

Neuere Entwicklungen im türkischen Strafrecht am Beispiel des Internet(=Informatik)strafrechts

Wiss. Ass. İlker Tepe¹

A. Einleitung

Es gibt keinen Bereich des sozialen Lebens, in dem nicht ein massiver Einsatz von Informationstechnologie denkbar wäre. Die Wirkung der Informations- und Kommunikationstechnologie zeigt sich in vielen Bereichen des alltäglichen Lebens. Ohne das Funktionieren des Internets wäre die moderne Gesellschaft heute kaum vorstellbar. Insofern ist der Schritt zur "Informationsgesellschaft" bereits getan. Die Vorstellungen von einer Rechtsordnung für die Informationsgesellschaft waren lange Zeit von weiten Freiheitsräumen geprägt; Staat und Recht wurden bei diesen Ansichten an den Rand gedrängt.

Neue technologische Grundlagen führen auch zu neuen Formen des Zusammenlebens. Diese Erkenntnis ist von großer Bedeutung, um die Entwicklungslinie des modernen Strafrechts richtig nachvollziehen zu können. Denn durch die Entwicklung eines moderneren Strafrechts wird versucht, angemessene und effektivere Lösungen für die neuartigen Probleme der modernen Gesellschaft zu finden.² Da es sich bei der modernen Gesellschaft um eine Informationsgesellschaft handelt, sind die (straf)rechtlichen Aspekte der Probleme der modernen Gesellschaft wichtiger als andere.³ Es handelt sich in diesem Zusammenhang um den Vorrang der Rechtsbereiche, die die Informationsgesellschaft direkt betreffen, insbesondere die des Computer- und Internet(straf)rechts.

Das am 1.7.1926 in Kraft getretene türkische StGB beruht auf der Übernahme des italienischen StGB in der Fassung von 1889 (Codice Zanardelli). Von den insgesamt 592 Artikeln des türk. StGB sind im Laufe der Zeit über die Hälfte neu gefaßt worden. Das türkische StGB wurde ca. 60-zig mal überarbeitet. Ein Reformbedürfnis besteht jedoch weiterhin. Nach den etwa 30 Jahre langen, intensiven Reformvorbereitungen, trat am 1.Juni 2005 das neue türkische Strafgesetz in Kraft. Durch dieses neue Strafgesetz wurden alle zuvor vorhandenen Gesetze vollständig außer Kraft gesetzt. Das

¹ Universität Akdeniz, Institut für Sozialwissenschaften, Abteilung für öffentliches Recht.

² Ünver, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Ankara, 2003, S. 443.

³ Ünver, *Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi*, IUHFM, C: LIX – S: 1-2, İstanbul, 2001, S. 61 ff.

neue türkische Strafgesetzbuch, die Strafprozessordnung und das Strafvollzugsgesetz wurden bereits modifiziert. In diesem Vortrag will ich versuchen, die gesetzlichen Regelungen des Computer- und Internetstrafrechts (Informatikstrafrechts) als die wichtigsten strafrechtlichen Aspekte der modernen Gesellschaft mit den aktuellen Entwicklungen in der Türkei nach dem in 2005 in Kraft getretenen türkischen StGB zusammenfassend darzustellen.

B. Geschichtliche Entwicklung der Informatikdelikte im türkischen Strafrecht

Die Auseinandersetzungen um die Informatikdelikte im türkischen Strafrecht lassen sich vor dem Hintergrund der etwa zwanzigjährigen Entwicklung bis zum Jahr 2004 erklären, freilich in ihren verschiedenen Facetten und Abwandlungen.

I. Vorentwurf zum türk. StGB vom 1989

Im Jahre 1984 wurde eine Kommission zur Vorbereitung eines Entwurfs für ein neues türkisches StGB gebildet, die 1987 erstmals einen Entwurf veröffentlichte. Im Anschluss an die Diskussion, in der auch kritische Einwände erhoben wurden, entstand im Jahr 1989 eine abschließende Fassung.⁴ Hinsichtlich der Straftaten im Informatiksystem ist der Vorentwurf zum türkischen StGB von 1989 von Bedeutung, da erst durch diesen Entwurf die Straftaten im Informatiksystem in das türkische Rechtssystem eingefügt wurden. Die im Folgenden aufgeführten Straftaten mit der Überschrift „Straftaten gegen die Öffentlichkeit“ bestehen insgesamt aus fünf Paragraphen und stehen im zweiten Teil, des neunten Abschnitts. Im Folgenden sind die im Vorentwurf 1989 geregelten Paragraphen kurz dargestellt:

Im § 342 mit der Überschrift „Durch Betrug an Daten gelangen und diese rechtswidrig benutzen“ ist die Tathandlung unter Strafe gestellt, Programme, Dateien oder irgendwelche Elemente aus einem automatisierten Datenverarbeitungssystem rechtswidrig zu erlangen, um diese zu übertragen oder zu verbreiten und dadurch einem Dritten Schaden zuzufügen.⁵

Im § 343 „Vorteil ziehen, Schaden zufügen“ ist die Tathandlung unter Strafe gestellt, einem Dritten Schaden zuzufügen, indem man ein automatisiertes Datenverarbeitungs-

⁴ *Hakeri*, Tötungsdelikte im Türkischen StGB-Entwurf 1997, http://www.akader.info/KHUKA/7_2000_ekim/totungsdeligte.htm (08.07.2007).

⁵ *Yazıcıoğlu*, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul, 1997, S. 208.

system oder Dateien oder irgendwelche Elemente teilweise oder gänzlich zerstört, oder verändert, um sich einen Vorteil zu verschaffen, oder durch die Behinderung eines Systems zusammen mit der Benutzung eines automatisierten Datenverarbeitungssystems sich oder einem Dritten rechtswidrig zu bereichern.⁶

Die Tathandlung, aus einem automatisierten Datenverarbeitungssystem Dateien und andere Komponenten zu speichern oder vorhandene Dateien oder irgendwelche Elemente zu zerstören oder diese zu nutzen, um eine Urkunde zu fälschen mit der Absicht diese als Beweismittel zu nutzen, ist im § 344 „Fälschung“ unter Strafe gestellt.⁷

§ 345 „Nebenstrafen“ enthält zusätzliche Regelungen zu den in § 342 und § 343 vorgesehenen Strafraumen. Beamte können vom Dienst ausgeschlossen werden, die durch die Straftaten der §§ 342 und 343 im Gewerbe oder im Handel erworbenen Sachen können beschlagnahmt werden und die Einrichtungen oder Unternehmen, die bei der Durchführung der Straftaten mitgewirkt haben, können geschlossen werden.⁸

Im § 346 „Juristische Personen und Versuchform“ wird durch die Einführung einer für den ganzen Abschnitt gültigen Regelung festgehalten, dass auch juristische Personen für die Straftaten dieses Abschnittes zur Verantwortung gezogen werden und dass bei einem Versuch das Strafmaß so hoch ist, wie bei einer vollendeten Tat.⁹

II. Eingeführte Regelungen durch das am 14.06.1991 in Kraft getretene Gesetz

Der Gesetzgeber hat mit dem Gesetz Nr. 3756 vom 14.06.1991 den Vorentwurf zum türkischen (türk.) StGB von 1989- wenn auch nur teilweise - in das türk. StGB (Nr. 765) eingefügt. Die Regelungen des Vorentwurfes über die Straftaten im Informatiksystem wurden als elfter Teil eingefügt und beginnen ab dem § 525. Die mit dem genannten Gesetz getroffenen Regelungen lauten wie folgt:

Die Regelung, die als § 525 lit. a türk. StGB ins Gesetzesbuch eingefügt wurde, gleicht dem § 342 „durch Täuschung Daten besitzen und diese rechtswidrig anwenden“ aus dem Vorentwurf des türk. StGB von 1989. Auch das Strafmaß und die Strafbegründung wurden exakt übernommen.¹⁰

⁶ Yazıcıoğlu, *Kriminolojik, Sosyolojik*, S. 208.

⁷ Kurt, *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Hukukundaki Uygulaması*, Ankara, 2005, S. 120.

⁸ Kurt (Fn. 7), S. 120.

⁹ Kurt (Fn. 7), S. 120-121.

¹⁰ Karagülmez, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara, 2005, S. 126 ff.; Yenidünya/Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul, 2003,

Genauso ist der § 525 lit. b türk. StGB mit seiner Strafbegründung („Vorteil ziehen, Schaden zufügen“) identisch mit der im Vorentwurf vorgesehenen Regelung aus § 343.¹¹

§ 525 lit. c türk. StGB unterscheidet sich in einigen Punkten von dem § 344 „Fälschung“ des Vorentwurfes zum türk. StGB von 1989. Die Strafbarkeit von „Speichern und Zerstören“ entspricht dem des Vorentwurfes.

Jedoch war im Vorentwurf auch für das „Benutzen“ die gleiche Bestrafung vorgesehen. Im Gesetz Nr. 3756 ist für die Tathandlung des Benutzens von zerstörten Dateien eine geringere Bestrafung vorgesehen.¹² Ein weiterer Unterschied zum Vorentwurf liegt darin, dass das Benutzen der zerstörten Datei oder der anderen Komponenten vorsätzlich geschehen muss.¹³

Bezüglich der Nebenstrafen wurde im § 525 lit. d türk. StGB, im Unterschied zu § 354 des Vorentwurfes, die Beschlagnahmung und die Schließung von Einrichtungen nicht aufgenommen.¹⁴ Ebenso wurden auch nicht die Regelungen aus dem § 346 des Vorentwurfes zum türk. StGB von 1989 übernommen, die besagten, dass auch juristische Personen für die Straftaten dieses Abschnittes zur Verantwortung gezogen werden und dass bei einem Versuch das Strafmaß so hoch ist, wie bei einer vollendeten Tat.¹⁵

III. Vorentwurf zum türk. StGB von 1997

Man kann zu Recht behaupten, dass die Regelungen im Vorentwurf zum türk. StGB von 1997 bezüglich der Straftaten im Informatiksystem aus der französischen Strafgesetzregelung von 1994 abgeleitet wurden und mit den Straftaten der § 323 Abs. 1 und § 323-7 des französischen Strafgesetzbuches übereinstimmen.¹⁶

Nachdem in § 347 Abs. 1 des Vorentwurfes „Zugang ins Datenverarbeitungssystem, Dateien schädigen und zerstören“ die Tathandlungen des unbefugten Zugangs ins Informatiksystem oder das weitere Verbleiben geregelt wurden, wurde im Abs. 2, die durch die Tathandlung vorgenommene Löschung oder Veränderung der Dateien im

S. 54.

¹¹ Kurt (Fn. 7), S. 122.

¹² Dülger, Bilişim Suçları, Ankara, 2004, S. 207.

¹³ Yazıcıoğlu, Kriminolojik, Sosyolojik, S. 284.

¹⁴ Kurt (Fn. 7), S. 124; Dönmezer, Kişiler ve Mala Karşı Cürümler, 16. Auflage, İstanbul, 2001, S. 623.

¹⁵ Yazıcıoğlu, Kriminolojik, Sosyolojik, S. 209.

¹⁶ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirmesi, YÜHFD, Band II, Heft 2, İstanbul, 2005, S. 394.

Informatiksystem als Erschwerungsgrund aufgeführt. Außerdem wurde für das Zerstören des Zugangs oder der im System gespeicherten Daten eine höhere Strafe als die des Abs. 1 festgelegt. Im 3. Absatz wird sogar der Versuch des unbefugten Zuganges in das Informatiksystem als vollendete Straftat bewertet.¹⁷

Es wurde zum ersten Mal in diesem Vorentwurf anstatt des Begriffs des „automatisierten Datenverarbeitungssystems“ der Begriff des „Informatiksystems“ verwendet.

Im § 341 Abs. 1 des Entwurfes „Durch die Behinderung bzw. Zerstörung des Systems, rechtswidrig Vorteile zu erlangen“ wird die Behinderung bzw. die Zerstörung des Systems, um dadurch einen rechtswidrigen Vorteil zu erlangen, unter Strafe gestellt. Im zweiten Absatz ist die rechtswidrige Zuführung von Dateien ins Informatiksystem und die Löschung oder Veränderung der gespeicherten Dateien als strafbare Handlung festgehalten. Im dritten Absatz heißt es, dass bei einer ungerechtfertigten Bereicherung zum Nachteil eines anderen die Bestrafung verschärft wird und im letzten Absatz, dass der Versuch mit dem gleichen Strafmaß geahndet wird, wie die vollendete Tat.¹⁸

Das Speichern von Dateien in einem Informatiksystem und das Zerstören von vorhandenen Dateien, um eine gefälschte Urkunde zu erstellen, in der Absicht, diese im Rechtsverkehr zu nutzen, ist im § 349 Abs. 1 „Täuschung“ als strafbare Handlung festgehalten. Im zweiten Absatz des § 349 ist die Benutzung dieser gefälschten Urkunde unter Strafe gestellt. Die von diesem Paragraphen vorgesehene Regelung ist identisch mit dem Gesetz Nr. 3756. Der einzige Unterschied besteht darin, dass der Begriff „Informatiksystem“ an Stelle von „automatisiertem Datenverarbeitungssystem“ benutzt wurde und dass die im Gesetz vorgesehene Strafrahmendifferenz zwischen dem, der die Urkunde herstellt und demjenigen, der diese Urkunde einsetzt, abgeschafft wurde.¹⁹

Im § 350 „Nebenstrafen“ wurde die Beschlagnahmung wieder eingefügt. Im § 351 „Verantwortung der juristischen Personen“ ist geregelt, dass bei den in §§ 347 und 348 genannten Straftaten auch juristische Personen zur Verantwortung gezogen werden. Mit dem § 352 des Vorentwurfes von 1997 „Bildung einer Bande, um eine Straftat zu begehen“ wurde erstmals das Bilden einer oder das Beitreten zu einer Bande, um eine der oben genannten Straftaten zu begehen, unter Strafe gestellt und mit einem höheren Strafmaß versehen.

¹⁷ Kurt (Fn. 7), S. 124.

¹⁸ Kurt (Fn. 7), S. 125-126.

¹⁹ Kurt (Fn. 7), S. 127.

IV. Vorentwurf zum türk. StGB von 2000

Die Straftaten im Informatiksystem sind im Vorentwurf zum türk. StGB von 2000 mit der Randüberschrift „Straftaten im Bereich der Informatik“ im zweiten Teil des neunten Abschnitts in den §§ 346-352 geregelt.

Die Regelungen des Vorentwurfes von 1997 wurden, abgesehen von wenigen Wortabweichungen und der Anpassung der Geldstrafen, samt Begründung in den Vorentwurf von 2000 übernommen. Nur im § 348, der die Nebenstrafen regelt, wurden folgende Phrasen eingefügt: „die Beschlagnahmung der bei der Straftat benutzten oder durch die Straftat erworbenen Sachen“ und „die Übertragung des Besitzes auf den Staat“.²⁰

Zum ersten Mal wurde die in den Vorentwurf von 2000 eingebrachte Regelung des „Missbrauchs von Bank- und Kreditkarten“ durch den § 349 eingeführt. Im ersten Absatz dieses Paragraphen wird das Benutzen oder Benutzen lassen einer Kreditkarte, die einer fremden Person gehört oder einer anderen Person abgegeben werden muss und die der Täter auf irgendeine Weise in Besitz genommen oder bei sich behalten hat und ohne Einwilligung des Eigentümers benutzt oder durch das Benutzen sich oder eine andere Person ungerechtfertigt bereichert, unter Strafe gestellt. Im zweiten Absatz wird die Bestrafung erschwert, wenn die oben genannte Tathandlung durch die Zerstörung der Bank- oder Kreditkarte verwirklicht wurde oder um zu täuschen.²¹ Bezüglich der Verantwortlichkeit von juristischen Personen ist die Regelung nur mit einem Unterschied zum Vorentwurf von 1997 in das türk. StGB von 2000 aufgenommen worden. Trotz des Vorentwurfs von 1997, der den Verantwortungsbereich der juristischen Personen auf die Handlungen, wie Zugang ins Informatiksystem, das Zerstören oder Schädigen von Daten, das Behindern oder Zerstören der Systemsfunktion und das sich damit ungerechtfertigt Bereichern, eingrenzt, können juristische Personen im türk. StGB von 2000 für alle in diesem Teil genannten Straftaten zur Verantwortung gezogen werden.²²

V. Vorentwurf zum türk. StGB von 2003

Straftaten im Informatiksystem sind im 2. Buch „Straftaten gegen die Öffentlichkeit“ im 9. Teil als „Straftaten im Bereich des Informatiksystems“ geregelt. Im § 346 ist der

²⁰ Özel, *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*, İstanbul Barosu Dergisi, Cild 75/ Sayı 7, 8, 9, S. 862.

²¹ Akıncı/Alıç/Er, *Türk Ceza Kanunu ve Bilişim Suçları*, in: *Internet ve Hukuk* (Hg.: Yeşim Atamer), İstanbul, 2004, S. 266.

²² Akıncı/Alıç/Er (Fn. 21), S. 272-273.

Zugang ins Informatiksystem, die Zerstörung und Änderung der Daten, im § 347 die Behinderung oder das Schädigen der Systemsfunktion um sich dadurch ungerechtfertigt zu bereichern, im § 348 Täuschung, im § 349 Nebenstrafen, im § 350 Missbrauch von Bank- und Kreditkarten, im § 351 Bildung einer Bande, um eine Straftat zu begehen und im § 352 der Verantwortungsbereich von juristischen Personen geregelt. Die §§ 346, 347, 348 des Vorentwurfes von 2000 wurden samt ihrer Begründung in den Entwurf von 2003 übernommen, nur die Geldstrafen wurden angepasst. § 349 wurde ohne Änderungen übernommen.

Der § 351 „Bildung einer Bande, um eine Straftat zu begehen“ wurde durch Beibehaltung der Überschrift und seiner Grundform nur mit einem einzigen Unterschied in dem Vorentwurf 2003 übernommen. Der Satzteil „die mit einer oder mehreren materiellen Eigenschaften verstandene Existenz“ wurde gestrichen.²³

Bei den §§ 350 und 352 gibt es keinen Unterschied zu den beiden Vorentwürfen (2000 und 2003).

C. Systematik des türkischen StGB Nr. 5237

Im neuen StGB werden die „Straftaten im Bereich der Informatik“ in einem gesonderten Teil aufgeführt; das Gesetz räumt diesen Straftaten im dritten Teil des zweiten Buches einen Platz ein. Computer und die mit deren Einsatz verwirklichte Kommunikation werden auch unter die Überschrift „Informatikbereich“ subsumiert. Daher schützt der Abschnitt „Straftaten im Bereich der Informatik“ einerseits den Computer, seine Elemente und die bei ihm verwirklichten Verfahren und andererseits ebenfalls die durch den Einsatz von Computern verwirklichte Datenverbindung- und weiterleitung sowie natürlich das Internet.²⁴

In der Literatur geht es um die verschiedenen Klassifikationsversuche der Informatikdelikte.²⁵ Unter diesen Versuchen ist die systematische Klassifikation von Yazicioglu zu erwähnen. Nach Yazicioglu werden die Informatikdelikte in zwei Gruppen unterteilt; einmal „Informatikdelikte im engeren Bereich“, die die aus dem

²³ Kurt (Fn. 7), S. 132.

²⁴ Yazicioglu, Yeni Türk Ceza Kanunundaki S. 403; Karagülmez (Fn. 10), S. 37; Dülger (Fn. 12), S. 66.

²⁵ Z.B. geht Dönmezer von zwei Klassifikation aus: 1. Die im Computersystem begangenen Straftaten, um das Computersystem, die Datenbanken und die Programme zu schützen, 2. Die gegen den Computer begangenen Straftaten, um den Computer als ein technisches Mittel zu schützen. Dönmezer (Fn. 14), S. 616. Noch ein weiterer Klassifikationsversuch von Ersoy: 1. Straftaten durch das Informatiksystem, 2. Straftaten gegen Informatiksysteme, 3. Straftaten gegen das Informatikmittel. Ersoy, Genel Hukuki Koruma Cercevesinde Bilisim Suclari, AÜSBFD., C. 49, S. 3-4, Ankara, 1994, S. 160.

Bereich des Informatiksystems resultierenden Rechtsgüter betreffen und zum anderen „Informatikdelikte im breiteren Sinne“, d. h. klassische Straftaten, die mit den Möglichkeiten des Informatiksystems verwirklicht werden.²⁶

Die erste Gruppe, die auch als „echte Informatikdelikte“ bezeichnet wird, wird wiederum in zwei Gruppen unterteilt. Zum einen die als „direkte Straftaten im Informatiksystem“ oder als „Straftaten im Informatiksystem im engeren Sinne“ bezeichneten echten Straftaten im Informatiksystem, welche aus der Besonderheit des Informatiksystems resultieren und im Bereich der neuen Rechtsgüter begangen werden. Dazu gehört der „unbefugte Zugang zum Informatiksystem“ (§ 243), der „Eingriff auf die im Informatiksystem befindlichen Daten“ (§ 244), die „Erlangung von ungerechtfertigten Vorteilen aus den Möglichkeiten des Informatiksystem“ (§ 244 Abs. 4) und der „Missbrauch der Bank- und Kreditkarten“. Die zweite Gruppe beinhaltet die anderen, indirekten Straftaten im Informatiksystem, die sich aus den Möglichkeiten der Techniken des Informatiksystems ergeben. Zu dieser Gruppe gehört z. B. der „Verstoß gegen das Kommunikationsgeheimnis“ (§ 132), das „Hindernis der Kommunikation“ (§ 124), das „Verhindern von Unterricht und Ausbildung“ (§ 112) und das „Verhindern von Tätigkeiten öffentlicher Anstalten oder Berufsinstituten, die wegen ihren Eigenschaften den öffentlichen Anstalten ähnlich sind“ (§ 113). Es ist auch möglich, klassische Straftaten, wie die „Verleumdung und Beleidigung“ (§ 125), die „Unzüchtigkeit“ (§ 226), die „Möglichkeiten- und Platzbeschaffung für Glücksspiele“ (§ 228) und die „Anstiftung zur Begehung einer Straftat“ durch die Möglichkeiten der Informatiksystemtechniken zu begehen. Die Benutzung des Informatiksystems ist ebenfalls ein erschwerender Grund für den Diebstahl (§ 142 Abs. 2 lit. e) und den Betrug (§ 158 Abs. 1 lit. f).

D. Begriffsbestimmung

Mit dem zunehmenden Interesse für das neue Kommunikationsmedium und der Verbreitung der Informatik- und Telekommunikationstechnologie wurden die Begriffe „Informatik“, „Datei“, „Internet“, „Computer“ und „Cyberspace“ sowohl in den allgemeinen Sprachschatz als auch in die gesetzlichen Texte aufgenommen. In diesem Zusammenhang gibt es eine Parallele zwischen dieser Begriffserklärung und -bestimmung und der technologischen Entwicklung, da alle neuen technologischen

²⁶ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki, S. 396 ff.; Yazıcıoğlu, Bilgisayar Ağları Marifetiyle İşlenen Suçlar: Sanal Suçlar, Bilişim Suçları (Panel – T.C. Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi Başkanlığı), Ankara, 2001, S. 36 ff.

Entwicklungen eine Bereicherung und Verwandlung der Begriffsinhalte mit sich führen.²⁷ Natürlich gibt es in der Hinsicht dazu viele Begriffe. Strafrechtlich relevante Begriffe sind jedoch folgende:

I. Der erste wichtige Begriff ist „Informatik“ (das Datenverarbeitungssystem im alten StGB). Das Wort Informatik kommt aus dem französischen „Informatique“, und setzt sich zusammen aus den französischen Wörtern „Information“ (Kenntnis, Wissen) und „Automatique“ (Automatisch) und beinhaltet demnach die Definitionen für Datenaufbewahrung, -organisation, -übertragung, -vervielfältigung, -weiterleitung, -benutzung, -überbringung, -zuführung, und -veränderung.²⁸ Die türkische Sprachgesellschaft definiert den Begriff „Informatik“ als eine Wissenschaft, die durch die Menschen für die Kommunikation im technologischen, ökonomischen und gesellschaftlichen Bereich genutzt wird und die Informationen von der elektronischen Maschine ordentlich und logisch verarbeitet.²⁹ Die Informatik wird somit als eine Wissenschaft anerkannt und es wird als die automatische Aufbewahrung, Ordnung, Auswertung, Übertragung, Weiterleitung, Benutzung, Überbringung, Ergänzung, Zuführung, Veränderung einer Information, aus irgendeinem Bereich definiert. Bei einer strafrechtlichen Begriffsbestimmung aus dem Bereich der Informatik ist die Begrifflichkeit des Gesetzgebers heranzuziehen, der sich mit den Problemen der Informatik auseinandergesetzt hat. Einen Hinweis auf den Informatikbegriff gibt die Begründung des türkischen StGB. Hier steht in der Begründung zu § 243 geschrieben: Das Informatiksystem ist ein magnetisches System, das die Daten nach der Sammlung und Lokalisation automatisch verarbeitet. Diese Bemühung eine Definition zu finden, ist leider unklar und strittig. Die Hauptansatzpunkte des Gesetzgebers sind das magnetische System und die Datenverarbeitung nach der Sammlung und Lokalisation dieser Daten. Nun ist zu fragen, was ein „magnetisches“ System ist, warum nur das magnetische System als Informatiksystem definiert wird und was „die Sammlung und Lokalisation der Daten“ bedeutet, wie und/oder von wem diese Daten gesammelt und lokalisiert werden... usw.³⁰

II. Ein Computer ist, je nach Speicherprogramm, ein Funktionsmittel, der arithmetische und logische Handlungen übernimmt, Entscheidungen trifft, die Anwendung der Programme und die zu verarbeitenden Daten speichert, um so mit

²⁷ Koca, Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, C. III, S. 787 ff.

²⁸ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki, S. 403.

²⁹ <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFFAAF6AA849816B2EF05A79F75456518C> (08.07.2007).

³⁰ Für die Diskussion dazu Yazıcıoğlu, Yeni Türk Ceza Kanunundaki, S. 404 ff.

seinem Umfeld zu kommunizieren.³¹ Mit anderen Worten ist ein Computer mit Datenverarbeitungseigenschaften ein Mittel, das jede ausreichend definierte und vervollständigte Aufgabe bearbeiten, Informationen behandeln, speichern, ordnen, auswerten, übertragen, benutzen, überbringen, verändern und ergänzen kann.³² Das Besondere an Computern mit Datenverarbeitungseigenschaften im Gegensatz zu anderen Datenträgern ist, dass die Informationen anders behandelt werden: Es ist ein Mittel das zu allgemeinen Zwecken genutzt wird.³³ Eine besondere Definition für den Begriff des Computers gibt es im türkischen StGB nicht.

III. Die Datei ist ein wichtiges Element für die Klärung des Begriffes „Informatiksystem“. Eine Datei wird als entsprechende Darstellung definiert, die alle möglichen Informationen für die Verarbeitung von dem Computer zu einem analytischen und numerischen Code umschreibt.³⁴ Gemäß dieser Definition kommt der Datei eine umfassende Bedeutung zu. Im alten StGB wurde der Begriff „irgendwelche Elemente“ benutzt, um die Straftaten gegen das Informatiksystem nicht zu begrenzen. Der Gesetzgeber bezweckte damit, dass die neuen Straftatbestände in dieser Hinsicht mit den neuen technologischen Entwicklungen mithalten können. Deswegen gab es keine Begrenzung gegen die technologische Entwicklung, es handelte sich vielmehr um eine dynamische gesetzliche Konstruktion für Informatikdelikte.³⁵ Diese Auffassung wurde jedoch durch das „Gesetzlichkeits- und Bestimmtheitsprinzip“ kritisiert. Nach diesem Meinungsstreit werden mit dem Begriff „Datei“ alle Elemente miteinbezogen und wiedergegeben.³⁶ Im türkischen StGB gibt es keine besondere Definition für die Datei.

E. Normenanalysen zu „Straftaten im Bereich der Informatik“ im türk. StGB

I. § 243 türk. StGB – Unbefugter Zugang ins Informatiksystem

Der Straftatbestand des unbefugten Zugangs gemäß § 243 I des türkischen StGB wird wie folgt geregelt: Wer sich rechtswidrig teilweise oder gänzlich Zugang in ein

³¹ *Yenidünya/Değirmenci*, S. 18 ff.; *Dülger* (Fn. 12), S. 36 ff.; *Karagülmez* (Fn. 10), S. 31 <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518C> (08.07.2007).

³² *Yazıcıoğlu*, *Yeni Türk Ceza Kanunundaki*, S. 404.

³³ *Yazıcıoğlu*, *Yeni Türk Ceza Kanunundaki*, S. 404.

³⁴ <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518CA> (08.07.2007); *Dülger* (Fn. 12), S. 48.

³⁵ *Yazıcıoğlu*, *Kriminolojik, Sosyolojik...*, S. 227; *Ersoy*, S. 168-169.

³⁶ *Dülger* (Fn. 12), S. 68.

Informatiksystem verschafft und darin verbleibt, wird mit einer Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.³⁷

Während Abs. 2 des § 243 die Tathandlung des Abs. 1 bei entgeltlichen Systemen als Milderungsgrund behandelt, wird im letzten Absatz dieser Norm die Veränderung oder Löschung der Daten als Strafverschärfungsgrund angesehen. Im § 243 wurde die Regelung „Wer sich rechtswidrig ganz oder teilweise Zugang in ein Informatiksystem verschafft oder darin weiterhin verbleibt“ eingeordnet und die Strafe für das Tatbestandsmerkmal „Zugang verschaffen und darin weiterhin verbleiben“ festgehalten. Aber die Norm des Entwurfes von 2003, welche die Strafbarkeit des unbefugten Zugangs in ein Informatiksystem regelte, beinhaltet den Wortlaut „wer sich zu einem Informatiksystem Zugang verschafft und darin verbleibt“. Durch die stattgefundene Debatte in der Generalversammlung des Parlaments und nach Zustimmung des Änderungsvorschlags, bekam die strafbegründende Tathandlung die Fassung: „Wer sich zu einem Informatiksystem Zugang verschafft und darin verbleibt“.

Die im Entwurf geregelte Norm zeigt Parallelen zum § 323 Abs. 3 des französischen- und zum § 615 des italienischen Strafgesetzbuches. „Zugang ins System verschaffen“ und „darin weiterhin verbleiben“ stellen zwei alternative Tathandlungen dar. Durch die im Wortlaut der Norm vorgenommene Veränderung wurden diese zwei Tatbestände zu einem Tatbestand zusammengefasst und lauten nun: „Zugang ins Informatiksystem verschaffen und darin weiterhin verbleiben“.³⁸

Es fällt jedoch auf, dass bei der Regelung dieser Norm mit wenig Sorgfalt gearbeitet wurde. Die im Entwurf enthaltene Tathandlung „zu einem Informatiksystem Zugang verschaffen oder darin verbleiben“ wurde zwar bei der Verhandlung bezüglich des Gesetzes als „in ein Informatiksystem Zugang verschaffen und darin verbleiben“ geändert, aber diese Veränderung kam in der Begründung nicht vor. Im Wortlaut des Gesetzes wurde also ein „und“ verwendet, während in die Begründung ein „oder“ genommen wurde.³⁹

Obwohl im Wortlaut der Norm der Zugang ins Informatiksystem und das darin Verbleiben eine einheitliche Tathandlung zu sehen ist, lautet die Überschrift nur „Zugang ins Informatiksystem“: Daher findet man bei der Abfolge der Vollendung der Tat eine Unstimmigkeit vor. Auch in § 243 Abs. 2 kommt es durch den Wortlaut „die Handlungen im 1. Absatz“ zu einer Diskrepanz und erweckt den Anschein, als ob es

³⁷ Erdağ, Ekonomi, Sanayi ve Ticarete İlişkin suçlar ve Bilişim Suçları, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

³⁸ Ketizmen, Türk Ceza Hukukunda Bilişim Suçları (Diss.), Ankara, 2006, S. 96.

³⁹ Karagülmez (Fn. 10), S. 166.

mehrere Tathandlungen geben würde. Aber eigentlich stellt die Handlung „Zugang ins Informatiksystem verschaffen und darin weiterhin verbleiben“ nur eine Tathandlung dar.⁴⁰

Über das Rechtsgut des in § 243 geregelten unbefugten Zugangs ins Informatiksystem wurden verschiedene Ansichten vertreten. Nach *Kurt* ist der unberechtigte Zugang ins Informatiksystem zugleich ein Eindringen in die Privatsphäre der betroffenen Systemeigentümer.

Er ist der Meinung, „*dass das geschützte Rechtsgut bei dem Zugang ins Informatiksystem und des darin weiterhin Verbleibens, das Beschützen der Privatsphäre und des Datengeheimnisses darstellt. Das Informatiksystem und die darin befindlichen Daten und Programme und die Privatsphäre der Systemeigentümer gehören auch dazu. Durch diesen Straftatbestand wurde versucht zu verhindern, dass durch Eindringen in dieses System das Sicherheits- und Wohlfühl gestört wird*“.⁴¹

Dülger ist der Ansicht, dass der Rechtsbereich des § 243, der die Strafbarkeit des unberechtigten Zugangs regelt, eine gemischte Eigenschaft trage. Durch die Verhinderung des unberechtigten Zugangs ins Informatiksystem wären viele Vorteile seitens der Systemeigentümer und -benutzer geschützt.

Weiterhin könne es unterschiedliche rechtliche Werte, wie Vorteile dieser Personen, Datenschutz, die Unantastbarkeit ihrer Privatsphäre oder das für Personen oder Anstalten notwendige Sicherheitsgefühl, geben. Im und über die Wirkung dieser Werte, die der Autor als unterschiedliche Arten von Vorteilen beschreibt, die „Sicherheit des Informatiksystems“ zu gewährleisten, bilde den eigentlichen Rechtsbereich.⁴²

Für die Erfüllung der Straftat des § 243 reicht ein vollständiger oder teilweise verschaffter Zugang ins System nicht aus, es muss auch ein Verbleiben im System stattfinden. Sich einen Zugang ins System zu verschaffen und dort eine Zeit zu verbleiben, stellt im Ganzen den Tatbestand des § 243 dar.⁴³ Wie am Anfang erwähnt, führt die Regelung des Tatbestandsmerkmals in dieser Form zur Veränderung des Charakters der Straftat. Hier sind besonders die Bedeutung und der Umfang des Ausdrucks „das Verbleiben weiterführen“ wichtig.

Unter der Annahme, dass das Verschaffen eines Zugangs in ein System und das dortige Verbleiben zwei unterschiedliche und voneinander unabhängige Handlungen

⁴⁰ *Karagülmez* (Fn. 10), S. 168.

⁴¹ *Kurt* (Fn. 7), S. 148.

⁴² *Dülger* (Fn. 12), S. 213 ff.

⁴³ *Yazıcıoğlu*, *Yeni Türk Ceza Kanunundaki*, S. 406; *Eker*, *Türk Ceza Hukukunda Bilişim Suçları*, TTB Dergisi, Sayı 62, Ankara, 2006, S. 122.

darstellen sollen, kommt man zu dem Ergebnis, dass für die Strafbarkeit des unberechtigten Zuganges i.S.v. § 243 mehr als eine Tathandlung notwendig ist. Wie es Straftaten mit mehreren Tathandlungen verlangen, reicht es bei dieser Norm nicht aus, sich nur einen Zugang zu dem System zu verschaffen, sondern das Tatbestandsmerkmal „dort zu Verbleiben“ muss vorliegen, damit der Straftatbestand erfüllt ist.⁴⁴ Wenn nun der Zugang und das dortige Verbleiben keine unterschiedlichen, voneinander unabhängigen Handlungen darstellen, kommt man folglich zu dem Ergebnis, dass die in der Norm geregelte Straftat eine zwangsläufig fortführende Straftat ist. Der Umstand, das über den Zugang zum System ein darüber hinaus gehendes Aufhalten in diesem System gefordert wird, dient dem Zweck, dass zur Vollendung der Straftat eine gewisse Zeitspanne vorliegen muss.⁴⁵

§ 234 setzt ferner einen rechtswidrigen Zugang voraus. Wenn nun der Zugang zu dem System im Rahmen des Rechtlichen erfolgt ist, später diese Einwilligung erst aufgehoben wird oder andere Umstände gegeben sind, die ein weiteres Verbleiben in dem System rechtfertigen, ist § 234 somit nicht einschlägig.⁴⁶

In § 243 wurden bezüglich der Vollendung dieser Straftat keine speziellen Regelungen getroffen. Wie auch bei der Begründung der Norm ausdrücklich erläutert wurde, spielt die Absicht der Person, die sich rechtswidrig Zugang in ein System verschafft, um an bestimmte Daten zu gelangen, hier keine Rolle. Bereits der rechtswidrige Zugang ins System reicht für die Erfüllung des Straftatbestandes aus. Das Delikt stellt kein Verletzungsdelikt dar, sondern eher ein Gefährdungsdelikt.⁴⁷ Da in der Norm bezüglich der Tathandlungen des Zugang ins Informatiksystem und dem dort Verbleiben die Rechtswidrigkeit besonders hervorgehoben wurde, wird die Ansicht vertreten, dass diejenigen bevorzugt werden müssten, die ohne Verschulden nicht wissen konnten, dass die begangene Handlung eine Straftat darstellt.

Nach Abs. 2 des § 243 liegt ein Strafmilderungsgrund vor, wenn die Tathandlung bei entgeltlichen Systemen begangen wurde. Es wird jedoch nicht erläutert, was unter einer entgeltlichen Datenbank zu verstehen ist und warum bei einem solchen Fall ein Strafmilderungsgrund vorliegt.

Nach *Dülger* umfasst der Begriff entgeltliche Systeme im Allgemeinen vier Situationen:

⁴⁴ Kurt (Fn. 7), S. 151.

⁴⁵ Karagülmez (Fn. 10), S. 170 ff.

⁴⁶ Ketizmen (Fn. 38), S. 130.

⁴⁷ Karagülmez (Fn. 10), S. 171.

- 1) Web-Seiten, die ihre Dienstleistungen gegen eine Gebühr übers Internet anbieten.
- 2) „Internet-Cafés“, in denen das System gegen eine bestimmte Gebühr angemietet wird.
- 3) Anbieten bestimmter Systeme gegen Gebühr durch ein Unternehmen (z. B. anhand der geschlossenen Verträge, über das Internetsystem an Personen zwecks Werbung, SMS verschicken).
- 4) Das Anschließen einer Internetverbindung über einen bestimmten Zeitraum oder Quartal.⁴⁸

Nach *Karagülmez* ist das Benutzen des Systems gegen eine Gebühr im Internet-Café und ähnliche Stellen in diesem Zusammenhang nicht zu erwägen, da im Gesetz nicht der Ort, an dem das System benutzt wird, sondern die entgeltlichen Dienstleistungen, die auf dem elektronischen Teil des Systems angeboten werden, ausdrücklich genannt werden. Auch die Internetverbindung für eine bestimmte Zeit ist nach seiner Meinung nicht unter diesen Absatz zu subsumieren.⁴⁹

Yazıcıoğlu interpretiert den Zugang in Systeme, die ihre Dienstleistungen gegen eine Gebühr anbieten, als Strafmilderungsgrund und begründet diese Auslegung mit dem breiten Anwendungsbereich der Strafbarkeit wegen unberechtigten Zugangs als zutreffend.⁵⁰

Der unberechtigte Zugang und das Verändern oder Löschen von Daten im System wird im letzten Absatz des § 243 als Strafverschärfungsgrund angenommen.

Laut *Erdağ* handele es sich in diesem Absatz um ein erfolgsqualifiziertes Delikt (§ 23 türk. StGB), d.h. der Straferhöhungsgrund liegt auch dann vor, wenn der Täter bei dem Verändern oder Löschen der Daten ohne Vorsatz gehandelt hat. Falls diese Handlungen allerdings vorsätzlich begangen wurden, kommt Abs. 2 des § 244 in Betracht.⁵¹ Wir stimmen der Ansicht des Verfassers nicht zu.⁵² Mit der im letzten Absatz vorgesehenen Anwendung der Straferhöhung und zwischen den im ersten oder im zweiten Absatz geregelten Voraussetzungen, sieht das Gesetz bezüglich des Strafmaßes keine Differenzierung vor.⁵³

⁴⁸ *Dülger* (Fn. 12), S. 227.

⁴⁹ *Karagülmez* (Fn. 10), S. 175 ff.

⁵⁰ *Yazıcıoğlu*, *Yeni Türk Ceza Kanunundaki...*, S. 406.

⁵¹ *Erdağ*, *Ekonomi, Sanayi ve Ticarete İlişkin suçlar ve Bilişim Suçları*, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

⁵² Detaillierte bilgi ve eleştiri için bkz. *Özbek*, TCK. İzmir Serhi, Ankara, 2006, S. 306 vd.

⁵³ *Erdağ*, *Ekonomi, Sanayi ve Ticarete İlişkin suçlar ve Bilişim Suçları*, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

II. § 244 türk. StGB – Beschädigung des Informatiksystems und der Daten

1. In der Zeit des alten türkischen StGB wurde die „Beschädigung des Informatiksystems und der Daten“ im Zusammenhang mit der „Sachbeschädigung“ bewertet. Diese Beziehung ist sogar auch in der Erläuterung die „Beschädigung des Informatiksystem und der Daten“ als ein besonderer Abschnitt der „Sachbeschädigung“ zu sehen.

Dönmezer vertritt die Ansicht, dass die Unantastbarkeit des Computers die Funktionsfähigkeit des Systems und den sinngemäßen Gebrauch ihres Inhaltes vorausgesetzt werde. Auf diese Weise würden in erster Linie eigentlich die Vorteile des Eigentümers oder des Benutzers geschützt.⁵⁴

Yazıcıoğlu ist ebenfalls der Meinung, dass durch diese Straftat – bezogen auf das System und der im System vorhandenen Komponenten – das Eigentumsrecht der Eigentümer besser geschützt werde.⁵⁵

Nach *Önder* ist der Schutzbereich dieser Straftat allerdings strittig. Es gäbe einige Verfasser, die der Meinung seien, dass dieses Delikt die im Computer vorhandenen Daten der betroffenen Personen schütze und es gäbe weiterhin Verfasser, die vertreten, dass die vorhandenen Daten funktionsgemäß in der Landeswirtschaft und in der Verwaltung entstehen würden und das daher anzunehmen sei, dass diese Straftat eine gegen das Wirtschaftsleben begangene Straftat darstellt.⁵⁶

Nach *Ersoy* beschütze dieser Straftatbestand das Eigentum der Personen.⁵⁷

Und *Dülger* vertrat die Ansicht, dass der Schutzbereich dieser Straftat eine gemischte Eigenschaft aufzeige, weil neben den abstrakten aus Daten und Software bestehenden Komponenten eines Datenverarbeitungssystems auch Ausstattungselemente unter Schutz gestellt werden.⁵⁸

2. Das Verhindern oder Zerstören der Funktionsweise eines Systems wird in § 244 Abs. 1 türk. StGB wie folgt definiert: „Wer die Funktionsweise eines Systems verhindert oder zerstört, wird mit einer Freiheitsstrafe von einem Jahr bis zu fünf Jahren bestraft“. Die „Verhinderung der Funktionsweise eines Systems“ und die „Zerstörung der Funktionsweise eines Systems“ sind alternative Tathandlungen des

⁵⁴ *Dönmezer* (Fn. 14), S. 622.

⁵⁵ *Yazıcıoğlu*, Kriminolojik, Sosyolojik..., S. 259-260.

⁵⁶ *Önder*, Sahislara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul, 1994, S. 508.

⁵⁷ *Ersoy* (Fn. 25), S. 167.

⁵⁸ *Dülger* (Fn. 12), S. 231 ff.

Straftatbestandes des § 244 Abs. 1 türk. StGB.⁵⁹ Im Gesetz werden Verhinderung und Zerstörung nicht definiert. Die Verhinderung der Funktionsweise eines Systems führt zu einem andauernden oder nur vorübergehenden Verhindern der Funktionsweise der verschiedenen Bereiche des Systems. Daher muss jede Art von Eingreifen in ein System in diesem Umfang bewertet werden.⁶⁰

Unter vollständiger Funktionsunfähigkeit des Systems wird das Beschädigen der Systemfunktion verstanden, also jede Veränderung der Verfahren eines Systems, welche es unter gewöhnlichen Umständen durchführt sowie die durch einen nicht gerechtfertigten Eingriff vorübergehende oder ganzliche Zerstörung der korrekten Funktionsweise des Systems.⁶¹

§ 244 Abs. 2 türk. StGB lautet folgendermaßen: „Wer im System gespeicherte Daten zerstört, löscht, verändert oder unzugänglich macht, Daten im System speichert oder vorhandene Daten weiterleitet, wird mit einer Freiheitsstrafe von 6 Monaten bis zu drei Jahren bestraft.“

Die erste alternative Tathandlung des Paragraphen ist die „Löschung der Daten“, die im Informatiksystem gespeichert sind. Das Löschen der im Datenverarbeitungssystem gespeicherten Daten, das Zerstören der Daten und das Vernichten kann als Verlust des Herrschaftsbereiches des Anspruchsinhabers, den er nicht mehr oder nur mit hohem Aufwand wiedererlangen kann, definiert werden.⁶²

Im § 244 Abs. 2 wird nicht, wie im § 525b des alten türkischen StGB, auf die Löschung der Daten eingegangen, sondern auf die Zerstörung der Daten. Vor diesem Hintergrund muss diskutiert werden, ob die Löschung der Daten im Informatiksystem unter den Begriff der Zerstörung fällt oder nicht.

Das Löschen und Zerstören von Daten ist laut *Yazicioglu* gleichbedeutend, da mit dem Löschen gemeint ist, dass die am Speicherplatz vorhandenen Daten zerstört werden.⁶³

Nach diesem Autor kommt eine körperliche Zerstörung nicht in Frage. Die Löschung soll sachlich verstanden werden, da bezüglich des Zugangs zu den gelöschten

⁵⁹ *Erdağ*, Ekonomi, Sanayi ve Ticarete İlişkin suçlar ve Bilişim Suçları, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

⁶⁰ Der türkische Kassationshof legt es parallel dazu aus, vgl. 4. Senat des Kassationshofs, Urt. v. 28.02.2000, 2000/1068 E. – 2000/1771 K.; 11. Senat des Kassationshofs, Urt. v. 24.10.2002, 2002/5771 E. – 2002/8416 K.

⁶¹ *Dülger* (Fn. 12), S. 234.

⁶² *Ketizmen* (Fn. 13), S. 169.

⁶³ *Yazicioğlu*, Kriminolojik, Sosyolojik, S. 263.

Komponenten, die Aufhebung von notwendigen Verbindungen und die Unlesbarkeit von Daten gemeint ist.

In diesem Zusammenhang hat nach *Önder* das Löschen eine deskriptive und logische Bedeutung und er definiert sie als die Zerstörung der vorhandenen Verbindung, die dafür gebraucht wird, um an ein Programm zu gelangen.⁶⁴

Die „*Unerreichbarkeit der Datei*“ ist die Verhinderung des gewöhnlichen Zuganges zu der Datei, ohne Eingriff in die Datei, wobei die Datei bezüglich des Inhaltes in seiner Gesamtheit geschützt wird. Die Datei wird weder zerstört noch geschädigt, aber die notwendige Verbindung für den Zugang zu den Dateien ist abgebrochen.⁶⁵

Das „*Weiterversenden der im System enthaltenen Datei*“ stellt in § 244 Abs. 2 die letzte der möglichen Tatausführungshandlungen dar. Die Übertragung der im Informatiksystem enthaltenen Dateien außerhalb des Informatiksystems auf ein anderes Informatiksystem oder auf einen Datenträger sowie das Speichern oder Kopieren wird als Weiterversendung der Dateien gewertet.⁶⁶

Bei einer Gesamtprüfung der Norm ist erkennbar, dass die Tatausführungshandlungen eines Eingriffs in ein System und in eine Datei geregelt sind. Diese Tatausführungshandlungen, die das Funktionieren oder die Benutzung eines Systems oder einer Datei verhindern, sind allgemein geregelt.

In Abs. 3 wird ein Strafverschärfungsgrund aufgeführt. Falls die in Abs. 1 und 2 bezeichneten Handlungen gegen Informatiksysteme von Banken, Kreditvereinigungen oder öffentliche Institutionen begangen werden, wird die in den Abs. 1 und 2 vorgesehene Strafe gemäß § 244 Abs. 3 um die Hälfte erhöht.

Abs. 4 stellt das „für sich oder für einen Dritten Vorteile ziehen“ durch die in den Abs. 1, 2 und 3 geregelten Tathandlungen unter Strafe, wenn diese Handlungen keinen anderen Straftatbestand erfüllen.

Bei der Analyse des letzten Absatzes des § 244 ist aus dem Wortlaut des Paragraphen zu entnehmen, dass nur wenn die Handlung keinen anderen Straftatbestand erfüllt, die Regelung des betreffenden Paragraphen einschlägig ist. Gemäß dieser Regelung kommt also nur eine Verurteilung nach diesen Paragraphen in Betracht, wenn die Handlung nach türk. StGB oder nach den anderen Sondergesetzen nicht strafbar ist.⁶⁷

⁶⁴ *Önder* (Fn. 56), S. 509.

⁶⁵ *Dülger* (Fn. 12), S. 237.

⁶⁶ *Dülger* (Fn. 12), S. 238.

⁶⁷ *Karagülmez* (Fn. 10), S. 193.

Während im Paragraphen die Formulierung „keine andere Strafbarkeit begründen“ genutzt wurde, heißt es in der Begründung des Paragraphen wie folgt: „*Aber um nach diesem Paragraphen des Absatzes eine Bestrafung verhängen zu können, darf die Tathandlung keine Straftat darstellen, bei der eine schwerwiegende Bestrafung verhängt werden muss. In dieser Hinsicht wird bei den Tathandlungen, wie z. B. Strafbarkeit wegen Betrug, Diebstahl, Untreue oder Unterschlagung, keine Bestrafung nach diesem Paragraphen des Absatzes verhängt.*“ Deutlich ist zu sehen, dass zwischen der Regelung und der Paragraphenbegründung ein Widerspruch besteht.

III. § 245 türk. StGB – Missbrauch von Bank- und Kreditkarten

Die im § 245 des neuen türk. StGB geregelte Strafbarkeit vom Missbrauch von Bank- und Kreditkarten wurde im alten türk. StGB im § 525 Abs. b Z. 2 geregelt. In diesem Paragraphen wurde der Missbrauch von Bank- und Kreditkarten nicht gesondert geregelt. Der Missbrauch von Bank- und Kreditkarten kam in der Türkei jedoch oft vor. Gericht und dieser Paragraph wurde für eine andere Regelung fast nie eingesetzt.⁶⁸ Deswegen war es notwendig, eine besondere Regelung für den Missbrauch von Bank- und Kreditkarten zu finden.

Die Tathandlung des ersten Absatzes lautet: wer eine Bank- oder Kreditkarte, die einer fremden Person gehört oder an eine fremde Person abgegeben werden muss, in irgendeiner Weise in Besitz nimmt, benutzt oder benutzen lässt [...].⁶⁹ Bei der Definition der Handlung wird nicht beschrieben, auf welche Weise die Karte in Besitz genommen wird, sondern nur, dass es sich dabei um eine rechtswidrige Besitzaufnahme handeln muss. Es wird also keine Eingrenzung – wie z. B. Betrug, Diebstahl⁷⁰, Untreue⁷¹ oder Unterschlagung⁷² – bei der erforderlichen rechtswidrigen Besitzaufnahme vorgenommen.⁷³ Mit anderen Worten wurde die Trennung des alten türk. StGB, auf welche Art und Weise eine Karte in Besitz genommen wird, abgeschafft und jede Art einer rechtswidrigen Besitzaufnahme einer Karte unter Strafe gestellt.⁷⁴ Wichtig ist, dass durch die Handlung ein rechtswidriger Nutzen erzielt wird. Dabei werden die von der „Kredit- und Kartenabteilung“ ausgestellten Bank- und Kreditkarten mittels

⁶⁸ Özel (Fn. 20), S. 862.

⁶⁹ Vgl. Großer Senat des Kassationshofs, Urt. v. 11.04.2000, 2000/6-62 E. – 2000/72 K.; 6. Senat des Kassationshofs, Urt. v. 24.09.2001, 2001/10933 E. – 2001/11095 K.

⁷⁰ Vgl. 6. Senat des Kassationshofs, Urt. v. 01.02.2002, 2001/17027 E. – 2002/1016 K.

⁷¹ Vgl. 11. Senat des Kassationshofs, Urt. v. 06.10.2003, 2003/6778 E. – 2003/6714 K.

⁷² Vgl. 6. Senat des Kassationshofs, Urt. v. 05.02.2002, 2001/16231 E. – 2002/1149 K.

⁷³ Kurt (Fn. 7), S. 178; Dülger (Fn. 12), S. 254; Karagülmez (Fn. 10), S. 196 ff.

⁷⁴ Akbulut, S. 21 ff.

beauftragter Mitarbeiter ihren Inhabern, privaten Verteilungsunternehmen, Post und Bankfilialen übergeben.

Auf diese Art und Weise kann das rechtswidrige Benutzen oder Benutzen lassen der Karte durch denjenigen, der im Besitz der Karte ist, strafbar sein.⁷⁵ Jedoch ist bei einer solchen Situation die Bank der Geschädigte, da die Karte ihren Eigentümer noch nicht erreicht hat.⁷⁶ Obwohl der mit der Übergabe der Karte beauftragte Mitarbeiter die Bank- und Kreditkarte nicht abgibt, sich nicht durch Benutzung dieser Karte bereichert und einen Vertrauensmissbrauch begeht, wird dieser Sachverhalt speziell geregelt.

Die Tathandlungen des zweiten Absatzes sind das Eingreifen in fremde Konten sowie das Fälschen, Verkaufen, Übergeben, Kaufen oder Annehmen von Bank- oder Kreditkarten. Die in diesem Absatz aufgeführten Handlungen wurden als Auffangtatbestände zum Straftatbestand des dritten Absatzes aufgenommen, da das sich ungerechtfertigte Bereichern durch das Benutzen einer gefälschten Karte den Straftatbestand des Abs. 3 erfüllt. Dieser Absatz war im ersten eingeführten türk. StGB nicht vorhanden. Daten über eine Bank- und Kreditkarte in Besitz zu nehmen, war vor dem 08.07.2005, falls dies keine andere Straftat darstellte, nicht unter Strafe gestellt, sondern nur die Erstellung von gefälschten Bank- und Kreditkarten. Diese Lücke wurde mit diesem Absatz geschlossen.⁷⁷

Das Benutzen einer gefälschten Bank- und Kreditkarte oder das Betrügen durch das Benutzen einer Bank- und Kreditkarte bilden die Tathandlungen des Abs. 3. Die Straftat des Absatzes umfasst mehrere Tathandlungen. Nachdem eine gefälschte Karte hergestellt wurde, ist die Tathandlung erst durch das Erfüllen der Grundtatbestandsmerkmale verwirklicht. Das erste Grundtatbestandsmerkmal ist, dass die Karte letztendlich benutzt wurde und das zweite Merkmal, dass der Täter für sich oder für einen anderen einen Vorteil erlangt hat.⁷⁸

Im Abs. 4 ist ein Strafmilderungsgrund aufgeführt. Falls die im Abs. 1 geregelten Tathandlungen gegen den Ehemann und/oder die Ehefrau, die Verwandten in gerader Linie, Adoptiveltern, Adoptivkinder, Stiefeltern, Stiefkinder, Schwiegereltern und Schwäger, die Geschwister, die im selben Haus leben, begangen werden, werden diese Tathandlungen nicht unter Strafe gestellt.

⁷⁵ 11. Senat des Kassationshofs, Urt. v. 17.02.2004, 12910 E. – 827 K.

⁷⁶ *Donay*, Bankacılık Ceza Hukuku, İstanbul, 2007, S. 168 ff.

⁷⁷ *Ekinci/Esen*, Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli İflas ve Taksirli İflas Karşılıksız Yararlanma Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara, 2005, S. 370.

⁷⁸ *Ekinci/Esen* (Fn. 77), S. 372.

Die Bankkarte verschafft einen rechtlichen Zugang zum System der Bank. Durch diese Karte kann der Karteninhaber mit einer festgelegten Nummer, die ihm bekannt ist, ohne Hilfe eines Sachbearbeiters von seinem Konto Geld abheben. Und Kreditkarten ermöglichen entsprechend eines abgeschlossenen Vertrages zwischen der Person und der Bank die Nutzung von Krediten, die von der Bank unter bestimmten Konditionen der Person gewährt worden sind. Demnach ist der Missbrauch dieser Karten, in dem hier ausgeführten Paragraphen als Straftat geregelt.⁷⁹

Laut der Begründung dieses Paragraphen erfüllen die unten beschriebenen Handlungen folgende Straftaten:

1. Eine fremde Bank- oder Kreditkarte auf irgendeine Weise in Besitz nehmen und diese ohne Einwilligung des Eigentümers zu benutzen oder benutzen lassen und dadurch sich oder eine andere Person ungerechtfertigt bereichern.

2. Das Benutzen und Benutzen lassen einer fremden Bank- oder Kreditkarte unter den gleichen oben genannten Voraussetzungen, bei der die Karte eigentlich dem Inhaber zurückgegeben werden muss; der Sachbearbeiter in der Bank, der eigentlich die Aufgabe hat, die Karte dem Inhaber zu geben, die Karte jedoch nutzt, um sich oder jemand anderen zu bereichern. Um Handlungen wie Diebstahl, Betrug, Vertrauensmissbrauch sowie deren ratio legis, als auch Unterschiede in der Rechtsprechen vorzubeugen, wurden diese Handlungen zu unabhängigen Straftaten erklärt.

IV. § 246 türk. StGB – Die Verantwortung der juristischen Personen für die Informatikdelikte

Im § 246 mit der Überschrift „Anwendung der Sicherungsmaßnahmen für juristische Personen“ wird festgelegt, dass im Falle einer Straftat, die in diesem Abschnitt geregelt wurde, juristische Personen unrechtmäßig Vermögen erlangen, die dafür bestimmte Sicherungsmaßnahmen angewandt wird. Zwar werden gemäß § 20 Abs. 2 juristische Personen nicht unter Strafe gestellt, hier handelt es sich jedoch um die vorgesehenen Sicherungsmaßnahmen.⁸⁰ Diese entsprechenden Sicherungsmaßnahmen werden in § 60 wie folgt geregelt:

1. Ungültigmachen der Tätigkeitserlaubnis.
2. Beschlagnahmung der durch die Straftat erworbenen Sachen.

⁷⁹ Vgl. Erläuterung § 245 türk. StGB.

⁸⁰ Karagülmez (Fn. 10), S. 223.

Die Beschlagnahmung der durch die Straftat erworbenen Sachen ist klar, aber es gibt zwei Voraussetzungen, um eine Tätigkeitserlaubnis ungültig zu machen.⁸¹

a) Eine Erlaubnis, die von der entsprechenden Institution für den bestimmten Tätigkeitsbereich gegeben wird.

b) Ein vorsätzlicher Missbrauch der Erlaubnis, um für die juristische Person Vorteile zu ziehen.⁸²

F. Fazit und Ausblick

Der Bedarf einer umfassenden Modernisierung des türkischen Strafrechts wurde bereits seit langem diskutiert. Zur Diskussion standen neben dem Strafgesetzbuch auch die Strafprozessordnung und das Strafvollzugsrecht. In dieser Modernisierungstendenz spielen die Informatikdelikte eine sehr wichtige Rolle. Denn der wichtigste Zweck dieser Reformbemühungen ist die Abdeckung der veränderten gesellschaftlichen Bedürfnisse als ein gesellschaftliches Subsystem. In diesem Zusammenhang handelt es sich um aktuelle Probleme der modernen (Informations-, bzw. sogar Risiko-) Gesellschaft. Weil die Informations- und Kommunikationstechnologien und gleichzeitig deren Probleme den Hintergrund der modernen Gesellschaft bilden, erscheint es natürlich auch in diesem Bereich wünschenswert, dass die mit den genannten Gründen bestimmte Umfassung durch den Gesetzgeber zweckmässig geregelt wird. Vor diesem Hintergrund möchte ich festhalten, dass die Regelungen im Bereich der Informatikdelikte nicht genügen. Wie ich festgestellt habe, gibt es viele begriffliche Unklarheiten (z. B. in welchem Teil des StGB sie geregelt werden) und Definitionsfehler (z. B. die des Informatiksystems) und -mängel (z. B. die des Computers, das des entgeltlichen Informatiksystems ect.). Hinzukommt die gefährliche Differenz zwischen den Gesetztexten und deren Erläuterungen (z.B. § 243, 245). Der Gesetzgeber müsste diese Normen vor der technologischen Wirklichkeit und mit Sorgfalt erneut wieder diskutieren, um sie dann umzuschreiben.

⁸¹ Zur Kritik vgl. *Yıldız*, 5237 Sayılı TCK. Seminer Notları, İstanbul, 2007, S. 34.

⁸² *Karagülmez* (Fn. 10), S. 224.

İnternet (=Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukukundaki Yeni Gelişmeler

Arş. Gör. İlker Tepe¹

A. Giriş

Günümüzde bilişim teknolojilerinin yansımalarının görülmediği hiçbir sosyal yaşam alanı düşünülemez. Bilişim ve Telekomünikasyon teknolojilerinin etkisi günlük yaşamın birçok alanında kendini hissettirmektedir. Öyle ki artık modern toplumun üstlendiği işlev internetin işlevselliği ile eş değer görülmekte ve hatta modern toplum bu yönüyle “bilgi toplumu” olarak anlandırılmaktadır. Böyle bir durum bilgi toplumunun açısından hukuk düzeninin ön kabullerini geniş özgürlüklerden yana tavırla şekillendirecek ve devlet ve hukuku bu tutum içinde değerlendirecektir. Bu da teknolojik alt yapıların yeni yaşam formlarının ortaya çıkmasına sebebiyet vermesini sağlayacaktır. Tabi ki bu tespit modern ceza hukukunu doğru bir biçimde algılamak adına oldukça önemlidir. Çünkü modern ceza hukuku tasarımı ile modern toplumunun yeni problemlerine etkili ve amacına uygun çözümler bulmaya çalışılmaktadır.² Az önce de ifade edildiği gibi modern toplum bilgi toplumu olarak kabul edildiği için, modern topluma ait problemlerin (ceza) hukuksal görünüşleri diğerlerine oranla daha çok önem kazanmıştır.³ Bu bağlamda Bilgisayar ve İnternet (Bilişim) Ceza Hukuku bilgi toplumunu doğrudan ilgilendiren hukuk alanları olarak önceliğe sahiptir.

1.7.1926 tarihinde kabul edilen Türk Ceza Kanununun 1889 tarihli İtalyan Ceza Kanunu (Codice Zanardelli) mehzaz alınarak ortaya çıkartılmıştır. 592 maddeden oluşan bu kanunun tarihsel süreç içinde neredeyse yarısı değişikliğe uğramış, bu güne kadar yaklaşık 60 kez “tadilat” a maruz kalmıştır. Bu da Türk Ceza Kanununda ciddi bir reform gerekliliğini 1930’lu yıllardan sonra ortaya koymuş ve bu düşünce meyvesini 1 Haziran 2005’de vermiştir. Bu reform hareketi sadece Türk Ceza Kanunu ile sınırlı olmayıp beraberinde Ceza Muhakemesi Kanunu, Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun ve diğer yan kanunlarla da desteklenmiştir. İşte ben bu tebliğimde modern toplumun ceza hukuku bakımından en önemli görünümü olan bilişim suçlarına

¹ Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D.

² Ünver, Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer, Ankara, 2003, S. 443.

³ Ünver, Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısı’nın İnternet Açısından Değerlendirilmesi, IUHFM, C: LIX – S: 1-2, İstanbul, 2001, S. 61 vd.

ilişkin düzenlemeleri 2005 yılında yürürlüğe giren yeni TCK'ya göre Türk Hukukunda ortaya çıkan aktüel gelişmeler ışığında özetlemeye çalışacağım.

B. Bilişim Suçlarının Tarihsel Süreçteki Gelişim Çizgisi

Türk Ceza Hukukundaki Bilişim Suçlarıyla ilgili tartışmalar geçmeden önce farklı görünüşleri ortaya koymak adına 2004 yılına kadar yaklaşık yirmi yıllık tarihsel gelişim sürecini çözümlenmek yerinde olacaktır.

1. 1989 TCK Ön Tasarısı

1984 yılında bir komisyon yeni bir Ceza Kanunu tasarısı hazırlamak için bir araya gelmiş ve çalışmalarını tamamlayarak tasarımı 1987 yılında ortaya çıkarmışlardır. Fakat oldukça eleştiri toplayan bu tasarı ikinci bir komisyonla yeniden ele alınmış ve 1989 yılında yeni tasarı tamamlanmıştır.⁴ 1989 TCK. Ön Tasarısı olarak adlandırılan bu tasarının bilişim suçları bakımından önemi, ilk kez bu tasarıyla bilişim suçları Türk Hukuk Sistemine alınmış olmasından kaynaklanmaktadır. Söz konusu suçlar “Topluma Karşı Suçlar” başlıklı ikinci kısmının dokuzuncu bölümünde yer almıştır ve toplam beş maddeden oluşmaktadır. Bu maddeler 1989 TCK. Ön Tasarısında düzenlenen haliyle özetlenecek olursa;

“Hile ile bilgi elde etme ve bunları haksız kullanma” başlıklı 342. maddesinde bilgileri otomatik işleme tabi tutmuş bir sistemden programları, verileri veya herhangi bir unsuru hukuka aykırı olarak ele geçirme ve bilgileri otomatik işleme tabi tutulmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere nakletme ve çoğaltma fiilleri suç olarak düzenlenmiştir.⁵

“Yarar sağlama, zarar verme” başlıklı 343. maddesi başkasına zarara verme veya kendisine yarar sağlamak amacıyla bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya sistemin işlemesine engel olma ile bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlama fiillerini düzenlemiştir.⁶

⁴ *Hakeri*, Tötungsdelikte im Türkischen StGB-Entwurf 1997, http://www.akader.info/KHUKA/7_2000_ekim/totungsdeligte.htm (08.07.2007).

⁵ *Yazıcıoğlu*, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, İstanbul, 1997, S. 208.

⁶ *Yazıcıoğlu*, Kriminolojik, Sosyolojik..., S. 208.

“Sahtecilik” başlıklı 344. maddesinde ise, delil olarak kullanılmak amacıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri, diğer unsurları tahrif etmek veya bunları kullanma fiili suç olarak düzenlenmiştir.⁷

“Feri cezalar” başlıklı 345. maddesinde, 342 ve 343. maddelerde belirtilen suçları işleyen failler hakkında öngörülen cezalara ek olarak, kamu hizmetinden veya sanat veya ticaretten yasaklanma, suçtan meydana gelen şeylerin müsadresi, suçun işlenmesinde kullanılan kurumların veya teşebbüsün kapatılması öngörülmüştür.⁸

“Tüzel kişiler ve teşebbüs hali” başlıklı 346. maddesinde bütün bölümü kapsayacak bir hüküm getirerek, bu bölüme giren suçlardan dolayı tüzel kişilerin de sorumlu olduğu, teşebbüs halinde ise tamamlanmış suçun cezasının verileceğinin belirtildiği görülmektedir.⁹

II. 3756 Sayılı Kanunla Gerçekleştirilen Düzenleme

Kanun koyucu 14.06.1991 tarih ve 3756 sayılı Kanunla 1989 TCK. Ön Tasarısı kısmen de olsa 765 sayılı TCK’ya eklenmiştir. Ön Tasarının bilişim suçlarına ilişkin maddeleri 525. maddenin sonuna eklemek üzere “Bilişim Alanında Suçlar” başlığı ile on birinci bölüm olarak eklenmiştir. Anılan Kanun ile yapılan düzenlemeler kısaca özetlenecek olursa;

TCK. m. 525/a olarak kanun metnine aktarılan düzenleme 1989 TCK. Ön Tasarısının 342. maddesinde öngörülen düzenlemeye (“Hile ile bilgi elde etme ve bunları haksız kullanma”) karşılık gelmektedir. Cezanın miktarı ve gerekçesi de dahil olmak üzere aynen aktarılmıştır.¹⁰

Aynı şekilde TCK. m. 525/b 1989 TCK. Ön Tasarısındaki 343. maddeye denk gelen düzenlemenin (“Yarar sağlama, zarar verme”) gerekçesi de dahil olmak üzere aynıdır.¹¹

TCK. m. 525/c maddesi ise kendisine karşılık gelen 1989 TCK. Ön Tasarısı’nın 344. maddesi (“Sahtecilik”) ile bazı yönleriyle farklıdır. “Yerleştirme ve tahrif etmenin”

⁷ Kurt, *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Hukukundaki Uygulaması*, Ankara, 2005, S. 120.

⁸ Kurt (Dipnot 7), S. 120.

⁹ Kurt (Dipnot 7), S. 120-121.

¹⁰ Karagülmez, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara, 2005, S. 126 vd.; *Yenidünya/Değirmenci*. Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, 2003, S. 54.

¹¹ Kurt (Dipnot 7), S. 122.

cezası Ön Tasarıyla aynı tutulmuştur. Ancak Ön Tasarıda “kullanma”ya da aynı cezayı öngörmüşken, 3756 sayılı Kanunda tahrif edilmiş olan verileri kullanmanın cezası için daha az bir ceza öngörülmüştür.¹² Bunun yanında Ön Tasarısından farklı olarak, tahrif edilmiş veri veya diğer unsurları kullanmanın “bilerek” yapılması hususu vurgulanmıştır.¹³

Feri Cezalarla ilgili 525/d maddesinde Ön Tasarının 345. maddesinden farklı müsadere ve kurum kapatma yer almamıştır.¹⁴ Ayrıca bu bölümdeki suçlardan tüzel kişilerin de sorumlu olduğuna ve teşebbüsün tamamlanmış suç gibi cezalandırılacağına ilişkin 1989 tarihli Öntasarının 346. maddesi alınmamıştır.¹⁵

III. 1997 TCK Ön Tasarısı

1997 TCK. Ön Tasarısı’nda yer alan bilişim alanındaki suçlar ile ilgili düzenleme 1994 Fransız Ceza Kanununu düzenlemesinden esinlendiği ve Fransız Ceza Kanununun 323–1 ila 323–7 maddesindeki suçlarla bir olduğu söylenebilir.¹⁶

Tasarının 347. maddesi “Bilişim sistemine girme, verileri tahrip ve bozma” başlıklı olup maddenin birinci fıkrasında, bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçu düzenlenmiş, ikinci fıkrasında ise bu fiil nedeniyle sistemin içerdiği verilerin yok edilmesi veya değiştirilmesi durumu ağırlaştırıcı neden olarak belirtilmiştir. Girme veya orada kalma fiili nedeniyle sistemin içerdiği bilgilere zarar verilecek olursa ayrıca birinci fıkradaki hükümden daha ağır bir ceza ile karşılanmaktadır. Üçüncü fıkrada sisteme hukuka aykırı olarak girmeye teşebbüs edilmesi halinde suç tanımlanmış bir suç gibi kabul edilmektedir. Söz konusu düzenlemenin ceza hukukunun suça teşebbüs edilmesi halinde, tamamlanmış suçtan daha hafif cezalandırılması yönündeki genel prensibi ile uyum içinde olmadığı kabul edilmiştir.¹⁷

İlk kez bu tasarıda “bilgileri otomatik olarak işleme tabi tutmuş sistem” kavramı yerine “bilişim sistemi” kavramı kullanılmıştır.

¹² Dülger, Bilişim Suçları, Ankara, 2004, S. 207.

¹³ Yazıcıoğlu, Kriminolojik, Sosyolojik..., S. 284.

¹⁴ Kurt (Dipnot 7), S. 124; Dönmezer, Kişiler ve Mala Karşı Cürümler, 16. Baskı, İstanbul, 2001, S. 623.

¹⁵ Yazıcıoğlu, Kriminolojik, Sosyolojik..., S. 209.

¹⁶ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirmesi, YÜHFD, C. II/ S 2, İstanbul, 2005, S. 394.

¹⁷ Kurt (Dipnot 7), S. 124.

Tasarının “Sistemi engelleme, bozma, haksız yarar sağlama” başlıklı 348. maddesinin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma ve bilişim sistemlerinden haksız yarar sağlama, ikinci fıkrasında da bilişim sistemine hukuka aykırı olarak veriler sokma veya sistemin içerdiği verileri yok etme, veya değiştirme suç olarak düzenlenmiştir. Üçüncü fıkrasında, bu fiillerle failin başkasının zararına ve kendisinin yararına haksız bir menfaat elde etmesi halinde cezanın ağırlaştırılacağı, son fıkrasında ise bu suçlara teşebbüs halinde faile tamamlanmış suçun cezasının verileceği belirtilmiştir.¹⁸

“Sahtecilik” başlığı taşıyan 349. maddesinde ise, hukuk alanında bir neticeye ulaşmak amacıyla sahte bir belge oluşturmak için bilişim sistemine veriler yerleştirme veya var olan verileri tahrif etme fiillerde, ikinci fıkrasında ise belirtilen sahte belgeyi kullanma suçu düzenlenmiştir. Bu anlamda madde ile düzenlenen alan ile 3756 sayılı kanunla yapılan düzenleme arasında bir farklılık yoktur. Tek fark, “bilişim sistemi” kavramının yerine “bilgileri otomatik olarak işleme tabi tutmuş sistem” ifadesinin yerine kullanılması ve belgeyi düzenleyen ile kullanan arasında kanunda var ceza farkının ortadan kaldırılmasıdır.¹⁹

“Feri cezalar” başlıklı 350. maddesine yeniden müsadere eklenmiştir. “Tüzel kişilerin sorumluluğu” başlıklı 351. maddesinde ise, 347 ve 348 maddelerinde düzenlenen suçlardan tüzel kişilerinde sorumlu olduğu kabul edilmiştir. “Suç işlemek için örgütlenme” başlığı taşıyan 1997 TCK. Ön Tasarısının 352. maddesinde, yukarıda maddelerde öngörülen suçları işlemek için oluşturulan bir örgütü kuran veya buna katılan kişilere işlemek istedikleri suçlardan en ağırının cezasının verileceği hükme bağlanmıştır. Bu şekilde düzenlemede ilk defa getirilmiştir.

IV. 2000 TCK Ön Tasarısı

2000 tarihli TCK. Ön Tasarısında bilişim suçları, tasarının İkinci Kısımının “Bilişim Alanında Suçlar” kenar başlığı Dokuzuncu Bölümünde, 346 - 352 maddeleri arasında düzenlenmiştir.

1997 Ön tasarısının maddeleri 2000 Ön tasarısına bir takım değişiklikler ve para cezalarındaki güncellenmesi dışında gerekçeleriyle dahil olmak üzere olduğu gibi aktarılmıştır. Yalnızca ferî cezaların düzenlendiği 348. maddede, suçta kullanılan veya

¹⁸ Kurt (Dipnot 7), S. 125-126.

¹⁹ Kurt (Dipnot 7), S. 127.

suçtan meydana gelen şeylerin müsaderesi “veya mülkiyetin devlete geçirilmesi” ifadesi kullanılmıştır.²⁰

2000 Ön tasarısında getirilen en önemli yenilik “Banka ve Kredi Kartlarının Kötüye kullanımı” başlıklı 349. maddesidir. Bu maddenin birinci fıkrası ile başkasına ait veya diğer bir kişiye verilmesi gereken bir kredi kartını herhangi bir şekilde ele geçiren veya bulunduran bir kişinin kart sahibinin rızası olmaksızın kullanarak veya kullandırarak kendisine veya başkasına haksız kazanç sağlaması suç olarak düzenlenmiştir. İkinci fıkrasında ise aynı fiilin banka veya kredi kartını tahrif ederek veya bunu sahtecilik suretiyle meydana getirerek işlendiğinde ceza ağırlaştırılmıştır.²¹

Tüzel kişilerin sorumluluğuna ilişkin düzenleme 1997 Ön Tasarısından bir fark dışında aynen düzenlenmiştir. 1997 Ön Tasarısında tüzel kişilerin sorumluluğu bilişim sistemine girme, verileri tahrip ve bozma, sistemi engelleme, bozma, haksız yarar sağlama fiilleri ile sınırlandırılmasına rağmen bu tasarıda tüzel kişilerin bu bölümdeki tüm suçlardan sorumlu olduğu düzenlenmiştir.²²

V. 2003 TCK Ön Tasarısı

İkinci Kitabın “Topluma Karşı Suçlar” başlıklı ikinci kısmının “Bilişim Alanında Suçlar” başlıklı 9. bölümünde bilişim suçları düzenlenmiştir.

Bu bölünme yer alan 346. maddesinde bilişim sistemine girme, verileri tahrip ve bozma, 347. maddesinde sistemi engelleme, bozma, haksız yarar sağlama, 348. maddesinde sahtecilik, 349. maddesinde ferî cezalar, 350. maddesinde banka veya kredi kartının kötüye kullanılması, 351. maddesinde suç işlemek için örgütlenme, 352 maddesinde tüzel kişilerin sorumluluğu düzenlenmiştir. 2000 TCK. Ön Tasarısındaki 346, 347, 348. maddeleri gerekçeleri de dahil olmak üzere 2003 tasarısına aynen alınmış, sadece zamanın şartlarına uygun olarak para cezası miktarları güncellenmiştir. 349 hiçbir değişiklik olmadan aynen alınmıştır. Suç işlemek için örgütlenme başlıklı 351. maddesinde ise, aynı başlık altında temelde aynı olmakla birlikte tek farkla 2003 tasarısına alınmıştır. Bu fark madde metninden “varlığı bir veya birden çok maddi nitelikteki hazırlıklardan anlaşılan” ifadesi çıkarılmıştır.²³

²⁰ Özel, Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, İstanbul Barosu Dergisi, Cild – 75/ Sayı 7, 8, 9, S. 862.

²¹ Akıncı/Alic/Er, Türk Ceza Kanunu ve Bilişim Suçları, İnternet ve Hukuk (Derleyen: Atamer), İstanbul, 2004, S. 266.

²² Akıncı/Alic/Er (Dipnot 21), S. 272-273.

²³ Kurt (Dipnot 7), S. 132.

350 ve 352. maddeler bakımından her iki Ön Tasarısında (2000 ve 2003) düzenleme farklılığı görülmemiştir.

C. 5237 Sayılı TCK'daki Sistematik

Yeni Ceza Kanununda İkinci Kitabının Üçüncü Kısımının Onuncu Bölüm başlığı altında “Bilişim Alanında Suçlar” özel bir bölümde düzenlenmiştir. Bilgisayar ve bilgisayar aracılığıyla gerçekleştirilen iletişim de bir üst başlık olarak bilişim alanı kapsamı altında değerlendirilmiştir. Bu sebeple “Bilişim Alanında Suçlar” başlığı, bir yandan bilgisayarı, unsurlarını ve bunlarda gerçekleştirilen işlemleri kapsarken bir yandan da internet de dahil olmak üzere bilgisayar marifetiyle veri iletişimi ve naklini de koruma altına almaktadır.²⁴

Doktrinde bilişim suçlarının sınıflandırılması ile ilgili farklı girişimler mevcuttur.²⁵ Bu sınıflandırma girişimleri içinde *Yazıcıoğlu*'nun sınıflandırması sistematik açıdan oldukça yerindedir. *Yazıcıoğlu*'na göre Bilişim suçlarını iki temel ayırım içinde düşünmek mümkündür. Bu suçlar bilişim alanının doğurduğu yeni hukukî yararlar karşılığında gerçekleştirilen «dar anlamda bilişim suçları» ve klâsik suçların bilişim olanakları marifetiyle gerçekleştirilmesi olarak karşımıza çıkan «geniş anlamda bilişim suçları»dır.²⁶

Gerçek bilişim suçları olarak adlandırılan birinci suç grubu da, “bilişim sistemlerine izinsiz girilmesi” (m.243), “bilişim sistemlerindeki verilere müdahalelerde bulunulması” (m.244), “bilişim sistemleri marifetiyle haksız menfaat temini” (m.244/4) gibi bilişim sistemlerinin özelliğinden kaynaklanan ve yeni hukuksal değerle bağlamında gerçekleştirilen doğrudan bilişim suçları ya da dar anlamda bilişim suçları şeklinde adlandırılan gerçek bilişim suçları ve bilişim teknolojilerinin getirdiği imkânlar dolayısıyla ortaya çıkan “haberleşmenin gizliliğini ihlâl” (m.132), “haberleşmenin engellenmesi” (m.124), “eğitim ve öğretimin engellenmesi” (m.112), “kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi”

²⁴ *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki..., S. 403; *Karağülmez* (Dipnot 10), S. 37; *Dülger* (Dipnot 12), S. 66.

²⁵ Örneğin *Dönmezer* ikili bir sınıflandırmaya gitmiştir: 1. Bilgisayar sistemlerini, veri bankalarını ve programları korumaya yönelik olarak bilgisayar sistemi içinde işlenen suçlar, 2. Teknolojik bir araç olarak doğrudan bilgisayarı korumaya yönelik olarak bilgisayara karşı işlenen suçlar. *Dönmezer* (Dipnot 14), S. 616. Başka bir sınıflandırma da *Ersoy'da* dikkati çekmektedir: 1. Bilişim sistemleri aracılığıyla işlenen suçlar, 2. Bilişim sistemine karşı işlenen suçlar, 3. Bilişim araçlarına karşı işlenen suçlar. *Ersoy*, Genel Hukuki Koruma Cercevesinde Bilişim Suçları, AÜSBFD., C. 49, S. 3-4, Ankara, 1994, S. 160.

²⁶ *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki, S. 396 vd.; *Yazıcıoğlu*, Bilgisayar Ağları Marifetiyle İşlenen Suçlar: Sanal Suçlar, Bilişim Suçları (Panel – T.C. Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi Başkanlığı), Ankara, 2001, S. 36 vd.

(m.113), gibi dolayısıyla bilişim suçları diye de ikiye ayrılmaktadır. Bununla birlikte “hakaret ve sövme” (m.125), “müstehcenlik” (m.226), “kumar oynanması için yer ve imkân sağlanması” (m.228) “suç işlemeye tahrik” (m.214) gibi klâsik nitelikli suçların bilişim teknolojileri marifetiyle işleyebilmesi de mümkündür. Hırsızlık ve Dolandırıcılık suç tipleri bakımından da, bu suçların bilişim sistemleri kullanmak suretiyle işlenmesi de ağırlaştırıcı neden olarak düzenlenmiştir.

D. Kavramlar

Bilişim ve Telekomünikasyon teknolojilerindeki yayılım ve yeni iletişim araçlarının kullanılmasına yönelik ilginin artmasıyla birlikte „Bilişim“, „Veri“, „İnternet“, „Bilgisayar“, „Siber Uzay“ gibi kavramlar hem sosyal alanda günlük konuşmalarda gerekse yasa metinlerinde daha sık olarak kullanılmaya başlanmıştır. Bu bağlamda teknolojik gelişmeler ile söz konusu kavramların belirlenmesi ve açıklanması arasında bir paralelliğin olduğu açıktır. Çünkü yeni teknolojik gelişmeler kavram içeriklerinin dönüşüme uğraması ve zenginleşmesine sebebiyet vermektedir.²⁷ Tabi ki bu yönde birçok kavram mevcuttur ancak ceza hukuku anlamında en önemli kavramlar ile ilgili kapsam belirlenimleri şöyle yapılmıştır:

I. Bu çerçevede ilk önemli kavram Bilişim Sistemi (eski TCK'deki haliyle verileri otomatik işleme tabi tutan sistem) kavramıdır. Bilişim kelimesi, Fransızca «informatique» kelimesinden Türkçe'ye çevrilmiş olup Fransızca “information” (bilgi) ve “automatique” (otomatik) kelimelerinin birleşiminden türemekte ve verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması gibi fonksiyonları da barındıran bir anlama sahiptir.²⁸ TDK sözlüğünde “*bilişim*”, “*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi*” olarak tanımlanmaktadır.²⁹ Bilişim, bir bilim dalı olarak da kabul edilmekle beraber, her hangi bir alandaki bilginin otomatik olarak işlenmesi yani saklanması, organize edilmesi, değerlendirilmesi, aktarılması, kullanılması, iletilmesi, ilâve yapılabilmesi, değiştirilebilmesi anlamındadır. Ceza Hukuku açısından bilişim suçlarının temelindeki bu kavramın yasa koyucu tarafından da tanımlandığı ve bu tanımın 243. maddenin gerekçesinde yer aldığı görülmektedir. Bu tanıma göre, bilişim sistemi verileri toplayıp yerleştirdikten sonra onları otomatik

²⁷ Koca, Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, C. III, S. 787 vd.

²⁸ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki..., S. 403.

²⁹ <http://www.tdk.gov.tr/TR/SozBul.aspx?F6§10F8892433CFFAAF6AA849816B2EF05A79F75456518CA> (08.07.2007).

işleme tabi tutma olanağı veren manyetik sistemdir. Ancak bu tanımlama girişimi oldukça muğlak ve tartışmaya açıktır. Yasa koyucunun temel hareket noktaları sistemin manyetik oluşu ve verilerin toplanıp yerleştirildikten sonra işlenmesi şeklinde ortaya konulmuştur. Ancak bu durumda şu soruların yanıt bulması zorunludur; neden sadece manyetik sistemler bilişim sistemi olarak kabul edilmiştir? “verilerin toplanması ve yerleştirilmesi”nden ne kastedilmektedir? Kim ve/veya kimler tarafından bu veriler toplanmakta ve yerleştirilmektedir? vb.³⁰

II. Diğer önemli bir kavram da Bilgisayardır. Bilgisayar, önceden aktarılmış veri ve programa bağlı olarak aritmetik ve mantıksal işlemleri yapabilen, kullanacağı programı ve verileri kaydedebilme yeteneğine sahip, çevresiyle etkileşimde bulunabilen araçtır.³¹ Bir başka ifade ile bilişim niteliğine sahip bir bilgisayar, yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen, bilgiyi işleyebilen, saklayabilen, organize edebilen, değerlendirebilen, aktarabilen, kullanabilen iletebilen, değiştirebilen ve ilâve yapılabilen bir araçtır.³² Bu tanımlardan da anlaşılacağı üzere, bilişim sistemi unsuru olarak bilgisayarın genel kullanım amacına hizmet etmesi öncelikli olarak aranan bir koşuldur. Ceza Kanununda özel bir bilgisayar tanımına yer verilmemiştir.³³

III. Veri kavramı bilişim sistemi kavramının açıklanması bakımından oldukça önemli bir kavramdır. Veri her türlü bilginin bilgisayar tarafından işlenebilmesi için analitik ve numerik kodlara dönüştürülmüş şeklidir.³⁴ Bu tanımdan hareket edildiğinde verinin kapsamsal bir anlama sahip olduğu görülmektedir. Eski Ceza Kanununda bilişim alanında işlenen suçlarda bir sınırlandırmaya gitmemek adına „diğer herhangi bir unsur“ kavramı kullanılmıştır. Bu girişimle yasa koyucu bu alanda işlenen suçlarda yeni suç unsurlarını yeni teknolojik gelişmelerle bu kapsama dahil etmeyi düşünmüştür. Bu suretle bilişim suçlarında dinamik bir yasal yapıya ulaşılabilecekti.³⁵ Ancak bu düzenleme „Kanunilik“ ve „Belirlilik“ prensipleri bakımından değerlendirilmiş ve eleştiriye tabi tutulmuştur. Bu yöndeki tartışmaların ardından „Veri“ Kavramı ilgili tüm unsurları da

³⁰ Bu konudaki tartışmalar için bkz. *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki..., S. 404 vd.

³¹ *Yenidünya/Değirmenci*, S. 18 vd.; *Dülger* (Dipnot 12), S. 36 vd.; *Karagülmez* (Dipnot 10), S. 31, <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518CA> (08.07.2007).

³² *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki, S. 404.

³³ *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki, S. 404.

³⁴ <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518CA> (08.07.2007); *Dülger* (Dipnot 12), S. 48.

³⁵ *Yazıcıoğlu*, Kriminolojik, Sosyolojik, S. 227; *Ersoy*, S. 168-169.

içerecek şekilde tek kavram olarak kullanılmıştır.³⁶ Veri için TCK'da herhangi bir tanıma rastlanmamaktadır.

E. TCK'daki Düzenlenen “Bilişim Alanında Suçlar”a İlişkin Norm Analizi

I. Md. 243 – Bilişim Sistemine Girme (Yetkisiz Erişim)

TCK'nin 243. maddesinin birinci fıkrasında yetkisiz erişim suçu “*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.*” şeklinde düzenlenmiştir.³⁷

243. maddenin 2. fıkrasında, birinci fıkrada tanımlanan fiilin bedeli karşılığı yararlanılabilen sistemler üzerinde gerçekleştirilmesi hali cezada indirim sebebi olarak öngörülürken, aynı maddenin son fıkrasında düzenlenen verinin yok olması ya da değişmesi, ağırlatıcı sebep olarak düzenlenmiştir. 243. maddede “*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden...*” hükmüne yer verilmiş ve suçun maddi unsuru “*girme ve orada kalmaya devam etme*” olarak düzenlenmiştir. Tasarıda yetkisiz erişim suçunun düzenlendiği maddede “*bir bilişim sistemine giren veya orada kalmaya devam eden*” hükmünü içermekte iken, TBMM Genel Kurul görüşmeleri sırasında bu maddeye ilişkin değişiklik önergesinin kabulü sonucunda, maddede suç teşkil eden eylem “*bir bilişim sistemine giren ve orada kalmaya devam eden*” halini almıştır.

Ketizmen'in isabetli olarak ortaya koyduğu üzere, tasarıdaki hüküm Fransız Ceza Kanununun 323-3 ve İtalyan Ceza Kanununun 615. maddesi maddi unsur itibariyle paralellik arz etmekte ve “*sisteme girme*” ve “*sistemde kalmaya devam etme*” seçimlik hareketleri oluşturmaktayken, madde metninde yapılan değişikliklerle bu iki hareket birleştirilmiş. “*sisteme girme ve kalmaya devam etme*” şeklinde tanımlanmıştır.³⁸

Ancak bu maddenin düzenlenişinde özensiz davranıldığı göze çarpmaktadır. Örneğin yukarıda değinildiği gibi Tasarıda yer alan “*bir bilişim sistemine girmek veya orada kalmaya devam etmek*” fiili kanun görüşmeleri esnasında “*bir bilişim sistemine girmek ve orada kalmaya devam etmek*” olarak değiştirilmiş ancak bu değişiklik gerekçeye

³⁶ Dülger (Dipnot 12), S. 68.

³⁷ Erdağ, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Suçları, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

³⁸ Ketizmen, Türk Ceza Hukukunda Bilişim Suçları (Yayımlanmamış Doktora Tezi), Ankara, 2006, S. 96.

yansıtılmamıştır. Yani madde metninde “ve” kullanılırken gerekçesinde “veya” kullanılmıştır.³⁹

Ayrıca madde metninde bilişim sistemine girmek ve orada kalmak tek bir eylem gibi düzenlenmiş olmasına rağmen madde başlığı sadece “bilişim sistemine girme” olarak kullanıldığından suçun tamamlanma aşaması bakımından bir uyumsuzluk doğmuştur. Ayrıca yine aynı şekilde 243. maddenin ikinci fıkrası, “birinci fıkradaki fiiller” diyerek yine benzer bir çelişkiye neden olmuş ve sanki birden fazla eylem varmış gibi düzenleme getirmiştir. Halbuki “bilişim sistemine girme ve orada kalma” fiili tek bir fiildir.⁴⁰

243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu ile ilgili olarak çeşitli görüşler ileri sürülmüştür. Kurt, bilişim sistemine yetkisiz erişim suçu ile sistem sahibinin kişisel alanına müdahale edildiğini ifade etmiştir.

Yazara göre; “Bilişim sistemine girme ve orada kalmaya devam etme suçunda korunan hukuki yarar, özel hayatın gizliliği ve sırların masuniyeti (gizliliği) olarak belirlenebilir. Bilişim sistemi ve içinde bulunan veriler, programlar sistem sahibinin özel alanı da bulunmaktadır. Bu suç ile bu alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır”.⁴¹ TCK’nin 243 maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun karma bir nitelik taşıdığını savunan Dülger yetkisiz erişimin engellenmesiyle sistemin sahibi ya da kullanıcıları olarak sistemden faydalanan kişilerin birçok çıkarları koruma altına alındığını belirtmektedir. Bu çıkarları, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabildiği üzerinde durmuştur. Yazar farklı açıdan ele alınan çıkarlar olarak kabul ettiği bu değerleri kapsayacak şekilde “bilişim sisteminin güvenliği”nin korunmasının asıl hukuki konuyu oluşturduğunu belirtmiştir.⁴²

243. maddede düzenlenen suçun gerçekleşmesi için sadece sistemin bütününe ya da bir kısmına hukuka aykırı olarak girme yeterli değildir, ayrıca sistemde kalınmaya devam edilmesi de gerekmektedir. Sisteme girme ve orada kalmaya devam etme, bir bütün olarak, 243. maddede düzenlenen yetkisiz erişim suçunun maddi unsurunu oluşturmaktadır.⁴³ Yukarıda da ifade edildiği üzere, suçun maddi unsurunun bu şekilde düzenlenmesi, suçun niteliğinde de değişikliğe neden olmuştur. Maddede yer alan suçun

³⁹ Karagülmez (Dipnot 10), S. 166.

⁴⁰ Karagülmez (Dipnot 10), S. 168.

⁴¹ Kurt (Dipnot 7), S. 148.

⁴² Dülger (Dipnot 12), S. 213 vd.

⁴³ Yazıcıoğlu, Yeni Türk Ceza Kanunundaki, S. 406; Eker, Türk Ceza Hukukunda Bilişim Suçları, TTB Dergisi, Sayı 62, Ankara, 2006, S. 122.

unsuru olarak “*girme ve orada kalmaya devam etme*”ye verilecek anlama göre, söz konusu suçun niteliği hakkında iki farklı düşüncenin ileri sürülmesi mümkündür. Özellikle “*kalmaya devam eden*” ifadesinin anlam ve kapsamı burada önemlidir.

Girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturduğunun kabulü halinde, Kanununun 243. maddesinde düzenlenen yetkisiz erişim suçunun birden fazla hareketi gerektiren bir suç olduğu sonucuna varılır. Birden fazla hareketi gerektiren suçlarda olduğu şekliyle, bu maddede sadece sisteme girme yeterli olmamakta, sistemde kalmaya devam edilmesi gerekmektedir.⁴⁴ Girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturmadığının kabul edilmesi halinde ise, maddede düzenlenen suçun zorunlu olarak mütemadi suç olduğu sonucuna varılır. Buna bağlı olarak sisteme girme sonrasında sistemde kalmaya devam edilmesi, suçun tamamlanmış sayılabilmesi için belli bir sürekliliğin dikkate alınmasını zorunlu kılar.⁴⁵

Yukarıda yapılan açıklamalar ışığında sisteme hukuka uygun bir şekilde girilmesi sonrasında rızanın ortadan kalkması ya da diğer nedenlerle hukuka aykırılığın gerçekleşmesi durumunda da sistemde kalmaya devam edilmesi, girişin hukuka aykırı olması şartından dolayı 243. madde kapsamı dışında değerlendirilecektir.⁴⁶

243. maddede düzenlenen suçun neticesi bakımından herhangi özel bir düzenlemeye yer verilmemiştir. Madde gerekçesinde de ifade edildiği gibi, sisteme hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş olup olmaması herhangi bir önem taşımaz. Sisteme hukuka aykırı olarak girilmiş olması suçun oluşması için yeterlidir. Bu bağlamda söz konusu suçun bir zarar suçu olarak değil bir tehlike suçu olarak düzenlendiği sonucuna ulaşılabilir.⁴⁷ Maddede bilişim sistemine girme ve orada kalma eylemleri bakımından hukuka aykırılık unsuru özellikle vurgulandığı için kusuru olmaksızın yaptığı eylemin suç teşkil ettiğini bilmeyenler bakımından bir ayrıcalık oluşturulduğunu da savunulmaktadır.

Yetkisiz erişim suçunun düzenlendiği 243. maddenin 2. fıkrasında, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, hafifletici neden olarak düzenlenmiştir. Buna karşın bedeli karşılığı yararlanabilen sistemlerin ne olduğu konusunda herhangi bir gerekçeye veya açıklamaya yer verilmemiştir. *Dülger*, bedeli karşılığı yararlanılabilen sistem ifadesinin genel olarak dört durumu kapsadığını ifade etmiştir. Yazara göre İnternet üzerinden ücret karşılığı hizmet veren web siteleri,

⁴⁴ Kurt (Dipnot 7), S. 151.

⁴⁵ Karagülmez (Dipnot 10), S. 170 vd.

⁴⁶ Ketizmen (Dipnot 38), S. 130.

⁴⁷ Karagülmez (Dipnot 10), S. 171.

“internet kafe” gibi yerlerde olduğu üzere belirli bir bedel karşılığı bilişim sisteminin kiralanması, bir kuruluş tarafından belli bir sistemin bedel karşılığında sunulması (örneğin sağlanan anlaşmayla kişilerin cep telefonlarına bilişim sistemi üzerinden reklam amaçlı mesaj çekilmesi) ve de belirli bir zaman ya da dönem sınırlaması ile İnternet bağlantı servisinin sağlanması bedeli karşılığı yararlanılabilen sistem kapsamındadır.⁴⁸ *Karagülmez* internet kafe ve benzeri yerlerde bedeli karşılığında sistemin kullanılmasının bu kapsamda düşünülmemeyeceğini ifade ederek maddede sistemin kullanıldığı mekanın değil sistem içerisindeki elektronik yapıda sunulan ücretli hizmetleri vurguladığını savunmaktadır. Yazara göre, belirli bir süre İnternet bağlantı servisinin sağlanması da bu fıkra kapsamında değildir.⁴⁹ *Yazıcıoğlu* ise, bu fıkra düzenlenmiş hafifletici sebebi, ücreti karşılığı hizmet veren sistemlere girilmesi şeklinde yorumlamakta ve devamında ve bu düzenlemenin yetkisiz erişim suçunun uygulanmasının genişliğinden doğacak sakıncaları gidermesi bakımından isabetli olduğunu ifade etmektedir.⁵⁰

243. maddenin son fıkrasında sisteme yetkisiz erişim sonucunda sistem içerisindeki verinin değişmesi veya yok olması ağırlatıcı neden olarak düzenlenmiştir. *Erdağ’a* göre, TCK’nin 23. maddesine paralel olarak, neticesi sebebiyle ağırlaşan bir suç söz konusu olduğu için ağırlatıcı nedenin uygulanabilmesi failde verinin değiştirilmesi ya da yok edilmesi yönünde bir kastının olmamasına bağlıdır.⁵¹ Aksi takdirde 244. maddenin 2. fıkrasında yer alan hüküm devreye girecektir. Yazarın neticesi nedeniyle ağırlaşan suç tespitini söz konusu durumda neticesi sebebiyle ağırlaşan bir suçun söz konusu olmaması nedeniyle isabetli bulmuyoruz.⁵² Bu fıkra düzenlenmiş ağırlatıcı nedenlerin uygulanması için birinci ya da ikinci fıkra düzenlenmiş sistemler bakımından maddede özellikle cezanın miktarı bakımından herhangi bir farklılığa gidilmemiştir. Fıkra belirtilen durumun gerçekleşmesi halinde verilecek ceza, yetkisiz erişimin konusunun bedeli karşılığı kullanılan sistemlerden olup olmamasına bakılmaksızın altı aydan iki yıla kadar hapis cezasıdır.⁵³

⁴⁸ *Dülger* (Dipnot 12), S. 227.

⁴⁹ *Karagülmez* (Dipnot 10), S. 175 vd.

⁵⁰ *Yazıcıoğlu*, Yeni Türk Ceza Kanunundaki..., S. 406.

⁵¹ *Erdağ*, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Suçları, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

⁵² Detaylı bilgi ve eleştiri için bkz. *Özbek*, TCK. İzmir Serhi, Ankara, 2006, S. 306 vd.

⁵³ *Erdağ*, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Suçları, <http://www.ceza-bb.adalet.gov.tr/makale/100.doc> (08.07.2007).

II. Md. 244 – Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değişirme

Eski TCK’da sisteme ve veriye zarar verme suçunun mala zarar verme suçu ile birlikte değerlendirilmekteydi. Sisteme ve veriye zarar verme suçuna ilişkin, mala zarar verme suçundan ayrı özel bir düzenlemenin yapılmasına ilişkin gerekçeler dikkate alındığında bu değerlendirme açıkça görülmektedir.

Dönmezer şu düşünceleri ileri sürmektedir: “*Bilgisayarın dokunulmaz olması gereği ve sistemin uygun şekilde işlev görmesi ve içeriğinin aynı suretle hizmet görmesidir. Böylece aslında başta malikin veya sistemi kullananın yararı korunmaktadır.*⁵⁴ *Yazıcıoğlu* da bu suç ile, kişilerin sistem ve içerisindeki unsurlar bakımından sahip oldukları mülkiyet hakkının korunduğunu düşünmektedir.⁵⁵ *Önder* suçun koruduğu yararın tartışmalı olduğunu dile getirerek bu suç tipi ile bilgisayarda mevcut veriler ile ilgili olan kişinin yararının korunduğunu savunanlar olduğu gibi, mevcut verilerin ülke ekonomisinde ve idarede gerçekleştirildiği fonksiyon gereği, bu suçun ekonomik yaşama karşı işlenmiş bir suç olduğunu iddia edenlerin de bulunduğunu dile getirmiştir.⁵⁶ *Ersoy* ise bu suç ile kişinin malvarlığının korunduğunu belirtmişti.⁵⁷ *Dülger* ise, bilişim sisteminin veri ve yazılımlardan oluşan soyut unsurları yanında donanım unsurunun da koruma altına alınması karşısında, suçun hukuki konusunun karma bir nitelik gösterdiğini belirtmiştir.⁵⁸

Sistemin işleyişini engelleme ve bozma TCK’nin 244. maddesinin 1. fıkrasında, “*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*” şeklinde düzenlenmiştir. 244. maddenin birinci fıkrasında suçun unsurunu oluşturan seçimlik hareketler “*bilişim sisteminin işleyişinin engellenmesi*” ve “*sistemin işleyişinin bozulması*”dır.⁵⁹ Kanunda engelleme ve bozma kavramları ile ilgili herhangi bir tanımlama yapılmamıştır. Bu kavramlar için doktrinde, sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiği,⁶⁰ sistemin tamamen çalışamaz hale gelmesi, sistemin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması, haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan

⁵⁴ *Dönmezer* (Dipnot 14), S. 622.

⁵⁵ *Yazıcıoğlu*, *Kriminolojik, Sosyolojik...*, S. 259-260.

⁵⁶ *Önder*, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*, İstanbul, 1994, S. 508.

⁵⁷ *Ersoy* (Dipnot 25), S. 167.

⁵⁸ *Dülger* (Dipnot 12), S. 231 vd.

⁵⁹ *Erdağ*, *Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Suçları*, <http://www.cezabb.adalet.gov.tr/makale/100.doc> (08.07.2007).

⁶⁰ Benzer yönde kararlar için bkz.: Yargıtay 4. CD., 28.02.2000, 2000/1068 E. – 2000/1771 K.; Yargıtay 11. CD. 24.10.2002, 2002/5771 E. – 2002/8416 K.

kaldırılmasının sistemin işleyişini bozma anlamına geleceği yönünde yorumlar mevcuttur.⁶¹

244. maddenin 2. fıkrası, “Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.” Olarak düzenlenmiştir.

Maddede düzenlenen ilk seçimlik hareket, bilişim sistemi içerisindeki “verinin yok edilmesi”dir. Bilişim sistemi içerisindeki verinin yok edilmesinden kastedilen, verinin varlığına son verilmesi, veri üzerinde hak sahibi olan kişinin veriyi tekrar elde edemeyeceği ya da büyük güçlükler sonucu elde edebileceği şekilde hakimiyetinden çıkarılmasıdır.⁶²

244. maddenin 2. fıkrasında, 765 Sayılı TCK’nin 525/b maddesinde olduğu gibi verinin silinmesi esas kabul edilmeyip, verinin yok edilmesi hareket noktası olarak kabul edilmiştir. Dolayısıyla bilişim sistemi içerisindeki verinin silinmesinin yok etme kapsamında olup olmadığı tartışması gündeme gelmektedir. *Yazıcıoğlu*, silmenin mevcut kayıtların bulunduğu yerden yok edilmesi ile aynı çerçevede kullanıldığını dile getirerek silme ve yok etmenin aynı anlamda olduğunu vurgulamıştır.⁶³

Yazar, maddi anlamda bir yok etmekten bahsedilemeyeceğini, sadece silinen unsura ulaşabilmek bakımından gereken normal bağın kaldırılması, bilgilerin tanınamaz hale gelmesinin söz konusu olduğunu, bu açıdan silmek anlamının şeklen anlaşılması gerektiğini ifade etmiştir.

Önder de, silmenin mecazi ve mantıki anlamda olduğunu, bir programa ulaşabilmek için aradaki mevcut bağın koparılması anlamına geldiğini ifade etmiştir.⁶⁴

“Verinin erişilmez kılınması” ise, genel olarak veriye müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup burada veri içerik bakımından bir bütün olarak korunmaya devam edilmektedir. Bu bağlamda veri yok edilmemekte ve/veya bozulmamaktadır. Bununla beraber verilere ulaşım için gereken işlem bağı devre dışı bırakılmaktadır.⁶⁵

244. maddenin 2. fıkrasında düzenlenen hareketlerin sonuncusu ise “sistem içerisindeki verinin başka bir yere gönderilmesi”dir. Bilişim sistemi içerisindeki

⁶¹ *Dülger* (Dipnot 12), S. 234.

⁶² *Ketizmen* (Dipnot 38), S. 169.

⁶³ *Yazıcıoğlu*, Kriminolojik, Sosyolojik, S. 263.

⁶⁴ *Önder* (Dipnot 56), S. 509.

⁶⁵ *Dülger* (Dipnot 12), S. 237.

verilerin bilişim sistemi dışında bulunan başka bir bilişim sistemine ya da veri taşıma aracına aktarılması, kaydedilmesi ya da kopyalanması verinin başka bir yere gönderilmesi olarak değerlendirilmektedir.⁶⁶

244. maddenin 3. fıkrasında bir ağırlaştırıcı neden düzenlenmiştir.⁶⁷ 244. maddenin üçüncü fıkrasına göre, aynı maddenin birinci ve ikinci fıkralarında yer alan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

244. maddenin 4. fıkrasında ise farklı bir suç tipi ile karşılaşılmaktadır. Buna göre yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması başka bir suç oluşturmaması halinde suç olarak düzenlenmiştir. Bu düzenlemeye göre, fiil, TCK. ve diğer özel kanunlarda yer alan başka bir suçu oluşturuyorsa, bu madde kapsamında değerlendirilmeyecek ve ilgili maddelerde düzenlenen suçlara göre hüküm kurulacaktır.

Maddede, “*başka bir suçu oluşturmaması*” hükmüne yer verilmiş iken, madde gerekçesinde, “*Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.*” İfadesine yer verilmiştir. Hüküm ile gerekçe arasında bir çelişkinin var olduğu açıkça görülmektedir.

III. Md. 245 – Banka ve Kredi Kartlarının Kötüye Kullanılması

Yeni TCK'nın 245. maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanılması suçu ile ilgili ihlaller için eski TCK. zamanında 525/b–2 maddesi kullanılıyordu. Bu madde özel olarak banka ve kredi kartlarının kötüye kullanılmasını düzenlememekteydi. Ancak ülkemizde banka ve kredi kartlarının kötüye kullanılması birçok kez mahkeme önüne gelmekte ve bu madde neredeyse başka bir düzenleme için kullanılmamaktaydı.⁶⁸ Bu yüzden banka ve kredi kartlarının kötüye kullanılmasına karşı özel bir düzenleme yapma ihtiyacı bir zorunluluk olarak kabul edilmiştir.

Maddenin birinci fıkrasındaki hareket, başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya sahibine verilmesi gereken bir banka veya kredi

⁶⁶ Dülger (Dipnot 12), S. 238.

⁶⁷ Karagülmez (Dipnot 10), S. 192.

⁶⁸ Özel (Dipnot 20), S. 862.

kartının başkası tarafından kullanılması veya kullandırılmasıdır.⁶⁹ Hareket tanımlanırken kartın hukuka aykırı olarak ele geçirilmesi aranmış, bunun dışında ne şekilde ele geçirildiği – Hırsızlık⁷⁰, Dolandırıcılık⁷¹, Yağma⁷² – önemsenmemiştir. Bu açıdan kartı hukuka aykırı ele geçirilmesinde bir sınırlama bulunmamaktadır.⁷³ Başka bir ifade ile eski TCK'daki kartın ele geçirilme biçimine göre yapılan ayrımlar ortadan kaldırılmış kart nasıl ele geçirilirse geçirilsin suç gerçekleşmiş sayılacaktır.⁷⁴ Önemli olan hareketin sonucunda hukuka aykırı yararın elde edilmesidir.

Bununla birlikte banka “Kredi ve Kart Merkezince” düzenlenen kredi ve banka kartları, sahiplerine, özel dağıtım şirketleri, PTT veya banka şubelerine de bizzat görevli elemanlar aracılığıyla teslim edilmektedir. Dolayısıyla kartı elinde bulunduran kişiler tarafından hukuka aykırı olarak kullanılması veya kullandırılması halinde de suç gerçekleşmiş olur.⁷⁵ Böyle bir durumda kart henüz sahibinin eline geçmediğinden suçtan zarar görenin banka olduğu yönünde görüş ağırlığı vardır.⁷⁶ Kartları sahiplerine teslim etmekle görevli elemanların, banka ve kredi kartını teslim etmeyerek kullanıp yarar sağlaması aslında görevi kötüye kullanmak suçunu suçunu oluşturmasına rağmen bu husus özel olarak düzenlenmiştir.

İkinci fıkradaki hareket başkalarına ait banka hesaplarıyla ilişki kurarak sahte banka ve ya kredi kartı üretmek, satmak, devretmek, satın almak, veya kabul etmektir. Fıkroda ön görülen hareket üçüncü fıkroda düzenlenen suça bir geçit suç olarak düzenlenmiştir. Çünkü sahte olarak üretilen kartın kullanılmasıyla yarar elde edilmesi durumunda üçüncü fıkradaki suç oluşur. fıkra ilk kabul edilen TCK'da yer almamaktaydı. 08.07.2005 tarihinden önce banka ve kredi kartlarına ait bilgilerin ele geçirilişi esasen başka bir suça vücut vermiyorsa sadece sahte kart oluşturulması suç olarak düzenlenmemiştir. Bu boşluk söz konusu fıkra ile doldurulmuştur.⁷⁷

Üçüncü fıkradaki hareket sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka ve kredi kartının kullanılmasıdır. Fıkradaki suç çok hareketi barındıran bir suç görünümündedir. Kartın sahte olarak üretilmesiyle birlikte hareket iki alt unsurun

⁶⁹ Bkz Yargıtay Ceza Genel Kurulu 11.04.2000, 2000/6-62 E. – 2000/72 K.; Yargıtay 6. CD. 24.09.2001, 2001/10933 E. – 2001/11095 K.

⁷⁰ Bkz. Yargıtay 6. CD, 01.02.2002, 2001/17027 E. – 2002/1016 K.

⁷¹ Bkz. Yargıtay 11. CD, 06.10.2003, 2003/6778 E. – 2003/6714 K.

⁷² Bkz. Yargıtay 6. CD, 05.02.2002, 2001/16231 E. – 2002/1149 K.

⁷³ Kurt, S. 178; Dülger (Dipnot 12), S. 254; Karagülmez (Dipnot 10), S. 196 vd.

⁷⁴ Akbulut, S. 21 vd.

⁷⁵ Yargıtay 11. CD, 17.02.2004, 12910 E. – 827 K.

⁷⁶ Donay, Bankacılık Ceza Hukuku, İstanbul, 2007, S. 168 vd.

⁷⁷ Ekinci/Esen, Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli İflas ve Taksirli İflas Karşılıksız Yararlanma Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara, 2005, S. 370.

gerçekleşmesiyle tamamlanmaktadır. Birinci alt unsur sonuçta kartın kullanılmış olması ikinci alt unsur ise failin kendisine veya başkasına yarar sağlamasıdır.⁷⁸

Maddenin dördüncü fıkrasında bir hafifletici neden düzenlenmiştir. Buna göre birinci fıkrada yer alan suçun eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

Banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımını olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır. Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır. İşte bu kartların kötüye kullanılmaları, söz konusu maddede suç olarak tanımlanmıştır. Maddeye göre, aşağıdaki şekillerde gerçekleştirilen hareketler bu suçu oluşturmaktadır:⁷⁹

“1. Başkasına ait bir banka veya kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası bulunmaksızın kullanılması veya kullandırılması ve bu suretle failin kendisine veya başkasına haksız yarar sağlaması.

2. Aynı failin, aynı koşullarla sahibine verilmesi gereken bir banka veya kredi kartının bunu elinde bulunduran kimse tarafından kullanılması veya kullandırılması; söz gelimi kartı sahibine vermekle görevli banka memurunun kartı kendi veya başkası yararına kullanması.

Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fillerin, duraksamaları ve içihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.“

IV. Md. 246 – Bilişim Suçlarında Tüzel Kişilerin Ceza Sorumluluğu

246. maddede „Tüzel Kişiler Hakkında Güvenlik Tedbirleri Uygulanması“ başlığıyla yapılan düzenlemede bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlayan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerinin uygulanacağı dile getirilmiştir. TCK. m. 20’ye göre de tüzel kişiler için ceza sorumluluğu öngörülmemiş olup kanunda belirlenen güvenlik tedbirlerinin

⁷⁸ Ekinci/Esen (Dipnot 77), S. 372.

⁷⁹ Bkz. m. 245 Gerekçesi.

uygulanacağı kabul edilmiştir.⁸⁰ Bu bağlamda tüzel kişilere uygulanabilecek güvenlik tedbirleri TCK. m. 60'da iki başlık halinde verilmiştir. Bunlar,

1. Faaliyet İzninin İptali
2. Suçtan meydana gelen şeyin müsaderesi

Müsadere konusunda herhangi bir sorun yoktur, açıkça anlaşılmaktadır. Ancak faaliyet iznin iptali için iki temel şartın gerçekleşmesi aranmaktadır.⁸¹

1. Özel hukuk tüzel kişisine belirli bir faaliyette bulunabilmeye ilgili kamu kurumunca verilen izin
2. Bu iznin sağladığı yetkinin kötüye kullanılması suretiyle tüzel kişi yararına kasıtlı bir suç işlenmesi.⁸²

F. Sonuç

Uzun yıllar boyunca türk ceza hukukunun modernize edilmesi yönündeki ihtiyaç daima tartışılmış ve bu tartışmalar neticesinde Ceza, Ceza Usul ve Ceza İnfaz Hukukunda reform niteliğinde değişikliklere imza atılmıştır. Bu modernize etme eğilimleri bakımından bilişim suçları çok önemli bir rol üstlenmiştir. Çünkü reform çabalarının en önemli amacı toplumsal bir alt sistem olarak değişen toplumsal ihtiyaçlara bir çözüm yolu ortaya koymaktır. Bu bağlamda modern (yani bilgi ve hatta risk) toplumunun güncel sorunları esas alınmaktadır. Bilişim ve iletişim teknolojileri ve bunların sorunları aynı zamanda modern toplumunun da arka planını teşkil ettiği için, belirtilen nedenler çerçevesinde söz konusu kapsamın yasa koyucu tarafından amaca uygun bir biçimde düzenlenmesi beklentisi kendini göstermektedir. Bu temelden hareketle şunu söylemek mümkündür ki, TCK. sistemi içerisinde bilişim suçlarına yönelik düzenlemeler yeterli değildir. Daha önce ortaya konulduğu gibi düzenlemede birçok belirsizlikler (örnek olarak bilişim suçları nerede düzenlenmelidir ?), tanım eksiklikleri (örneğin bilgisayar, bedeli karşılığı yararlanılan sistemler gibi) ve hataları (bilişim sistemi gibi), bunların yanında madde metinleri ile gerekçeler arasındaki tehlikeli ikilemler (md. 243 ve 245 de olduğu gibi) bu düzenlemelerin yeterli ve yerinde olmadığını kanıtlar. Yasa koyucunun tekrardan bu normları teknolojik gerçekliklere uygun ve özenli bir biçimde tartışması ve yeniden yapılandırması şarttır.

⁸⁰ Karagülmez (Dipnot 10), S. 223.

⁸¹ Maddenin eleştirisi için bkz. Yıldız, 5237 Sayılı TCK. Seminer Notları, İstanbul, 2007, S. 34.

⁸² Karagülmez (Dipnot 10), S. 224.