Die Verhältnismäßigkeit im Cyberstrafrecht*

LEE Won-Sang**

I. Einleitung

Der Cyberspace ist ein idealer Kommunikationsraum. Bei der Cyberkriminalität geht es darum, dass Delikte aus der realen Welt durch das Medium des Cyberspace begangen werden können. Dazu können Cyberpornografie, Cyberstalking, Extremistische Propaganda, Cybermobbing usw. zählen. Der Cyberspace wird auch als der Gesamtraum aller Netze bezeichnet. Hier sind die zeitlichen und räumlichen Grenzen der Realwelt nahezu bedeutungslos. Vor allem haben die Staatsgrenzen der Realwelt keine Bedeutung mehr, denn der Cyberspace ist schon weltweit vereinheitlicht. Man kann fast sagen, dass die Cyberkultur weltweit gleich ist. Zum Beispiel stellt die Kommunikation durch Social Network Service (SNS) wie Twitter oder Onlinespiele schon eine weltweit gleiche Cyberkultur dar. Aber die Kriminalität im Cyberspace entwickelt sich anders als die Cyberkultur: Kriminalität ist nämlich ein dunkles Produkt der Kultur.

Als Reaktion auf Cyber-Verbrechen verwendet Südkorea hauptsächlich Strafen. Dies liegt daran, dass die Cyberkriminalität ein großes Risiko darstellt. Allerdings ist es notwendig zu überdenken, ob Internetkriminalität immer dagewesen ist. Auch ist es notwendig, die Verwendung des Strafrechts in erster Linie auf Bedrohungen im Cyberraum zu berücksichtigen. Denn es gibt zum Beispiel ein Problem mit der automatischen Bestrafung, obwohl es mit technischen Mitteln ausreichend gehandhabt werden kann. Daher möchten wir in dieser Arbeit annehmen, ob wir ein Proportionalitätsprinzip in Bezug auf die Wahrscheinlichkeit einer Strafaktion gegen die Bedrohung durch den Cyberraum benötigen.

II. Der aktuelle Zustand der Cyberkriminalität in Korea

1. Koreanische Kriminalitätsstatistik

Die Nationale Koreanische Polizeibehörde teilt die Cyberkriminalität in Cyberterrorismus und allgemeinene Cyberverbrechen ein. Als Cyberterrorismus werden Angriffe auf Informations- und Kommunikationsnetze als solches durch den Einsatz modernster Techno-

---

* Dieser Artikel basiert auf einer neu bearbeiteten Doktorarbeit.

** Assistant Professor, College of Law, Chosun University.

logien wie Hacking und Schadsoftware definiert. Im Gegensatz dazu sind die allgemeinen Cyberverbrechen ein umfassenderer Begriff: Dazu zählen Draht- oder Spielbetrug, illegales Kopieren, der Betrieb illegaler und schädlicher Webseiten, Verleumdung, Verletzung privater Informationen, Cyberstalking, sexuelle Gewalt im Cyberraum, Erpressung und Einschüchterung. Die Statistiken über die Cyberkriminalität in Korea in den letzten fünf Jahren sind wie folgt:

	Total	
	Occurred	**Arrested**
2011	116,961	91,496
2012	108,223	84,932
2013	155,366	86,105
2014	110,109	71,950
2015	144,679	104,888

2. Die strafrechtliche Diskussion in Korea

In Korea wird ständig über die Verstärkung der Strafen gegen Cyberkriminalität diskutiert. Daraus gehen die Maßnahmen der Kriminalpolitik, die Erforderlichkeit der integrierten Gesetzgebung, die Änderung der Theorie aus. Diese Herausforderungen hängen auch mit der Entwicklung der Internet-Technologie und den daraus folgenden Veränderungen des Alltags zusammen. Denn Korea ist bereits auf dem Weg von einer Informationsgesellschaft in die allgegenwärtige Gesellschaft (ubiquitous society). Insbesondere sind die Schwerpunkte der Diskussion der Versuch des Hackings, das illegale Datensammeln von Internet-Konzernen, die Cyberbeleidigung (gelegentlich auch `flaming´ genannt) usw.

A. Der Versuch des Hackings

Das Hacking entstand als Schattenseite des Cyberraums. Das Hacking, das die Energie des Verbrechens enthält, kann als das Verbrechen bezeichnet werden: Hacking, das mit der kriminellen Absicht im Cyberspace durch die digitalisierten technischen Mitteln das Telekommunikationsnetz stört, unterbricht oder unbefugt das Computersystem oder die Daten von Dritten verletzt.

In 2011 wurde des Computersystems der Landwirtschafts-Genossenschaftsbank Nonghyup in Korea lahmgelegt. Ein Hacker hat durch einen Laptop, das am Server von Nonghyup angeschlossen war, den Befehl zur Datenlöschung erteilt.[1)] Bei den Störungen

1) Die koreanische Staatsanwaltschaft hat festgestellt, dass einige IP-Adressen im Ausland, darunter in China, für den Angriff eingesetzt wurden. Deswegen hat sie ermittelt, ob die IP-Adressen in China mit Nordkoreas Hackerangriffen auf südkoreanische Regierungsbehörden im vergangenen März und im Juli 2009 zusammenhängen. Nach dem Ergebnisse ihrer Ermittlung wird dies Hacking auf einen↗

im Computernetzwerk von Nonghyup Mitte April 2011 gingen zahlreiche Transaktionsdaten von Kunden verloren. Deswegen fasste die Nationale Koreanische Polizeibehörde einen neuen Plan für die Strafe des Versuchs von Hacking.

In Deutschland trat das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität am 11.8.2007 in Kraft. In diesem Gesetz ist es bemerkenswert, dass das bloße Hacking, d. h. das bloße Eindringen in ein Computersystem ohne ein Ab- oder Aufrufen der Daten, nach §202a StGB strafbar sein kann und insbesondere §202c StGB die Vorbereitungshandlungen im Zusammenhang mit sogenannten Hackertools unter Strafe stellt, weil dadurch das Hacking im Vorfeld kriminalisiert wird. Aber das Hacking wird in Korea immer noch als ein besonderes Verbrechen behandelt. So wird das Hacking im Nebenstrafrecht, dem Gesetz zur Benutzung bzw. Schutz der Information des Telekommunikationsnetzes, geregelt. Demnach[2)] wird Jemand bestraft, der durch die Überwindung der Zugangssicherung eines Computers über ein Informations- und Kommunikations-Netzwerk unbefugt oder mit der überschrittenen Befugnis in ein Computersystem eingedrungen ist. Auch der Versuch dieser Tat ist unter Strafe gestellt. Aber nach der Polizei gab es bisher keinen Fall, wo gegen den Versuch des Hackings ermittelt wurde. Durch die jüngsten übersehbaren Schäden durch Hacking hat die Polizei den Plan, nachher bei Hacking-Versuchen aktiv zu ermitteln. Jedoch sind die Grenzen zwischen dem Versuch und der Vorbereitung im Hacking in Korea theoretisch immer noch fließend. Dies ist ein sehr wichtiges Thema bei uns, weil die Hacking-Vorbereitung in Korea immer noch nicht bestraft wird, anders als Deutschland. Vor allem ist der Fall des Versuchs wirklich nicht zu viel. Wenn ein Hacker nach dem Anfang des Hackings die Überwindung der Sicherheit eines Computers fehlschlägt, dann kann man es für den Versuch des Hackings halten. Aber ein Guru[3)] kann die Sicherheit des Computersystems relativ einfach überwinden. Deswegen wird seine Tat vollendet sein sobald er die Zugangssicherheit überwunden hat. Und vor der Vollendung des Hacking ist die Erkenntnis nicht einfach, ob ein Hacker in einen Server versucht einzudringen oder nicht, weil die Angriffszeit sehr kurz ist. Wegen der Knappheit zwischen dem Anfang und der Vollendung ist der Umfang des Hacking-Versuchs sehr eng. Schließlich gibt es trotz des Plans der koreanischen Polizei fast keine Chance, den Versuch des Hackings zu bestrafen.

↘ Cyberterrorakt von Nordkorea zurückgeführt.

2) §48 (Prohibition on intrusive Acts, etc. on Information and Communications Network) (1) No one shall intrude on an information and communications network without a rightful authority for access or beyond a permitted authority for access.
§72 (Penal Provisions) (1) A person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than three years or by a fine not exceeding 30 million won:
1. A person who intrudes on an information and communications network in violation of Article 48 (1)(2) An attempt of the crime under paragraph (1) 1 shall be punishable.

3) Hacker werden normalerweise in Guru (höchste Stufe des Hackers), Wizard (mittlere Stufe des Hackers) und script kids (niedrige Stufe des Hackers) eingestuft.

B. Die Illegale Datensammlung

Die koreanische Polizei durchsuchte wegen des Verdachts auf illegalen Datensammelns die Büros von Google Korea. Ermittler beschlagnahmten im Büro von Google Korea in Seoul Festplatten und weitere Daten über die Werbe-Plattform AdMob. Google, der die ortsbezogene Werbungsplattform vermarktet, steht in Verdacht, durch die Tochtergesellschaft für Mobilwerbung – AdMob – illegal personenbezogene Aufenthaltsdaten gesammelt zu haben. Gegen Google wurde im Zusammenhang mit seinem umstrittenen Straßenbilder-Dienst "Street View" im vergangenen Jahr in Korea schon ermittelt, weil Google für den Dienst personenbezogene Informationen aus ungesichterten WLAN-Netzen mitspeicherte.

Aber das Problem der illegalen Datensammlung gehört nicht lediglich zum Internet-Konzern Google. Koreas Behörden prüfen auch juristische Schritte gegen den US-Konzern Apple. Es war auch in Korea bekannt geworden, dass Apple die Bewegungsprofile von Nutzern des iPhone und des iPad auf den Geräten nicht gesichert speicherte und irgendwann abrufbar war. Die illegale Datensammlung der Großkonzerne ist nicht nur in Korea in die Kritik geraten, sondern auch weltweit.

Für diese Art von illegaler Datensammlung gab es bisher in Korea kein integriertes Gesetz. Im Zusammenhang mit der Datensammlung existierten einige Paragraphen in der verschiedenen Gesetze fragmentiert. Deswegen war es nicht einfach, darauf einen richtigen straflichen Paragraphen zu anwenden. Aber in Korea tritt das Datenschutzgesetz, worin die datenschutzbezogenen Vorschriften integriert sind, am 30.9.2011 in Kraft. Es wird erwartet, mit diesem Gesetz die illegale Datensammlung der Konzerne richtig kontrollieren zu können. Dennoch ist die Effektivität zweifelhaft. Denn es ist sehr schwer, dass koreanische Ermittler tatsächlich den verantwortlichen Betroffenen aufrufen oder einen betroffenen Server beschlagnahmen. In Wirklichkeit wollte die koreanische Polizei in dem Fall der illegalen Datensammlung den verantwortlichen Betroffenen in Google USA aufrufen. Jedoch verweigerte Google USA den Aufruf der koreanischen Polizei. Und obwohl ein wichtiger Server und Daten in den USA stehen, konnten koreanische Ermittler wegen der Verweigerung Googles diese beschlagnahmen oder durchsuchen. Bei diesem Fall ist nicht nur der gesetzlicher Grund wichtig, sondern auch die Rechtshilfe.

C. Cyberbeleidigung

Die Entwicklung des Cyberraums in Korea hatte beträchtliche Auswirkungen auf die Art der Kommunikation. Durch die neuen Medien wie SNS, Messenger, Email usw. können Koreaner ihre Meinungen im Cyberspace noch freier sagen, weil sich die Meinungsfreiheit in der bisherigen koreanischen Gesellschaft durch die Tradition (Konfuzianismus), die Militärdiktatur usw. oft beschränkt war. Aber ehrverletzende Äußerung im Cyberraum steigt mit dem Aufstieg der Internet-Medien-Benutzung weiter auf. Deswegen wird die Beleidigung im Internet zu einer großen sozialen Frage in Korea. Zurzeit ist die sog. Cyberbeleidigung vor allem wegen des Selbstmords einiger berühmten Schauspiele-

rinnen/Schauspieler wiederum in der Öffentlichkeit aufgetaucht. So gibt es lebhafte Diskussionen für die Einführung der Cyberbeleidigung. Nach einem Lager muss man nicht die Beleidigung im Cyberspace durch einen neuen Artikel zu regulieren. Dagegen behauptet das andere Lager, dass die immer schlimmer werdenden Beleidigungen im Cyberspace unbedingt mit einem höheren Strafmaß gestraft werden muss.

Die Beleidigung im KoStGB ist wie folgt:

Article 311 (Insult) A person who publicly insults another shall be punished by imprisonment or imprisonment without prison labor for not more than one year or by a fine not exceeding two million won

Article 312 (Complaint)

(1) The crimes of Articles 308 through 311 shall be prosecuted only upon complaint.

Die Beleidigung in Korea wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu zwei Million Won (§311 KoStGB) geahndet und gehört zum Antragsdelikt. Dazu wurde der Gesetzesentwurf für die Cyberbeleidigung abgegeben. In der Beleidigung im Cyberraum erhöht sich das Strafmaß der Cyberbeleidigung mit Freiheitsstrafe bis zu drei Jahre oder mit Geldstrafe bis zu dreißig Million Won. Damit soll das Antragsdelikt der bestehenden Beleidigung ins Widerspruchsdelikt geändert werden. die Einführung der Cyberbeleidigung ist es immer noch umstritten.

Ich glaube, es kann in der Aspekte der Opfer nötig sein, dass man bestimmte Handlungen in Bezug auf die Beleidigung im Cyberraum neu unter Strafe stellen kann. Dennoch ist es zweifelhaft, dass sich das Strafmaß der Beleidigung im Cyberraum aufgrund der Verbreitungsmöglichkeit erhöht und das Antragsdelikt der Beleidigung ins Widerspruchsdelikt in der Cyberbeleidigung transformiert wird. Denn wir können die Beleidigung im Cyberraum durch das geltende Strafrecht genug bestrafen und ich finde, dass die strikte Bestrafung der Cyberbeleidigung nicht verhältnismäßig sein kann.

III. Spamming im Rahmen des Verhältnismäßigkeitsgrundsatzes

1. Der Auftritt des Spamming-Problems im Cyberraum

Wenn von der sehr erfolgreichen Leistung des Cyberraum geredet wird, kann zunächst die Erweiterung des Kommunikationsraums z. B. durch E-Mail genannt werden, da die E-Mail – obwohl sie heute aufgrund echtzeitiger Kommunikationsmittel wie Facebook Messenger an Bedeutung verloren hat – immer noch als das wichtigste Kommunikationsmittel im Cyberraum gilt. Jedoch nimmt die Anzahl von Spam, die ein nützliches Kommunikationswerkzeug verwendet, stark zu.[4] In dieser Situation bemüht man sich darum, durch

4) Laut Symantec Intelligence Report betrug der Anteil an Spam-Mails im Juli 2015 rund 50 Prozent(de. statista.com).

technologische oder gesetzliche Mittel den Kampf gegen den Spam zu führen, jedoch wollen Spammer mit der entsprechenden Hilfe der neuen Hacking-Techniken den Gewinn durch das Spamming weiterhin abschöpfen. Im Zusammenhang mit diesem Spamming-Problem wurde die Rechtfertigung des strafrechtlichen Eingriffs bereits vor langer Zeit aufgehoben und in einigen Staaten, in denen die Informations- und Kommunikationstechnologie hoch entwickelt ist, wurde das Spamming unter Strafe gestellt.[5] Darüber hinaus wird zudem gefordert, fast alle Arten des Spammings im Cyberraum strafrechtlich zu kontrollieren. Da ein solcher grenzenloser Eingriff des Strafrechts von den Spammern – insbesondere von vielen Firmen – abgelehnt wird, spitzt sich der Konflikt zwischen Spammern und Anti-Spammern immer mehr zu. Das Spamming-Problem ist zwar besonders mit dem Rechtfertigungsproblem des Strafrechteingriffs im Cyberspace verbunden, aber auch mit der Unterscheidung der gesetzlichen Maßnahme in der Realwelt und der im Cyberspace.[6] An dieser Stelle muss deswegen die Strafrechtspolitik gegen Spamming durch den Verhältnismäßigkeitsgrundsatz abermals überprüft werden.

2. Die Grenze des Spammings im Cyberspace

Vor der eigentlichen Diskussion ist es notwendig Spam zu definieren und die Grenze zum Spam zu ziehen, da keine einheitliche Terminologie vorliegt und das Spamproblem im Zusammenhang mit dem Hacking- und Spywareproblem gebracht wird. Denn durch den unklaren Begriff und die verschwommene Grenze kann vor allem der strafrechtliche Eingriff leicht erweitert werden.

Der Begriff „Spam“ im Cyberspace wird heute in der Regel als Sammelbegriff für unerwünschte elektronische Nachrichten oder unverlangte elektronische Zusendungen verwendet. Dagegen wird in der Mitteilung der europäischen Kommission „Spam“ als ungebetene Werbung über elektronische Post definiert.[7] Der Begriff „Spam“ wird daneben als eine Art Sammelbegriff nicht nur bei unaufgefordert zugesendeten Telefaxen oder SMS, sondern auch beim

---

5) Z. B. Nach dem Gesetz zur Information und Kommunikation von Korea wird, wer mit Hilfe der E-Mail-Adresse, die rechtswidrig erworben wird, eine Spam-Mail verschickt, gemäß § 65 Abs. 1 Nr. 6 mit Freiheitstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 10 Millionen Won bestraft.

* ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.

Article 50-8 (Prohibition on Transmission of Advertising Information for Unlawful Act) No one shall transmit any advertising information for goods or services prohibited by this Act or any other Act through an information and communications network.

Article 74 (Penalty Provisions) (1) Any of the following persons shall be punished by imprisonment with labor for up to one year or by a fine not exceeding 10 million won:

6) Dass in den USA am Chicago John Marschall Law School das Spamming als ein Hauptkurs angeboten wird, zeigt das Ausmaß der Spamproblems. Dazu http://news.com.com/2100-1028_3-1012404.html(28.01.2008).

7) KOM(2004) 28 endg., 5. Es wird kritisiert, dass diese Definition teilweise zu weit, teilweise zu eng sei. Dazu näheres in Hilgendorf, Hamonisierung des Internetstrafrechts auf Europäischer Ebene, S. 280 ff.

Meta-Tag-Spamming genutzt.[8] Darüber hinaus wird sogar das Spamming im Blog mit in diesen Sammelbegriff einbezogen, da der Blog bei der Übermittlung von Informationen mit E-Mail gleichgesetzt werden kann. Der Begriff „Spam“ im Cyberraum beinhaltet somit nicht nur einfache Massen-E-Mails, sondern alle Arten von unerwünschten elektronischen Nachrichten.

In diesem Zusammenhang ist allerdings fraglich, ob alle unerwünschten elektronischen Nachrichten als Spam bezeichnet werden können. Nach einer in der Literatur vertretenen Ansicht sollte Spam in folgende vier große Gruppen unterteilt werden: in Werbesendungen, in Schikanemails, in rechtswidrige oder sogar kriminelle Botschaften, betrügerische oder pornographische Angebote, Sendungen mit grundsätzlich sinnvollem Inhalt wie religiöse oder politische Nachrichten oder Mails der Online-Marktforschung. Dabei sollte die vierte Gruppe trotz ihrer Form von Sanktionen ausgeschlossen werden.[9] Wenn diese Ansicht etwas erweitert wird, könnten somit die unerwünschten elektronischen Nachrichten des öffentlichen Interesses trotz ihrer Form als Spamming ausscheiden. Grundsätzlich sollte beim Spamming geprüft werden, ob die Nachrichten eine kommerzielle Eigenschaft haben, da problematische Nachrichten meist aus kommerziellem Grund entstehen.[10] Aus diesem Grund kann man unter Spamming unerwünschte elektronische Nachrichten verstehen, die ohne öffentliches Interesse hauptsächlich aus kommerziellen Gründen zugesandt werden. Unter diese Definition lassen sich der Umfang und das Niveau des strafrechtlichen Eingriffs durch den Verhältnismäßigkeitsgrundsatz überprüfen.

3. Das Modell der Regulierung im Cyberspace

Lessig hat die Regulatoren des Cyberraums wie in der Realwelt in vier Elemente eingeteilt. Aber die den Cyberraum regulierenden Elemente scheinen geringe Unterschiede zu denen der Realwelt aufzuzeigen. Denn beim Cyberraum ist eine spezielle Kultur und Technik mit einem einzigartigen Charakter vorhanden. Meines Erachtens nach lassen sich die Regulatoren im Cyberspace in fünf Elemente, d. h. Ruf, Markt (Kapital), Architektur (Code), Gesetz und soziale Norm einteilen.

a) Der Ruf spielt in der Realwelt eine wichtige Rolle. Wenn man eine gute Reputation hat, kann man großen Respekt erlangen und besonders erfolgreich sein. Insbesondere evaluieren die Firmen anhand der angesammelten Bonuspunkte die Treue der Kundschaft und können mit Hilfe dieser Datenbank auch die Neigung der Kunden voraussehen.[11] Bei Politikern spielt ihr Ruf bei der Wahl eine entscheidende Rolle und vor Gericht kann er zur Milderung oder Erhärtung der Strafe beitragen.[12] Aber der Ruf wird darüber hinaus im

8) Frank, Zur strafrechtlichen Bewältigung des Spamming, S. 4.

9) Hilgendorf, a.a.O., S. 282.

10) Es wird jedoch auch die Ansicht vertreten, nur Werbenachrichten als Spam zu erfassen sei zu wenig. Dazu Hilgendorf, a.a.O., S. 281.

11) Rheingold, smart Mobs. The next social rovolution, Cambrige, Mass.,2002, S. 113.

12) Nach § 51 StGB von Korea ist die Bedienung der Strafzumessung arrangiert. Aber es ist das Beispiel, sodass die anderen Elemente wie Ruf in der Strafzumessung eine wichtige Rolle spielt.

Cyberspace evolutioniert. Firmen schaffen so neue Unternehmenswerte. Bei Firmen wie eBay spielt er für das Geschäft eine entscheidende Rolle.[13] Der Ruf hat im Cyberspace auch eine filternde Funktion. Infolgedessen kann man vertrauliche Informationen von falschen Informationen unterscheiden. Insbesondere kann man ihn beim E-Commerce für das wichtigste Element im Marketing halten. Denn bei E-Commerce-Webseiten wie Amazon.com und eBay.com kann man mit Hilfe der Kundeneinschätzungen zu den ins Auge gefassten Produkten eine richtige Kaufentscheidung treffen und dadurch weitere Treuepunkte ansammeln.[14] Kurz gesagt, beeinflusst der Ruf nicht nur die individuelle Entscheidung, sondern auch das System des E-Commerce.

Wichtig ist vor allem, dass die Reputation als Regulator eine große Rolle spielt. In den verschiedenen Portal-Webseiten wie Google, werden die Seiten nach der Benutzerbeliebtheitsfrequenz klassifiziert und angezeigt. Beliebte Seiten können in der Cybergesellschaft einen guten Ruf aufbauen und man kann dadurch sogar ein bis drei Cent verdienen.[15] Dagegen ist eine Seite nicht mehr interessant für Netizen, wenn eine Portalseite in der Beliebtheitsskala als niedrig klassifiziert wird. Schließlich kann die Seite selektiert werden. Deswegen lässt sich die Reputation im Cyberspace als Bedingung für die Existenz einer Webseite ansehen. Gleichzeitig kann sie als ein Mittel inneren Drucks angesehen werden.[16] Mithin funktioniert der Ruf im Cyberspace als eine Art von Selbstregulierungsmittel. Aber er wird nicht durch die unmittelbare Steuerung erworben, sondern durch die Teilnahme der Netizen mittelbar gebildet. Infolgedessen fällt er in der Überprüfung für die Kontrolle im Cyberraum aus

b) Das Element der Architektur lässt sich im Cyberraum durch Codes ersetzen. Denn der Cyberraum besteht aus zahlreichen Codes und diese bilden, beschränken und regulieren wiederum den Cyberraum. Dort haben sich die Netizen an die Umgebung, die in der Regel vom Code geschaffen wurden, angepasst, weil das Cyberspace bei ihnen Boden, Luft, Gesellschaft und System ist. So tendiert sie dazu, die Regeln des Codes zu verinnerlichen, die Technik selbst zu assimilieren und selbst zu regulieren.[17] Die Cyberkultur beruht auf dieser Grundlage. Vor der WWW-Technik war die textbasierte Technik Online-Mainstream. In der neueren Zeit trat die Web 3.0-Technik im Cyberraum hinzu und als die Technik der nächsten Generation neu auf. Durch diese neue Technik der Codes wird zwar die jetzige Technik wiederum verbessert, so dass die Netizen im Cyberraum mehrere Vorteile der neuen Zivilisation genießen können. Jedoch wird die Freiheit des Netizens auch gleichzeitig durch die Regulierung des Codes mehr kontrolliert. Auf diese Art und Weise kann der Code im Cyberraum mit Hilfe der Waffe der Annehmlichkeit eine neue

13) Rheingold, a.a.O., S. 114 ff.
14) Rheingold, a.a.O., S. 117.
15) Rheingold, a.a.O., S. 119.
16) Rheingold, a.a.O., S. 120.
17) Rheinhard, a.a.O., S. 199.

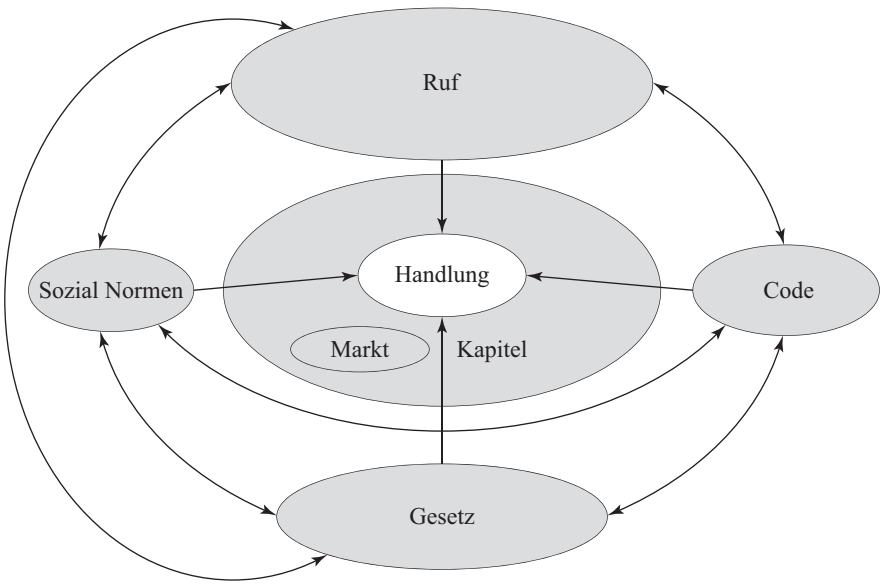
Art der Regulierung durchführen; denn diese wird mit der Durchführung des neuen Codes automatisch verwirklicht.[18)]

c) Der Markt, in der vorliegenden Arbeit genauer gesagt das Kapital, kann vielleicht heutzutage der beste praktikable Regulator sein. Denn die Notwendigkeit der Regulierung im Cyberraum wurde durch das E-Commerce bedingt und der wirtschaftliche Wert in diesem Raum ist praktisch die Energie der Entwicklung des Cyberraums. Deswegen hat das Kapital durch die Bildung des Marktes mehr kostenloses Gemeineigentum und auch vermehrt neues Kapital geschaffen. So übt das Kapital, mit dem Markt als Regulator des Cyberraum, auf den Netizen unmittelbaren Einfluss aus und gleichzeitig auch mittelbar auf Basis der Interaktion zwischen den anderen Regulatoren. Es kolonisiert im Cyberraum viele Bereiche so rasant wie in der Realwelt, weil z. B. die bisherigen kostenlosen Bereiche wie E-Mail durch den Eingriff des Kapitals kommerzialisiert wurden.

d) Bezüglich der sozialen Normen ist die Regulierungsfähigkeit im Cyberraum zurzeit sehr gering; wegen der Anonymität in diesem Raum können die normativen Sanktionen einfach unnütz werden. Private Vorwürfe gegen die Netikettabweicher sind als Zwangsmittel tatsächlich nicht effektiv, so dass jetzt viele Bereiche der sozialen Normen durch das Gesetz reglementiert werden müssen.

e) Das Gesetz ist der deutlichste Regulator und kann durch das Urheberrecht, Internet- und Computerstrafrecht usw. den Netizen unmittelbar, daneben durch verschiedene Normen die anderen Regulatoren mittelbar kontrollieren.[19)] Natürlich gibt es bei der

Die Regulierungselemente im Cyberspace



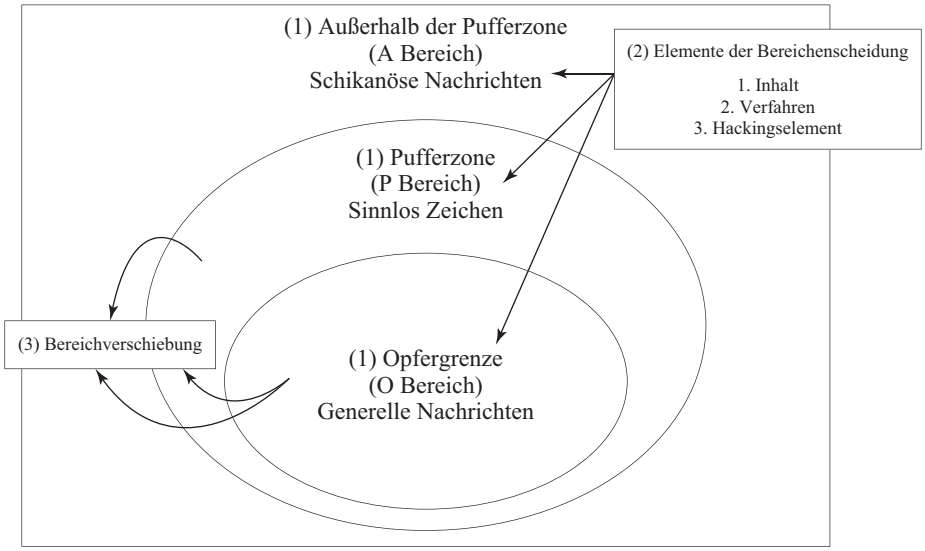
18) Lessig, Code2.0, 2006, S. 155.
19) Lessig, a.a.O., S. 129 ff.

Vorschrift, wie auch bei den sozialen Normen, einige Probleme. Das Gesetz hat jedoch starke Vollzugsmittel. Zum Beispiel kann man durch die Ermittlungsmethoden wie die digitalisierte Forensik[20] gegen die Cyberkriminalität geeigneten Maßnahmen einleiten. Darüber hinaus beinhaltet die Norm Rechtssicherheit. Wenn eine Vorschrift einmal in Kraft tritt, dann erhält diese bis zum Urteil der Verfassungswidrigkeit seine Gültigkeit. Dazu sind nicht so viele Kosten wie bei anderen Regulatoren notwendig, z. B. weil der Staat für die Verwirklichung des Codes viele Arbeitskräfte und finanzielle Investierung braucht. Deswegen wird die Verrechtlichung gegen die Netikettabweichung vor den anderen Regulatoren ins Vorfeld gestellt. Diese Verhältnisse kann man im folgenden Bild sehen.[21]

4. Die Verhältnismäßigkeit im Spamming

Die Verhältnismäßigkeit bedeutet, dass jede Maßnahme zwischen dem Eingriff in die Grundrechte und dem angestrebten Ziel einen legitimen öffentlichen Zweck verfolgt und überdies geeignet, erforderlich und verhältnismäßig im engeren Sinn ist.[22] Die Anwendung der Grundsätze des Spam-Problems wurde in meiner Doktorarbeit ausführlich besprochen.[23] Der Kern ist wie folgt.

Der Handlungsbereich des Spammers im Spamming



20) Die digitalisierte Forensik wird normalerweise benutzt, um den Beweis für Computerkriminalität zu erheben. Die digitalisierte Forensik wird Computerforensik oder IT-Forensik genannt. Zur digitalisierten Forensik näher Willer/Hoppen, Computerforensik – Technische Möglichkeiten und Grenzen, CR 9/2007, S. 610 ff.

21) Vgl. mit der Abbildung von Lessig; Lessig, a.a.O., S. 130.

22) Daniel Jositsch, Grundriss des schweizerischen Strafprozessrechts, DIKE, 2013, S.115.

23) Won-Sang Lee, Die Verhältnismässigkeit im Cyberstrafrecht, Logos, 2009, S. 109 ff.

Generelle Nachrichten liegen grundsätzlich im Bereich O. Deshalb können sie immer noch im Bereich O bleiben, auch wenn beide Versendungsverfahren ohne das Hackingelement erfüllt wurden. In dieser Hinsicht können z. B. Sendungen mit sinnvollem Inhalt wie religiöse oder politische Nachrichten oder Online-Marktforschungen grundsätzlich als sanktionsfreies Spamming im Bereich O bleiben,[24] solange die Botschaften ohne das Hackingelement versendet wurden. Fraglich ist in dieser Fallkonstellation die Menge des Spamming. Allerdings wird die Menge des Spammings nur bei den Hackingelementen wie dem Denial-of-Service-Angriff in Betracht gezogen, so dass die Menge grundsätzlich auf die Bereichsverschiebung keinen Einfluss hat. Bei der Bereichsverschiebung wird das fehlende Verfahren überlegt. Würde es an mittelbaren Verfahren (Opt-in- oder Opt-out-Verfahren) des Versendungsverfahrens trotz des fehlenden Hackingelements, dann sollen sie sich erstmal in den Bereich P verschieben; denn die Verletzung des mittelbaren Verfahrens lässt sich vom unmittelbaren Verfahren wie die Klarheit des Versenders kontrollieren. Im Gegensatz dazu wird das fehlende oder falsche unmittelbare Verfahren in den Bereich A verschoben, da dieses fehlende oder falsche Element den Irrtum des Empfängers verursacht und zugleich beim schikanösen Spamming durch das Anklicken das schikanöse Programm aktiviert.[25]

Könnten beide Versendungsverfahren nicht ohne das Hackingelement erfüllt werden oder würde trotz der Erfüllung des Inhalts- und Verfahrenselementes das Hackingelement weiter bestehen, sollten sie in den Bereich A verschoben werden. Schikanöse Nachrichten müssten immer noch im Bereich A bleiben, da ihre inhaltliche Rechtswidrigkeit auf keinen Fall geheilt werden kann. Natürlich fehlt bei den meisten inhaltlich rechtswidrigen Nachrichten neben dem Hackingelement auch das Versendungsverfahren.

Die Spammails mit sinnlosen Zeichen, die überwiegend eine Art von Spielmail sein können, liegen wegen ihrer inhaltlichen Unschädlichkeit grundsätzlich im Bereich P, allerdings werden sie meist in den Bereich A verschoben, da sie mit dem Hackingelement sehr eng verbunden sind. Aus diesem Grund sollte man den Eingriff des Strafrechts im Bereich A überprüfen.

---

24) Hilgendorf, a.a.O., S. 282.

25) Im konkreten Einzelfall ist es jedoch nicht so leicht. Gesetzt des Falls, dass der Empfänger den Willen der Aufnahmeablehnung äußert, aber der Spammer dennoch dem betroffenen Empfänger generelle Nachrichten gemäß des Versendungsverfahrens ohne das Hackingelement weiterhin zuschickt, ist der Fall unproblematisch. Denn in diesem Fall wird das Spamming nach der Differenzierung im Bereich O bleiben. Aber wenn der Spammer trotz des Willens der Aufnahmeablehnung weiterhin dem betroffenen Empfänger, Spamm-Mails zuschickt, kann das mit einer fehlenden Versenderklarheit gleichgesetzt werden. Deswegen fehlt in diesem Fall das unmittelbare Versendungsverfahren. So wird diese Art von Spamming in den Bereich A verschoben.

IV. Zusammenfassung und Fazit

Die Verbreitung neuer Medien ist in Korea in einem Jahrzehnt rasch fortgeschritten. Die Geschwindigkeit des Internets und die Technologie des Mobiltelefons in Korea ist weltweit führend. Die koreanische Benutzerzahl des Internetmediums und Internetservices wie Social Network System (SNS) ist auch sehr groß. Aber verschiedene Cyberverbrechen entstehen leider in Korea durch die hohe Anzahl des Netizens. Deswegen werden im Strafrechtsbereich über die verschiedene Themen für die aktuelle Cyberkriminalität diskutiert. Um die Cyberkriminalität effizient zu bekämpfen, ist es erforderlich, die strafrechtliche Theorie für Cyberkriminalität zu entwickeln und die Erfahrung der kriminalpolitischen Maßnahmen mit einander zu teilen. Korea hat reiche Erfahrungen und verschiedene Ermittlungen der Cyberkriminalität. Allerdings gibt es auch Probleme, alle Cyberspace-Probleme mit strafrechtlichen Mitteln lösen zu wollen. Ein typisches Beispiel ist die Spamming-Problematik.

Die Spamming-Problematik wurde mit dem Verhältnismäßigkeitsgrundsatz beleuchtet. Insbesondere steht bei dieser Überprüfung die Rechtfertigung eines strafrechtlichen Mittels im Mittelpunkt, da in Bezug auf das Spamming der Ruf nach Strafrechtseingriffen immer lauter wird. Der Strafrechtseingriff hat sich bei der Analysierung des Zweck-Mittel Verhältnisses als geeignet und erforderlich erwiesen. Es geht aber in dieser Hinsicht tatsächlich um die Einschränkungsintensität. Solange nicht alle Direktmarketingaktivitäten im Cyberraum als rechtwidrig betrachtet werden, liegt der Schlüssel des Spammingproblems in seiner logischen Differenzierung, demnach hängt davon die Einschränkungsintensität oder die Freiheit des Spammings ab. Deswegen wurde das Spamming in drei Elemente (Inhalt, Verfahren (des Schickens), Hackingelement) untergliedert und in den drei Bereichen (O, P, A) differenziert betrachtet. Nur im Bereich A dürfen Strafrechtseingriffe gestattet werden, da der Bereich O als die Opfergrenze des Spammings auf keinen Fall verletzt werden darf und trotz der gegebenen Problematik der Bereich P als Pufferzone, von einem anderem Mittel, als dem des Strafrechts, reguliert werden muss. Grundsätzlich stellt das Spamming zwar dem Inhalt nach den Bereich O dar, durch das fehlende Verfahren oder die Hackingelemente lasse es sich in die A-Stelle einordnen.

Ich denke, zumindest dass das Problem des Spams in Korea in Bezug auf technische Lösungen sehr weit entwickelt ist. In der Tat haben in den letzten fünf Jahren südkoreanische Spamangriffe quantitativ stark abgenommen.[26] Der Anteil der qualitativ schädlichen Spam-Mails durch E-Mail oder Malware haben stark zugenommen. Zusammenfassend kann man sagen, dass strafrechtliche Eingriffe bei der Spamproblematik auf den Bereich A beschränkt werden müssen. Sollten strafrechtliche Eingriffe in andere (P &O) Bereiche

26) https://www.statista.com/statistics/647840/south-korea-spam/.

vollzogen werden, müssten sie als Verstöße gegen den Verhältnismäßigkeitsgrundsatz betrachtet werden. Wenn dem nicht so ist, wird einem neben dem strafrechtlichen Eingriff ins Spamming noch einmal der bereits geführte Abnutzungsdisput der Entkriminalisierung in neuem Lichte geführt werden.[27)]

27) Zur Entkriminalisieurng näher Kaiser, Kriminalisierung und Entkriminalisierung in Strafrecht und Kriminalpolitik, in: Festschrift für Ulrich Klug, Band II, 1983, S. 579 ff.