Rollenbeschreibung für die 1. Auswertungsphase

Fall A: Ausbildungsplatz in der Apotheke

Auswertungsgruppe GELB

Die Rathaus-Apotheke vergibt in jedem Jahr einen Praktikumsplatz für das Betriebspraktikum der 10. Klassen. Nach erster Begutachtung der Bewerbungsunterlagen kommen in diesem Jahr drei Schülerinnen in die engere Auswahl: **Petra, Paula und Franka**. In der Apotheke erwartet die Praktikantin eine verantwortungsvolle Arbeit, insbesondere im Umgang mit Medikamenten und mit Kunden. Ihr werdet vom Apotheker Herrn Farmazius beauftragt**,** die Internet-Aktivitäten der drei Schülerinnen unter die Lupe zu nehmen.

Welche Schülerin soll den Praktikumsplatz bekommen? Begründet eure Entscheidung für jede der drei Bewerberinnen schriftlich.

Eine mögliche Auflösung des Falles A

Petra gibt auf ihrer Community-Seite keine negativen persönlichen Daten von sich preis. Ihr Blogeintrag mit Hinweis auf die Drogenberatung kann sich positiv auf die Bewerbung auswirken; ebenso der Kauf eines Buchs über Chemieexperimente im Webshop mit dem aussagekräftigen Nick „petra“. Die anonymen Chat-Behauptungen, insbesondere über das Kiffen, könnten gegen sie ausgelegt werden.

Paula kommt für den Praktikumsplatz gar nicht in Frage. Sie hat mehrmals mit dem Nickname „rockerbraut“ negative Datenspuren hinterlegt. Die Verbindung von Paula zum Nick „rockerbraut“ lässt sich über ihre Community-Seite herstellen. Insbesondere das Anbieten von Drogen im Chat und der Blog über Drogen disqualifizieren sie. Außerdem hat sie im Webshop Cannabis-Pflanzen gekauft.

Bei **Franka** ist die Entscheidung zunächst nicht einfach. Auf der Community-Seite wirken sich das Lieblingsfach Chemie und der Berufswunsch Apothekerin positiv für ihre Bewerbung aus. Zwar ist sie im Multimediabereich auf dem Video von der „Kifferparty“ nicht zu sehen, doch das Video wurde mit dem Nick „frankamaus“ hochgeladen. Mit dem gleichen Nick wurden im Webshop Nahrungsergänzungsmittel bestellt. Die Apotheke lehnt die Bewerbung ab.

Fazit

Viele Unternehmen recherchieren über ihre Bewerber im Internet. Es gibt Firmen, die sich einen Account bei den gängigen sozialen Netzwerken, z. B. SchülerVZ anzulegen, um sich auch dort Informationen über die möglichen Auszubildenden / Praktikanten zu suchen. In einer vom Verbraucherschutzministerium in Auftrag gegebenen dimap-Meinungsumfrage bei deutschen Arbeitgebern erklärten im Juli 2009 28 Prozent der befragten Unternehmen, dass sie bei der Auswahl von Bewerbern gezielt Informationen aus dem Internet nutzten, dabei vorwiegend aus Sozialen Netzwerkportalen. Ein Viertel

davon gab wiederum an, dass man schon einmal Bewerber aufgrund ihrer Internetpräsenz nicht zum Vorstellungstermin geladen hätte. Für 56 Prozent kann jemand aber auch genau wegen der Informationen aus dem Internet interessanter werden. [3] Nach einem Gesetzentwurf vom August 2010 zum Beschäftigtendatenschutz soll es Arbeitgebern zukünftig untersagen werden, nach Bewerbern und Mitarbeitern in sozialen Netzwerken zu recherchieren. Personalchefs dürfen im Web 2.0 nur solche Informationen lesen, die der beruflichen Präsentation dienen.[4]

Wer seine persönlichen Daten etwa bei Facebook vor Unbekannten schützen will, muss umständlich die Einstellungen suchen und ändern. Auch wenn das Profil auf „privat" gesetzt ist, kann es passieren, dass durch Sicherheitslücken Daten ausgelesen werden.

Zunächst einmal ist für die Bewerbung die Qualifikation wichtig. Die Unternehmen suchen natürlich nur Menschen, die auch in die Firma passen, sich um den Job bemühen und die Ausbildung auch wirklich haben wollen. Eigentlich geeignete Bewerber wie Franka haben Probleme, wenn sie negative Spuren im Netz hinterlassen, auch wenn sie eigentlich nichts dafür können. Der Einkauf von illegalen Nahrungsergänzungsmitteln für einen Freund oder das von der Freundin unter einem falschen Nicknamen eingestellte Video können schnell zur Ablehnung der Bewerbung führen. Durch die Anonymität des weltweiten Netzes werden Täuschung und Betrug begünstigt: Impersonation – das Annehmen einer falschen Identität – ist eine Form von Cybermobbing. Im vorliegenden Fall (Paula verwendet Frankas Nick) ist die Wirkung nicht beabsichtigt. In der Praxis kommt es vor, dass Passwörter ausgespäht oder geknackt werden, um verletzende Nachrichten an die Freunde des Opfers zu verschicken oder auch falsche oder schädigende Gerüchte über das Opfer zu verbreiten. Das besonders Tückische daran: Oft weiß der Betroffene gar nichts von seiner „zweiten Online-Existenz". Regelmäßige Selbstsuche bei Personensuchmaschinen wie z. B. www.yasni.de oder www.123people.de gehören laut Klicksafe heute zur „Onlinehygiene".[5] Weiter ist dort zu lesen: „Die Anonymität im Netz macht es zudem zunächst einmal schwerer, den Urheber zu finden, ändert aber nichts daran, dass auch im Netz das allgemeine Strafrecht gilt. Man sollte den jeweiligen Plattformbetreiber über den Rechtsverstoß unterrichten. Die erste Maßnahme sollte dann die Löschung des entsprechenden Fake-Profils sein. Es besteht außerdem die Möglichkeit einer Verleumdungsklage oder einer Unterlassungsforderung."

3 http://www.bmelv.de/SharedDocs/Downloads/Verbraucherschutz/InternetnutzungVorauswahlPersonalentscheidungen.html

4 Siehe http://www.tagesspiegel.de/politik/facebook-soll-fuer-arbeitgeber-tabu-sein/1910944.html

5 https://www.klicksafe.de/themen/aktuelles-thema/datenschutz/wie-sicher-sind-meine-daten-im-netz-5459.html

Fall B: Diebstahl eines Camcorder aus dem Auto einer Lehrerin
Auswertungsgruppe BLAU

Als die Sportlehrerin Frau Purzelbaum am Mittwoch nach der Schule zu ihrem Auto geht, ist das Auto aufgebrochen und der Camcorder auf der Rückbank gestohlen. Sie schaltet die Polizei ein. Am nächsten Tag wird diese von einem Schüler darauf aufmerksam gemacht, dass im Chat Hinweise auf den Diebstahl zu lesen sind.

Findet heraus, wer den Camcorder gestohlen hat. Begründet eure Entscheidung für jeden Verdächtigen schriftlich.

Eine mögliche Auflösung des Falles B

Aufbrechen eines Autos und Diebstahl eines Camcorder sind Strafbestände, deshalb wird im vorliegenden Fall die Staatsanwaltschaft eingeschaltet. Diese kann sich mit Richterbeschluss den Zugriff auf die entsprechenden Daten des Providers verschaffen.

Zunächst wird **Arno** verdächtigt, weil er im Chat prahlt, die Tat begangen zu haben. Außerdem hat er in der Suchmaschine nach „Polenschlüssel“ und „Camcorder“ gesucht, was sich durch die IP-Adresse nachweisen lässt. Aber es stellt sich schnell heraus, dass Arno für die Tatzeit ein Alibi hat, da er mit seinem Erdkundekurs bei einer Exkursion war.

Jan macht sich durch seine Suchanzeige nach einem Camcorder im Webhsop und durch seine Frage nach einem günstigen Camcorder im Chat verdächtig.

Der eigentliche Täter **Johannes** hat sich ein Video mit dem Titel „Polenschlüssel im Einsatz“ angeschaut. Auch das lässt sich nur durch die IP-Adresse nachweisen. Außerdem hat er im Webshop kurz nach der Tat ein teures Handy gekauft, dessen Wert ungefähr dem Wert des gestohlenen Camcorders entspricht.

Die Datenspuren im Netz liefern somit drei verdächtige Personen. Eine endgültige Auflösung des Falls geschieht erst nach Anhörung und Befragung der Verdächtigen.

Fazit

Bei Straftaten lässt sich der Anschlussinhaber eines Internetanschlusses leicht feststellen. Da bei jeder Nutzung des Internets eine IP-Adresse vergeben wird, haben die Strafverfolgungsbehörden relativ einfach die Möglichkeit, über diese Adressen, sofern sie nicht gefälscht sind, an den Anschlussinhaber heranzukommen. Dies gilt erst recht, wenn weitere Daten, wie Namen, E-Mailadressen oder Informationen über Zahlungen vorliegen. Mit Hilfe der IP-Adresse lässt sich der Provider ermitteln. Der kann zur Auskunft über die Kundendaten des Anschlussinhabers verpflichtet werden. Wenn die Staatsanwaltschaft weiteres Beweismaterial benötigt, kann es auch zu einer Hausdurchsuchung kommen.

Was ist eine IP-Adresse?

Ein Computer, der sich in einem Netzwerk befindet, wird über die so genannte IP-Adresse eindeutig identifiziert. Nach dem derzeit aktuellen Protokoll IPv4 bestehen diese IP-Adressen aus vier Zahlen, die jeweils zwischen 0 und 255 liegen und mit einem Punkt

getrennt werden, beispielsweise 146.15.255.234. Da der Bestand dieser Adressen langsam zu Neige geht, verteilen die Internet-Provider diese Adressen aus einem ihnen gehörenden Adresspool bei jeder Einwahl neu - wenn man nicht gerade in einer größeren Firma mit Standleitung sitzt oder sich eine feste IP-Adresse gekauft hat.

Die IP-Adresse kann aus unterschiedlichen Gründen mit Fehlern behaftet sein. Die meisten IPs werden nur für 24 Stunden vergeben, eine Ermittlung des Anschlusses nach dieser Zeitspanne erfordert daher eine Speicherung der Verbindungsdaten. Dies war eigentlich durch das Gesetz zur Vorratsdatenspeicherung vorgesehen, durch das Internetdienstanbieter verpflichtet werden sollten, Verbindungsdaten ihrer Vertragspartner für sechs Monate zu speichern und an Behörden herauszugeben. Am 02.03.2010 hat das Bundesverfassungsgericht jedoch entschieden, dass die Gesellschaften die Daten ihrer Kunden zwar ein halbes Jahr speichern, sie aber nur bei dem begründeten Verdacht auf schwere Straftaten an die Behörden weitergeben dürfen. „Der Bund muss dabei den Ländern klare Maßgaben machen, inwieweit die Polizei zur sogenannten Gefahrenabwehr auf Vorratsdaten zugreifen darf. Den Richtern zufolge muss der Gesetzgeber für mehr Transparenz sorgen: So müssten Betroffene in der Regel über die Auswertung ihrer Daten informiert und Verstöße dagegen sanktioniert werden.“[6]

„Weniger strenge Auflagen verlangen die Karlsruher Richter an die Nutzung von IP-Adressen in Form von behördlichen Auskunftsansprüchen gegenüber Diensteanbietern. Hier sei zum einen bedeutend, dass dabei die zuständigen Ämter die vorsorglich zu speichernden Daten nicht kennen. Vielmehr gehe es nur um "personenbezogene Auskünfte" über den Inhaber eines bestimmten Anschlusses, der von Providern unter Rückgriff auf diese Daten ermittelt worden sei. Für solche Auskünfte sei kein Richtervorbehalt nötig, allerdings seien die Betreffenden von der Abfrage zu benachrichtigen. Die Anonymität im Internet dürfe nur aufgehoben werden, wenn zumindest eine Rechtsgutbeeinträchtigung vorliegt, der "ein hervorgehobenes Gewicht beigemessen wird". Das könnten auch "im Einzelfall besonders gewichtige Ordnungswidrigkeiten" sein, die der Gesetzgeber ausdrücklich benennen müsse.“[7] Im vorliegen Fall des Diebstahls liegt eine solche Ordnungswidrigkeit vor.

Eine endgültige gesetzliche Klärung der Vorratsdatenspeicherung steht noch aus.

6 http://www.focus.de/digital/internet/bundesverfassungsgericht-karlsruhe-kippt-vorratsdatenspeicherung_aid_485730.html

7 http://www.heise.de/newsticker/meldung/Bundesverfassungsgericht-legt-Huerde-fuer-kuenftige-Vorratsdatenspeicherung-hoch-944021.html

Fall C: Cybermobbing gegen einen Lehrer

Auswertungsgruppe BLAU

Als der Mathematiklehrer Herr Logariti seinen Rechner anschaltet, traut er seinen Augen nicht. Jemand hat ihm eine „anonyme“ E-Mail gesendet. Aus der E-Mail erfährt Herr Logariti, dass er im Blog des Schülers Lukas massivst beleidigt und bedroht wird. Den anonymen Blog-Kommentar kann Herr Logariti lesen: „Ich hasse Herrn Logariti. Ich könnte ihn auf der Stelle aufschlitze, diese Fehlgeburt.“[8]

Am nächsten Tag wendet sich Herr Logariti an die Schulleitung. Der Schulleiter besteht darauf, die Polizei einzuschalten. Ihr seid Ermittler der Polizei. Findet heraus, wer die Bedrohung verfasst hat.

Eine mögliche Auflösung des Falles C

Beleidigungen und Bedrohungen sind Straftaten gegen die persönliche Freiheit, deshalb wird im vorliegenden Fall die Staatsanwaltschaft eingeschaltet.
Nach § 241 des Strafgesetzbuches gilt

(1) Wer einen Menschen mit der Begehung eines gegen ihn oder eine ihm nahestehende Person gerichteten Verbrechens bedroht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer wider besseres Wissen einem Menschen vortäuscht, dass die Verwirklichung eines gegen ihn oder eine ihm nahestehende Person gerichteten Verbrechens bevorstehe.

Die Staatanwaltschaft hat somit Zugriff auf alle Daten (vgl. Fall 2).

Zunächst versuchen die Ermittler vermutlich herauszufinden, wer den Blog-Kommentar verfasst hat. Der Blog wurde von „luci77“ angelegt, über die IP-Adresse lässt sich **Lukas** zuordnen. Den Kommentar hat „lehrerhasser“ geschrieben, die zugehörige IP-Adresse gehört zu **Tilo**. Dieser hat Mathematik als Hassfach angegeben und eine Gruppe „Wir hassen Mathe“ gegründet.

Vermutlich fällt den Ermittlern aber auch Leons Eintrag im Community-Bereich auf. Zwar hat **Leon** seine Policy-Einstellungen auf „privat“ gestellt, trotzdem bekommt die Staatsanwaltschaft im vorliegenden Fall Zugriff auf die Daten. Herr Logariti wird dort als „arrogantes A…“ bezeichnet. Außerdem liest man den Eintrag „Den würde ich am liebsten abschlachten und ausnehmen wie einen Fisch“. Dass diese Eintragungen von Tilo stammen, der Leons Passwort ausgespäht hat, wissen die Ermittler nicht.

Die anderen Aktivitäten von Leon (Verkauf eines Taschenmessers im Webshop, Suche nach „große Taschenmesser Fische ausnehmen“ und Anschauen eines Films „Fische richtig ausnehmen“) könnten den Verdacht erhärten.

Wenn die Ermittler Tilos E-Mail-Verkehr kontrollieren, fällt ihnen eine E-Mail in die Hände, die den Fall aufklärt. Tilo hat in einer E-Mail an seinen Freund Lukas geschrieben, dass er

8 Quelle: http://www.rp-online.de/duesseldorf/duesseldorf-stadt/nachrichten/Schuelerin-beleidigt-Lehrer-im-Netz_aid_724767.html

Leons Community-Passwort ausspioniert hat. Damit kommt Tilo als Verfasser der Drohungen auf Leons Seite in Frage.

Erst eine Befragung der beiden Verdächtigen kann den Fall aufklären. Dabei wird Leon die Eintragungen in seinem Community-Bereich abstreiten, da er sie nicht verfasst hat.

Fazit

Ein Gesetz, das speziell bei Cybermobbing bzw. Cyberbullying in Kraft tritt, gibt es in Deutschland derzeit nicht. Jedoch existieren bereits verschiedene Gesetze des Strafgesetzbuches (StGB), die bei Cybermobbing wirksam sein können. Werden online in Foren, Netzwerken und Blogs Beleidigungen (§ 185 StGB), üble Nachrede (§ 186 StGB), Verleumdungen (§ 187 StGB) oder gar Bedrohungen (§ 241 StGB) über eine Person verbreitet, kann Unterlassungsanspruch geltend gemacht und Strafanzeige erstattet werden. Findet das Mobbing nicht öffentlich, sondern über private E-Mails, Instant Messenger oder SMS auf ein Handy statt, tritt möglicherweise das Anti-Stalking-Gesetz (§ 238 StGB Nachstellung) in Kraft und man kann gegen den Täter auch rechtlich vorgehen.

Das Gesetz sieht bei Beleidigungen als Höchststrafe ein Jahr Freiheitsentzug oder eine Geldstrafe vor. Da der Täter im vorliegenden Fall noch minderjährig ist, wird das mildere Jugendrecht angewendet.

Der Fall basiert auf einen realen Fall aus Nordrhein-Westfalen (siehe Quelle in der Rollenbeschreibung oben) Die Schülerin wurde als Reaktion auf ihre Taten von der Schule verwiesen und wegen Verstoßes gegen den Verhaltenskodex von „SchülerVZ“ ausgeschlossen. Ihre Schmäh-Beiträge im Internet wurden selbstverständlich gelöscht.

Tilo hat Leons Passwort für den Community-Treff ausspioniert und verwendet es, um mit Leons Namen Bedrohungen über Herrn Logariti zu verfassen. In § 202a und § 202c des Strafgesetzbuches steht dazu:

§ 202a Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Fall D: Cybermobbing gegen eine Schülerin

Auswertungsgruppe GELB

Die Schülerin Marta findet im Multimediabereich ein Video aus dem Sportunterricht ihrer Klasse. In diesem Video sieht man, wie sie sich beim Volleyball ungeschickt bewegt und mehrmals von ihren Mitspielern und der Sportlehrerin Frau Purzelbaum scharf kritisiert wird. Am Ende des Videos weint Marta. Frau Purzelbaum kommentiert: „Erst nicht die Bälle treffen und dann noch heulen, so etwas habe ich gerne! Sieh mal zu, dass du dein Make-Up wieder hinbekommst."

Marta vermutet, dass ihr Ex-Freund Alex das Video erstellt hat. Sie ist seelisch am Boden und wendet sich an ihre Eltern. Diese gehen zusammen mit Marta am nächsten Tag zur Schulleitung. Die Schulleitung nimmt den Vorfall sehr ernst. Ihr seid Konfliktlotsen der Schule und werdet um Hilfe gebeten.

Findet heraus, wer das Video erstellt und hochgeladen hat. Was soll passieren, wenn ihr den „Täter" gefunden habt?

Auflösung

Die Schülerin **Mart**a wird durch ein Video im Internet bloßgestellt. Das Video wurde mit dem „anonymen" Nickname „zicke" hochgeladen, so dass der „Täter" nicht offensichtlich ist. Im Chat wird **Alex** von **Frida** gelobt, das Video erstellt zu haben. Alex ist der Ex-Freund von Marta. Auf dessen öffentlicher Seite im Community-Bereich ist ein Link auf das Video zu finden. Außerdem können die Mitschüler bezeugen, dass Alex in der Sportstunde gefilmt hat. Somit ist Alex verdächtig.

Mit dem Nickname „zicke" wurde im Webshop ein- und verkauft. Da die Ermittler auch Zugriff auf Sender, Empfänger und Text von E-Mails haben, stellen Sie fest, dass es eine Nachricht vom Sender „zicke" an Alex mit einem Hinweis auf das Video gibt. Das kann bedeuten, dass Alex erst durch die E-Mail von der Existenz des Videos erfahren hat. Dann kann er aber nicht der „Täter" sein. Falls Frida ihre Community-Seite nicht auf privat gestellt hat, wird sie eventuell verdächtigt, weil sie sich selbst als „Zicke" bezeichnet.

Eine endgültige Aufklärung ist nur nach Befragung der Beteiligten möglich. Frida hat das Video erstellt und hochgeladen. Sie muss es sofort aus dem Multimediabereich entfernen. Weitere „pädagogische" Maßnahmen sind abhängig vom Fall innerhalb der Schule zu ergreifen, z. B. Entschuldigungen, Wiedergutmachungen, Thematisierung von Cybermobbing im Unterricht usw.

Wird der Täter nicht gefunden, können im vorliegenden Fall rechtliche Maßnahmen ergriffen werden. Werden nämlich Bilder oder Videos ohne Zustimmung des Betroffenen veröffentlicht, wird das Persönlichkeitsrecht verletzt. Zunächst einmal sollte man den Vorfall beim Betreiber des Multimedia-Bereichs melden und diesen auffordern, das Video zu löschen. Da der Betreiber aber nicht veranlasst werden kann, die Benutzerdaten herauszugeben, ist eine endgültige Aufklärung nur durch die Staatsanwaltschaft über die IP-Adressen möglich (vgl. Fall 2 und 3).

Fazit

Unter Cybermobbing (bzw. Cyberbullying) versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe moderner Kommunikationsmittel – meist über einen längeren Zeitraum. Oft handelt der Täter anonym, so dass das Opfer nicht weiß, von wem die Angriffe stammen. Cybermobbing geht meistens von Personen aus dem Umfeld des Opfers aus.

Im vorliegende Fall wird eine Schülerin durch ein Video im Internet bloßgestellt. Der „Fall" sollte möglichst innerhalb der Schulgemeinschaft geklärt werden. Die Entscheidung, die Schulleitung einzubeziehen, ist richtig. Ein gutes Vertrauensverhältnis zwischen Eltern und ihren Kindern, aber auch zwischen Lehrern und Schülern trägt dazu bei, dass sich „Opfer" schneller an Erwachsene wenden.

Cybermobbing wird zwar gesetzlich nicht direkt bestraft. Es gibt aber Möglichkeiten, rechtliche Maßnahmen zu ergreifen (vgl. Fall 3). Werden Bilder oder Videos ohne Zustimmung veröffentlicht, wird das Persönlichkeitsrecht des Betroffenen verletzt (hier das Recht am eigenen Bild).

Ein Anti-Cyberbullying-Gesetz wäre für die Opfer sicherlich von Vorteil, ist aber letztlich nur eine Symptom-Behandlung. Effektiver können Präventionsmaßnahmen und schnelles Handeln bei konkreten Fällen sein. Wie solche Maßnahmen aussehen können, weitere Sachinformationen und Unterrichtsmaterialen zum Thema Cybermobbing hat die Initiative „klicksafe" (www.klicksafe.de) im Internet veröffentlicht. Klicksafe ist ein Projekt im Rahmen des „Safer Internet Programms" der Europäischen Union.