

Risikofaktoren der Onlinekriminalität

Bernd-Dieter Meier

Gliederung

- | | |
|--|---|
| 1. Ausgangslage: Offene Fragen in der Kriminologie | 2.2 Fragebogen |
| 2. Ergebnisse einer Befragung zur Online-Alltagskriminalität | 2.3 Ergebnisse |
| 2.1 Anlage der Untersuchung | 3. Bedeutung für die Erklärung der Onlinekriminalität |

1. Ausgangslage: Offene Fragen in der Kriminologie

„Technology changes everything – crime included.“¹ Es ist schon mehr als zehn Jahre her, dass der britisch-amerikanische Kriminologe und diesjährige Gewinner des Stockholm Prize in Criminology *Ronald Clarke* auf den Zusammenhang von technologischer Entwicklung, Veränderungen in der Kriminalitätsstruktur, neuen Möglichkeiten der Kriminalitätskontrolle und den sich hieraus ergebenden Herausforderungen für die Kriminologie aufmerksam machte. Besondere Herausforderungen gehen ersichtlich von der Digitalisierung aus, die weltweit die Speicherung von Informationen und die gesellschaftliche Kommunikation vereinfacht, beschleunigt und verändert hat. Neue Kriminalitätsformen sind mit der Digitalisierung entstanden, wobei hier pars pro toto nur drei neuartige Phänomene genannt seien: der „Diebstahl“ von digitalen Identitäten, das gezielte Überlasten von Systemen durch systematisch geführte DDoS-Attacken und die Verbreitung von kinderpornographischem Material, mit dem nicht nur krude Bedürfnisse befriedigt, sondern vor allem auch die Allgemeinen Persönlichkeitsrechte der abgebildeten Kinder und Jugendlichen auf Dauer belastet werden. Ebenfalls entstanden sind neue Formen der Kriminalitätskontrolle, wobei auch insoweit nur drei Beispiele genannt seien: der Ausbau der Überwachung, die heute sämtliche Bereiche der internetbasierten Kommunikation erfasst, die Speicherung von Massendaten, die von staatlichen und privaten Stellen für eine

1 *Clarke* (2004), S. 55.

spätere Auswertung aufbewahrt werden, und die elektronische Aufenthaltsüberwachung, die sich als neue Kontrollmöglichkeit im System der strafrechtlichen Sanktionen etabliert hat. Und in der Kriminologie?

Auch in der Kriminologie hat die Digitalisierung zu Veränderungen geführt. Genannt seien etwa die deutlich verbesserten Möglichkeiten zur statistischen Auswertung von Daten, die Veränderungen bei den Methoden, wobei hier nur auf die Möglichkeit der Onlinebefragung hinzuweisen ist, sowie die schnellere und verlässlichere Distribution von Wissen in der Form von Datenbanken, Bücherbeständen und Zeitschriftenbibliotheken. Die Veränderungen in der Kriminologie indes betreffen vor allem das Handwerkszeug des Fachs, die „tools of the trade“; sie machen kriminologische Forschung effizienter und vielleicht auch effektiver. Die Veränderungen haben demgegenüber nicht – oder jedenfalls nicht in der Breite – zum Aufkommen neuer Forschungsfragen geführt, was bei einem Wandel, der wie die Digitalisierung sämtliche Bereiche der gesellschaftlichen Lebens durchzieht, überrascht. Wie und warum verändert die Digitalisierung, verändert das Internet die Bereitschaft zur Begehung von Straftaten? Inwieweit erhöht sich die Gefahr der Viktimisierung? Sind die Strukturen bei der Onlinekriminalität dieselben wie bei der Offlinekriminalität? Dominieren also auch im Internet die einfachen Delikte mit geringen Schäden? Dominieren auch im Internet die Taten der Männer, der Jugendlichen, der Gelegenheitstäter? Welche Risiko- und welche Schutzfaktoren gibt es? Sind die theoretischen Erklärungsansätze auf die Onlinekriminalität übertragbar? Oder bedarf es einer eigenen „Cyberkriminologie“, die die Onlinekriminalität erklärt? Zu allen diesen Fragen gibt es nach wie vor keine befriedigenden Antworten, und wenn man die Themen Revue passieren lässt, die auf der diesjährigen Tagung der Kriminologischen Gesellschaft behandelt werden, scheint auch das Interesse der „community“ an diesen Fragen nur erstaunlich gering zu sein.

Die Defizite können hier nicht aufgearbeitet werden. Im Folgenden kann aber über die Ergebnisse einer kleinen Befragung berichtet werden, die in Hannover zu den Besonderheiten der Onlinekriminalität durchgeführt wurde.

2. Ergebnisse einer Befragung zur Online-Alltagskriminalität

2.1 Anlage der Untersuchung

Ziel der Befragung war es, einen Überblick zu gewinnen über die Umstände, die die Begehung von Straftaten im Internet wahrscheinlicher machen. Im Mittelpunkt stand die Alltagskriminalität, konkret: der illegale Download, der im Nebenstrafrecht (§ 106 UrhG) mit Geldstrafe oder Freiheitsstrafe bis zu drei Jahren bedroht wird und über den in der Kriminologie nur wenig bekannt ist. Schätzungen gehen von einem erheblichen Dunkelfeld aus; die §§ 106 ff. UrhG wurden einmal als diejenigen Strafnormen bezeichnet, die in Deutschland am häufigsten verletzt werden.² Die Zahlen dürften indes in den letzten Jahren deutlich zurückgegangen sein, zum einen weil die Industrie inzwischen zahlreiche neue Möglichkeiten für die kostengünstige legale Nutzung entwickelt hat, zum anderen weil sich in der Rechtswissenschaft zunehmend die Ansicht durchgesetzt hat, dass die Nutzung von Streaming-Portalen anders als die Nutzung von filesharing-Systemen nicht von den §§ 106 ff. UrhG erfasst wird.³ Das Hellfeld der Urheberrechtsdelikte ist demgegenüber klein; im Jahr 2014 wurden von der Polizei nur ca. 3.000 Fälle wegen Urheberrechtsverstößen bearbeitet.⁴ Und es gibt nur wenige empirische Untersuchungen zu dem Thema, die auf den Einfluss von Selbstkontrolle, persönlicher Moral und Furcht vor Strafverfolgung hinweisen.⁵ In lockerer Anlehnung an den Routine Activity Approach ging die eigene Untersuchung vor diesem Hintergrund davon aus, dass der illegale Download eine Folge von Kompetenz und fehlender Kontrolle ist: Strafbare Urheberrechtsverletzungen, so wurde vermutet, werden vor allem dann begangen, wenn bei den Tätern eine gewisse technisch-instrumentelle Kompetenz und die Bereitschaft zur Nutzung des Internet in Grenzbereichen mit schwachen Ausprägungen von Selbstkontrolle und geringer Furcht vor Strafverfolgung einhergehen.

Die Befragung wurde als Onlinebefragung von September bis Dezember 2014 durchgeführt. Der Zugang zur Befragung war nicht eingeschränkt; jeder Interessierte konnte teilnehmen. Mit unterschiedlichen Medien (Face-

2 Schäufele (2012), S. 302.

3 Vertiefend Reinbacher (2014), S. 61 f.

4 PKS (2014), Tab. 01 (Schlüssel 715050, 715100 und 715200).

5 Moon/McCluskey/McCluskey (2010); Wingrove/Korpas/Weisz (2011); Aaltonen/Salmi (2013).

book, Handzetteln mit QR-Code, Vorlesungen, Unterricht) besonders angesprochen wurden Jurastudierende im ersten Semester sowie etwa gleichaltrige Berufsschüler. Der Untersuchung liegt damit eine nicht-repräsentative Gelegenheitsstichprobe (convenience sample) zugrunde; die Ergebnisse können nicht verallgemeinert werden, sondern haben nur Indizwirkung. Insgesamt beteiligten sich an der Untersuchung mit vollständig ausgefüllten Fragebögen 583 Personen.⁶

2.2 Fragebogen

Der illegale Download wurde mit folgender Frage erfasst: „Haben Sie schon einmal ohne hierfür zu bezahlen im Internet (z. B. in Tauschbörsen) Musiktitel, Fotos, Filme oder andere urheberrechtlich geschützte Werke heruntergeladen (kein Streaming), obwohl Sie wussten, dass dies verboten war?“ Die Frage ist komplex formuliert und vielleicht auch nicht für jeden sofort verständlich. Dies war indes erforderlich, um die schwierige Rechtslage angemessen abzubilden; es ging nicht um eine Untersuchung zum Freizeitverhalten, sondern zur Überschreitung rechtlicher Grenzen. In den Antwortkategorien wurde die Frage zeitlich präzisiert: Ja, aber das liegt länger zurück – ja, einmal innerhalb des letzten Monats – ja, mehrfach innerhalb des letzten Monats. Insgesamt gab mehr als die Hälfte der Befragten an (56 %), schon einmal eine Straftat nach § 106 UrhG begangen zu haben.

Breiten Raum nahmen in dem Fragebogen die Aktivitäten im Netz und die Dauer der Internetnutzung ein. Jedenfalls die Onlineaktivitäten interessierten dabei weniger, weil hierüber schon aus den ARD/ZDF-Onlinestudien viel bekannt ist;⁷ die Fragen wurden lediglich deshalb aufgenommen, weil in den Werbematerialien allgemein gesagt worden war, es gehe um das „Nutzungsverhalten im Internet“. Um der Heterogenität der Stichprobe Rechnung zu tragen, wurde in den entsprechenden Fragen deutlich gemacht, dass es allein um die Nutzung des Internet „für private Zwecke“ gehe.

Neben der Nutzungsdauer wurde auch nach der Nutzungskompetenz gefragt. Grundsätzlich ist der illegale Download zwar kein Delikt, das dem Nutzer ein besonderes technisches Verständnis abverlangt; wenn es aber um die Frage geht, ob auf breiter gefächerte illegale Angebote zugegriffen werden kann, ob technische Schutzmaßnahmen überwunden und Maßnahmen gegen

⁶ Ausführliche Darstellung der Ergebnisse bei *Meier* (2015).

⁷ *Eimeren/Frees* (2014); zur Verteilung der Onlineaktivitäten in der eigenen Stichprobe genauer *Meier* (2015a), S. 105 f.

die Nachverfolgung und Rechtsdurchsetzung ergriffen werden können, ist eine gewisse technisch-instrumentelle Handlungskompetenz vonnöten. Erfasst wurden diese Kompetenzen mit Fragen nach Programmierkenntnissen und dem aktuellen oder schon einmal erprobten Einsatz von Anonymisierungssoftware oder anderen Verschleierungsformen, um die Datenspuren im Netz zu verwischen.

Von Interesse ist allerdings nicht nur die technisch-instrumentellen Nutzungskompetenz. Von Interesse ist auch, *wie* die Möglichkeiten des Netzes genutzt werden, ob sich die Nutzung also auf die rechtmäßigen und unproblematischen Bereiche des Netzes bezieht („chatten, shoppen, facebooken“) oder ob die „dunkleren Seiten“ mit einbezogen werden, die mit Grenzverletzungen verbunden sind. In der Literatur wird in diesem Zusammenhang gelegentlich von „Internetdissozialität“ gesprochen,⁸ was Assoziationen an dissoziales bzw. antisoziales Verhalten im Offline-Bereich weckt. Da das Konzept der „Internetdissozialität“ aber noch nicht ausgereift erscheint und insbesondere seine Operationalisierung Schwierigkeiten bereitet, sollte in der eigenen Untersuchung eher von „Bereitschaft zur Nutzung im Grenzbereich des moralisch Anstößigen und Unerlaubten“ gesprochen werden, worunter illegale Handlungen wie Mobbing, Identitätsdiebstahl und die Nutzung von Kinderpornografie, aber auch legale Handlungen wie der Besuch von Internetseiten mit links- oder rechtsextremistischer Hetzpropaganda oder der Konsum von Gräuelfideos wie der Folterung oder Hinrichtung von Menschen verstanden wurden.

Für die Erklärung der Internetkriminalität wird in der Literatur gerne auf den Routine Activity Approach verwiesen; das Internet sei ein typischer Gelegenheitsraum.⁹ Mit seinen drei „almost always“-Elementen offender, target und absence of capable guardian¹⁰ beschreibt der Routine Activity Approach, welche Situationen sich für Straftaten eignen, also eine Tatgelegenheit bieten (opportunity). *Ob* es zu einer Straftat kommt, richtet sich dabei nach der Entscheidung des (potentiellen) Täters. Damit ist allerdings noch nicht gesagt, *warum* der (potentielle) Täter die Entscheidung zur Begehung einer Straftat trifft; er kann die Tatgelegenheit ja auch ungenutzt verstreichen lassen und sich rechtstreu verhalten. Der Routine Activity Approach bietet deshalb auch im Zusammenhang mit der Internetkriminalität nur einen Erklärungsrahmen, noch keine vollständige Erklärung für die Begehung von

8 Katzer/Fetchenhauer/Belschak (2009), S. 36 f.

9 Reyns (2013).

10 Cohen/Felson (1979), S. 589 ff.; Felson/Boba (2010), S. 28.

Straftaten. Soweit es um die Erklärung des Täterhandelns geht, müssen zusätzliche Aspekte hinzutreten.

Als einer dieser erklärenden Umstände kommt nach den bislang zum illegalen Download durchgeführten Untersuchungen jedenfalls die Selbstkontrolle in Betracht, also die Fähigkeit, sein Handeln nicht an der kurzfristigen Bedürfnisbefriedigung, sondern an den langfristigen Interessen auszurichten.¹¹ In der Untersuchung wurde die Selbstkontrolle über ein Modul aus 12 Items erhoben, in dem sich unterschiedliche Dimensionen des Konstrukts ausdrückten. Die Fähigkeit der Befragten zur Selbstkontrolle kann danach durch einen Punktwert zwischen 1 und 4 ausgedrückt werden, wobei 1 für eine geringe und 4 für eine hohe Selbstkontrolle steht.

Allein mit der Selbstkontrolle kann indes – entgegen den Annahmen von *Gottfredson* und *Hirschi* – normabweichendes Verhalten nicht abschließend erklärt werden, denn um die Fähigkeit zur Selbstkontrolle zu aktivieren, besteht nur dann Anlass, wenn der potentielle Täter über die Folgen seines Handelns reflektiert und die kurzfristige Bedürfnisbefriedigung gegen seine langfristigen Interessen abwägt. Benötigt wird mit anderen Worten ein Impuls, auf den der potentielle Täter reagieren kann, indem er die Tat entsprechend seiner Fähigkeit zur Selbstkontrolle begeht oder unterlässt. Dabei muss sich dieser Impuls auf die Rechtswidrigkeit des möglichen Handelns beziehen, da sich Straftaten von anderen, „analogen“ Formen kurzfristiger Bedürfnisbefriedigung wie Rauchen oder Alkoholgenuss¹² gerade hierin unterscheiden. Anders als in manchen Untersuchungen zur Situational Action Theory und auch in Abweichung zu dem im Zusammenhang mit der Selbstkontrolle verwendeten Messinstrument wurde das Unrechtsbewusstsein in der eigenen Untersuchung nicht mit einem Index individueller Moralität,¹³ sondern mit einer weit gespreizten Skala zur Bewertung des Unrechtsgehalts der Tat gemessen: „Unabhängig davon, ob Sie so etwa schon einmal gemacht haben: Wie schwer wiegt aus Ihrer Sicht das Unrecht eines solchen Verhaltens (illegaler Download)? Ordnen Sie dem Verhalten bitte eine Zahl zwischen 0 und 100 zu (zum Vergleich: Mord = 100).“ Die Skala hatte sich schon in früheren Untersuchungen bewährt.¹⁴

Neben dem Unrechtsbewusstsein und der Selbstkontrolle können bei der Internetkriminalität auch die Mechanismen der äußeren, externalen Kontrolle

11 *Moon/McCluskey/McCluskey* (2010); *Aaltonen/Salmi* (2013).

12 Beispiele von *Gottfredson/Hirschi* (1990), S. 91.

13 Vgl. etwa *Hirtenlehner* (2015), S. 264.

14 *Meier* (2010), S. 178 ff.

handlungsleitend sein. In früheren Untersuchungen zum illegalen Download hat sich gezeigt, dass die Abschreckung, definiert als Furcht vor Strafverfolgung oder persönlichen Kosten, ein wesentliches Merkmal ist,¹⁵ und auch in der erwähnten Situational Action Theory spielt die Abschreckung eine wichtige Rolle.¹⁶ Objektiv ist das Strafverfolgungsrisiko bei illegalem Download wie gezeigt nur gering, allerdings kommt es hierauf für die Abschreckungswirkung nicht an; abschreckend kann nur die eigene Risikoeinschätzung wirken. Erhoben wurde die Einschätzung zum Verfolgungsrisiko wiederum auf einer breit gespreizten Hunderterskala, bei der lediglich vorgegeben wurde „0 = kein Risiko“ und „100 = jede Straftat wird von der Polizei entdeckt und verfolgt“. Dabei wurde unterschieden zwischen dem Auftreten im Netz unter dem richtigen Namen und dem Auftreten unter einem Pseudonym.

Zusätzlich hatte sich in einer früheren finnischen Untersuchung zum illegalen Download durch Jugendliche auch ein Einfluss sozialer Kontrollmechanismen, konkret: der Kontrolle durch die Eltern gezeigt,¹⁷ so dass dieser Gesichtspunkt auch in der eigenen Befragung berücksichtigt wurde. Da die Zielgruppe im Wesentlichen aus Jurastudierenden bestand, wurde allerdings nicht nach elterlicher Kontrolle gefragt, sondern danach, ob der Befragte allein oder mit anderen Personen zusammen wohnte, sowie danach, ob er verheiratet war oder in einer festen Beziehung stand. Damit wurde auch das landläufige Vorurteil aufgegriffen, dass Computerdelikte vor allem von sozial isoliert lebenden Sonderlingen („Nerds“) begangen werden, die ein hohes Interesse an naturwissenschaftlich-technischen Fragen haben, aber beziehungsunfähig sind. – Die Ausprägungen der einzelnen Variablen und die Verteilungen sind in Tab. 1 zusammengefasst.

2.3 Ergebnisse

Betrachtet man zunächst die bivariaten Beziehungen, zeigt sich, dass mit Ausnahme der sozialen Bindungen sämtliche geprüften Variablen mit dem illegalen Download in einem statistisch nachweisbaren, wenigstens auf dem 10 % - Niveau signifikanten Zusammenhang stehen (Tab. 2). Die sozialen Bindungen wirken sich auf die Straftat nicht aus; es sind keineswegs nur die „Nerds“, die das Delikt begehen. Daneben ist erwartungswidrig, dass das

15 *Wingrove/Korpas/Weisz* (2011).

16 *Wikström* (2015), S. 183 f.

17 *Aaltonen/Salmi* (2013).

Tab. 1: Variablen und deskriptive Statistik

<i>Variable</i>	<i>Skala</i>	<i>Mittelwert</i>	<i>SD</i>
<i>Illegaler Download</i>	<i>0 = nein, 1 = ja</i>	.56	.50
<i>Jugendl./Heranw.</i>	<i>0 = nein, 1 = ja</i>	.42	.49
<i>Geschlecht</i>	<i>0 = m; 1 = w</i>	.58	.49
<i>Dauer Onlinenutzung</i>	<i>1 = ≤ 2h, 2 = > 2h</i>	1.63	.48
<i>Programm.-kenntnisse</i>	<i>0 = nein, 1 = ja</i>	.16	.37
<i>Verschleierung jemals</i>	<i>0 = nein, 1 = ja</i>	.24	.43
<i>Verschleierung aktuell</i>	<i>0 = nein, 1 = ja</i>	.06	.23
<i>Grenznutzung</i>	<i>0 = nein, 1 = ja</i>	.40	.49
<i>Unrechtsbewusstsein</i>	<i>0 ... 100</i>	27.45	21.05
<i>Selbstkontrolle</i>	<i>1 = gering, ... 4 = hoch</i>	3.02	.42
<i>Alleinleben</i>	<i>0 = allein, 1 = nicht allein</i>	0.82	.39
<i>Feste Beziehung</i>	<i>0 = nein, 1 = ja</i>	.58	.49
<i>Strafverfolgungsrisiko Klarname</i>	<i>0 ... 100</i>	53.31	26.22
<i>Strafverfolgungsrisiko Pseudonym</i>	<i>0 ... 100</i>	33.47	24.99

SD = Standardabweichung

Delikt häufiger von Erwachsenen (59,3 %) als von Jugendlichen oder Heranwachsenden (51,3 %) begangen wird; der illegale Download ist augenscheinlich kein typisches Jugenddelikt. Da sich die angegebenen Werte auf die Lebenszeitprävalenz beziehen, ist allerdings nicht auszuschließen, dass sich in den Werten auch ausdrückt, dass es heute mehr kostengünstige und legale Nutzungsangebote gibt als in früheren Zeiten.

Die weiteren bivariaten Beziehungen entsprechen den Erwartungen. Der illegale Download wird hochsignifikant häufiger von Männern als von Frauen begangen, und er wird hochsignifikant häufiger von Personen begangen, die täglich durchschnittlich länger als 2 Stunden mit privaten Aktivitäten im In-

ternet unterwegs sind, als von Personen, die das Netz weniger intensiv nutzen. Zusammenhänge lassen sich auch herstellen mit der Nutzungskompetenz: Unabhängig davon, ob auf Programmierkenntnisse oder den Einsatz von Verschleierungsmaßnahmen abgestellt wird, wird das Delikt häufiger von Personen mit einer hohen Fachkompetenz begangen als von Personen mit einer eher geringen Kompetenz. Die Tätergruppe hat das Internet darüber hinaus hochsignifikant häufiger schon einmal im Grenzbereich des moralisch Anstößigen und Unerlaubten genutzt als die Gruppe der Nichttäter, d. h. sie haben sich schon einmal in den „dunkleren“ Bereichen des Internet bewegt und das Netz für Delikte wie Mobbing, Identitätsdiebstahl oder die Nutzung von Kinderpornografie genutzt. Die Täter sind als aktive und technisch versierte Nutzer auch in den abgründigen Bereichen des Netzes unterwegs.

Das Unrechtsbewusstsein im Hinblick auf den illegalen Download war bei allen Befragten nur gering. Im Durchschnitt vergaben die Befragten auf der Hunderterskala für den illegalen Download einen Unrechtswert von 27,45 Punkten (Tab. 1), was deutlich unterhalb der Werte für Handlungen wie Cybermobbing (55,9), den Einsatz von Schadprogrammen zum Zweck des Identitätsdiebstahls (59,3), das Betrachten von Bildern von der Hinrichtung eines Menschen (64,2) oder gar das Betrachten kinderpornografischen Materials lag (80,1). Unabhängig von dem geringen Ausgangswert zeigte sich dann aber, dass das Unrechtsbewusstsein der Tätergruppe im Hinblick auf den illegalen Download hochsignifikant geringer war als das der Nichttäter; die Tätergruppe ordnete das Unrecht als deutlich weniger gravierend ein (23,15 gegenüber 33,05 Punkten). Ebenfalls verfügten sie – ganz in Übereinstimmung mit den Thesen von *Gottfredson* und *Hirschi* – über eine hochsignifikant geringere Selbstkontrolle als die Nichttäter. Und auch das Strafverfolgungsrisiko schätzten sie signifikant geringer ein als die Nichttäter, und zwar unabhängig davon, ob sie sich im Netz mit ihrem Klarnamen oder unter einem Pseudonym bewegen. Nach den bivariaten Analysen lassen sich die Täter mithin als technisch versierte Nutzer kennzeichnen, die beim illegalen Download nur über ein geringes Unrechtsbewusstsein verfügen und sich in ihrem Handeln weder durch Selbststeuerung noch durch Furcht vor Strafverfolgung abhalten lassen.

Tab. 2: Bivariate Beziehungen (Prozentangaben bzw. Mittelwerte)

	Illegaler Download		Sign.
Jugendl./Heranw. (n/j)	59.4	51.3	†
Geschlecht (m/w)	67.2	47.8	***
Dauer Onlinenutzung (\leq / $>$ 2 h)	45.4	62.5	***
Programmierkenntnisse (n/j)	53.4	68.2	*
Verschleierung jemals (n/j)	52.2	71.3	***
Verschleierung aktuell (n/j)	54.7	73.3	†
Grenznutzung (n/j)	47.1	69.2	***
Unrechtsbewusstsein (Mittelwerte bei illeg. Download n/j)	33.05	23.15	***
Selbstkontrolle (Mittelwerte bei illegalem Download n/j)	3.12	2.95	***
Alleinleben (allein / nicht allein)	53.9	56.5	n.s.
Feste Beziehung (n/j)	55.6	55.5	n.s.
Strafverfolgungsrisiko Klarname (Mittelwerte bei Download n/j)	56.98	49.42	**
Strafverfolgungsrisiko Pseudonym (Mittelw. Download n/j)	36.07	31.23	*

† $p < .10$; * $p < .05$; ** $p < .01$; *** $p < .001$; n.s. = nicht signifikant

Nun liegt es auf der Hand, dass die Frage nach den Risikofaktoren mit bivariaten Analysen nicht abschließend zu klären ist; erforderlich sind multivariate Analysen, bei denen der Einfluss sämtlicher geprüften Variablen gleichzeitig untersucht wird. Zu diesem Zweck wurde eine binäre logistische Regression gerechnet, in die die dargestellten Variablen mit Ausnahme der Angaben zur sozialen Kontrolle aufgenommen wurden; letztere blieben deshalb unberücksichtigt, weil sie sich in den bivariaten Analysen nicht als aussagekräftig erwiesen hatten. Die Ergebnisse der logistischen Regression sind in Tab. 3 zusammengefasst.

Danach sind es nur drei Variablen, die sich signifikant auf die Begehung der Straftat auswirken: die Dauer der Onlinenutzung, das Unrechtsbewusstsein und die Selbstkontrolle. Das Vorzeichen des Regressionskoeffizienten B signalisiert dabei, dass die Wirkungsrichtung in der Regressionsanalyse dieselbe ist wie bei den bivariaten Analysen. Von geringerer Bedeutung als die drei genannten Merkmale sind das Alter der Nutzer und die Bereitschaft zur Nutzung des Netzes im Grenzbereich; beide Merkmale sind nur auf dem 10 % - Niveau signifikant. Die übrigen Umstände erwiesen sich in der Regressionsanalyse als bedeutungslos: Weder das Geschlecht noch die technisch-instrumentelle Nutzungskompetenz noch die Furcht vor Strafverfolgung haben einen statistisch nachweisbaren Einfluss auf die Begehung von Urheberrechtsdelikten.

Tab. 3: Einflussfaktoren bei logistischer Regression

	B	SE	$Exp(B)$
<i>Jugendlich / Heranwachsend</i>	-.383 [†]	.205	.682
<i>Geschlecht</i>	-.253	.229	.777
<i>Dauer Onlinenutzung</i>	.527*	.211	1.694
<i>Programmierkenntnisse</i>	.120	.295	1.127
<i>Verschleierung jemals</i>	.282	.291	1.325
<i>Verschleierung aktuell</i>	.074	.501	1.077
<i>Grenznutzung</i>	.421 [†]	.219	1.523
<i>Unrechtsbewusstsein</i>	-.018***	.005	.982
<i>Selbstkontrolle</i>	-.575*	.248	.563
<i>Strafverfolgungsrisiko Klarname</i>	-.006	.006	.994
<i>Strafverfolgungsrisiko Pseudonym</i>	-.002	.006	.998
<i>Konstante</i>	2.064*	.923	7.877

Nagelkerke $R^2 = .182$; $N = 489$

B = Regressionskoeffizient; SE = Standardfehler; $Exp(B)$ = Exponential-funktion von B ;
 $p < .10$; * $p < .05$; *** $p < .001$

3. Bedeutung für die Erklärung der Onlinekriminalität

Die Ergebnisse machen deutlich, dass Onlinekriminalität, jedenfalls soweit es um Alltagskriminalität wie den illegalen Download geht, eine Folge der besonderen Gelegenheitsstruktur ist, die das Internet bietet. Die Bedienung der Geräte ist einfach, so dass eine besondere technisch-instrumentelle Kompetenz nicht erforderlich ist, um urheberrechtlich geschützte Werke herunterzuladen und damit in strafbarer Weise zu vervielfältigen. Furcht vor Strafverfolgung spielt keine Rolle, und zwar selbst dann nicht, wenn sich der Nutzer unter seinem Klarnamen im Internet bewegt; hierin drückt sich vermutlich nicht nur aus, dass die Institution der Polizei bei Onlineaktivitäten schon wegen der fehlenden physischen Wahrnehmung eines Gegenüber eher als „weit weg“ empfunden wird; vermutlich drückt sich hierin auch die Erfahrung der Netznutzer aus, dass eine polizeiliche Verfolgung bei Urheberrechtsdelikten tatsächlich kaum stattfindet. Auch die sonst in der Kriminologie bekannten Mechanismen der informellen sozialen Kontrolle wirken nicht kriminalitätshemmend, was vielleicht damit zu tun haben mag, dass der illegale Download in der Bevölkerung so weit verbreitet ist, dass auch die potentiellen informellen Kontrollinstanzen selbst (Mitbewohner, Beziehungspartner) die strafbaren Handlungen begehen; die in der Untersuchung ermittelte hohe Prävalenz von 56 % könnte hierfür einen Hinweis bieten. Letztlich sind es nach den Untersuchungsergebnissen nur drei Umstände, die den illegalen Download begünstigen und damit als Risikofaktoren strafbarer Urheberrechtsverletzungen einzuordnen sind: eine hohe zeitliche Nutzungsintensität, die sich in einer überdurchschnittlichen Dauer der Onlineaktivitäten für private Zwecke ausdrückt, ein geringes Unrechtsbewusstsein und eine geringe Selbstkontrolle. Illegaler Download ist, mit anderen Worten, Ausdruck bestimmter Routineaktivitäten im Netz und des Versagens interner Kontrollmechanismen, oder noch etwas zugespitzter formuliert: Illegaler Download ist Alltagshandeln ohne Unrechtsbewusstsein.¹⁸

Bei der Einordnung und Bewertung der Ergebnisse muss indes zweierlei beachtet werden. Zum einen ist auf das geringe Maß an aufgeklärter Varianz hinzuweisen (Nagelkerke $R^2 = .182$). Der geringe Wert deutet auf das Wirken weiterer Umstände hin, die in die Untersuchung nicht oder nur unzureichend einbezogen wurden. Das gilt insbesondere für das soziale Umfeld der (Nicht-) Täter und hier insbesondere für die Peers und ihren Einfluss auf die Entscheidung des Täters zur unerlaubten Vervielfältigung urheberrechtlich geschützter Werke. Naheliegend ist die Annahme, dass illegaler

¹⁸ Meier (2015), S. 625.

Download vor allem dann begangen wird, wenn auch die Peers strafbare Urheberrechtsverletzungen als Bestandteil ihres Alltagshandelns ansehen und die Täter hierdurch in ihrer Vorstellung bestärken, beim illegalen Download handele es sich um eine gebräuchliche und in keinerlei Hinsicht problematische Form der Netznutzung. Auch in der verschiedentlich erwähnten Situational Action Theory wird die Bedeutung der Peers als Eigenschaft des Settings thematisiert, in dem der Wahrnehmungs-Entscheidungs-Prozess des Täters abläuft.¹⁹

Zum anderen ist darauf hinzuweisen, dass sich die hier dargestellten Befunde nur auf ein einziges Delikt beziehen, den illegalen Download, und dass sie sich auf andere Delikte aus dem Bereich der Onlinekriminalität nicht zwingend verallgemeinern lassen. Deutlich machen lässt sich dies an der Variable technisch-instrumentelle Nutzungskompetenz: Der illegale Download ist ein Delikt, das in technischer Hinsicht keine Anforderungen stellt, während andere Onlinedelikte wie etwa das Ausspähen von Daten, die Datenveränderung oder die Computersabotage ohne eine gewisse Fachkompetenz nicht durchführbar sind und in Ausnahmefällen sogar auch das Zusammenwirken mehrerer Spezialisten voraussetzen können; Cybercrime kann damit sogar Bezüge zur Organisierten Kriminalität bekommen. Anders als es die hier vorgestellte Untersuchung anzudeuten scheint, sind Internetdelikte nicht per se „Jedermanndelikte“, sondern der Kreis der als Täter in Betracht kommenden Personen kann sich u. U. auf einzelne, technisch versierte Fachleute verengen.

Für sich genommen sind die hier vorgestellten Untersuchungsergebnisse deshalb eher trivial; sie bereichern das Wissen über die Onlinekriminalität nicht wirklich. Die Untersuchung mag aber Anlass geben, in der Kriminologie künftig stärker als bisher über die besonderen Bedingungen der Onlinekriminalität im Vergleich zur Offlinekriminalität zu forschen und weitere, differenziertere Untersuchungen durchzuführen. Die Kriminologie darf – und zu diesem Ergebnis kommt auch der eingangs erwähnte Beitrag von *Ronald Clarke* – den Anschluss an die technische Entwicklung und die Veränderungen in der Kriminalitätsstruktur nicht verpassen.

19 *Wikström* (2015), S. 179; *Gerstner/Oberwittler* (2015), S. 207.

Literatur

- Aaltonen, M./Salmi, V.* (2013): Versatile Delinquents or Specialized Pirates? A Comparison of Correlates of Illegal Downloading and Traditional Juvenile Crime. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 14, S. 188 - 195.
- Clarke, R.* (2004): Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research*, 10, S. 55 - 63.
- Cohen, L./Felson, M.* (1979): Social Change and Crime Rate Trends: A routine Activity Approach. *American Sociological Review*, 44, S. 588 - 608.
- Felson, M./Boba, R.* (2010): *Crime and Everyday Life*, 4. Aufl. Los Angeles u. a.: Sage.
- Gerstner, D./Oberwittler, D.* (2015): Wer kennt wen und was geht ab? *Monatsschrift für Kriminologie und Strafrechtsreform*, 98, S. 204 - 226.
- Gottfredson, M./Hirschi, T.* (1990): *A General Theory of Crime*. Stanford: Stanford UP.
- Hirtenlehner, H.* (2015): „Gelegenheit macht Diebe“ oder „Wer raucht, der stiehlt“. *Monatsschrift für Kriminologie und Strafrechtsreform*, 98, S. 257 - 279.
- Katzer, C./Fetchenhauer, D./Belschak F.* (2009): Cyberbullying in Internet-Chatrooms – Wer sind die Täter? *Zeitschrift für Entwicklungspsychologie und Pädagogische Psychologie*, 41, S. 33 - 44.
- Meier, B.-D.* (2010): „Hunde, die bellen, beißen nicht.“ Einstellungen Studierender zu Kriminalität und Strafe. In: Dölling, D./Götting, B./Meier, B.-D./Verrel, T. (Hg.): *Verbrechen – Strafe – Resozialisierung*. Festschrift für Heinz Schöch. Berlin: deGruyter, S. 167 - 182.
- Meier, B.-D.* (2015): Illegaler Download: Alltagshandeln ohne Unrechtsbewusstsein. In: Brüning, J./Rotsch, T./Schady, J. (Hg.): *Festschrift für Heribert Ostendorf*. Baden-Baden: Nomos, S. 615 - 629.
- Meier, B.-D.* (2015a): Kriminologie und Internet: ein ungeklärtes Verhältnis. In: Beck, S./Meier, B.-D./Momsen, C. (Hg.): *Cybercrime und Cyberinvestigations*. Baden-Baden: Nomos, S. 93 - 118).
- Moon, B./McCluskey, J./McCluskey, C.-P.* (2010): A General Theory of Crime and Computer Crime: An Empirical Test. *Journal of Criminal Justice*, 38, S. 767 - 772.
- Reinbacher, T.* (2014): Zur Strafbarkeit der Betreiber und Nutzer von kino.to. *Neue Zeitschrift für Strafrecht*, 34, S. 57 - 62.
- Reyns, B.* (2013): Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offences. *Journal of Research in Crime and Delinquency*, 50, S. 216 - 238.
- Schäufele, M.* (2012): *Zur Strafbarkeit des Raubkopierens im Internet. Filesharing von urheberrechtlich geschützten Werken im Internet*. Münster: Lit.
- Eimeren, B. van/Frees, B.* (2014): 79 Prozent der Deutschen online – Zuwachs bei mobiler Internetnutzung und Bewegtbild. *Media Perspektiven (7-8)*, S. 378 - 396.
- Wikström, P.-O.* (2015): Situational Action Theory. *Monatsschrift für Kriminologie und Strafrechtsreform*, 98, S. 177 - 186.
- Wingrove, T./Korpas, A./Weisz, V.* (2011): Why were millions of people not obeying the law? Motivational Influences on non-compliance with the law in the case of music piracy. *Psychology, Crime & Law*, 17, S. 261 - 276.