben über die letzten Jahre stetig Kundenportale entwickelt, welche sie ihren

Klienten zur Verfügung stellen um administrative Anpassungen effizienter abzuwickeln. Beispielhaft können hier das AXA Winterthur und das Sanitas Kundenportal genannt werden. Die Versicherungsnehmer können darauf ihre Police abrufen, sämtlichen Schriftverkehr in PDF abrufen oder auch kleine Mutationen, wie Adressänderungen, selber vornehmen. Um sicherzustellen, dass nur der Kunde selbst auf seinem Profil Anpassungen vornehmen kann, wird ihm bei jedem Login ein Zahlencode per SMS zugestellt, welchen er bei der Anmeldung angeben muss. Bei diesem direkten Kontakt zwischen Kunde und Versicherung stellt der Datenschutz ein weniger grosses Problem dar. Betrachtet man jedoch die Situation, wenn zwischen dem Kunden und der Versicherung ein Versicherungsbroker steht, birgt diese die Frage, ob der Versicherungsbroker berechtigt ist, die Kundendaten einzusehen, eine enorme Hürde. Zwischen der Datensicherheit, welche von der Versicherungsgesellschaft in Bezug auf die Kundendaten erbracht werden muss, und der Freigabe der Daten an einen Versicherungsbroker, besteht ein Zielkonflikt. Ziel eines Kundenportals für Versi-

cherungsbroker ist es, dass einerseits die Versicherungsgesellschaft von administrativen Arbeiten, wie Adressmutationen und Offerterstellungen entlastet wird und andererseits, dass die Versicherungsbroker effizient und innert kürzester Zeit die benötigten Offerten erstellen können. Bei bereits bestehenden Kunden mit Versicherungspolice, welche bereits dem Versicherungsbroker in Betreuung sind, kann die Versicherungsgesellschaft im System festhalten, dass der Versicherungsbroker auch die Berechtigung zur Anpassung der Daten hat. Die Problematik ergibt sich bei Neukunden, wenn der Versicherungsbroker noch keine Police vom Versicherungsnehmer betreut und die Versicherungsgesellschaft somit nicht automatisch über das System nachvollziehen kann, ob der Versicherungsbroker berechtigt ist die Daten einzusehen. Hier ergibt sich die Fragestellung, welche Kundendaten die Versicherungsgesellschaft den Versicherungsbrokern zur Verfügung stellen können ohne dass sichergestellt ist, dass der Versicherungsnehmer die Vollmacht erteilt hat oder wie die Sicherstellung effizient lösbar ist. Auf der anderen Seite ergibt sich die Frage, welche Daten der Versicherungsbroker benötigt damit das Kundenportal für ihn einen Mehrwert generiert. In diesem Artikel werden Vorschläge ausgearbeitet, wie ein solches Brokerportal gestaltet sein muss, welche Daten in welcher Form ausgehändigt werden und wie sichergestellt ist, dass diese Abläufe sowohl für den Versicherungsbroker einen Mehrwert generieren, als auch datenschutzkonform sind. In diesem Fachartikel wird insbesondere das Brokerportal der AXA Winterthur beleuchtet.

Rechtsslage

In der EU trat im März 2018 eine neue Datenschutzgrundverordnung in Kraft (EU-DSGVO), ebenso hat die Schweiz einen Entwurf zur Totalrevision des DSG ausgearbeitet (E-DSG), welcher derzeit in der Vernehmlassung ist. Dieser Entwurf orientiert sich an der neuen Datenschutzverordnung der EU, weil das Schweizer Datenschutzgesetz durch die EU als angemessen und gleichwertig beurteilt werden muss. Ansonsten resultieren Probleme für einen reibungslos funktionierenden Datenaustausch mit den europäischen Nachbarländern. Dieser Fachartikel basiert somit mehrheitlich auf der Gesetzeslage mit dem Entwurf des neuen DSG.

Verhältnis zwischen Kunde, Versicherung und Versicherungsbroker

Die Zusammenarbeit eines Versicherungsbrokers mit der Versicherung basiert auf einer Zusammenarbeitsvereinbarung. In dieser sind die Rechte und Pflichten der beiden Parteien festgehalten. Wesentlicher Bestandteil dieser Rechte und Pflichten bilden die Courtagelohnungen des Versicherers an den Versicherungsbroker und im Gegenzug die zu erbringenden Dienstleistungen des Versicherungsbrokers an die Versicherung. Darüber, wie dieser Vertrag zu qualifizieren ist, gibt es unterschiedliche Ansichten. In diesem Fachartikel wird die Meinung vertreten, dass der Vertrag sowohl Elemente des Auftrag (wobei hierunter die Betreuung des Versicherungsnehmers im Rahmen der Aufgaben des Versicherungsbrokers falle) als auch des Maklervertrags

(worauf die Vermittlung des Geschäfts hinweist) beinhaltet. Daher handelt es sich um einen Innominatvertrag. Zwischen dem Versicherungsbroker und dem Versicherungsnehmer besteht ebenfalls ein Vertrag. Dieser Vertrag wird als Versicherungsbrokermandat bezeichnet und bildet die Grundlage für die Tätigkeit des Versicherungsbrokers im Auftrag des Versicherungsnehmers. Hierbei ist zu beachten, dass zwischen dem Versicherungsbroker und dem Kunden ein Treueverhältnis besteht. Kommt ein Versicherungsvertrag zustande, so besteht dieser direkt zwischen dem Versicherungsnehmer und der Versicherung. Der Versicherungsnehmer entrichtet die Prämienzahlung und die Versicherung erbringt den vereinbarten Versicherungsschutz. Damit wird ersichtlich, dass die Parteien in einem Dreiecksverhältnis zueinanderstehen.

Verantwortlichkeit und Pflichten

Für den Datenschutz verantwortlich ist diejenige Person, welche über den Zweck, die Mittel und den Umfang der Bearbeitung entscheidet. Welchem Zweck die Daten dienen und wie der Umfang der Bearbeitung gestaltet ist, entscheidet im Falle der besagten Kundendatenbank die Versicherungsgesellschaft in dem sie das Kundenportal dementsprechend programmiert und zur Verfügung stellt. Somit trifft die Verantwortlichkeit grösstenteils die Versicherungsgesellschaft. Der Verantwortliche kann die Bearbeitung auch an einen Auftragsbearbeiter in Auftrag geben. Auftragsbearbeiter ist diejenige Person, welche im Auftrag des Verantwortlichen Personendaten bearbeitet. Wie vorhin ausgeführt, liefert der Versicherungsbroker der Versicherung zwar eine Dienstleistung im Rahmen der Vermittlungstätigkeit und Kundenbetreuung, er steht aber im einem eindeutigen Treueverhältnis zum Kunden und handelt in dessen Interesse und Auftrag. An dieser Stelle ist festzuhalten, dass der Versicherungsbroker nicht als Auftragsbearbeiter i.S.d. E-DSG fungiert. Die Versicherungsgesellschaft sichert sich hier auch soweit wie möglich ab, indem sie in den Zusammenarbeitsverträgen mit den Versicherungsbrokern eine Datenschutzklausel integriert.

Der Verantwortliche der Datenbank steht in der Pflicht, den Datenschutz i.S.d. E-DSG zu gewährleisten. Die Versicherungsgesellschaft ist daher dafür verantwortlich, dass die Bearbeitung der Personendaten rechtmässig nach Treu und Glauben sowie verhältnismässig erfolgt. Ebenso darf die Versicherung die Personendaten nur zu einem bestimmten Zweck beschaffen und nur in diesem Rahmen bearbeiten. Daneben muss für die betroffene Person dieser Zweck klar erkennbar sein. Aufbewahrt werden dürfen die Daten nur solange, wie der Zweck der Bearbeitung dies bedingt. Ausserdem muss der Bearbeiter der Daten, in diesem Falle der Versicherungsbroker, überprüfen, ob die Daten korrekt sind, muss sie nachführen und ergänzen oder andernfalls vernichten. Im Weiteren muss der Verantwortliche die Sicherheit der Personendaten gewährleisten und durch angemessene, technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten oder Verlust schützen und die betroffenen Personen müssen über die Datenbeschaffung im gesetzlichen Rahmen informiert werden. Führt die Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die

Persönlichkeit oder die Grundrechte der betroffenen Person, so ist der Datenschutzverantwortliche zusätzlich verpflichtet, vorgängig eine Datenschutz-Folgeabschätzung durchzuführen. Liegt ein Datenverlust oder eine unbefugte Bearbeitung vor, so muss der Verantwortliche dies umgehend an den Datenschutzbeauftragten melden. Um das Risiko von Persönlichkeits- und Grundrechtverletzungen zu minimieren, muss der Verantwortliche angemessene Massnahmen ab dem Zeitpunkt der Planung der Datenbearbeitung treffen. Die Datenbearbeitung muss zudem dokumentiert werden und den Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, Datenschutzverletzungen oder Einschränkungen der Bearbeitung informieren, sofern der Aufwand dafür verhältnismässig ist.

Umfang Gewährleistung Datenschutz

Zweck des Datenschutzes ist der Schutz der Persönlichkeits- und Grundrechte der Personen, deren Daten bearbeitet werden. Damit die Daten in den Anwendungsbereich des DSG fallen, muss eine Bearbeitung dieser Daten vorliegen. Die bearbeiteten Daten müssen sich auf eine bestimmte oder zumindest bestimmbare Person beziehen. Als Bearbeitung i.S.d. E-DSG gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Dass die Bearbeitung von Daten in einer Persönlichkeitsverletzung resultiert, ist nicht bei allen Personendaten gleich risikoreich. Aus diesem Grund nennen, sowohl das bisherige Gesetz als auch das E-DSG, eine Liste mit besonders schützenswerten Personendaten. Im Umgang mit diesen Daten ist daher besondere Vorsicht geboten.

Zuwiderhandlungen

Bei der bisherigen Gesetzeslage wurden Verletzungen der Auskunft-, Melde- und Mitwirkungspflichten auf Antrag mit Haft oder Busse bestraft. Ebenso wurden Verletzungen der beruflichen Schweigepflicht lediglich auf Antrag mit Haft oder Busse bestraft. Nur in qualifizierten Fällen, wenn die Bekanntgabe von Datensammlungen ins Ausland nicht oder mit falschen Angaben gemeldet wird oder dem Datenschutzbeauftragten falsche Auskunft erteilt wurde, wurden Haftstrafen oder Bussen ohne vorhergehenden Antrag verordnet. Im neuen Gesetzesentwurf hingegen wurden die Strafbestimmungen umfangreich angepasst, konkretisiert und erweitert. Neu kann beim Verletzungen der Auskunft-, Melde und Mitwirkungspflichten eine Busse von bis zu CHF 500'000.- verhängt werden. Teilweise zwar nur auf Antrag aber jedenfalls in mehr Fällen als zuvor ohne Antrag. Ebenso ist eine Bestimmung vorgesehen, dass eine Verletzung der Sorgfaltspflichten mit einer Busse in derselben Höhe abgestraft werden kann. Zusätzlich wurde die Bestimmung zur beruflichen Schweigepflichtverletzung erweitert, konkretisiert und in einem weiteren Schritt wurde das Gesetz um eine Bestimmung zu Übertretungen in Geschäftsbetrieben ergänzt. Konkret lässt sich zur Rechtslage sagen, dass sie durch den neuen Entwurf zum DSG nicht gänzlich neu zu liegen kommt. Vielmehr wird Bestehendes

konkretisiert, den neuen Gegebenheiten angepasst und Bereichsweise erweitert. Besondere Bedeutung kommt wohl den Strafbestimmungen zu. Diese sind im Vergleich sehr viel detaillierter als im bisherigen Gesetz. Dies lässt die Vermutung zu, dass durch die Konkretisierung der zu erwartenden Strafe eine höhere Abschreckungswirkung für Zuwiderhandlungen gegen das Datenschutzgesetz erzielt werden soll.

Voraussetzungen für Versicherungsbroker

Der Zweck eines Kundenportals, welches den Versicherungsbrokern zur Verfügung gestellt wird, ist, dass die Versicherung einerseits von einfachen administrativen Tätigkeiten, wie Adressänderungen oder kleine Mutationen entlastet wird, und andererseits, dass den Versicherungsbrokern eine Möglichkeit zur schnellen und effizienten Offerterstellung gegeben wird. Aus Sicht der Versicherungsbroker generiert ein Kundenportal den Versicherungen den Mehrwert, dass selbständig und effizient gearbeitet werden kann. Die Versicherungsbroker können im Idealfall alles von der Offerterstellung bis zur Policierung selber vornehmen. Da nicht immer gewartet werden muss, bis die Gesellschaft die Offerten erstellt hat, generiert dies eine Effizienzsteigerung. Die Kundenportale werden vor allem für die Offerterstellungen genutzt, allerdings auch um Policen abzurufen, Leistungen einzusehen und kleine Mutationen, wie Adressänderungen und Änderungen der Zahlungsmodalität, vorzunehmen.

Um die Bearbeitung und Einsehbarkeit der Kundendaten zu analysieren, muss zwischen Neukunden und bestehenden Kunden unterschieden werden. Unter Neukunden im Sinne dieses Fachartikels ist zu verstehen, dass es sich für den Versicherungsbroker um einen Neukunden handelt. Möglicherweise hat der Versicherungsnehmer bereits Policen bei der Versicherung, diese sind im System aber noch nicht für den Versicherungsbroker hinterlegt, da das Brokermandat neu ist. Bestehende Kunden bedeutet, dass der Versicherungsbroker bereits bei den aktiven Verträgen zur Betreuung hinterlegt ist. Bei den Versicherungsgesellschaften sind die Kundendarstellungen sehr unterschiedlich. Es gibt Versicherungen, bei denen gar keine Daten angezeigt werden. Jeder Kunde muss bei jeder Offerterstellung durch den Versicherungsbroker neu erfasst werden. Intern weisen diese Versicherungen die Kunden dann selber einem allfällig bestehenden Kundenspiegel zu. Andere Gesellschaften, wie die AXA, stellen die Kundendaten so zur Verfügung, dass der Kunde zumindest mit der Adresse gesucht und der korrekte Kundenspiegel gefunden werden kann, sofern es sich um einen Neukunden handelt. Ausserdem werden Kundenspiegel mit bestehenden Verträgen, die vom Versicherungsbroker betreut werden, komplett inklusive der Vertragsübersicht dargestellt. So können auch Mutationen vorgenommen werden. Es lässt sich daher sagen, dass die Versicherungsbroker bei dem Brokerportal der AXA primär die Daten sehen müssen, die mit dem Abgleich der selbst vorhandenen Daten eine Identifikation des korrekten Kundenspiegels ermöglichen. Ansonsten führt dies zu Doppelerfassungen. Da der Versicherungsbroker selbst auch ein Vertrag mit dem Kunden hat, sollte er grundsätzlich bereits über die benötigten Daten verfügen. Es ist daher nicht die Aufgabe der Versicherung, neue Daten zu

Neukunden vom Versicherungsbroker zu liefern. Bei Neukunden mit bestehenden Verträgen kann es nach der Mandatseinreichung durch den Broker bei der AXA etwa 3 Tage dauern bis der Vertrag freigeschaltet ist, weil derzeit alles manuell umcodiert werden muss. Bei Kunden ohne aktive Verträge kann es im System gar nicht hinterlegt werden und somit bleibt die Kundenansicht, ausser der Adresse, leer bis ein Vertrag über den Broker abgeschlossen ist. Folglich kann gesagt werden, dass insbesondere die Freigabe der Kundenspiegel mit den aus der Digitalisierung entstehenden Möglichkeiten effizienter gestaltet und umgesetzt werden muss.

Umsetzung durch die Versicherung

In der Versicherungsgesellschaft ist man sich durchaus bewusst, dass die Verschärfung des Datenschutzgesetzes diverse Anpassungen in den verschiedenen Kundenportalen erfordert.

Vorgaben und Konzepte

Um die Grundsätze des Datenschutzes einzuhalten, wurden bei der Versicherung diverse Projekte in Zusammenarbeit mit der Abteilung Legal and Compliance gestartet. Dies obwohl die Grundsätze des Datenschutzes im Vergleich zum bestehenden Gesetz nicht grundlegend geändert wurden aber dennoch die Gelegenheit genutzt werden soll, alle Prozesse zu überprüfen und optimieren, um allfällige Risiken zu minimieren. Insbesondere ist es wichtig, dass bei den internen Prozessen ein Qualitätsmanagement für die Kundendaten implementiert wird. Bei der Versicherungsgesellschaft bestehen diverse Portale und Applikationen, teilweise ist es daher schwierig zu bestimmen, woher die gelieferten Daten kommen und um was für Daten es sich konkret handelt. Dieses Qualitätsmanagement setzt voraus, dass die Versicherungsgesellschaft von sich aus die Daten kontrolliert und, soweit es in ihren Möglichkeiten liegt, aktuell hält oder ergänzt. Im Weiteren ist die Versicherungsgesellschaft jedoch auch darauf angewiesen, dass Kunden gewisse Daten proaktiv melden. Wenn ein Kunde konkret meldet, dass seine Daten unvollständig sind, oder, dass Daten von ihm gelöscht werden sollen, dann braucht es auch ein System zur Sicherstellung, dass dies auf allen Plattformen geschieht. Die Versicherungsgesellschaft hat zwar ein zentrales Kundensystem, welches CRM genannt wird, allerdings werden von dieser Grunddatenbank die Informationen zu diversen Plattformen und Applikationen geliefert. Es muss folglich Teil des Qualitätsmanagements sein, dass die Daten nach der eingetroffenen Meldung flächendeckend in allen Applikationen und Systemen mutiert werden. Dies wird derzeit noch häufig manuell vorgenommen. Ebenso sollte der Gedanke der Datenschutzfreundlichkeit bei allen Kundenportalen, ob nun für Versicherungsbroker oder für Kunden direkt, allgegenwärtig werden. Bestehende Portale müssen überarbeitet werden und bei der Entwicklung neuer Portale soll dieses Prinzip von Beginn an verankert sein. Hierzu gehören auch Konzepte, wie die Informationen an den Inhaber der Daten erfolgt: Transparenz muss absolute Priorität haben. Ebenso sollte aus Gründen der Kundenfreundlichkeit flexibel agiert und auf individuelle Wünsche eingegangen werden. Von Bedeutung ist insbesondere den Kunden die Hinterlegung ihrer

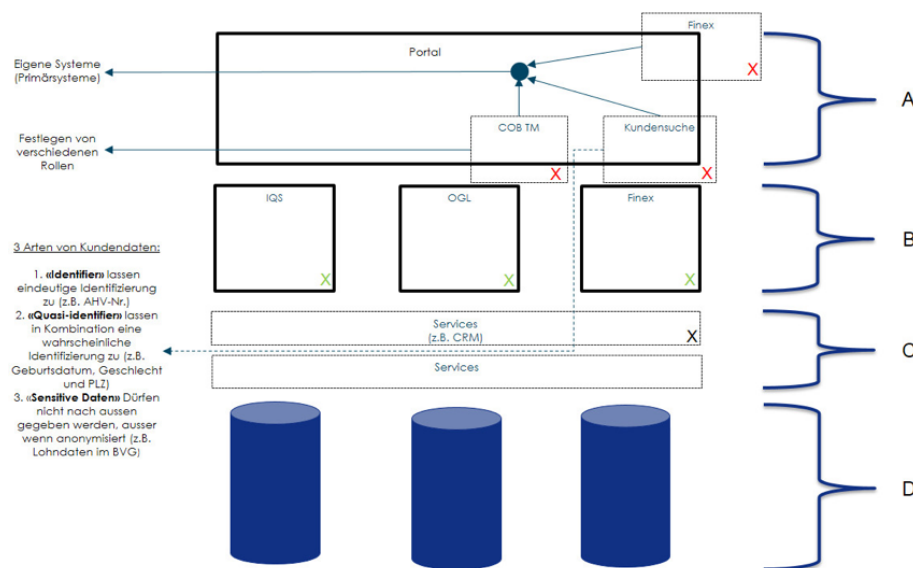
individuellen Datenschutzanliegen zu ermöglichen und diese auch wunschgemäss umzusetzen. Um diesem Ziel gerecht zu werden, wurden bereits erste Schritte eingeleitet, wie beispielsweise, wenn Kunden eine Werbesperre wünschen.

In einem weiteren Schritt muss sich die Versicherungsgesellschaft hinterfragen, welche Daten tatsächlich absolut notwendig sind. In der Vergangenheit wurden auch Daten eingefordert, die nicht zwingend für den gewünschten Zweck, wie beispielsweise den Abschluss der entsprechenden Versicherung, erforderlich waren. Die einzuholenden Daten sollen in Zukunft auf das absolute Minimum beschränkt werden. Dies minimiert sodann auch das Risiko, dass der Kunde sich nicht einverstanden erklärt und ein Versicherungsabschluss deswegen nicht zustande kommt. Bei der Ausarbeitung neuer Konzepte ist von grösster Bedeutung, dass alle betroffenen Fachbereiche im Projekt involviert sind. Nur so können benutzerfreundliche, gesetzeskonforme Portale und Prozesse ausgearbeitet werden. Im Sinne der Digitalisierung müssen die Portale sowie die Prozesse effizient gestaltet werden, aber dennoch dem Gesetz standhalten und benutzerfreundlich sein. Es besteht daher der Bedarf einer engen Zusammenarbeit zwischen der Rechtsabteilung, welche den rechtlichen Rahmen vorgibt, der IT, welche die technischen Möglichkeiten aufzeigt, sowie der Person aus dem entsprechenden Kernprozess, welche den Prozessablauf einbringt. In einer späteren Phase ist es zudem essentiell, dass bei den betroffenen Mitarbeitern Awareness geschaffen wird. Die von der Umstellung betroffenen Sachbearbeiter müssen wissen, weswegen genau andere Vorgaben einzuhalten sind bzw. warum Prozesse verändert wurden. Im Falle eines Portals für Versicherungsbroker muss sodann auch berücksichtigt werden, dass allfällige Beschwerden von Versicherungsbrokern eintreffen, weil die Kundendaten nicht sofort geliefert werden und sich der Prozess verzögert. Wenn die Sachbearbeiter korrekt geschult sind und die Gründe verstehen, werden Vorgaben weniger missachtet. In einer ersten Betrachtung erscheint es, als ob zwischen dem Ziel des Datenschutzes und der Digitalisierung ein Zielkonflikt besteht. Ebenso kann ein solcher zwischen dem Datenschutz und der Kundenfreundlichkeit bestehen. Im Sinne der Digitalisierung ist angedacht, Prozesse effizienter zu gestalten wozu auch das Ziel der Lieferzeit von benötigten Daten gehört. Ähnliches gilt bei der Kundenzufriedenheit, auch die Kunden möchten ihren Service innert Kürze abrufen können. Die einzuhaltenden Richtlinien des Datenschutzes verhindern derzeit aber noch einen raschen Datenaustausch. Dies sind Aspekte, welche derzeit in der Rechtsentwicklung sowie in der Wirtschaft behandelt werden und zu denen Lösungen ausgearbeitet werden müssen.

Technische Struktur

Das zur Rede stehende Portal für Versicherungsbroker (Brokerportal genannt) ist ein Primärsystem. Hierarchisch gesehen kommt es, wie in der nachfolgenden Grafik ersichtlich, an die oberster Stelle, die mit A bezeichnet ist. Es zeigt sich, dass es somit abhängig

ist von allen vorhergehenden Systemen, bezeichnet mit B – D. Sämtliche Daten werden aus der Stufe D, den Grundsystemen bezogen. I.d.R. geschieht dies mittels Services, Stufe C, welche die entsprechenden Daten aus den Grundsystemen abrufen und an das Primärsystem weitergeben.



Welche Daten exakt angezeigt werden, wird durch zwei Stellen entschieden. Bereits in den einzelnen Services auf Stufe C sind Regelungen festgelegt, welche Daten überhaupt zur Ansicht gegeben werden und bei welchen eine Mutation zugelassen ist. Da die Services in der Hierarchie sehr weit unten angesiedelt sind, können diese Restriktionen von allen nachfolgenden Applikationen nicht umgangen werden. Zusätzlich zu diesen vordefinierten Restriktionen, werden im Primärsystem anschliessend weitere Restriktionen festgelegt, um konkret auf die bereichsspezifischen Bedürfnisse einzugehen. In welcher Form und in welchem Umfang die erhaltenen Daten anschliessend im Brokerportal angezeigt werden, wird auf Stufe A mittels Rollen festgelegt. Bei der Distribution der Rollen wird unterschieden, ob es sich um Unternehmensexterne, z.B. den Versicherungsbroker, oder um einen Unternehmensinternen, z.B. den Sachbearbeiter, handelt. Die Rollen werden mit entsprechenden Rechten ausgestattet. Dabei wird festgelegt, welche Daten dem User angezeigt werden und bei welchen Kunden er mehr Rechte hat als bei Anderen. Betreut der Versicherungsbroker beispielsweise bereits die Versicherungsverträge des entsprechenden Kunden und kann das System dies nachvollziehen, so erhält er den vollen Datenzugriff auf die ausgewiesenen Daten. Im Weiteren gibt es noch die Situation mit Neukunden. Sind die Verträge eines Kunden noch nicht auf den Versicherungsbroker hinterlegt oder handelt es sich um einen Kunden, der lediglich erfasst ist aber keine Verträge hat, kann die Versicherung mit den derzeitigen Möglichkeiten nicht wissen, ob der Versicherungsbroker berechtigt ist, die Daten einzusehen. In diesen Fällen erhält er nur das Recht, den Namen und die Adresse einzusehen, die restlichen Daten werden nicht angezeigt. In der abgebildeten Grafik veranschaulichen die „X“ in unterschiedlichen Farben, dass die jeweiligen Rollen von den einzelnen Stufen separat vergeben werden.

Verantwortlichkeiten

Beim Primärsystem existiert eine hohe Verantwortlichkeit dafür, dass keine falschen Rechte an unberechtigte Personen vergeben werden. Da die Services die Daten in der Form an das Primärsystem liefern müssen, dass sowohl Interne als auch Externe damit arbeiten können, besteht hier kein Potenzial die Restriktionen zur Datenbearbeitung durch einen Versicherungsbroker auf dieser Stufe zu lösen. Folglich liegt es an dem zuständigen Projektteam des Primärsystems, diese Feinjustierungen zu definieren und umzusetzen. Im Rahmen der Gesetzesverschärfung ist angedacht, Projekte zu starten, welche sich unter anderem dem Thema der Datenanzeige widmen. Ebenso ist ein Projekt in Arbeit, bei welchem man sich insbesondere der Dokumentation der Datenänderungen annimmt und diese überarbeitet. Neben der Datenanzeige besteht auch die Verantwortung dafür, welche Kundendokumente den Versicherungsbrokern zur Verfügung gestellt werden. Zum jetzigen Zeitpunkt geschieht dies noch in Zusammenarbeit mit dem Kundenportal, welches direkt für die Kunden gedacht ist. Für die Freigabe im direkten Kundenportal werden die Dokumente intern entsprechend kategorisiert und nur angezeigt, wenn alle Kriterien für die Freigabe vorhanden sind. Auch dieser Mechanismus wird hinsichtlich der Gesetzesverschärfung überprüft. Möglicherweise ergibt sich, ob es Kundendokumente gibt zu denen der Versicherungsbroker nicht notwendigerweise Zugriff haben muss. Denkbar wäre beispielsweise, dass das Brokermandat zwischen dem Versicherungsbroker und dem Kunden den entsprechenden Bereich nicht umfasst.

Optimierungsvorschläge Effizienz

Um den Versicherungsbrokern ein effizienteres Arbeiten im Sinne der Digitalisierung zu ermöglichen, besteht insbesondere bei der Zuteilung von Kunden Optimierungspotenzial. Dazu bieten sich unter den genannten Umständen unterschiedliche Optionen an. Systemtechnisch wäre eine Option, dass die bisher manuelle Verarbeitung von eingereichten Mandaten für bestehende Verträge automatisiert und direkt im System integriert wird. Dazu wäre die Möglichkeit einzurichten, dass der Versicherungsbroker ein Mandat auf dem Kundenspiegel hochladen kann. Anschliessend wäre eine Applikation zu integrieren, welche das Mandat direkt überprüft und als valid erkennen kann. Ist dies geschehen, wird der Kundenspiegel freigeschaltet. Eine andere Möglichkeit wäre, das bestehende Modell der Mandatseinreichung in eine individuelle Freigabe zu transformieren. Bereits im aktuellen Zeitpunkt wird im Zusammenhang mit der Freigabe für Kundendokumente mit dem direkten Kundenportal zusammengearbeitet. Hier bietet sich die Möglichkeit an, dass der Versicherungsbroker auf dem Kundenspiegel im Brokerportal direkt eine Freigabeanfrage erstellen kann. Dabei muss er angeben, welche Daten er zu welchem Zweck benutzen will. Anschliessend wird diese Freigabeanfrage in das direkte Kundenportal gesendet und der Kunde selbst kann die Freigabe zu seinen Bedingungen erteilen oder auch ablehnen. Dies stünde auch im Einklang mit der angestrebten Datenschutzfreundlichkeit gegenüber den Kunden.

Die Abteilung Legal and Compliance steht, wie ausgeführt, zur Verfügung, um in Projekte miteinbezogen zu werden und ist auch bereits in vielen Projekten involviert. Beim Projekt zum Brokerportal wurden sie allerdings seit längerem nicht mehr miteinbezogen. Hinsichtlich der Verschärfung des Datenschutzgesetzes sind allerdings Projekte angedacht, um das bisherige Konstrukt der Datenanzeige zu überprüfen. Insbesondere, weil die Daten in der IT anders kategorisiert werden als aus rechtlicher Sicht, wobei bei der rechtlichen Sicht insbesondere die besonders schützenswerten Daten zu berücksichtigen sind, sollte hierbei von Beginn des neuen Projekts an die Abteilung Legal and Compliance konsultiert werden. Bisher geschah dies eher gegen Ende, um das bereits erarbeitete Konzept abzusegnen. Diese Vorgehensweise lässt vermuten, dass die hohen Standards betreffend Datenschutz möglicherweise noch nicht ganz bei den Mitarbeitern verankert sind. Um die Personen sowohl aus dem Business als auch aus dem IT-Bereich mehr auf den essentiellen Gehalt der Datenschutzrichtlinien zu sensibilisieren, sind sodann gezielte Schulungen zu empfehlen. In einem weiteren Schritt sind zudem die Datenschutzklauseln in den Zusammenarbeitsverträgen mit den Versicherungsbrokern zu überprüfen, da sich die Versicherungsgesellschaft grundsätzlich mittels dieser Verträge absichert.

Schlussfolgerungen

Datenschutz ist kein gänzlich neues Thema, deswegen bestehen bereits zahlreiche Mechanismen, um Datenschutzkonform zu handeln. Dennoch, mangels hoher Strafen, wurde die Thematik Datenschutz in der Vergangenheit zwar beachtet, allerdings nicht unter allen Umständen versucht einzuhalten. Zu

dieser Schlussfolgerung kann gelangt werden, wenn aufgezeigt wird, dass sämtliche Bereiche in der Unternehmung ihre derzeitigen Prozesse nochmals überprüfen und gegebenenfalls optimieren. In der Versicherungsbranche herrscht derzeit eine dezente Verunsicherung hinsichtlich der kommenden Verschärfung des Datenschutzgesetzes. Gleichzeitig nimmt die Digitalisierung ihren Lauf, dies bietet eine hervorragende Chance, um die Überprüfung der internen Prozesse auch im Einklang mit dem Datenschutz zu beleuchten. Insbesondere beim Brokergeschäft gilt es, die bisherigen Prozesse nochmals detailliert durchzugehen. Die Konstellation mit dem rechtlichen Dreiecksverhältnis stellt eine Herausforderung dar, wenn die Versicherung einerseits wirtschaftlich effizient tätig sein will, gleichzeitig aber auch wachsam sein muss, dass gesetzeskonform agiert wird. Aus wirtschaftlicher Sicht soll dem Versicherungsbroker so viel wie möglich zur Verfügung gestellt werden, damit dieser auch gewillt ist, bei der entsprechenden Versicherung selbständig Abschlüsse zu tätigen. Andererseits ist es unter den derzeitigen technischen Gegebenheiten schwierig, in allen Geschäftsvorfällen über eine effiziente Lösung zu verfügen damit sichergestellt wird, dass dem Versicherungsbroker nicht zu viele Kundendaten zur Einsicht und zur Bearbeitung gegeben werden.

Im aktuellen Zeitpunkt empfinden die Versicherungsbroker die Applikation der Versicherung noch nicht als ineffizient. Dies lässt sich aber damit begründen, dass noch nicht alle Versicherungsgesellschaften ein umfangreiches Brokerportal zur Verfügung stellen und die Versicherungsbroker zurzeit schätzen, dass zumindest ein System vorhanden ist. Mit dem Fortschritt der Versicherungen im Bereich der Digitalisierung kann und wird sich dies in Zukunft vermutlich ändern. Dann erzielt diejenige Gesellschaft, welche die effizientesten Prozesse und Systeme zur Verfügung stellt, einen Wettbewerbsvorteil. Dieser ist jedoch nur dann tatsächlich gegeben, wenn auch die Reputation der Versicherungsgesellschaft positiv ausfällt. Versicherungsgesellschaften, welche nicht datenschutzkonform agieren, werden mit hohen Geldstrafen abgemahnt und verlieren ihre positive Reputation. Geschieht dies, kann der Wettbewerb mit anderen Versicherungsgesellschaften kritisch werden.

Die in diesem Fachartikel behandelte Versicherungsgesellschaft ist sich der Verantwortlichkeit zum Datenschutz sehr bewusst. Ebenfalls ist sie auch bereits auf die Änderungen der Gesetzeslage sensibilisiert und überarbeitet die vorhandenen Prozesse überaus pflichtbewusst. Die bestehenden Prozesse im vorhandenen Brokerportal werden aufgrund der Gesetzesveränderung in Zukunft noch beleuchtet und angepasst. Eine zweckbringende Lösung, wie Zugriffe auf Daten gesteuert werden, ist mit den zu vergebenden und anpassungsfähigen Rollen vorhanden. Bei den Prozessen, wie die Einhaltung des Gesetzes hingegen effizient und für den Versicherungsbroker innert Kürze mit den erlaubten Daten und Bearbeitungsfähigkeiten zu beliefern ist, besteht allerdings noch Optimierungspotenzial. Abschliessend ist festzuhalten, dass Datenschutzverletzungen kein Kavaliersdelikt sind und deswegen ist es auch notwendig, eine Verschärfung einzuführen.



Kostenlose Rechtsberatung?

Lassen Sie sich von engagierten Rechts-Studierenden in der law-clinic helfen.

Ausgangslage

Die ZHAW ist sich ihrer Verantwortung gegenüber Studierenden und der Bevölkerung bewusst und hat deshalb das Projekt law-clinic ins Leben gerufen. Dort bieten Studierende des Studiengangs Wirtschaftsrecht – unter der Aufsicht

von Rechtsanwälten – kostenlose Rechtsberatung für sämtliche Rechtsuchende an. Die Studierenden erhalten so die Gelegenheit, die erlernten Grundlagen praxisorientiert anzuwenden und Erfahrungen mit «echten» Fällen zu sammeln.

Inhalte

Eine Win-win-Situation für alle!

- Denn Studierende wollen und müssen ihr Wissen anwenden und in der Praxis umsetzen.
- Denn in der Praxis gibt es viele Rechtsstreitigkeiten, die aufgrund des geringen Streitwerts von Anwälten nicht betreut werden.

Das Angebot ist übrigens kostenlos.

Melden Sie uns Ihren Fall unter:

>>> www.zhaw.ch/lawclinic

Weitere Informationen

Dr. iur. Fabio Babey

Stv. Leiter Zentrum für Wettbewerbs-
und Handelsrecht

ZHAW School of Management and Law

Telefon +41 58 934 76 56

fabio.babey@zhaw.ch

Law Clinic: Neues Wahlpflichtmodul

Ab dem Herbstsemester 2018/19 ist für Wirtschaftsrechtsstudierende ein neues Wahlpflichtmodul im Angebot: die law-clinic. WOB hatte die Möglichkeit, mit dem Modulverantwortlichen Dr. Fabio Babey ein Interview zu führen.

Was erwartet die Studierenden in der law-clinic?

In der law-clinic können die Studierenden unter der Betreuung von Rechtsanwälten/Dozentinnen bei echten Fällen eine Rechtsberatung anbieten. Die Studierenden wenden so ihr erlerntes Wissen in der Praxis an und bereiten sich somit auf ihre spätere berufliche Tätigkeit optimal vor. Plus: Es sieht immer auch im CV gut aus, wenn die Studierenden in der Rechtsberatung bereits erste Erfahrungen sammeln konnten.

Was für Fälle erhalten die Studierenden?

Es sind alles «echte» Fälle, die Unternehmen und Einzelpersonen via Formular auf der Internetseite der law-clinic gemeldet haben. Es handelt sich vor allem um Rechtsstreitigkeiten, die aufgrund des geringen Streitwerts von Anwälten nicht betreut werden und somit unbehandelt bleiben würden oder Streitigkeiten von Personen, die eine «Ersteinschätzung» wünschen, bevor sie viel Geld an einen Anwalt zahlen.

Was muss man als Student für die law-clinic mitbringen?

Erwartet wird von den Studierenden eine hohe Flexibilität und Leistungsbereitschaft, da die Fälle neben dem normal weiterlaufenden Studium bearbeitet werden müssen und keinem Stundenplan folgen. Zudem richtet sich das Wahlpflichtmodul an Studierende, die das Assessment bereits hinter sich haben. Alle weiteren Kenntnisse, die für die law-clinic benötigt werden, werden den Studierenden an einer Schulung mitgegeben.

Wer darf sich für eine Beratung an Euch wenden?

Die law-clinic der ZHAW ist eine Rechtsberatung für jederfrau und -mann. Und kostenlos! Einfach den Fall unter www.zhaw.ch/lawclinic melden!



Dr. Fabio Babey

The London experience - UCL Summer School

° Ein Bericht von Angelina Rau

*N*achdem ich das vierte Semester meines Wirtschaftsrechtsstudiums in Taiwan absolviert hatte, konnte ich meinen Auslandsaufenthalt mit einer Summer School am University College in London (UCL) verlängern – eine anspruchsvolle, aber auch sehr lehrreiche Erfahrung.

Schon zu Beginn meines Wirtschaftsrechtsstudiums war es mein Traum, ein Semester im Ausland zu verbringen. Ich informierte mich über das Mobilitätsangebot der ZHAW und konnte diesen Traum im vierten Semester in Taiwan erfüllen. Da es mir so gut gefiel, informierte ich mich während dem Semester in Taipeh, an der National Taiwan University, erneut über Möglichkeiten, den Auslandsaufenthalt zu verlängern. Dank der vielen Partnerhochschulen der ZHAW weltweit finden sich auch einige Summer Schools, die ein kompaktes Kursangebot offerieren.

Vorbereitung und Anmeldung

Sobald das Summer School-Angebot im Intranet aufgeschaltet wurde, suchte ich nach anrechenbaren Kursen, die mit den Semesterdaten der Universität in Taiwan kompatibel waren. Ich entschied mich für das Modul «International Trade and Maritime Law» am UCL, da ich aus einer früheren beruflichen Tätigkeit bereits über etwas Praxiserfahrung verfügte und es sich sehr anbot, diese Erfahrung mit Theorie zu ergänzen.

Ich konnte mich direkt über die Website der UCL anmelden, die im Intranet der ZHAW verlinkt ist. Die Summer Schools zählen als Wahlpflichtmodule, die sich im fünften oder sechsten Semester des Vollzeitstudiums anrechnen lassen. Der gesamte Bewerbungsprozess verläuft deshalb direkt mit der UCL und nicht mit dem International Office der ZHAW. Die UCL prüfte meine Online-Anmeldung und informierte mich über den Zulassungsbescheid. Je nach Sprachnachweis entscheiden ein Englischtest und ein persönliches Skype-Interview mit dem Leiter der Summer School Programme über die definitive Zulassung, die ich erfreulicherweise kurz darauf erhielt. Durch einen persönlichen Online-Zugang hatte ich die Übersicht über Kurswahl, Immatrikulation und Studiengebühren. Das Summer School Team der UCL ist sehr professionell und steht den Studierenden mit Rat und Tat zur Seite falls etwas nicht funktioniert oder Fragen auftauchen.

Unterkunft, Universität und Campus

Ich war froh, dass ich für meinen relativ kurzen Aufenthalt von vier Wochen kein Zimmer suchen musste. Das UCL organisiert auf Wunsch eine Unterkunft in den Wohnheimen von Unite Students. Die meisten sind in unmittelbarer Nähe des UCL Campus gelegen, verfügen über einen relativ modernen Ausbaustandard, ein eigenes Zimmer mit Nasszelle, gemeinsame Küchen und Aufenthaltsräume. Der zentrale Campus liegt im Stadtteil Bloomsbury. In den zahlreichen Nebengebäuden finden je nach Fakultät unterschiedliche Kurse statt. Ich besuchte das Modul International Trade and Maritime Law am UCL Centre for Languages & International Education (CLIE). Am Einführungstag lernte unsere Gruppe auf einer Campustour sämtliche wichtigen Gebäude kennen.

In meinem Modul fand der Unterricht in einer kleinen Klasse von zwölf Personen statt, sodass ein persönliches Klima mit viel Raum für Interaktion entstand. Die Dozentin verfügt über langjährige Berufserfahrung auf ihrem Fachgebiet, war sehr offen und pflegte ein kollegiales Verhältnis zu den Studierenden. Da wir täglich jeweils vom Mittag bis am Abend Unterricht hatten, lernten wir uns schnell kennen und verbrachten auch ausserhalb des Klassenzimmers viel Zeit miteinander.

Das Modul war spannend, aber auch sehr anspruchsvoll und umfasste viel Lektüre, mit der wir morgens den Unterricht vorbereiten mussten. Angesichts dieser Intensität überraschte es mich, dass das Modul an der ZHAW lediglich mit 3 statt 6 ECTS angerechnet wird. Die Abschlussprüfung besteht aus einem individuellen Moot Court, bei welchem man entweder die Rolle des Klägers oder des Beklagten einnimmt. Trotz des hohen Anspruchs kann ich dieses sehr lehrreiche Modul nur weiterempfehlen.



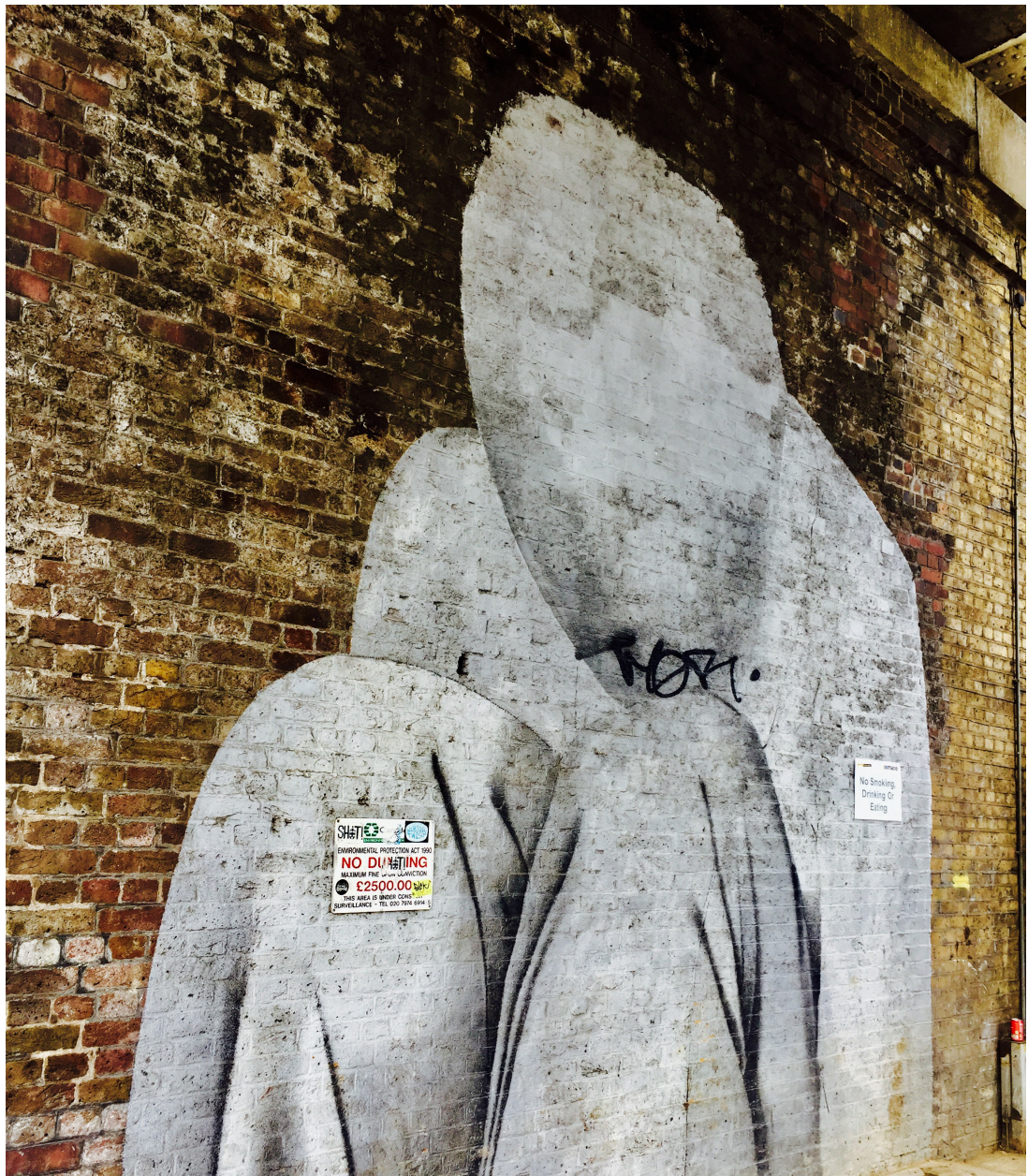
Freizeit und Reisen

Aufgrund der Intensität des Moduls hatte unsere Klasse, im Vergleich zu anderen Modulen, relativ wenig Freizeit. Dennoch blieb Zeit, um gemeinsam etwas zu unternehmen und die Vielseitigkeit Londons zu genießen. Das Summer School Team der UCL stellt den Studierenden vor dem Modulbeginn sogar ein Kulturprogramm zusammen, aus dem man verschiedene Aktivitäten auswählen kann – ein sehr dienstleistungsorientierter Service, den ich so von Schweizer Hochschulen weniger kannte.

An den Wochenenden lagen auch Ausflüge in malerische Orte wie Windsor, Bath, Dover oder Cotswolds drin, welche entweder mit Mietauto, Bus oder Zug gut erreichbar sind. Aber eigentlich müsste man London gar nicht verlassen – Langeweile kommt in dieser Stadt bestimmt nie auf. Der letzte Abend der Summer School wird traditionellerweise mit einer Boat Party abgeschlossen. Falls die Partynächte bis dahin zu kurz gekommen sind, erhält man spätestens dann nochmals die Gelegenheit mit neuen Freunden bis in die Morgenstunden zu feiern.

Fazit

Das University College London ist eine der angesehensten Universitäten der Welt; seit einigen Jahren belegt sie Platz 7 im weltweiten QS University Ranking. Zu Beginn der Summer School fragte ich mich, ob die Diskussionen um solche Rankings nicht nur zum «Hype» der internationalen Privatuniversitäten gehöre. Meine Skepsis wurde jedoch gänzlich beseitigt. Besonders hervorzuheben ist die Professionalität der Schule, die durch die Qualität der Lehrpersonen, die hervorragende Organisation und den persönlichen Service des Summer School Teams besticht. Insgesamt war die UCL Summer School ein grossartiges Erlebnis, aus welchem ich schöne Erinnerungen und neue Freundschaften mitnehmen konnte. Gleichzeitig war es eine fantastische Gelegenheit, meinen Auslandsaufenthalt nach Taiwan erneut zu verlängern. Ich kann die «London experience» an der UCL nur wärmstens weiterempfehlen.





Der Weg zum Rechtsanwalt

° Ein Interview mit Sebastian P. Weber,
M Law; Rechtsanwalt bei VISCHER in Zürich

- Das Interview wurde geführt von Angelina Rau



Sebastian P. Weber

Bitte stellen Sie sich dem Leser vor.

Mein Name ist Sebastian P. Weber, ich bin 31 Jahre alt und wohne seit Mitte Juni 2018 in Wallisellen. Ich arbeite seit März 2018 bei VISCHER in Zürich als Rechtsanwalt (Corporate/M&A).

Warum haben Sie sich damals für ein Wirtschaftsrechtsstudium entschieden?

Ich habe bereits während meiner Ausbildung zum Kaufmann ein besonderes Interesse für rechtliche Fragestellungen festgestellt. Noch während des Besuchs eines Informationsanlasses der ZHAW habe ich mich entschieden, Wirtschaftsrecht zu studieren.

Würden Sie sich nochmals für den Studiengang Wirtschaftsrecht entscheiden?

Ja, ich würde mich aufgrund der Kombination aus Recht, Wirtschaft und Sprachen sowie der Möglichkeit, nach dem Bachelor mit vertretbarem Zusatzaufwand den MLaw erlangen zu können, nochmals für den gleichen Studiengang entscheiden.

Haben Sie während des Studiums gearbeitet oder Weiterbildungen besucht?

Nein. Ich habe nach der Rekrutenschule und vor Studienbeginn während 9 Monaten Vollzeit und danach noch einige Monate Teilzeit bei einer Grosskanzlei in Zürich als Assistent gearbeitet. Danach habe ich mich voll auf das Studium konzentriert. In den Sommermonaten bin ich jeweils meiner Dienstpflicht nachgekommen.

Was ist Ihnen positiv oder negativ in Erinnerung geblieben, wenn Sie an Ihre Studienzeit an der ZHAW zurückdenken?

Als eher negativ in Erinnerung geblieben sind mir die teilweise nervenaufreibenden Gruppenarbeiten. Die positiven Erinnerungen überwiegen jedoch eindeutig. Ich habe zum Beispiel sympathische Menschen kennengelernt – zu einigen habe ich noch heute einen guten Kontakt –, und als Wochenaufenthalter in Winterthur so Einiges erlebt.

Wie verliefen die Vorbereitungen für die Passerellenprüfungen an der Unilu?

Die Vorbereitungen sind meinen Vorstellungen entsprechend verlaufen. Ich habe die Vorlesungen besucht, die Literatur gelesen und den Lehrstoff bei Gelegenheit repetiert.

Wann haben Sie die Passerellenprüfungen absolviert?

Die Prüfungen Strafrecht I+II, Verwaltungsrecht I+II und ZGB I+II habe ich nach dem zweiten, die Prüfung Grundlagen des Rechts im dritten und die Verbundprüfung im fünften Semester des Masterstudiums absolviert.

Sie haben während den Passerellenprüfungen bereits Fächer aus dem regulären Masterprogramm belegt. Können Sie dies empfehlen? Falls ja/nein, warum?

Die Vorlesungen bspw. in Strafrecht I+II - deren Zeitaufwand (inkl. Vor- und Nachbereitung) überschaubar ist - erstrecken sich über zwei Semester. Am Ende des ersten Semesters hätte man ohne Mastermodule keine Prüfungen. Es ist deshalb zu empfehlen, bereits im ersten Semester einige Mastermodule zu besuchen und dann auch die Prüfungen abzulegen.

Welche Vorlesungen aus dem regulären MA haben Sie hauptsächlich besucht (in Kürze, keine Auflistung)? Welche können Sie besonders empfehlen?

Die Wahl der Mastermodule hängt erheblich von den persönlichen Präferenzen und Zielen nach dem MLaw ab. Wer die Anwaltsprüfung abzulegen gedenkt, sollte eine möglichst breitgefächerte Wahl treffen (Anwaltsrecht; Bau-, Planungs- und Umweltrecht; Internationales Privatrecht; SchKG; Strafprozessrecht; etc.).

Wo haben Sie die Praktika für die Anwaltsprüfung absolviert und wie lange? Was empfehlen Sie Masterstudenten und -absolventen für die Praktik suche?

Ich habe ein Anwaltspraktikum bei einer Aargauer Anwaltskanzlei (Nettojahr) und ein Gerichtspraktikum beim Bezirksgericht Dietikon (10 Monate) absolviert. Ich empfehle, bereits frühzeitig mit der Suche zu beginnen. Wer sich erst kurz vor Studienende um ein Praktikum bemüht, wird je nach Kanton und gewünschter Praktikumsstelle feststellen, dass diese für die nächsten Jahre bereits vergeben ist.

Wie lange haben Sie sich auf die Anwaltsprüfung vorbereitet und wo haben Sie diese abgelegt?

Ich habe mich während rund sechs Monaten auf die schriftlichen Prüfungen und während rund 2½ Wochen auf die mündliche Prüfung vorbereitet. Die Anwaltsprüfung habe ich im Kanton Aargau abgelegt.

„Der Einstieg – und damit der Transfer von der Theorie in die Praxis – verlief sowohl unmittelbar nach dem Studium als auch nach der Anwaltsprüfung erfreulich gut.“

Wie verlief Ihr Einstieg in die Berufswelt nach dem Studium und nach der Anwaltsprüfung? Was waren die Schwierigkeiten?

Der Einstieg – und damit der Transfer von der Theorie in die Praxis – verlief sowohl unmittelbar nach dem Studium als auch nach der Anwaltsprüfung erfreulich gut. Dies führe ich namentlich auf die bereits erworbene Arbeitserfahrung und auf die solide Ausbildung (einschliesslich Lehre und Berufsmaturität!) zurück.

War Ihnen von Anfang an klar, dass Sie den MLaw an der Universität Luzern machen werden und im Anschluss die Anwaltsprüfung oder haben Sie andere Berufsmöglichkeiten geprüft?

Zu Beginn des Wirtschaftsrechtsstudiums hätte ich nicht gedacht, dass ich eines Tages als Rechtsanwalt tätig sein werde. Vielmehr waren das FH- und dann auch das Uni-Studium für mich zunächst bloss eine logische Konsequenz der jeweils vorher erfolgreich abgeschlossenen Schule. Die Möglichkeit, nach dem MLaw noch Praktika zu absolvieren und zur Anwaltsprüfung anzutreten, habe ich erst nach dem Start in Luzern so richtig in Betracht gezogen.

„Die Lern- und Erfahrungskurve ist steil.“

Streben Sie eine Weiterbildung an?

Ich werde voraussichtlich in zwei Jahren ein LL.M.-Studium im angelsächsischen Raum absolvieren. Überdies möchte ich zu gegebener Zeit eine Dissertation verfassen.

Wie lautet Ihre Berufsbezeichnung und was sind Ihre Tätigkeiten? Können Sie uns einige Beispiele aus dem Alltag nennen?

Ich arbeite als Rechtsanwalt („Associate“) bei VISCHER in Zürich und bin vorwiegend in den Bereichen Mergers & Acquisitions sowie Gesellschafts- und Handelsrecht tätig. Meine Tätigkeiten umfassen etwa die Mitarbeit bei der Durchführung einer Legal Due Diligence, die Vornahme von rechtlichen Abklärungen und die Erarbeitung von rechtlichen Dokumenten. Die Lern- und Erfahrungskurve ist steil.

Was hat Sie dazu bewogen, sich bei einer grossen Kanzlei wie VISCHER zu bewerben?

Der Wunsch nach einer Spezialisierung im Wirtschaftsrecht hat den Entscheid in einem gewissen Umfang vorweggenommen. Neben den Tätigkeitsgebieten haben insbesondere auch die Entwicklungsmöglichkeiten (intern und extern), die Infrastruktur und Lage der Kanzlei und die Unternehmenskultur zu diesem Entscheid beigetragen.

Warum ist dieser Beruf interessant (Herausforderungen)? Was gefällt Ihnen gut, was eher weniger?

Die spannenden Tätigkeitsgebiete und das leistungsorientierte Umfeld gefallen mir besonders gut. Das Ziel ist stets, juristische Dienstleistungen auf höchstem Niveau zu erbringen. Eine sorgfältige und genaue Arbeitsweise sowie eine gewisse Hartnäckigkeit sind unerlässlich. Wer in einer Kanzlei wie VISCHER arbeitet, muss überdies bereit sein, abends länger zu bleiben und auch einmal an Feiertagen und Wochenenden zu arbeiten, wenn die Arbeitsbelastung es erfordert.

Wie sehen die Karrieremöglichkeiten aus?

Die Karrieremöglichkeiten sind vielfältig. Nach mehreren Jahren der erfolgreichen Mitarbeit besteht allenfalls die Möglichkeit, Counsel oder Partner der Kanzlei zu werden. Ein weiteres Beispiel ist der Wechsel in den Rechtsdienst eines Unternehmens.

Welche Erwartungen hatte Ihr Unternehmen an Sie in Bezug auf Ihren Universitätsabschluss (Noten, Leistungen)?

Es ist kein Geheimnis, dass grössere Wirtschaftskanzleien mindestens das Prädikat „magna cum laude“ erwarten.

Denken Sie, es gibt Verbesserungspotential im Studiengang Wirtschaftsrecht?

Wenn ja, welches?

Es gibt immer etwas zu verbessern. Ich habe gesehen, dass die Modultafel mit Wirkung per HS2014 mehrere Änderungen erfahren hat. Soweit für mich überhaupt beurteilbar, steht diese Modultafel insgesamt für eine Verbesserung des Studiengangs.

Können Sie uns aus Ihrer Sicht zwei Stärken und zwei Schwächen des Studienganges Wirtschaftsrecht nennen?

Eine Stärke und – soweit man später die Anwaltsprüfung absolvieren möchte – zugleich eine Schwäche im Vergleich zum Jus-Bachelor an der Universität ist die Gewichtung von Wirtschaft und Sprachen. Eine Schwäche ist jedenfalls, dass man teilweise nur die Folien in- und auswendig können muss, um eine Prüfung zu bestehen. Eine klare Stärke des Studiengangs ist, dass viele Dozenten auch noch in der Praxis tätig sind.

Was würden Sie einem zukünftigen Wirtschaftsrechtsabsolventen mit auf den Weg geben?

Das Bewusstsein um die eigenen Stärken ist wichtig. Man sollte einer Tätigkeit nachgehen, in der man seine Stärken ausspielen kann – und die auch noch Spass macht!

Vielen Dank!

„Das Bewusstsein um die eigenen Stärken ist wichtig. Man sollte einer Tätigkeit nachgehen, in der man seine Stärken ausspielen kann – und die auch noch Spass macht!“

Rechtswissenschaft – ein Fall für Sie?



MLaw (Luzern)

Das Masterstudium Rechtswissenschaft in Luzern

- bietet eine freie Fächerwahl aus über 100 Masterfächern mit einem breiten Angebot in englischer Sprache
- erlaubt eine flexible fachliche Profilierung mit Schwerpunkten nach persönlichen Interessen
- kann mit dem zweisprachigen Doppelmaster-Diplom Luzern/Neuchâtel oder einem internationalen Double Degree abgeschlossen werden
- bietet drei interdisziplinäre «Master Plus»-Studiengänge

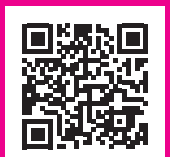
Masterinfoabende

Zweimal im Jahr informieren wir Sie persönlich über das Masterstudium:

- Zulassung und Studienablauf mit Bachelor in Wirtschaftsrecht der ZHAW
- Aufbau und Inhalt des Studiengangs
- Mobilität
- Das Studium aus Studierendensicht

Mittwoch, 17. Oktober 2018 und Dienstag, 19. März 2019

www.unilu.ch/masterinfo-rf





Impressum

Redaktion

Chefredaktor: Angelina Rau,
rau01@students.zhaw.ch.

Ivo Schnyder
Amina Ouakrim
Aurora Melo Moura

Lektorat

Carla Achermann, carla.achermann@gmail.com
Florian Wehrli, florian.wehrli@gmail.com

Herausgeberin

Studentenverein Wirtschaftsrecht
www.wr-studenten.ch, info@wr-studenten.ch.

Vorstandsmitglieder:

Amina Ouakrim, ouakrami@students.zhaw.ch.
Aurora Melo Moura, melomaur@students.zhaw.ch.
Aurelia Brand, brandaur@students.zhaw.ch
Itamar Piller, pilleita@students.zhaw.ch

Druck

RH-Marketing GmbH, Gossau SG.
Die Druckkosten wurden von Departement
Wirtschaftsrecht der ZHAW übernommen.

Design

Sina Markwalder, Zürich
marwalder.sina@gmail.com.

Artikel Masterstudierende

Die Fachartikel wurden von Masterstudierenden der
ZHAW geschrieben und sind durch die ZHAW
urheberrechtlich geschützt. Die Studierenden sowie
die ZHAW haben der Veröffentlichung in
dieser Ausgabe zugestimmt.

Bilder

Die in dieser Ausgabe abgedruckten Bilder wurden
von den Autoren selber gemacht oder zur Verfügung
gestellt. Sie sind urheberrechtlich geschützt und
dürfen weder kopiert, verändert, vervielfältigt oder in
einer anderen Weise veröffentlicht werden.

Wiedergabe von Artikeln, auch auszugsweise oder in
Ausschnitten, nur mit ausdrücklicher Genehmigung
der Redaktion.

Winterthur, 15. August 2018



Angelina Rau



Ivo Schnyder



Amina Ouakrim



Aurora Melo Moura



Itamar Piller



Aurelia Brand

