Carta informativa 1/2012

INTRODUCTION

Prof. Dr. John A.E. Vervaele

(1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has

fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society (Castells, 1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

(2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

1. The integrity and functionality of the cyber-ICT system (CIA offences)
2. Protection of privacy
3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, The Coming of Post-Industrial Society, New York, Basic Books , 1976.

Manuel Castells, The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1. Malden: Blackwell. 2d Edition, 2000

S. Sassen, The global city , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, Mastering Complexity in the Global Cyberspace, in M. Delmas-Marty & M Pieth. Les chemins de l'harmonisation Pénale, Paris 2008, 127-202.

GİRİŞ

Prof. Dr. John A.E. Vervaele

(1) Bilgi Toplumu tanımı? Bir tanımın temel unsurları

Baskın, tek bir bilgi toplumu kavramı mevcut değildir. Bilim adamları kavramın tanımları ve değerleri konusunda çalışırken zorlanıyor ve ekonomik, teknik, sosyolojik ve kültürel modeller üzerinde yoğunlaşıyorlar. Bilgi ve İletişim Teknolojilerinin (BİT) oldukça geniş bir alan yayılmış erişilebilirliği ve kullanımı nedeniyle, post modern toplum genellikle bir "bilgi toplumu" olarak nitelendirilmektedir. Bilgi toplumunun yaygın tanımı ise gerçekten de teknolojik yenilikler üzerinde durmaktadır. Bilgi işleme, depolama ve iletme, bilgi ve iletişim teknolojilerinin (BİT) uygulanması ile sonuçlanmış, neredeyse toplumun her köşesine biyoteknoloji ve nanoteknolojiyi taşımıştır. Bilgi toplumu, bilginin ve bilgi birikiminin en temel kaynaklar ve başrol oyuncusu olduğu bir sanayi sonrası toplumudur (Bell, 1973 & 1979).

Ne var ki, bilgi toplumları yalnızca mevcut teknolojik altyapılarca şekillenmiş olmayıp, daha ziyade çok boyutlu fenomenler olarak tarif edilmektedir. Bates'in (1984) tüm bilgi toplumlarının, sadece teknolojik bir altyapıdan değil, aynı zamanda ekonomik bir yapıdan, bir sosyal ilişkiler modelinden, örgütsel modellerden ve sosyal örgütlenmenin diğer değişik görünüşlerinden oluşan karmaşık bir ağ olduğuna işaret etmiştir. Bu yüzden, bilgi toplumunun sadece teknoloji ile ilgili cephelerine değil; bilgi devriminin toplumsal örgütlenmelerdeki etkisi, ceza adaleti sistemindeki toplumsal etkisi de dahil olmak üzere, aynı zamanda bilgi toplumunun toplumsal nitelikleri üzerine de eğilmek önem arz etmektedir.

Dahası, bilgi teknolojisinin postmodern çağı, ceza yargılaması sistemi de dahil olmak üzere toplumsal örgütlenmede bilginin ve bilgi birikiminin içeriği, ulaşılabilirliği ve kullanımını değiştirmiştir. Bilgi birikimi ve düzen arasındaki ilişki köklü bir değişikliğe uğramıştır.

İletişimlerin anlık bilgi üretim teknolojisine dönüşmesi, toplumun bilgi birikimine değer verme şeklini değiştirmiştir. Hızla değişen bu çağda, geleneksel otorite yapısı sarsılmakta ve yerini alternatif bir toplumsal kontrol mekanizmasına bırakmaktadır. BİT temelli yeni bir teknolojik paradigmanın ortaya çıkışı, temel toplumsal yapıların ve aktivitelerin, elektronik şekilde işlenmiş bilgi iletişim ağları etrafında düzenlendiği bir iletişim ağı toplumu doğurmuştur (Castells 1996). İletişim ağı toplumundaki siyasi kurumlarda ise daha da derin bir dönüşüm söz konusu olmuştur: endüstri çağının ulus devletlerini yavaş yavaş yerini almakta olan, yeni bir devlet şeklinin (iletişim ağı devleti) ortaya çıkışı. Hızla değişen bu çağda, geleneksel otorite yapısı zayıflamakta ve yerini alternatif bir toplumsal kontrol mekanizmasına (gözetim toplumu) bırakmaktadır. Ulus devletten iletişim ağı devletine geçiş, iletişim ağı toplumunun koşullarında, siyasi idarenin, temsilin ve egemenliğin niteliğinin dönüşümü ile başlamış, örgütsel ve politik bir süreçtir. Tüm bu değişimler, kamu sektörünün örgütlenme şekli olmak üzere, interaktif, çok katmanlı bir iletişim ağı oluşturma faaliyetinin yayılmasını gerektirmektedir.

Bilgi ve bilgi birikimi, toplumun ve devletin sosyal ve siyasal yapısına etki eden ve ceza adaleti sisteminin işleyişine, yapısına ve içeriğine de yine etki eden temel bilgi toplumu kaynaklarını oluşturmaktadır.

(2) Bütün dört bölümün sorularının birbiriyle bağlantılı olması

İlk olarak ortak bir tanım kullanmamız gerekmektedir. Bilgisayar suçunun konumuz açısından çok dar kapsamlı kaldığı açıktır ve "bilişim ceza hukuku ve bilgi toplumuyla ilişkili suçlar" da yerleşmiş bir kavram değildir.

Bu gerekçelerle ortak bir tanımdan ve sınırlanmış bir bakış açısından yararlanmamız gerekmektedir.

Tanım konusuna gelirsek, ben siber suç kavramını kullanmayı öneriyorum; ancak çok çeşitli yeni fenomenleri ve gelişmeleri kapsayacak bir tanımlama ile.

Bütün siber suçların soruşturmasının ortak paydası ve tipik özellikleri bir yandan bilgisayar sistemleri- bilgisayar iletişim ağları-bilgi-

sayar verisi ile ilgili, öte yandan siber sistemler- siber iletişim ağları-siber bilgi ile bağlantılarında da bulunabilir. Klasik bilgisayarlardan başlayıp çevrimiçi bilgi dağıtımı ve siber verilerin kullanımına kadar uzanan bir çerçeve oluşmaktadır.

İkinci olarak, bu ifade edilen alan oldukça geniş kapsamlı olduğundan, çıkarımlarımızın artı değer oluşturabileceği en ilginç yeni alanlara odaklanmamız gerekmektedir. Dört genel raportör ile yapılan tartışmalardan elde edilen sonuç gösteriyor ki siber suç alanında belirtilen hukuki menfaatler üzerine odaklanacağız:

1. Siber-BİT sisteminin bütünlüğü ve işlevselliği (GBE suçları)
2. Özel hayatın gizliliğinin korunması
3. Dijital kişiliğin korunması
4. Yasal olmayan içeriğe karşı korunma
5. Mülkiyetin korunması (fikri mülkiyet hakları da dahil olmak üzere)
6. Sadece sanal ortamda gerçekleştirilen eylemlere karşı korunma
7. Uygulama sisteminin korunması (itaatsizlik suçları)

(3) Yararlanılan kaynaklar

Daniel Bell, The Coming of Post-Industrial Society, New York, Basic Books , 1976.

Manuel Castells, The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1. Malden:Blackwell. 2d Edition, 2000

S. Sassen, The global city ,New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, Mastering Complexity in the Global Cyberspace, in M. Delmas-Marty & M Pieth. Les chemins de l'harmonisation Pénale, Paris 2008, 127-202.

Preparatory Colloquium Section I

SECTION 1 : CONCEPT PAPER AND QUESTIONNAIRE

Prof. Dr. Thomas Weigend

(A) Scope of questionnaire (see Introduction and Annex)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Thomas Weigend: thomas.weigend@uni-koeln.de

(B) Criminalisation

Please note that in this questionnaire only general characteristics of cyber crime offense definitions are of interest. Specific questions of individual crime definitions will be discussed in Section II of the Congress.

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?

(2) Please give typical examples of criminal laws concerning

(a) attacks against IT systems

(b) violation of IT privacy

(c) forgery and manipulation of digitally stored data

(d) distribution of computer viruses

(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities

(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

(3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined ("data", "writings", contents)?

(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?

(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the internet?

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,

- how are changes in the use of internet and social networks taken into account?
- how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea? Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

(4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?

(5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?

(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?

(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

(G) Internationalisation

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?

(2) To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?

(3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

ANNEX - GENERAL CONSIDERATIONS

Prof. Dr. Thomas Weigend

(1) Information technology in need of protection

To an extent that was hardly foreseeable even 30 years ago, social life on a worldwide scale depends on the proper functioning of information and communication technology (ICT) and the internet. This dependence extends to both the public and the private spheres. On an individual level, interpersonal communication, but also large parts of leisure activity including information-gathering are ICT-based, and many individuals have heavily invested in the development and maintenance of their digital personality (or personalities), e.g. in personal websites and blogs or communication services such as Facebook and Twitter.

These developments have led to a situation where attacks on the integrity of ICT have become serious threats that can affect not only individual interests but also the security of states, important business interests, and the economic system as a whole. Hacking and data falsification, violations of the privacy of digitally transmitted communications, and "identity theft" on the internet are threatening the well-being not only of individuals but also of business firms and states.

(2) Information technology and the worldwide web as a means to commit crime

ICT also has transformed the quantitative dimension of certain assaults on legally protected interests. Whereas in earlier times persons with criminal intentions to defraud or to spread libellous information had to approach each potential recipient of information individually, it is now possible to spread information to hundreds of thousands of persons within a second by using automated e-mail services or websites. The use of computer viruses to create bot

networks can further multiply the effectiveness of an assault and involve up to a million of computers belonging to persons who are unaware of the fact that their addresses are being misused. The existence of a worldwide web and the possibilities of computer technology thus enable persons with criminal intentions to cause maximal harm with minimal effort.

Other features of ICT further contribute to the attractiveness of the net for criminal assaults on individual or collective interests. The possibility of acting anonymously and of using a false identity enables criminals to remain undetected. Detection is further complicated by the extremely high speed of data transfer coupled with routine deletion of transfer data by service providers. The origins of the worldwide web as a device for the quick transfer of secret military information further contribute to the shielding of network users from detection: the worldwide web was purposely devised as a network with many overlapping and independent lines of communication, thus making the web resistent to any attempt of disturbing its functioning through external intervention. The web structure also makes it highly difficult to trace individual items of information back to one source or to effectively block access to an information.

(3) The Role of the Criminal Law

(a) Protecting ICT against Crime

The special sensitivity of ICT to criminal attacks, and the great harm that can be caused by such attacks, make it necessary to employ the criminal law in preventing and sanctioning acts that interfere with the integrity of communications based on ICT. Many legal systems have enacted criminal provisions dealing with such phenomena as data theft, data falsification, and invading protected data bases. Due to the inherently transnational character of the worldwide web, international organisations have attempted to harmonize national legislation in this area (see, e.g., the Cybercrime Convention drafted by the Council of Europe).

Many of the general problems of criminalization (precisely defining the criminal act, avoiding overreach and chilling effects on legitimate conduct, keeping up with technological progress) pose themselves in this area, and some of them are especially acute when a legislature sets out to incriminate assaults on the integrity of IT. The following specific problems come to mind:

(i) Does the progress of ICT lead to new legal interests, and how can they be defined and protected? For example, is there a need to protect "virtual identities" against theft or forgery, and if so, how can that goal be accomplished?

(ii) How can criminal law keep up with the quick pace of development of information technology and the character and contents of the worldwide web?

(iii) Given the sophisticated and ever-changing character of the interests to be protected, how can criminal laws be sufficiently precise to satisfy the principle of legality and yet avoid glaring loopholes? How can criminal "acts" be defined when all that can be noticed are certain effects whereas the "act" is committed by an automated computer system?

(iv) What role can or should incrimination of conduct play in relation to other means of protecting sensitive ICT interests? According to the ultima ratio principle, criminal law should not be employed as the primary means for preserving the integrity of ICT systems. Should criminal laws, for example, apply in addition to effective civil sanctions, e.g., payment of damages for copyright violations? ICT itself provides efficient devices (e.g., encryption, anti-virus and anti-hacking programs, protection against unauthorized download of copyrighted materials) for defending against attacks. This leads to the question whether criminal law should apply only where such devices cannot provide sufficient protection. But one might also think of obliging users by law to install protective programs, and of creating criminal liability for any failure to reasonably protect one's computer against virus infection (because careless users help to spread viruses).

(v) Many legal systems do not generally regard as punishable activity that is merely in preparation of harmful behavior. In the context of ICT criminality, however, the impending harm that can be so grave that certain preparatory measures may be criminalized. For example, some legal systems have criminal provisions against offering or selling (or even possessing?) software especially designed for the commission of internet crime, e.g., for "cracking" passwords or for bypassing download protection. In consonance with the Council of Europe's Cybercrime Convention, some states have also criminalized the sale or purchase of software designed to facilitate the commission of computer fraud. The limits of the legitimate extension of ICT criminality still need to be discussed.

(b) Protecting against Crime Committed through ICT

As has been mentioned above, ICT has created a whole new world of opportunities for individuals intending to commit criminal offenses. Criminal legislation may seek to adapt to this development by using specific tools for controlling and sanctioning the abuse of ICT and especially the internet for committing "ordinary" offenses. Since the focus of the questionnaire is not on these legislative measures, they will be mentioned here only briefly.

(i) Limiting anonymity

One aspect of the internet that offers opportunities for crime is the protection of anonymity that the web provides. Several measures have been suggested to limit anonymity, so as to enhance the chance of detection and identification of offenders. One (controversial) measure imposed by the European Union is an obligation on access providers to store transfer data for several months in order to make it possible to retrace data transfers back to the computer of origin. Other measures under discussion include limits on the complexity of encryptions and an obligation of computer owners to divulge passwords. Such measures may appear defensible in the context of an ongoing investigation for serious crime, but they necessarily spill over to instances of

permissible use of the internet and have the potential of strongly reducing the attractiveness (and thus the profitability) of the net as well as of violating users' legitimate privacy interests.

(ii) Controlling content

There is an understandable tendency of legal systems to extend existing criminal prohibitions with regard to written or printed materials (e.g., pornography, incitement to religious or racial hatred, instruction to commit crimes, disclosure of protected state, military or business secrets) to similar materials distributed by means of ICT. This tendency raises a number of specific problems: first, the transnational character of the worldwide web makes it difficult to enforce national standards, and international agreement on the proper scope of restrictions of speech is difficult to achieve. Second, the ultima ratio principle raises the issue whether measures short of the imposition of criminal sanctions are at least equally effective. Third, the anonymity of the net leads to the question whether it is possible to extend criminal responsibility for illegal contents to (easily identifiable) providers of internet services, which might reduce the difficulty of piercing the shield of anonymity when attempting to effectively control internet content.

The difference of national interests and standards in prohibiting (or protecting) speech seems to be difficult to overcome (this is an aspect to be treated mainly in Section IV of the Congress) Legal system differ strongly as to (i) what content they regard as harmful or dangerous and (ii) where they draw the line between materials protected by freedom of speech and materials the proliferation or even possession of which will be criminally prosecuted. Beyond the technical issue of the applicability of national criminal laws to materials available on the internet (but presumably "posted" by foreign citizens in foreign countries), these differences create a great impediment to international cooperation in the prosecution of (possible) content offenses. International conventions in this area might resolve that problem, but their drawback is that they tend to maximize criminalisation, because each participating

country adds its "pet crimes" to the list of prohibited conduct and there is little political support for retaining breathing space for individual freedom of expression.

Alternatives to criminal prosecution for offensive content are blocking of access to (through the use of software) and deletion of undesirable websites. However, even if access blocking is technically possible it requires cooperation of all nations to be effective, because a block installed by one national agency can easily be circumvented by using an access provided by a foreign firm that does not cooperate with the national agency in question. Deletion, if possible, might be likewise of limited effect because an offending webpage can easily (even automatically) be restored under a different name.

This leads to the issue of making access and/or service providers criminally responsible for maintaining and keeping accessible illegal content. Under this approach, providers would be obliged to "police" and if necessary censor the net. Content providers could be required to either react to complaints about illegal content or even to proactively investigate the contents they provide for prohibited materials. Even if that were technically possible, the normative question arises on what legal basis a (costly) duty to police the net could be imposed on content providers. If one postulates an affirmative legal duty for providers, their criminal liability for breaching this duty could be based on the doctrines of accessorial liability or omission. In that regard, provider liability is to be discussed in Section I on the General Part.

Preparatory Colloquium Section I

REPORT OF THE TURKISH NATIONAL GROUP

Prepared by:
Assoc. Prof. Dr. Vesile Sonay Daragenli Evik*
Assistant Prof. Dr. Hasan Sınar**
Assistant Prof. Dr. Barış Erman***
Dr. Gülşah Kurt****

(B) Criminalisation

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?

There are several legal interests protected by various criminal offences, some of which have been criminalised under the Turkish Penal Code (TPC), whereas others can be found in specific laws. As a result, it is necessary to mention these legal interests according to different criminal offences.

The crime of "illegally entering an IT system or staying there" protects the security of IT systems, data security, and privacy. As for the crime of "prevention of the functioning, or destruction of an IT system, destruction or manipulation of data", it is the interest of the authorised person to be able to access the IT system or to data protected within.

The crime of "obtaining illegal benefits through IT systems" protects the material or moral rights that are subject to the illegal benefit obtained through the offence. The legal interest protected

* Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure Law

** İstanbul Kemerburgaz University Law Faculty, Department of Criminal Law and Criminal Procedure Law

*** Yeditepe University Law Faculty, Department of Criminal Law and Criminal Procedure

**** Galatasaray University Law Faculty, Department of Criminal Law and Criminal Procedure Law

by the crime of "fraud in debit and credit cards" is personal property, trust of the general public towards valid and persuasive legal documents. As for the crimes of "storing personal data" and "giving or obtaining personal data", the protected legal interests are the privacy of persons, and data security. Following these criminal offences, the crime of "failure in destroying personal data" protects not only the privacy and data security, but also the trustworthiness and functioning of the state administration. The crime of "violation of the confidentiality of communication" protects the interest of persons regarding the confidentiality of the private communication, whereas the crime of "prevention of the communication" it is the freedom of communication without undue interruption that is being protected.

The crime of "theft through the abuse of IT systems" protects the private property, while the crime of "pornography / obscenity" protects the general morals and, in particular, the healthy sexual development of minors.

The crime of "illegally copying or using software", regulated under the Turkish Intellectual Property Law (IPL), protects the financial and personal rights of the author on the software.

Additionally, crimes regulated under the Electronic Signature Law (ESL), "illegally using e-signature data, illegally obtaining, giving, copying data or tools, illegally creating an e-signature, falsification of electronic certificates", mainly protect data security and public trust of the general public towards valid and persuasive legal data.

As a last point the crime of "providing access to gambling and betting activities in abroad through internet or other means", as regulated under the Law on Gambling and Betting Games, has been introduced in order to protect the general morals, and the financial interests of state-regulated gambling organisations.

(2) Please give typical examples of criminal laws concerning;

(a) Attacks against IT systems

Art. 243 TPC regulates a criminal offence of "illegally entering, or staying in an IT system", punishable with a prison sentence of up to one year or with a fine. It is a mitigating circumstance that the object of the offence is an IT system that may be used in exchange for a fee. If, however, as a result of the conduct, data included in the IT system in question has been erased or manipulated, the sentence shall be aggravated to that of prison from six months to two years.

Art. 244/1 TPC provides for a criminal offence of obstructing or disturbing the functioning of an IT system, and punishes such acts with a prison sentence of up to five years. Art. 244/2 TPC regulates the offence of "corrupting, destroying or manipulating data, rendering data inaccessible, inserting data into the IT system, or sending existing data elsewhere", punishable with a prison sentence from six months up to three years. An aggravating circumstance has been regulated under art. 244/3 TPC, according to which the sentence shall be aggravated by one half, if the object of the criminal conduct is an IT system belonging to a bank or credit institution, or to a public institution.

Art. 244/4 TPC provides for a criminal offence of "obtaining illegal benefits through IT systems", punishable with a prison sentence of two to six months, as long as such conduct does not constitute another criminal offence.

It is mentioned in the doctrine that the lack of a criminal offence regarding "obtaining data from an IT system" would cause a gap in criminalisation. However, this gap can be filled through art. 136 TPC (illegally obtaining personal data), and, regarding copyright infringements, through art. 71 IPL.

(b) Violation of IT privacy

Art. 132 TPC regulates the offence of "violation of confidentiality of communications". According to this regulation, it is an act

punishable with a prison sentence from one to three years to violate the confidentiality of communications between persons. The sentence shall be doubled in cases where the conduct involves the recording of communications. Those who illegally disclose the content of the communication shall be punished with a prison sentence of two to five years. The same sentence shall be applicable if the disclosure has been realised via press or similar media.

Art. 134 TPC provides for a criminal offence generally protecting the private life of persons. According to the regulation, any act of violating the private life of a person is punishable with a prison sentence of one to three years. In cases where the violation occurs through recording images or sounds, the sentence shall be doubled. Illegal disclosure of such images and sounds is a separate offence punishable from two to five years under art. 134/2 TCP. As such, any conduct related to privacy that does not fall under other criminal offences shall be punishable under this regulation.

Art. 135 TPC provides for a prison sentence of six months to three years for those who illegally record personal data, followed by art. 136, which criminalises illegally giving, disseminating or obtaining personal data as an act punishable with a prison sentence from one to four years.

Art. 138 TPC criminalises the failure to destroy personal data within IT systems despite the fact that the legal period of time regarding their destruction has expired. Such conduct is subject to a prison sentence from six months to one year.

(c) forgery and manipulation of digitally stored data

According to art. 244/2 TPC it is a criminal offence to corrupt, destroy, manipulate data within an IT system, rendering such data inaccessible, inserting data into the system, or sending such data elsewhere. Such conduct is punishable with a prison sentence from six months to three years.

In addition, art. 245 TPC criminalises the debit and credit card fraud. This article includes three separate criminal offences, one of

which regards the forgery, selling, giving, buying or receiving of false debit or credit cards connected with bank accounts belonging to other people. According to the article 245/2, such conduct is punishable with a prison sentence of three to seven years. Under the Law on Debit and Credit Cards (art. 3/e), a "credit card" has been defined in a way to encompass the "card number without the requirement of the material existence of the card". As such, the electronic forgery of the card number would suffice in order to fulfil the requirements of art. 245 TPC.

(d) distribution of computer viruses

As there is no separate offence under Turkish law regarding the distribution of computer viruses, such conduct shall be considered according to art. 244 TPC (obstructing or disrupting an IT system, destroying or manipulating data within an IT system), as explained above.

If, through the distribution of a computer virus, the hardware of an IT system has been harmed, the conduct could also be considered under the criminal offence of "intentionally damaging property" (art. 151 TPC).

(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities

There are no specific criminal offences regarding the virtual identities of users. Such conduct may be considered under the general offence of "violation of the private life" (art. 134 TPC), libel and slender (art. 125 TPC), or illegally obtaining, giving or disseminating personal data (art. 136), as long as these articles are applicable. If the conduct does not fulfil the specific elements of these offences, it can be punishable under art. 244/4 TPC (obtaining illegal benefit through the abuse of IT systems).

(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

In general, the violation of financial interests on copyrights has been regulated as a criminal offence under IPL art. 71. According to the article, the intentional dissemination and distribution of copyright protected data through any means, and the possession or storage of such data for purposes other than self-use is punishable with a prison sentence of one to five years and with a fine. As such, any Internet content that has the characteristics of a "copyright protected work" could be the object of this offence.

Additional art. 4 IPL specifically addresses "content providers" infringing copyrights under the same law, providing for a notify-and-remove system. According to this article, content providers violating copyrights shall only be criminally responsible if they have been duly notified by the copyright holders, and still persisted in the violation. In this case, the copyright holder shall inform the prosecutor, upon which the prosecutor may order the discontinuance of the service provided to the content provider. This order can only be lifted if the content provider removes the content infringing the copyright.

Another innovative criminal prohibition in the area of ICT and the Internet is the criminal offence regarding e-signature fraud. Art. 16 ESL regulates acts of "illegally obtaining, giving, copying, reconstructing signature creating data or tools, or creating an unauthorized electronic signature through using tools obtained illegally" as a criminal offence punishable with a prison sentence of one to three years in addition to a fine. Art. 17 ESL deals with the crime of "fraud in electronic certificates", providing for a prison sentence of two to five years for those who, in full or in part, forge a false electronic certificate, or falsify valid electronic certificates, or those who knowingly use such certificates.

(3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined ("data", "writings", contents)?

In most cases, the criminal conduct has been typified as alternative acts. An exception is art. 243 TPC, where the act of "entering, and staying in an IT system" is a compound of two consecutive acts building the criminal conduct.

Again, in most IT-related crimes, the criminal conduct has been defined by description of the act. Consequences following the conduct have only been regulated under art. 243 TPC, where the destruction or manipulation of data "as a consequence" of illegally entering an IT system has been described as a consequence-based aggravating circumstance.

In some cases, crimes in the area of ICT have been defined as endangerment offences. The crime of entering, and staying in an IT system is punishable even if no harm has resulted from the act. Thus, it falls under the category of abstract endangerment offences. However, most crimes in this area require a clear harmful result as part of the legal definition.

As to the object of the crimes, the terms "IT systems" and "data stored within IT systems" has repeatedly been used under in defining the crimes of "entering, and staying in IT systems" (art. 243 TPC), "obstructing the functioning of an IT system" (art. 244/1 TPC), "corrupting, destroying, manipulating data within IT systems, or rendering such data inaccessible" (art. 244/2 TPC).

Articles 135, 136 and 138 TPC are related to "personal data", although the definition of this term is not included within the regulations of these articles. In fact, there is an on-going debate in Turkish legal doctrine as to the scope of the concept "personal data", as shall be explained below.

Another point to be mentioned under this title is the definition of the "through press or similar media" under art. 6 TPC. According to this article, any mention of the said term within the Code would

encompass acts committed through electronic media, including the Internet. The term has been used in various places, sometimes as an element of crime, in other instances as an aggravating circumstance. The term has also been mentioned in art. 132 TPC regarding the disclosure of contents of a private communication, and in art. 134 TPC, regarding the illegal distribution of images or sounds concerning the private life of individuals. As a result, these crimes shall be deemed as "realised through press or similar media", if they are committed through the use of the Internet.

(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

Under Turkish law generally there are no limitations for certain cyber crime related offences regarding particular groups of perpetrators and/or victims. However, it is an aggravating circumstance in the crimes of storing, giving, distributing or obtaining personal data (arts. 135, 136 TPC), if this crime has been committed by a public servant in abuse of his or her authority. In addition, the crime of "failure in destroying personal data" (art. 138 TPC) can only be committed by a person legally obligated to erase or destroy personal data at the expiration of legally set time periods.

Another instance, where a specific group of perpetrators has been defined as an aggravating circumstance can be found under the ESL. According to arts. 16 and 17, the sentence shall be doubled if the perpetrator is an "employee of the electronic certificate service provider".

(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

In general, criminal liability in the area of ICT and Internet only encompass conduct with intent. However, the consequence-oriented aggravating circumstance as defined under art. 243/2 TPC under the crime of "entering, and staying in an IT system", provides for an aggravation of the sentence, if "as a consequence of said conduct, data has been destroyed or manipulated". Such

consequence-oriented aggravation can result in the criminal liability of the perpetrator, even if he or she did not intent the consequence, but solely the initial act, whereas the consequence may have been the result of negligence by the perpetrator, according to art. 23 TPC.

(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

There are no specific differences between the definition of cyber crimes and traditional crimes. However, many of the crimes mentioned above, in particular, the crimes of entering an IT system (art. 243 TPC), violation of the confidentiality of communications (art. 132 TPC), disclosure of images or sounds related to the private life of individuals (art. 134/2 TPC), recording, giving, distributing or obtaining personal data (arts. 135, 136 TPC) include the requirement that such conduct to be committed "illegally". The predominating opinion of the legal doctrine holds that the specific mentioning of the "illegality" of the conduct means that the intent of the perpetrator should include the illegal nature of his or her conduct for these crimes.

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?

Although certain concerns exist regarding the principle of legality, these problems are not related to IT-specific crimes defined under arts. 243-245 TPC, but rather to other crimes that can be committed through the use of IT systems, i.e. Violation of the private life of individuals (art. 134 TPC), crimes of illegally storing, giving or obtaining personal data (art. 135-136 TPC), and failure to destroy personal data (art. 138 TPC).

The object of the crime of violation of the private life has only been defined as "private life of individuals", without any restrictions regarding the criminal conduct. This concept has not been clearly

constructed, is subject to discussions in criminal law literature, and is a particularly vague concept in its scope[1], it is held that this crime could create problems regarding the principle of legality[2].

The criminal conduct of the crime provided under art. 135 TPC is defined as "illegally recording personal data". However, the term "personal data" has not been defined by law. A draft proposal for a Law on Personal Data has been prepared by the government, and the proposal has been sent to the Turkish Parliament in 2008. Although it is expected that this new law would define the concept of "personal data", it has still not entered into force. The motives of Art. 135 TPC state that "personal data" should be interpreted as "any information related to a real person". However, the "Regulation on the Processing and Protection of Confidentiality in Electronic Communications", in force since 24 July 2012, defines personal data as "any information related to real or legal persons, whose identity is determined or determinable". As such, there is a discrepancy between various possible definitions of the same term that constitutes the object of the crimes under arts. 135-136 and 138 TPC. The term can only be interpreted through the incorporation of other legal texts, and would still be vague. As a result, there exists a heavy criticism in the Turkish legal literature about the conformity of this crime with the principle of legality[3]. The legal opinion holds that a consequence of this problem is that the said articles are almost never applied in practice[4].

As an additional point regarding the principle of legality, the crime of "violation of the confidentiality of communications" has also been criticized for being extremely vague in its definition. According to this criticism, the terms "communications" and "confidentiality of communications" bear an extremely broad and vague sense, resulting in a breach of the principle[5].

1 ZAFER, Hamide, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, Istanbul, 2010, s. 55, ŞEN, Ersan, "5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İstanbul Barosu Dergisi, Vol: 79, Issue: 2005/3, p. 716.

2 AKYÜREK, Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, Seçkin, Ankara 2011, p. 189.

3 ŞEN, p. 718; AKYÜREK, p. 202.

4 AKYÜREK, p. 202.

5 ŞEN, p. 712.

In addition to crimes regulated under the TPC, another regulation causing problems regarding the principle of legality is the measure of "blocking access" under the Law on the Regulation of Internet Broadcasting and on Combatting Crimes Committed Through Internet Broadcasting (Internet Law). It should be mentioned that this problem does not arise from the definition of a criminal offence, but is rather the result of the application of a measure. As such, the principle in question is "nulla poena sine lege". The measure of "blocking access to Internet content" has been regulated as a criminal procedural measure under art. 8 of Internet Law, to be ordered in cases where a sufficient level of suspicion exists pointing to the commission of crimes listed under the same article[6]. This measure is to be ordered by the judge (or, in urgent cases, by the prosecutor) during criminal investigation, and by the court during the trial. As such, the decision to block access shows the typical characteristics of a criminal procedural measure.

However, the Internet Law also authorizes the Presidency for Telecommunications to order the measure, if the content provider or the service provider of the content resides in abroad, or, if the crime in question is the sexual harassment of minors, or pornography. In these cases, the Presidency can order the measure ex officio, notifying the prosecutor only about the identity of alleged perpetrators, if their identity can be determined. Failing to obey the decision of the Presidency can result in a fine, or even the annulment of the permit to act as an access provider.

The problem regarding the principle of legality is that the measure ordered by an administrative authority involves an assessment on the level of suspicion regarding the commission of a criminal offence. In addition, such measures mostly involve people not related to Turkey, who, according to Turkish legal practice, would be the sole persons eligible to file a motion to annul the measure. Since these people rarely resort to such legal actions, and

6 This list includes the following crimes: Incitement to suicide, sexual harassment of children, facilitating the abuse of narcotic drugs, providing material dangerous to public health, obscenity / pornography, providing place or means for gambling, and crimes against the memory of Atatürk.

since users are not accepted as an eligible party to challenge the decision of the Presidency, the result is an indefinite ban, or blockage of access, to certain websites. The measure does not have any time limit, and is not necessarily followed by a criminal prosecution. This is particularly the case, if the identity of the suspect cannot be determined. Therefore, it can be argued that the measure of blocking access, when applied by the Presidency, no longer fulfils the characteristics of a criminal procedural measure, and lacks the element of provisionality[7]. It rather aims, like a security measure, at the prevention of a dangerous activity. However, security measures are also bound by the principle of legality, and can only be ordered by the court, upon a valid criminal sentence. Thus, the administrative measure provided by the Turkish Internet Law does cause problems regarding the principle of legality.

(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the Internet?

Until now, the Turkish legislator avoided criminalising dual-use software and other conduct that can follow legitimate as well as illegitimate purposes online. However, it would be necessary to mention the undue chilling effects created by the measures provided by the Turkish Internet Law, and particularly their application in practice.

In practice, courts and the Presidency ordering the blocking of an alleged illegal content under art. 8 of the Turkish Internet Law choose to block the access to the entire domain or server, instead of focusing on the specific file. "This (...) resulted not only in blocking the alleged illegal content, but also millions of web pages carrying perfectly legal content through those blocked domains"[8]. A prominent example of such practice has been the blocking of Youtube, as a consequence of content allegedly defaming Atatürk. The ban continued for two years, and prevented users from

7 AKDENİZ, Yaman; Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 32, **http://www.osce.org/fom/41091** (access date: 31.08.2012)

8 AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 28, **http://www.osce.org/fom/41091** (access date: 31.08.2012)

accessing the whole website[9]. As a result, legitimate use of these domains is being suppressed with insufficient access to legal remedies.

A memorandum[10] (dated 1 March 2010) published by the Board of IT Technologies and Communications, Presidency of Telecommunications mentions that websites with illegal content are being warned through notifications before ordering a blocking of the said site. According to this memorandum, this "warn and remove" system resulted in the removal of 3521 different contents. It should be mentioned that this system has neither been mentioned in the Internet Law, nor in the Regulation that has entered into force as its by-law[11].

It should also be mentioned that no statistical data regarding the total number of blocked websites is available since 2009. The memorandum mentioned above included the latest statistical data available. Since May 2009, the Presidency is refraining from sharing this information, even following legal claims under the Public Information Law. There is an ongoing administrative legal action about the matter[12].

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,

- **how are changes in the use of internet and social networks taken into account?**
- **how is the law adapted to technological progress (e.g., by reference to administrative regulations)?**

Criminal legislation regarding ICT entered the Turkish criminal legal system in 1991, through the addition of arts. 525a-525d to the (now abrogated) Criminal Code Nr. 765. The definition included

9 http://haber.mynet.com/youtubea-erisim-engellendi-275750-guncel/ (access date: 18.08.2012)

10 http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010.pdf (access date: 20.08.2012)

11 By-Law on the Regulation of Internet Broadcasting, 30.11.2007 tarihli ve 26716 sayılı Resmi Gazete.

12 AKDENİZ, Yaman, "TİB'e Erişim Engelleme İstatistiklerini Gizlemekten Dava", 13 Mayıs 2010, Bianet (http://bianet.org/bianet/ifade-ozgurlugu/121956-tibe-erisim-engelleme-istatistiklerini-gizlemekten-dava) (access date: 26.08.2010)

some technology-specific wording, and vague terms regarding the object of the crimes. (such as "systems automatically processing data"), which were out-dated and soon caused gaps in criminalisation. With the entry into force of the 2005 Turkish Criminal Code Nr. 5237, these definitions have been changed significantly. However, it must be noted that the amount of criminalised activities is not very high, and still does not include all types of infractions that evolve through technological innovation.

The lack of specific criminal offenses not only results in gaps of criminalisation, but also in overlapping criminal offenses, or overcriminalisation. As an example, the lack of a "skimming" type of offense results in the sentencing of the perpetrator because of various independent offenses (theft, falsification, credit card fraud and, in some cases, obstruction of an IT system).

Crime definitions regarding IT criminality do not involve any references to administrative regulations. Although laws and by-laws related to ICT do give some authority to the Board and the Presidency, these powers are limited to surveillance, monitoring, regulation and administration of measures or fines related to these activities. However, it must be noted that such administrative measures include the blocking of websites, which results in a quasi-criminal mechanism, as mentioned above.

As a result, it can be said that the Turkish legislator does not take any particular precautions for crimes becoming obsolete through technical innovations.

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

Preparatory acts regarding IT criminality are rarely included in the crime definitions. However, there are two instances where

acquisition of possession of material that can be used in crimes involving IT systems has been criminalised.

According to art. 72 IPL, it is a crime punishable by a prison sentence from six months to two years "to produce, offer, sell or ***possess for purposes other than self-use*** programs or technical hardware that have the aim of neutralizing additional programs built to prevent a computer program from being illegally copied".

Additionally, art. 245/2 TPC provides for a crime of "forgery, selling, giving, buying or receiving of false debit or credit cards connected with bank accounts belonging to other people", punishable with a prison sentence of three to seven years.

Although art. 243 TPC regarding "illegally entering, and staying in an IT system" constitutes a crime of abstract endangerment, it can't be said to criminalise mere preparatory acts, since entering illegally would constitute a part of the criminal conduct for the crime of "hacking", art. 244 TPC. Nevertheless, the crime defined under art. 243 TPC has been criticised in the legal doctrine for being too vague and for not including any criteria for a conduct to become harmful to the victim.

There is no widespread legal debate about the inclusion of preparatory acts in crime definitions. However, there are several "warning" accounts about the general trend to include an increasing number of preparatory acts in other legal systems, and it is deemed as an example of "risk criminal law"[13].

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

The crime of "obscenity" or pornography defined under art. 226 TPC has been modelled after the German Criminal Code, and

13 See, i.e. ERMAN, Barış, "Ceza Hukukunun Dönüşümü", Prof. Dr. Duygun Yarsuvat'a Armağan, in print.

includes two types of conduct where the mere possession of pornographic (in the wording of the definition: "obscene") material is a punishable act. Such instances include the possession of pornographic material involving children (punishable with a prison sentence from two to five years) and "hard pornography" defined as pornography involving violence, animals, dead human bodies or "unnatural" sexual behaviour (punishable with a prison sentence of one to four years). Naturally, the term "unnatural sexual behaviour" is extremely vague, and can be interpreted as to include homosexuality, BDSM or fetishism. Such an interpretation would result in the punishing of otherwise legal activities, would violate the prohibition of discrimination, and ultimately, the human rights of the involved.

Another example for a crime of possession of data is provided by the IPL, art. 71. According to this crime definition, it is an act punishable with a prison sentence of one to five years to "possess for purposes other than self-use, or to store" copyright-protected material.

Additionally, the crimes of "illegally obtaining personal data" (art. 136 TPC) and "failing to destroy personal data" (art. 138 TPC) may be mentioned as examples indirectly criminalising the act of possessing certain types of data.

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea?

Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

According to art. 4 of the Internet Law, the author, or content provider, is primarily responsible by his or her own content. However, links to other websites provided by the content provider may result in his or her criminal liability, under the condition that the presentation of the linked content makes it obvious that the content provider accepts the linked content as his or her own, and intents that users access the linked content.

According to art. 6 of the Internet Law, access providers are not obligated to check whether contents users access through their systems are illegal or not. However, they are obligated to comply with the restraining orders issued by the Presidency of Telecommunications, and have to block access to banned sites insomuch as their technical configuration allows this. Non-compliance with this obligation does not result in any form of criminal liability.

According to art. 8/b of the By-Law on the Regulation of Internet Broadcasting, the access provider is obligated to store traffic data related to its services for the duration of one year, and provide for their authenticity, integrity and confidentiality. In case of non-compliance with this obligation, the access provider is subject to an administrative fine.

An additional obligation of the access provider is to give the telephone numbers used to provide access to the Internet and data related to its users to the Presidency of Telecommunications. Again, this obligation is not bound with any sort of administrative or criminal liability.

The hosting provider is not obligated to check the content about its illegality, according to art. 5 of the Internet Law. It is, however, obligated to remove illegal if it has been notified about its existence. The notification occurs following the rules of arts. 8 and 9 of the Internet Law. The former concerns notifications of a court or the Presidency, while the latter is related to real or legal persons whose legal interests have been affected by the content in question. According to art. 9 of the Internet Law, any person claiming to be

affected by an illegal content may notify the content provider or the hosting provider, requesting its removal and replacement with a reply sent by the notifying person. Failing to comply with this "right to reply and removal", however, does not result directly in the criminal liability of the hosting provider, except when it can be proven that the hosting provider has acted as an accomplice to the crime, and shared the criminal intent.

(4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?

The main point of concern regarding Internet crimes in Turkey is the freedom of speech and Internet censorship. This concern is mainly related to the regulations and application of the measure on blocking websites. According to the OSCE report: "The use of the blocking orders to silence speech amounts to censorship and a violation of Article 10 of ECHR"[14]. This practice results in a "prior restraint", which may result in censorship, particularly in cases regarding Internet press[15].

Internet censorship has again been a major point of discussion with the entry into force of the "Rules and Procedures on the Safe Use of the Internet", issued by the Presidency of Telecommunications, on 22 August 2011. These rules included an obligation for Internet access providers to introduce filtering options for families, children and schools. These filters have to comply with "black and white lists" created by the Presidency. Users who choose the "child protection" option would only be able to access sites on the white list, while the filter for "family protection" would automatically ban the sites on the "black list". For users not choosing any filtering option, any site not banned by

14 AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, p. 30, http://www.osce.org/fom/41091 (access date: 31.08.2012)

15 Ibid, p. 31.

the Presidency or by court order would be accessible, as before. Although these lists are optional, it is a cause concern about the freedom of expression that lists are prepared by a central governmental authority. In addition, schools are obligated to choose the "family protection" types of filtering, and are not free to choose between various types of protection.

Another point of concern is the "harm principle", according to which only conduct causing harm or immanent danger may be subject to criminal liability. As explained above, most of the crimes provided under the TPC require a specific harm or at least a concrete danger to occur as a result of the conduct. However, art. 243 TPC regarding "entering, and staying in an IT system does not follow this model, and criminalizes any action without any condition regarding the possibility of harm, or intent towards causing harm. As such, it is a crime of abstract endangerment, and is not subject to any constraint regarding the mens rea.

Other concerns regarding the principle of culpability especially arise because of the practical implementation of the regulations by courts. Due to technical difficulties in investigating IT related crimes, and due to the adaptation issues of the prosecutors and courts, sometimes the standards of strict culpability are not met. As a result, people can be sued or held responsible just for owning the telephone line linked to the IP number that has been used to upload illegal content to the Internet. In such situations, no further investigation is made as to prove the act or intent of the suspect or defendant.

A similar problem arises regarding web 2.0 applications, where the traditional concepts of "content provider" and "hosting provider" are not easily distinguishable. There are no specific regulations concerning the actors of such platforms and their duties to prevent criminal activity within their area of responsibility. This creates a "grey area", where the criminal liability of such actors is not easily determinable.

(5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

There are no specific criminal measures or sanctions targeting cyber criminals. However, a general rule (art. 50/1/d TPC) allows the court to sentence criminals to alternatives for criminal punishment instead of a prison sentence of up to one year. These sanctions are not mentioned according to a *numerus clausus* principle. As a result, it is possible for a court to introduce a temporary ban for a particular offender from using the Internet, if it regards this sanction to be beneficial for special preventive purposes.

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the Internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

Criminal law always plays a leading role in the struggle against the abuse of ICT and the Internet. Turkish legislator always considers the criminal law measures as the best effective legal tools; thus there is a constant tendency on using the criminal law tools to solve the legal problems of ICT and the Internet. Therefore, civil and administrative measures have a secondary role in the field of ICT and the Internet.

In some cases, civil and administrative measures have regulated in a combined manner with criminal measures. For instance, although Law Nr. 5651 mainly regulates the liability of providers and procedures of fighting with Internet crimes; Article 9 of Law Nr. 5651 specifically deals with private matters and regulates 'content removal' and 'right to reply' as non-criminal measures.

According to Article 9, people who claim that their rights are infringed by content on a website may contact to the content provider –or the hosting provider if the content provider cannot be contacted – and request the removal of the infringing content.

The complainants have also a right to reply in Article 9(1) and may request the content or hosting provider to publish their reply on the same web page, the infringing content was published for 1 week.

If the content or hosting providers are failed to comply with a 'removal request' within 48 hours of receipt of request, the complainant can take his case to a local Criminal Court of Peace within 15 days and request the court to issue a removal order and enforce his right to reply as provided under Article 9 (1).

(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?

Although criminal law measures are the most preferable tools to struggle with ICT problems, they are not eligible to use in all problems. Offensive websites and particularly illegal and harmful content carried out in those web sites is a major problem that requires the aid of non-criminal means. In Turkish law, the struggle against these sorts of offensive websites is legislated in Law Nr. 5651- "The Law on the Regulation of the Broadcasting on the Internet and Fighting Against Crimes Committed Through Internet Broadcasting".

In Law Nr. 5651, "blocking Access to websites" is designed both as a criminal procedure measure and also as an administrative measure. However, in particularly, the excessive use of the latter measure brought the "internet censorship" into the agenda and created a real threat for media freedom and freedom of expression. Thus, there is an on-going campaign carried out by the representatives of ICT industry for the abolition or redesign of those measures.

(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to

private networks by password? Does the lack of reasonable self-protection provide a defence for defendants accused of illegally entering or abusing another person's network or abusing their data?

In Turkish legal system, governmental bodies (such as Telecommunications Communication Presidency-*afterwards Presidency*) play a proactive role for the protection of children, young people and families against the illegal and harmful content on the net. The main purpose of the Presidency is to centralize, from a single unit, the surveillance of communications and execution of interception of communications warrants subject to different laws in Turkish legal system. Under Law Nr. 5651, the Presidency was chosen as the organisation responsible for monitoring Internet content and executing blocking orders issued by judges, courts and public prosecutors.

Therefore, the burden of the protection of ICT users usually taken over by the Presidency and ICT users are not much expected to protect themselves by using encryption, passwords or any kind of protective software.

However, a self-protection choice is also provided to ICT users. In February 2011 Turkish government implemented an internet filtering system for citizens which supposed to be enforced in August 2011. Although the 'original' filtering system was compulsory with 4 different profiles when it was first announced; the government had to revise it after the increasing 'censorship' claims of ICT industry and different NGO's. In November 2011 the new 'revised' internet filtering system which is a voluntary model with 2 different profiles implemented. In this model, ICT users have a right to choose one of the 'family' or 'child' profiles which are meant to protect minors from illegal and harmful content on the Net.

Article 7 of Law Nr. 5651 regulates the mass use providers, including internet cafes which needs to fulfil specific requirements in terms of the protection of their computers to a certain extent. Mass use providers are required under Article 7(2) of Law Nr. 5651, to deploy and use filtering tools approved by the

Telecommunications Communication Presidency to block access to illegal Internet content. Mass use providers who operate without an official permission would face administrative fines between 3,000 TL and 15,000 TL.

The illegally entering or abusing another person's network or abusing their data is designed as an offence in Article 243 of Turkish Penal Code and the lack of reasonable self-protection does not provide any kind of defence for the perpetrators.

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

Internet service *(hosting)* providers are regulated at Article 5 of Law Nr. 5651. This provision is introduced a notice-based liability system which is in line with Article 15 of the EU E-Commerce Directive. According to this provision, there is no general obligation to monitor the information which the hosting companies store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity.

However, through Article 5(2), the hosting companies are obliged to take down illegal or infringing content once served with a notice through the Presidency or subject to a court order according to the Article 8 of Law Nr. 5651.

Access providers are also regulated at Article 6 of Law Nr. 5651 and it introduces similar obligations and requirements for Access providers with hosting companies.

Apart from the regulation in Law Nr. 5651, the government published a specific regulation in October 2007 named as "*Regulations Governing the Access and Hosting Providers"* which includes the principals and procedures for granting activity certificates for such providers.

According to the Article 15 and 16, only the traffic data has to be stored by Access providers (for 1 year) and hosting providers (for 6 months). However, there is no regulation which obliges those providers to store users' personal data or to provide such data to law enforcement agencies.

(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?

As mentioned above, "*Regulations Governing the Access and Hosting Providers"* introduces an obligation on the service (both hosting and Access) providers to store "traffic data" for a certain period. Apart from this obligation, service providers are not obliged to register users prior to providing services.

(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

There are no laws or regulations in Turkish legal system limiting the encryption of files or messages on the Internet.

(G) Internationalisation

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?

There are no specific laws on the application of Turkish law to data entered in abroad. Therefore, general rules of Turkish criminal law have to be applied in such cases as well. A brief summary of the rules concerning the application of Turkish law on the offences committed in abroad is in below:

In principal, Turkish laws are applied for the offences that are committed in Turkey (Article 8 of Turkish Penal Code-TPC). In this context, it is necessary to mention that the Turkish penal code defines the concept of territoriality in an extremely broad sense. According to Article 8, any crime shall be considered as committed in Turkey if the conduct has been in part or in full perpetrated on

Turkish territory or if the result has occurred in Turkey. Thus, any act of entering data into the Net in abroad shall be deemed to have been committed in Turkey.

However, there also are certain exceptions which Turkish laws can be applied for the offences committed in abroad.

The first exception is the commitment of an offence in abroad by a Turkish citizen, regulated in Article 11 of TPC. If a Turkish citizen, excluding the offences listed in Article 13, commits an offence in a foreign country which requires punishment with a minimum limit of less than one year imprisonment according to the Turkish laws, and if the offender is found in Turkey, then he is punished according to the Turkish laws provided that he is not convicted in the said foreign country for the same offense and there is possibility to proceed a trial in Turkey. Where the offence requires a prison sentence with a minimum limit of less than one year, the trial is filed only upon rise of complaint by the injured party or the foreign country. In such case, the complaint has to be brought within six months as of the date of entry of the citizen into Turkey.

The second exception is the commitment of an offence in abroad by a foreigner, regulated in Article 12 of TPC:

(1) If a foreigner, excluding the offences listed in Article 13, commits an offence in a foreign country causing injury to Turkey, which requires a punishment with a minimum limit of less than one year imprisonment, and if the offender is found in Turkey, then he is punished according to the Turkish laws. However, the trial is filed upon request of the Ministry of Justice.(2) If the offence mentioned in the afore subsection is committed with the intension of causing injury to a Turkish citizen or a legal entity incorporated according to the Turkish laws and subject to special law, and if the offender is found in Turkey, then the perpetrator is punished according to the Turkish Laws upon complained of the injured party provided that that he is not convicted in the said foreign country for the same offense.(3) If the aggrieved party is a foreigner, he is tried upon request of the Ministry of Justice in case of

existence of the following conditions; a) Where the offence requires punishment with a minimum limit of less than three years imprisonment according to the Turkish Laws; b) Where there is no extradition agreement or the demand of extradition is rejected by the nation where the crime is committed or the person accused of a crime holds citizenship.(4) A foreigner who is convicted of an offence in a foreign country within the scope of first subsection, or the action filed against him is extinguished or the punishment is abated, or the offence committed is not qualified for the prosecution, then a new trial can be filed in Turkey upon request of the Ministry of Justice.

Turkish laws can also be applied in case of commitment of certain "catalogue offences" designed in Article 13 of TPC by the citizens or foreigners in a foreign country. However, cyber crimes are not listed in these catalogue offences.

Lastly, Turkish Penal Code does not recognize the requirement of "double criminality" for offences committed in Turkey (under the principle of territoriality), offences that have been committed against the security of state or against Turkish citizens and legal entities.

(2) To what extent has your country's criminal law in the area of ICT and Internet been influenced by international legal instruments?

Since technology is always one step ahead of the law, the area of ICT and Internet constitute a hard task for national legislators. Therefore, international legal instruments (and legislations in comparative law) are the first sources that are taken into consideration while preparing laws or regulations on ICT and internet.

The first criminal law legislation in the area of ICT was "The Offences Committed Via Computers"-(Article 525a-d of former Turkish Penal Code) enacted in 1991. This former and current (Article 243-246 of Turkish Penal Code) "computer crimes" laws of Turkey are highly influenced by the Directives of EU.

In the same context, "The Law on the Regulation of the Broadcasting on the Internet and Fighting Against Crimes Committed Through Internet Broadcasting" (Law Nr. 5651) is also influenced by international legal instruments. Some specific provisions (e.g. the liability of internet providers-Article 4-7) are taken from EU Electronic Commerce Directive and consistent with the EU legislation.

Nevertheless, it is important to stress that Turkey has not signed the European Convention on Cybercrime yet. Therefore there still are some gaps that need to be filled by the signing and ratification of the Convention. However, some specific provisions of Convention, as in "content related offences-*Child Pornography*" has taken into account in the preparation process of the sexual offences in Turkish Penal Code 2005.

(3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

Despite the fact that the Turkish government is always willing to participate in almost all international legislative activities including the discussions about the harmonisation of cybercrime legislation; the Government is not that willing to announce its work to public by delivering regular reports or by another means.

Therefore, we are not fully informed about the recent contribution of Turkish government on the discussions about the harmonisation of cybercrime legislation. However, several NGO's working in the field of ICT and the Internet are following the recent improvements on international and comparative cybercrime legislation.

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

The current trend of ICT legislation in Turkey is essentially focused on the improvement of electronic commerce. Therefore there are several law drafts concerning the regulation of e-commerce activities in order to meet the requirements of contemporary era.

The first draft is "The Law on the Regulation of Electronic Commerce" which has been prepared to accomplish full harmonisation with the EU E-Commerce Directive. The Draft particularly concerns restrictions regarding spam mail and the protection of personal data in e-commerce activities. Such violations regarding these activities shall be subjected to criminal responsibility.

Another draft is "The Law on The Protection of Personal Data" which has been prepared to provide adequate standards for the protection of personal data for all users.

Hazırlık Kollokyumu Bölüm I

BÖLÜM I: KAVRAM AÇIKLAMASI VE SORULAR

Prof. Dr. Thomas Weigend

(A) Soruların kapsamı (bkz. Giriş ve EK)

Bu Bölümdeki sorular, genel olarak "siber-suç" ile ilgilidir. Bu terim; bilgisayar sistemlerinin ve internetin düzgün işleyişi, gizlilik ve bilgi ve iletişim teknolojilerinin (BİT) içinde depolanan veya bunlar aracılığıyla transfer edilen verilerin bütünlüğü, ya da internet kullanıcılarının gerçek kimlikleri gibi BİT kullanımıyla bağlantılı yararları etkileyen suç oluşturan fiilleri kapsayacak şekilde kullanılmaktadır. Siber-suçluluk alanına giren bütün suçların ve siber-suç soruşturmalarının ortak paydası ve karakteristik özelliği; bunların, bir taraftan bilgisayar sistemleri, bilgisayar ağları ve bilgisayar verileri ile ve diğer taraftan siber sistemler, siber ağlar ve siber verilerle bağlantılı olmaları noktasında bulunabilir. Siber suç alanı, geleneksel bilgisayarların yanında bulut bilişim ağları (cloud cyber spaces) ve siber veri bankalarıyla ilgili suçları da içine alır.

(B) Suç olarak düzenleme

Bu sorularda, siber suç alanındaki suç tanımlarının yalnızca genel özellikleri ile ilgilenildiğini dikkatinize sunarız. Münferit suç tanımlarına ilişkin özel sorular Kongrenin 2. Bölümünde tartışılacaktır.

(1) Hangi özel hukuki yararların ceza hukuku korumasına ihtiyaç duyduğu kabul edilmektedir? (örn. veri işleme sistemleri, depolanmış verilerin gizliliği)?

(2) Aşağıdaki konularla ilgili cezai düzenlemelere tipik örnekler veriniz:

(a) BT (bilgi teknolojileri) sistemlerine yönelik saldırılar,

(b) BT gizliliğinin ihlali,

(c) dijital olarak depolanmış verilerde sahtekarlık ve bu verilerin manipülasyonu,

(d) bilgisayar virüslerinin dağıtılması,

(e) kullanıcıların sanal kimliklerine ilişkin suçlar, örn. sanal kişiliklerin çalınması, bunlara zarar verilmesi veya bunlar üzerinde sahtekarlık fiilleri,

(f) BİT ve İnternet alanındaki diğer yenilikçi, suç oluşturan yasaklar, örn. bir takım sanal görüntülerin yaratılmasını ve elde bulundurulmasını, sanal alanda telif hakkının ihlalini cezalandıran düzenlemeler.

(3) Suç teşkil eden davranış (actus reus / maddi unsur) bu suçlarda tipik olarak ne şekilde tanımlanmaktadır (hareketin, neticenin tarif edilmesi, diğer)? Maddi konu ne şekilde tanımlanmaktadır ("veri", "yazılar", içerikler) ?

(4) Belirli siber suçlar bakımından ceza sorumluluğu özel bir takım fail ve/veya mağdur grupları ile sınırlanmakta mıdır?

(5) BİT ve İnternet alanında ceza sorumluluğu, yalnızca taksirli veya tedbirsiz davranışı içerecek şekilde genişletilmiş midir?

(6) Siber suçların ve "geleneksel" suçların tanımları arasında belirli farklar bulunmakta mıdır?

(C) Yasama tekniği

(1) Yasallık ilkesi ile ilgili özel bir takım sorunlar mevcut mudur (örn. muğlaklık, suçun başka bir takım düzenlemelere atıf yapılarak ucu açık şekilde tanımlanması)?

(2) Yasal düzenlemeler, BİT'in veya İnternet'in hukuka uygun kullanımı üzerindeki yersiz ve aşırı caydırıcı etkilerinden nasıl kaçınmaktadır?

(3) Ceza yasalarının, hızlı teknolojik yenilikler karşısında geri kalmasından nasıl kaçınılmaktadır? Örn;

- İnternet ve sosyal ağların kullanımındaki değişiklikler ne şekilde dikkate alınmaktadır?

- yasa, teknolojik ilerlemeye nasıl uyarlanmaktadır (örn. idari düzenlemelere atıfta bulunularak)?

(D) Cezai düzenlemelerin kapsamı

(1) Ceza yasalarında, "hackleme", "e-dolandırıcılık"[1], bilgisayar sahtekarlığı veya download (karşıdan yükleme) korumasının baypas edilmesi için kullanılabilecek yazılımın bulundurulması gibi, yalnızca kötüye kullanımın devam ettirilmesi riskini taşıyan hazırlık hareketleri ne ölçüde cezalandırılmaktadır? Bu hareketler cezalandırılmaktaysa, bu tür yasaların kabul edilmesi tartışmalara neden olmakta mıdır? Yasa koyucular aşırı cezalandırmanın önüne geçmek için özel bir çaba göstermekte midir?

(2) Bir takım verilerin yalnızca bulundurulması ne ölçüde suç oluşturmaktadır? Hangi alanlarda ve neye dayanarak? Veri "bulundurulması" nasıl tanımlanmaktadır? Bu tanım, geçici olarak bulundurmayı veya yalnızca görüntülemeyi içermekte midir?

(3) Bir takım verilerin bulundurulması ya da bunlara erişim elde etme suç teşkil ettiği takdirde, ceza sorumluluğu servis sağlayıcıları da içerecek şekilde genişletilmekte midir (örn. yer veya içerik sağlayıcılar)? Bunların sorumluluğunun söz konusu olması için, özellikle kusurluluk yönünden gerekli koşullar nelerdir?

(Servis) Sağlayıcılar, sağladıkları ya da erişime sundukları bilgileri gözlemlemek ya da denetlemekle yükümlü müdür? Sağlayıcılar, kullanıcıların kimliklerine ilişkin bilgi sağlamakla yükümlü müdür? Sağlayıcıların, belirli bilgilere erişimi önlemek zorunluluğu bulunmakta mıdır? Yanıt olumlu ise, hangi koşullarda? Bu tür yükümlülükleri yerine getirmemek ceza sorumluluğuna neden olmakta mıdır?

1 Sahte e-posta veya web siteleriyle kullanıcıların kredi kartı bilgileri ele geçirilerek yapılan dolandırıcılık.

(4) BİT ve İnternet suçlarıyla ilgili olarak, belirli hareketlerin suç olarak düzenlenmesi yönünden hangi anayasal sınırlar genel ve özel olarak tartışma konusu olmuştur (örn. ifade özgürlüğü, basın özgürlüğü, örgütlenme özgürlüğü, gizlilik, "başkalarına zarar vermeme ilkesi" (harm principle), (suç oluşturan) bir hareketin bulunması gerekliliği (requirement of an act), kusurlu iradenin gerekliliği (mens rea requirements))?

(5) Yasada siber suçluları hedef alan ceza yaptırımları öngörülmekte midir (örn. internet kullanımının geçici olarak yasaklanması)?

(E) Cezalandırmaya Seçenekler

(1) BİT ve İnternet'in kötüye kullanımı ile mücadelede ceza hukuku, diğer yollarla karşılaştırıldığında nasıl bir rol üstlenmektedir? BİT alanında hukuki ve idari yaptırımlar (zararın giderilmesi, işyerinin kapatılması, vb.), ceza hukukuyla nasıl bir ilişki içerisindedir?

(2) Suç teşkil eden faaliyetler içerisinde olan web siteleriyle mücadelede ceza hukuku alanı dışında ne gibi araçlar kullanılmaktadır / çoğalmaktadır (örn. web sitelerinin kapatılması, bunlara erişimin engellenmesi)?

(3) BİT kullanıcılarının kendilerini ne ölçüde korumaları beklenmektedir (örn. mesajların şifrelenmesi, şifre kullanımı, koruyucu yazılımların kullanılması)? Kişinin bilgisayarının makul ölçüde korunmaması karşısında yaptırımlar öngörülmekte midir, örn. virüsten koruyucu yazılım kullanılması veya özel ağlara erişimin şifre ile engellenmesi? Makul ölçüde oto-koruma eksikliği, bir başkasının ağına yasadışı girmek ve kötüye kullanmakla ya da bir başkasının verilerini kötüye kullanmakla suçlanan kişiler bakımından bir savunma gerekçesi oluşturmakta mıdır?

(F) Kimliğin gizlenmesinin sınırlanması

(1) İnternet servis sağlayıcılarını; İnternet kullanım geçmişi de dahil olmak üzere, kullanıcıların kişisel verilerini depolamakla yükümlü kılan yasalar ya da düzenlemeler bulunmakta mıdır?

Servis sağlayıcılar, kanun uygulayıcı makamlara bu tür verileri sağlamak yükümlülüğü altında tutulabilir mi?

(2) İnternet servis sağlayıcıyı, servis sağlama hizmeti öncesinde kullanıcılara kayıt yaptırma zorunluluğu altında bırakan yasalar ya da düzenlemeler mevcut mudur?

(3) İnternet'te dosyalara ve mesajlara şifrele konulmasını sınırlayan yasalar ya da düzenlemeler bulunmakta mıdır? Şüpheliler, kullandıkları şifreleri ifşa etmeye zorlanabilir mi?

(G) Uluslararasılaştırma

(1) Ulusal düzenlemeler, ülke dışında, internete girilen veriler bakımından uygulanır mı? Yurt dışından veri girmek yönünden bir "çifte cezalandırma" gerekliliği bulunmakta mıdır?[2]

(2) Ülkenizin BİT ve İnternet alanındaki ceza hukuku düzenlemeleri, uluslararası hukuki belgelerden ne ölçüde etkilenmiştir?

(3) Ülkeniz, siber-suç yasalarının uyumlaştırılması konusundaki tartışmalara katılmakta mıdır (örn. BM nezdinde oluşturulan, siber-suç konusunda hükümetlerarası uzmanlar grubu) ?

(H) Gelecekteki gelişmeler

Lütfen ülkenizde BİT ve İnternet suçları konusundaki mevcut yasama eğilimlerini ve hukuki tartışmaları belirtiniz.

2 Is there a requirement of "double criminality" with respect to entering data from abroad?

EK - GENEL DÜŞÜNCELER

Prof. Dr. Thomas Weigend

(1) Bilgi teknolojilerinin korunma ihtiyacı

30 yıl önce dahi bir dereceye kadar güçlükle öngörülen, dünya çapında sosyal hayat, bilgi ve iletişim teknolojileri (BİT) ve internetin düzgün işlemesine dayanmaktadır. Bu bağımlılık hem kamu hem de özel çevreleri kapsamaktadır. Bireysel bir düzeyde, kişiler arası iletişim ve ayrıca bilgi toplamak da dahil olmak üzere boş zaman aktivitelerinin büyük kısmı BİT temellidir. Pek çok kişi; kişisel web sayfaları ve bloglar veya Facebook ve Twitter gibi iletişim servislerinde kendi dijital kişiliklerinin geliştirilmesine ve korunmasına çok fazla yatırım yapmaktadır.

Bu gelişmelerin sonucu olarak, BİT'in bütünlüğüne yönelik saldırılar, sadece kişisel menfaatleri değil, devletin güvenliğini, önemli ticari menfaatleri ve bir bütün olarak ekonomik sistemi de etkileyebilecek ciddi tehditler haline gelmiştir. İnternet üzerinden yapılan bilgisayar korsanlığı (hack'leme) ve veri sahteciliği, dijital olarak aktarılan iletişimin gizliliğinin ihlali ve internet üzerinde "kimlik hırsızlığı"; sadece kişilerin değil, şirketlerin ve devletlerin de refahını tehdit etmektedir.

(2) Suç işleme aracı olarak bilgi teknolojileri ve internet sunucuları ağı

BİT ayrıca hukuken korunan menfaatlere yönelik kimi saldırıları nicel boyutunu da değiştirmiştir. Hâlbuki eskiden, dolandırmak ya da hakaret içerikli bilgileri yaymak isteyen suç eğilimli kişiler, bilginin her muhtemel alıcısına kişisel olarak yaklaşmak zorundaydılar. Artık otomatik e-posta servisleri ya da internet siteleri kullanılarak, bilginin bir saniyede yüzlerce ve hatta binlerce insana yayılması mümkündür. Bilgisayar virüslerinin gizliliği ihlal edilmiş ağlar yaratması (bot networks) da, saldırının etkinliğini arttırabilir ve e-posta adreslerinin kötüye kullanıldığından haberi olmayan kişilerin sahip

oldukları bir milyon kadar bilgisayarı buna dahil edebilmektedir. İnternet sunucuları ağının varlığı ve bilgisayar teknolojisinin sunduğu imkânlar bu şekilde, suça eğilimli kişilerin en az çaba ile en fazla zararı vermesine olanak vermektedir.

BİT'in diğer özellikleri, bireysel ve kolektif menfaatlere yönelik saldırılar için internetin çekici hale gelmesine, daha da fazla katkıda bulunmaktadır. Anonim olarak hareket etme ve sahte kimlik kullanma imkanları, suçlulara fark edilmeme olanağı vermektedir. Aşırı hızlı veri transferi ile birlikte servis sağlayıcıların veri aktarımını düzenli olarak silmesi, suçluların tespit edilmesini daha da karmaşık hale getirmektedir. İnternet sunucuları ağının kaynağının gizli askeri bilgilerin hızlı aktarılması için tasarlanmış bir araç olması, ağ kullanıcılarının saptanmaya karşı korunmasına da katkıda bulunmaktadır: internet sunucuları ağı kasıtlı olarak, üst üste binen ve birbirinden bağımsız iletişim hatlarından oluşan bir ağ olarak tasarlanmıştır. Böylece dışardan gelen müdahalelerle ağın işleyişini bozmak için yapılan her türlü girişime karşı, ağın dayanıklı olması sağlanmıştır. Ağın yapısı, bilginin münferit öğelerinin bir kaynağa doğru izlenmesini ya da etkin bir şekilde bir bilgiye erişimi engellemeyi de oldukça zorlaştırmaktadır.

(3) Ceza hukukunun rolü

(a) BİT' in suça karşı korunması

BİT'in suç teşkil eden saldırılara karşı gösterdiği özel hassasiyet ve bu tip saldırıların sebep olabileceği büyük zarar, BİT dayanaklı iletişimin bütünlüğünü bozacak fiillerin önlenmesi ve cezalandırılmasında ceza hukukunun kullanılmasını zorunlu hale getirmektedir. Birçok hukuk sistemi; veri hırsızlığı, verilerin değiştirilmesi, korunan veri tabanlarının ele geçirilmesi gibi olguları ele alan yasal düzenlemelerde karşılığını bulan cezai hükümlere sahiptir. İnternet sunucuları ağının uluslarüstü karakterinin doğası gereği, uluslararası kuruluşlar bu alandaki ulusal yasal düzenlemeleri uyumlaştırmayı denemişlerdir (Örneğin bkz. Avrupa Konseyi tarafından kaleme alınan Siber Suç Konvansiyonu).

Fiilleri suç olarak kabul etmeye (eksiksiz bir şekilde suç hareketini tanımlamak, bunun ötesine geçmeyi engellemek ve meşru hareket üzerinde soğutucu etki, teknolojik gelişmelere ayak uydurmak) ilişkin genel sorunlarından çoğu, kendilerini bu alanda göstermekte ve bazıları da kanun koyucu Bilgi Teknolojilerinin (BT) bütünlüğüne yapılan saldırıları suç kabul etme yönünde hareket ettiğinde, özellikle şiddetlenmektedir. Bu durumda aşağıdaki spesifik sorular akla gelmektedir:

(i) BİT'teki gelişmeler yeni hukuki menfaatlerin doğumuna neden olmuş mudur ve bunlar nasıl belirlenebilir ve korunabilir? Örneğin "sanal kimlikleri" hırsızlığa ve sahteciliğe karşı korumaya ihtiyaç var mıdır? Eğer varsa bu amaç nasıl gerçekleştirilebilir?

(ii) Ceza hukuku bilgi teknolojisinin hızla ilerlemesine ve internet sunucuları ağının ve doğasına nasıl ayak uydurabilir?

(iii) Korunacak menfaatlerin sürekli değişen ve karmaşık karakterleri göz önüne alındığında, ceza kanunları nasıl kanunilik prensibine uygun olacak kadar yeterince belirli olacak ve bununla birlikte bariz kanun boşluklarından kaçınacaktır? Otomatik bilgisayar sistemi tarafından işlenen fiilin yalnızca bazı neticeleri ortaya çıktığında fark edilmesi mümkün iken, suç teşkil eden fiiller nasıl tanımlanacaktır?

(iv) Hassas BİT menfaatlerini korumadaki diğer vasıtalar karşısında bu hareketleri suç olarak tanımlamak nasıl bir rol oynayabilir ya da oynamalıdır? Ölçülülük ilkesine göre, ceza hukuku BİT sistemlerinin bütünlüğünü korumada birincil vasıta olarak kullanılmamalıdır. Ceza hukuku örneğin telif hakkı ihlallerinden doğan zarara ilişkin tediyeler gibi etkili özel hukuk yaptırımlarına ek olarak uygulanmalı mıdır? BİT'in kendisi saldırılara karşı savunma için etkili araçlar sağlamaktadır (Örneğin şifreleme, anti-virüs programları, hack'lemeye karşı programlar, telif hakları alınmış eserlerin izinsiz indirilmesine karşı koruma). Bu durum ceza hukukunun sadece bu cihazların yeterli koruma sağlayamadığı durumlarda mı uygulanması gerektiği sorusunu doğurmaktadır. Kullanıcıla-

rın koruma programları yüklemelerinin yasal olarak zorunlu tutulması ve kişinin bilgisayarına virüs bulaşmasına karşı makul bir koruma sağlanması konusunda gösterdiği herhangi bir hataya karşı, cezai sorumluluğun doğması da düşünülebilir (çünkü özensiz kullanıcılar virüslerin yayılmasına yardımcı olmaktadırlar).

(v) Birçok hukuk sisteminde zararlı davranışın yalnızca hazırlığını teşkil eden hareketler, genellikle cezalandırılabilir bir fiil olarak görülmemektedir. Ancak BİT'e ilişkin suçlar bağlamında, bazen yayılan zarar o kadar büyük olabilir ki bazı hazırlık hareketleri de cezalandırılabilir. Örneğin, bazı hukuk sistemleri özellikle internet suçu işlemek için tasarlanmış yazılımların arzı ve satımına (veya hatta elde bulundurulmasına) karşı cezai hükümlere sahiptirler (Örneğin, şifrelerin kırılması veya internet üzerinden dosya indirme güvenliğinin aşılması). Avrupa Konseyi'nin Siber Suç Sözleşmesine uygun olarak, bazı devletler bilgisayar dolandırıcılığı suçunun işlenmesine yardımcı olmak için tasarlanmış yazılımların satım veya alımını da suç olarak kabul etmektedir. BİT suçlarının meşru kapsamının sınırları hala tartışmaya ihtiyaç duymaktadır.

(b) BİT aracılığıyla işlenen suçlara karşı koruma

Yukarıda da değinildiği üzere BİT, suç işlemeye eğilimli kişiler için yepyeni bir fırsatlar dünyası yaratmıştır. Ceza hukuku düzenlemeleri, sıradan suçların BİT ve internetin kötüye kullanılması suretiyle işlenmesinin denetlenmesi ve cezalandırılması için özel araçlar kullanılarak bu gelişmeye uyum sağlamayı amaçlayabilir. Soruların odağı bu yasal tedbirler olmadığından bu konulara burada kısaca değinilecektir.

(i) Anonimliği sınırlandırma

Suç işleme imkânı sunan internetin bir cephesi de, ağın sağladığı anonimliğin korunmasıdır. Anonimliğin sınırlandırılmasında, suçluların bulunması ve kimliklerinin belirlenmesi ihtimalini artırmak amacıyla alınabilecek birkaç önlem önerilmiştir. Avrupa Birliği tarafından dayatılan önlemlerde (tartışmalı olan) biri de, erişim sağ-

layıcılarının, veri transferlerinin kaynak bilgisayara kadar izlerinin takip edilmesini mümkün kılmak amacıyla, veri transferlerini birkaç ay süreyle saklama zorunluluğudur. Bu konuda tartışmalı olan diğer tedbirler, şifrelemenin karmaşıklığını sınırlandırma ve bilgisayar sahiplerinin şifrelerini açıklamaya zorlanmasıdır. Bu gibi tedbirler ağır suçların devam eden soruşturması bağlamında savunulabilir görünebilir, ancak bu tedbirler en nihayetinde internetin izin verilebilir kullanım alanına taşacaktır ve bunların kullanıcıların özel hayatına ilişkin meşru menfaatlerini ihlal etmesi sebebiyle internetin çekiciliğini (ve böylece faydalanılabilirliğini) ciddi oranda azaltma olasılığı vardır.

(ii) İçeriğin kontrolü

Yasal sistemlerin, yazılı ya da basılı materyallere (Örneğin pornografiye, dini ya da ırksal nefrete teşvik, suç işlemenin öğretilmesi, devlet sırlarının, askeri ve ticari sırların ifşası) ilişkin cezai yasakları, BİT yoluyla dağıtılan benzeri materyaller üzerinde de genişletmeye değin anlaşılabilir bir eğilimleri vardır. Bu eğilim, bir takım spesifik sorunları da beraberinde getirir; ilk olarak, internet kullanıcıları ağının uluslarüstü karakteri, ulusal standartların uygulanmasını zorlaştırır ve keza ifadenin kısıtlandırılmasının uygun kapsamı üzerine uluslararası bir anlaşmaya varmak da zordur. İkinci olarak, ceza hukukuna son çare olarak başvurulması kuralı, cezai yaptırım yerine başvurulan tedbirlerin de, bu alanda en azından eşit ölçüde etkili olup olmadığı sorununu ortaya çıkarmaktadır. Üçüncü olarak, internetin anonimliği, cezai sorumluluğun kanuna aykırı içeriklerden (kolaylıkla belirlenebilir, saptanabilir) internet servis sağlayıcılarına kadar genişletilip genişletilemeyeceği sorusunu doğurur. Bu da, internet içeriğinin etkin denetimi yapılmaya çalışıldığında, anonimlik zırhının delinmesi zorluğunu azaltabilecektir.

İfadenin yasaklanmasına (yahut korunmasına) değin ulusal menfaatler ve standartlardaki farklılık, aşılması güç bir etmendir (bu boyut Kongre'nin 4. Bölümünde ana hatlarıyla incelenmiştir). Hukuk sistemleri, (i) Hangi içeriği zararlı ve tehlikeli olarak kabul ettikleri ii) İfade özgürlüğüyle korunan materyaller ile yayılması ve hatta bulundurulması cezai yargılamaya tâbi materyaller arasında, sınırı

nereye koyacakları konularında son derece farklılık göstermektedir. Bu farklılıklar, ulusal ceza hukukunun, internet üzerinde bulunan (fakat "muhtemelen" yabancı ülkelerde bulunan yabancı vatandaşlar tarafından koyulmuş) materyallere uygulanabilmesi gibi teknik bir sorunun ötesinde; muhtemel içeriklere ilişkin suçların yargılanmasında uluslararası işbirliğinin önünde büyük bir engel teşkil etmektedir. Bu alandaki uluslararası sözleşmeler bu sorunu çözebilir fakat bunların sakıncası da, eylemleri suç olarak kabul etmeyi azami seviyeye çıkarma eğiliminde olmalarıdır. Çünkü, katılan her devlet, yasak fiiller listesine kendi yasal sistemleri içinde öngördükleri suçları da eklemekte ve bireyin ifade özgürlüğü için nefes alacak yeri korumaya yönelik yeterli siyasi destek bulunmamaktadır.

Suç teşkil eden içeriklere ilişkin ceza yargılamasına alternatif olarak, sakıncalı internet sitelerine (yazılım kullanımı vasıtasıyla) erişimin engellenmesi ve bu sitelerin silinmesidir. Bununla birlikte, erişimin engellenmesi teknik olarak mümkün olsa dahi, bunun etkili olabilmesi için tüm devletlerin işbirliğine ihtiyaç vardır. Çünkü bir devlet birimi tarafından yapılan engelleme, söz konusu kurumla işbirliği yapmayan yabancı bir firmanın sağladığı erişim imkânının kullanılmasıyla, kolayca aşılabilmektedir. İnternet sitesinin silinmesi, mümkünse bile, rencide edici internet sayfası başka bir isim altında kolayca (hatta otomatik olarak) yeniden yüklenebileceğinden, benzer şekilde sınırlı etkiye sahip olabilmektedir.

Bu durum, erişim ve/veya servis sağlayıcılarının, yasa dışı içeriği korudukları ve erişilebilir tuttukları için cezai sorumluluğu sorununa yol açmaktadır. Bu yaklaşıma göre, sağlayıcılar interneti 'denetlemeye' zorlanacak ve eğer gerekirse internete sansür uygulayacaklardır. İçerik sağlayıcılarının ya yasa dışı içerikler hakkında yapılan şikâyetlere karşı harekete geçmeleri ya da yasaklanmış materyaller için sağladıkları içerikleri temkinli bir şekilde soruşturmaları gerekebilir. Bu teknik olarak mümkün olsa bile, içerik sağlayıcılarına hangi yasal dayanakla (masraflı bir) interneti denetleme yükümlülüğü yüklenebileceğine dair norma ilişkin soruyu meydana çıkmaktadır. Eğer sağlayıcıların pozitif hukuki yükümlülükleri kabul edilirse, onların bu görevin ihlalinden doğan cezai sorumlulukları yataklık veya ihmal doktrinine dayandırılabilir. Bu bağlamda sağlayıcıların sorumluluğu Genel Kısmın 1. Bölümünde tartışılacaktır.

Hazırlık Kollokyumu Bölüm I

TÜRKİYE ULUSAL GRUP RAPORU

Doç. Dr. Vesile Sonay Daragenli Evik*
Yard. Doç. Dr. Hasan Sınar**
Yard. Doç. Dr. Barış Erman***
Dr. Gülşah Kurt****

(B) Suç olarak düzenleme[1]

Bu sorularda, siber suç alanındaki suç tanımlarının yalnızca genel özellikleri ile ilgilenildiğini dikkatinize sunarız. Münferit suç tanımlarına ilişkin özel sorular Kongrenin 2. Bölümünde tartışılacaktır.

(1) Hangi özel hukuki yararların ceza hukuku korumasına ihtiyaç duyduğu kabul edilmektedir? (örn. veri işleme sistemleri, depolanmış verilerin gizliliği)?

Bir kısmı Türk Ceza Kanunu'nda (TCK), bazıları ise özel kanunlarda düzenlenmiş olan çeşitli suçlar tarafından korunan pek çok hukuki yarardan söz etmek mümkündür. Bu nedenle, çeşitli suçlar tarafından hangi hukuki yararların korunduğunu tek tek belirtmek daha yerinde olacaktır.

"Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma" suçu açısından korunan hukuki yararlar; bilişim sisteminin güvenliği, verilerin gizliliğinin korunması ve özel hayatın dokunulmazlığıdır. "Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçu açısından ise; bilişim sistemi veya içerdiği veriler üzerinde tasarruf yetkisi olan kişinin herhangi bir engel, arıza, gecikme olmaksızın ulaşması ve kullanmasındaki menfaati korunmaktadır.

* Galatasaray Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

** İstanbul Kemerburgaz Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

*** Yeditepe Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

**** Galatasaray Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

"Bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlama" suçu açısından; failin bilişim sistemi aracılığıyla gerçekleştirdiği eylemler neticesinde zarara uğratılan maddi veya manevi hak, suçla korunan hukuksal değeri oluşturmaktadır. "Banka ve kredi kartlarının kötüye kullanılması" suçu açısından; kişilerin mal varlığı, kişisel güven, hukuk alanında inandırıcılığı olan belgelere olan güven korunmaktadır. "Kişisel verilerin kaydedilmesi" suçu ile "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" suçu açısından; kişisel veriler, kişilerin özel hayatı ve hayatın gizli alanı korunmaktadır. "Kişisel verilerin yok edilmemesi" suçu açısından; kişisel veriler ve bunlar açısından oluşturulmak istenen güvenirlik, kamu idaresinin güvenilirliği ve işleyişi korunmaktadır. "Haberleşmenin gizliliğini ihlal" suçu ile; kişiler arasındaki haberleşmenin gizli kalmasındaki menfaatleri, "haberleşmenin engellenmesi" suçu açısından; haberleşmenin kendisi, kesintisiz, engelsiz olarak haberleşme özgürlüğü korunmaktadır.

"Bilişim sistemlerinin kullanılması yoluyla işlenen hırsızlık" suçunda mal varlığı, "müstehcenlik" suçu açısından genel ahlak, özellikle çocukların cinsel gelişiminin korunması söz konusudur.

5846 sayılı düzenlenen "bilişim yazılımlarını hukuka aykırı olarak çoğaltmak veya kullanmak" suçu açısından yazılım üzerinde hak sahibinin mal varlığı, manevi hakları korunmaktadır.

Bundan başka; 15.01.2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suçlar (elektronik imza oluşturma verilerinin izinsiz kullanma, verilerin veya aracın elde edilmesi, verilmesi, kopyalanması, izinsiz elektronik imza oluşturulması, elektronik sertifikalarda sahtekarlık suçları) açısından ise hukuk alanında inandırıcılığı olan verilere karşı güven korunmaktadır.

Son olarak, 7258 sayılı Futbol ve diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun'da yer alan "yurt dışında oynatılan her çeşit bahis veya şans oyunlarının İnternet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkan sağlama" suçu ile genel ahlak ve devletin verdiği izin ve yetkiyle bahis ve şans oyunları düzenleyen kuruluşların mali çıkarlarıdır.

(2) Aşağıdaki konularla ilgili cezai düzenlemelere tipik örnekler veriniz;

(a) BT (bilgi teknolojileri) sistemlerine yönelik saldırılar

TCK 243'te bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı girme ve sistemde kalma suçu bir yıla kadar hapis veya adli para cezası ile cezalandırılmıştır. Bu fiillerin bedel karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde ceza yarı oranına kadar indirilmektedir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse altı aydan iki yıla kadar hapis cezasına hükmolunur.

TCK madde 244/1'de bir bilişim sisteminin işleyişini engelleme veya bozma, yok etme bir yıldan beş yıla kadar hapisle cezalandırılmıştır. 244/2'de verileri bozma, yok etme veya değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka yere gönderme altı aydan üç yıla kadar hapis cezası ile cezalandırılmaktadır. TCK 244/3'e göre bu fiillerin banka ve kredi kurumuna ya da bir kamu kurumu veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde ceza yarı oranında artırılır.

TCK 244/4'te bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlama fiili, başka bir suçu oluşturmaması halinde iki yıldan altı yıla kadar hapis cezası ile cezalandırılmaktadır.

Doktrinde TCK 244. maddede bilişim sisteminden veri ele geçirmenin suç olarak düzenlenmemesinin bir eksiklik olduğu dile getirilse de[1]; bu eksiklik, kişisel veriler hakkında TCK'nun 136. maddesinde kişisel verilerin hukuka aykırı olarak ele geçirme, yayma suçu ile ve eser niteliğinde kabul edilen veriler açısından FSEK'nun 71. maddesinde düzenlenen suç ile giderilebilmektedir.

(b) BT gizliliğinin ihlali

TCK 132'de haberleşmenin gizliliğini ihlal suçu düzenlenmiştir. Buna göre kişiler arasındaki haberleşmenin gizliliğini ihlal bir yıldan üç yıla kadar hapis cezası ile cezalandırılmaktadır. Bu gizlilik ihlali, haberleşme içeriklerinin kaydı suretiyle gerçekleşirse verilecek

1 Avşar Zakir-Öngören Gürsel, Bilişim Hukuku, Türkiye Barolar Birliği Yayını, İstanbul, 2010, 137.

ceza bir kat arttırılmaktadır. Haberleşmenin içeriğini hukuka aykırı olarak ifşa ise iki yıldan beş yıla kadar hapisle cezalandırılmaktadır. İfşa edilen bu verilerin basın ve yayın yoluyla yayınlanması halinde de aynı ceza verilmektedir.

134'te kişilerin özel hayatının gizliliğini ihlal etme bir yıldan üç yıla kadar hapis cezası ile cezalandırılmaktadır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde verilecek ceza bir kat arttırılmaktadır. 134/2'ye göre kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa etme iki yıldan beş yıla kadar hapis cezası ile cezalandırılmaktadır. Başka bir normun ihlalini teşkil etmediği sürece, özel hayatın gizliliğine ilişkin her türlü fiil bu maddeye göre cezalandırılacaktır.

TCK madde 135'te hukuka aykırı olarak kişisel verilerin kaydedilmesi, altı aydan üç yıla kadar hapis ile cezalandırılmaktadır. 136. maddede kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme bir yıldan dört yıla kadar hapis cezası ile cezalandırılmaktadır.

TCK'nun 138. maddesine göre kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemeleri altı aydan bir yıla kadar hapis cezası ile cezalandırılmaktadır.

(c) Dijital olarak depolanmış verilerde sahtekarlık ve bu verilerin manipülasyonu,

TCK 244/2'de; bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, siteme veri yerleştirme, var olan verileri başka yere gönderme altı aydan üç yıla kadar hapis cezası ile cezalandırılmaktadır.

Ayrıca TCK 245'te banka ve kredi kartlarının kötüye kullanılması suçu düzenlenmiştir. Buna göre başkalarına ait banka hesaplarıyla ilişkilendirerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme üç yıldan yedi yıla kadar hapis cezası ile cezalandırılmaktadır. 5464 sayılı Banka ve Kredi Kartları

Kanunu'nda (madde 3/e), "kredi kartı", fiziki varlığı bulunmayan kart numarasını da içerecek şekilde tanımlanmıştır. Böylece, kart numarası kullanılmak suretiyle elektronik ortamda gerçekleştirilen sahtekarlık fiilleri de 245. maddenin ihlalini teşkil edebilecektir.

(d) Bilgisayar virüslerinin dağıtılması

Türk hukukunda bilgisayar virüslerinin dağıtılması ayrı bir suç olarak düzenlenmediğinden, bilgisayar virüsleri bulaştırılması suretiyle bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme söz konusu ise, bu fiil, TCK 244'de düzenlenen suç tipine göre bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun kapsamında cezalandırılacaktır.

Ayrıca bilgisayar virüsünün dağıtılması sonucunda BT sisteminin zarar görmesi halinde, bu fiil mala zarar verme suçu kapsamında incelenebilir (TCK madde 151).

(e) Kullanıcıların sanal kimliklerine ilişkin suçlar, örn. sanal kişiliklerin çalınması, bunlara zarar verilmesi veya bunlar üzerinde sahtekarlık fiilleri

Bu konuda özel bir suç tipi olmamakla birlikte, bu kapsamda işlenen fiiller, "kişilerin özel hayatının gizliliğini ihlal etme" şeklinde nitelendirildiği takdirde TCK madde 134'e göre cezalandırılabilir. Yine, bu fiiller, bir kimsenin onur, şeref veya saygınlığına saldırı niteliğinde kabul edilirse TCK 125'te düzenlenen hakaret suçuna veya kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme şeklinde nitelendirildiğinde TCK madde 136'ya göre cezalandırılabilir. İşlenen fiil, bu sayılan suçlardan hiçbirine girmediği takdirde, hukuka aykırı yarar sağlama söz konusu ise, TCK madde 244/4 kapsamında değerlendirilebilir.

(f) BİT ve İnternet alanındaki diğer yenilikçi, suç oluşturan yasaklar, örn. bir takım sanal görüntülerin yaratılmasını ve elde bulundurulmasını, sanal alanda telif hakkının ihlalini cezalandıran düzenlemeler

Genel olarak, fikir ve sanat eserleri üzerindeki mali hakların ihlali FSEK'nun 71. maddesinde suç olarak düzenlenmiştir. Bu maddeye

göre; "bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur. Buna göre; İnternet üzerinde FSEK kapsamında korunan "fikir ve sanat eseri" niteliğindeki her türlü içerik bu suçun konusunu teşkil edebilecektir.

Aynı Kanunun ek 4 üncü maddesinde; bu Kanunda tanınmış hakları ihlal eden "içerik sağlayıcılar" bakımından bir "uyar-kaldır" sistemi öngörülmüştür. Bu maddeye göre; hak ihlalini gerçekleştiren içerik sağlayıcıların, ancak hak sahibi gerçek veya tüzel kişinin usulüne uygun olarak başvurmasına karşın, ihlale devam etmeleri halinde ceza sorumluluğu doğacaktır. İhlalin devamı halinde Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlale devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlalin durması (ihlal teşkil eden içeriğin çıkarılması) halinde içerik sağlayıcıya yeniden servis sağlanır.

İnternet ve BİT alanındaki bir diğer yenilikçi yasak, elektronik imza sahtekarlığı suçudur. 5070 sayılı Elektronik İmza Kanununun 16. maddesinde düzenlenen "imza oluşturma verilerinin izinsiz kullanımı" ve 17. maddede yer alan "elektronik sertifikalarda sahtekarlık" suçlarının da bu kapsamda değerlendirilmesi uygun olacaktır. 16. maddede düzenlenen "imza oluşturma verilerinin izinsiz kullanımı" başlığı altında; "*elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde etmek, vermek, kopyalamak ve bu araçları yeniden oluşturmak ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturmak*" fiilleri, bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılmaktadır. 17. maddede ise, "Elektronik sertifikalarda sahtekarlık" başlığı altında; "*tamamen veya kısmen sahte elektronik sertifika oluşturmak veya geçerli olarak oluşturulan*

elektronik sertifikaları taklit veya tahrif etmek ile bu elektronik sertifikaları bilerek kullanmak" iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılan bir suç olarak düzenlenmiştir.

(3) Suç teşkil eden davranış (actus reus / maddi unsur) bu suçlarda tipik olarak ne şekilde tanımlanmaktadır (hareketin, neticenin tarif edilmesi, diğer)? Maddi konu ne şekilde tanımlanmaktadır ("veri", "yazılar", içerikler)?

Bu suçlarda maddi unsuru oluşturan hareketler tanımlanırken genelde seçimlik hareketli suç şeklinde bir tercihte bulunulmuştur. Ancak TCK 243'te düzenlenen bilişim sistemine girme suçu, bilişim sitemine girme ve orada kalmaya devam etme şeklinde birden fazla hareketli suç şeklinde düzenlenmiştir.

Yine, BT-bağlantılı pek çok suç bakımından; maddi unsur, hareketin tarif edilmesi şeklindedir. Neticenin açıkça öngörüldüğü tek düzenleme, TCK'nun 243. maddesinde, bilişim sistemine hukuka aykırı olarak girme sonucunda sistemin içerdiği verilerin yok olması veya değişmesinin suçun netice sebebiyle ağırlaşmış hali olarak öngörüldüğü üçüncü fıkrada yer almaktadır.

Bazı hallerde, BİT alanındaki suçların tehlike suçu olarak düzenlendiği görülmektedir. Bilişim sistemine hukuka aykırı olarak girme ve orada kalma fiili neticesinde herhangi bir zarar oluşmasa dahi, bu fiil ceza yaptırımı gerektirmektedir. Bu bakımdan 243. maddedeki suçun basit hali bir soyut tehlike suçu teşkil etmektedir. Bununla birlikte, bu alandaki suçların bir çoğunda, yasal tanımın bir sonucu olarak açıkça zararlı bir neticenin ortaya çıkması aranmaktadır.

Suçların maddi konuları bakımından ise; TCK 243'teki bilişim sistemine girme ve 244/1'deki bilişim sisteminin işleyişini engelleme, bozma ve 244/2'deki bilişim sistemindeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçlarında "bilişim sistemi", "bilişim sistemindeki veriler" terimlerinin sıklıkla tekrarlandığı görülmektedir.

TCK'nun 135, 136 ve 138. maddelerinde düzenlenen suçlar ise kişisel verilere ilişkindir. Bununla birlikte, "kişisel veri" terimi, bu maddelerde tanımlanmamıştır. Esasında, Türk hukuk öğretisinde, aşağıda açıklanacağı üzere "kişisel veri" kavramının kapsamı konusunda bir tartışma bulunmaktadır.

Bu başlık altında belirtilmesi gereken bir diğer konu, TCK'nun 6. maddesinde yer alan "basın ve yayın yoluyla" tanımıdır. Buna göre; bu terim, İnternet de dahil olmak üzere elektronik kitle iletişim aracıyla yapılan yayınları da kapsar. Bu terim, suçun unsuru ya da ağırlaştırıcı neden olarak pek çok yerde kullanılmaktadır. Söz konusu terime, aynı zamanda kişiler arasındaki haberleşmenin içeriklerinin hukuka aykırı olarak ifşasına ilişkin 132. maddede ve kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa edilmesini düzenleyen 134. maddede de yer verilmektedir. Bu nedenle, bu suçlar İnternet aracılığıyla işlendiği takdirde, basın ve yayın yoluyla işlendikleri kabul edilmelidir.

(4) Belirli siber suçlar bakımından ceza sorumluluğu özel bir takım fail ve/veya mağdur grupları ile sınırlanmakta mıdır?

Türk hukukunda, bilişim suçlarında fail ve mağdur grupları açısından yasamızda herhangi bir sınırlandırma bulunmamaktadır. Bu suçların faili de mağduru da herkes olabilir. Ancak kişisel verilerin kaydedilmesi suçu (TCK md. 135) ile kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma, ele geçirme suçunun (TCK md. 136) kamu görevlisi tarafından görevin verdiği yetki kötüye kullanmak suretiyle işlenmiş olması cezayı ağırlaştıran sebep olarak öngörülmüştür. Bundan başka, "verileri yok etmeme" (TCK md. 138) suçu, yalnızca, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlarca işlenebilir.

Aynı şekilde, 5070 sayılı EİK'nun 16 ve 17. maddelerinde öngörülen suçların "elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenmesi" halinde cezaların yarıya kadar artırılacağı düzenlenmiştir.

(5) BİT ve İnternet alanında ceza sorumluluğu, yalnızca taksirli veya tedbirsiz davranışı içerecek şekilde genişletilmiş midir?

BİT ve İnternet alanında ceza sorumluluğu yalnızca kasten işlenen fiillerde söz konusudur. TCK 21'e göre suçun oluşması kastın varlığına bağlıdır. TCK 22'ye göre ise taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır. BİT ve İnternet alanındaki suçların taksirle işlenebileceğine ilişkin yasal düzenleme yapılmamıştır. Ancak yasa koyucu TCK 243/2 'de (netice sebebiyle ağırlaşmış suçlarda fiilin kastedilenden daha ağır veya başka netice açısından sorumluluk için en azından taksiri arayan TCK 23 ile birlikte değerlendirildiğinde) bilişim sistemine girme nedeniyle sistemin içerdiği verilerin taksirle yok edilmesi veya değiştirilmesi durumunu nitelikli hal olarak öngörmüştür.

(6) Siber suçların ve "geleneksel" suçların tanımları arasında belirli farklar bulunmakta mıdır?

Siber suçlarla geleneksel suçların tanımları arasında belirgin farklar yoktur. Yalnızca TCK 243'te düzenlenen bilişim sistemine girme suçu, 132. maddedeki haberleşmenin gizliliğini ihlal suçu, 134/2 maddedeki kişilerin özel hayatına ilişkin görüntü veya seslerin ifşa edilmesi suçu, 135. maddedeki kişisel verilerin kaydedilmesi suçu, 136. maddedeki kişisel verilerin bir başkasına verme, yayma veya ele geçirme suçu açısından hukuka özel aykırılık öngörülmüştür. Öğretide ağırlıklı olarak kabul edilen görüşe göre; bunun anlamı; bu suçlar açısından failin gerçekleştirdiği eylemin hukuka aykırı olduğunu bilmesinin aranacağıdır.

(C) Yasama tekniği

(1) Yasallık ilkesi ile ilgili özel bir takım sorunlar mevcut mudur (örn. muğlaklık, suçun başka bir takım düzenlemelere atıf yapılarak ucu açık şekilde tanımlanması)?

Yasallık ilkesi ile ilgili bir takım sorunlar mevcut olmakla birlikte, bunları bilişim suçlarının niteliğinden kaynaklanan özel sorunlar olarak sınıflandırmak mümkün değildir. Bu sorunlar, kanunda doğrudan bilişim suçu olarak tanımlanan hükümler bakımından değil,

bilişim sistemleri aracılığıyla işlenebilecek bir takım suçlar bakımından ortaya çıkmaktadır. Özellikle bilişim sistemi aracılığıyla işlenen özel hayatın gizliliğini ihlal (TCK md. 134), kişisel verilerin kaydedilmesi (TKC md. 135), kişisel verileri hukuka aykırı olarak verme veya ele geçirme (TCK md. 136) ve kişisel verilerin yok edilmemesi (TCK md. 138) suçlarına ilişkin düzenlemeler "yasallık" ilkesi bakımından ciddi sakıncalar içermektedir.

134. maddede "kişilerin özel hayatının gizliliğini ihlal etme" bir yıldan üç yıla kadar hapis cezası ile cezalandırılmaktadır. Suçun konusunu, halen tartışmalı ve sınırları yer yer belirsizleşen bir kavram olan[2] "özel hayat"ın oluşturması nedeniyle, hükmün geniş bir içeriğe ve uygulama alanına sahip olacağı ve yasallık ilkesi bakımından sıkıntı doğurabileceği kabul edilmektedir[3].

TCK madde 135'teki suçun maddi unsurunu "hukuka aykırı olarak kişisel verilerin kaydedilmesi" oluşturmaktadır. Bununla birlikte suçun maddi konusunu oluşturan "kişisel veri" Türk hukukunda tanımlanmamıştır. Bu konuyla ilgili olarak bir yasa tasarısı hazırlanmış ve 2008 yılında TBMM Başkanlığı'na sevk edilmiştir. Ancak, henüz tasarı yasalaşarak yürürlüğe girmemiştir. 135. maddenin gerekçesinde, kişisel verinin; "***gerçek kişiyle ilgili her türlü bilgi"*** olarak kabul edilmesi gerektiği belirtilmektedir. Son olarak 24.07.2012 tarihinde yayınlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik"te kişisel veri; "***belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"*** olarak tanımlanmıştır. Böylece, TCK'nun 135, 136 ve 138. maddelerinde öngörülen suçların konusunu oluşturan aynı kavramın çeşitli tanımları arasında bir tutarsızlık bulunmaktadır. Söz konusu terim, ancak diğer yasal metinlerle birlikte yorumlanabilirse de, kişisel verinin kapsamı tam olarak belirlenebilir değildir. Bu nedenle, söz konusu hükümler haliyle yasallık ilkesi açısından sıkıntı yaratabilecek niteliktedir. Öğre-

2 ZAFER, Hamide, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, İstanbul, 2010, s. 55. Aynı yönde bkz. ŞEN, Ersan, "5237 sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İstanbul Barosu Dergisi, Cilt: 79, Sayı: 2005/3, s. 716.

3 AKYÜREK, Güçlü, Özel Hayatın Gizliliğini ihlal Suçu, Seçkin, Ankara 2011, s. 189.

tide de bu yönde eleştiriler bulunmaktadır[4]. Hatta TCK'nın yürürlüğe girdiği 2005 yılından bu yana maddenin pek uygulamasının bulunmamasının bu eksikliği ortaya koyduğu ileri sürülmüştür[5].

Yukarıdaki hükümlerin yanı sıra, öğretide 132. maddede düzenlenen "haberleşmenin gizliliğini ihlal" suçu bakımından da benzer eleştiriler getirilerek, "haberleşme" ve "haberleşmenin gizliliği" kavramlarının son derece geniş ve soyut olması nedeniyle, bu hükümlerin de yasallık ilkesini ihlal eder nitelikte olduğu ileri sürülmüştür[6].

Bu konuda, TCK'da yer alan bu suçların yanı sıra, "yasallık" ilkesi bakımından sakınca doğurabilecek bir diğer düzenlemenin yer aldığı 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanundan da söz edilmesi gereklidir. Ancak bu Kanunda, doğrudan bir fiili suç haline getiren bir düzenlemenin yasallık ilkesine aykırılığı değil, bir ceza muhakemesi tedbiri olarak "erişimin engellenmesi" kararının uygulanmasından doğan bir halin, dolaylı olarak yasallık ilkesi karşısında yarattığı sakıncalardan bahsedilecektir. Diğer bir ifadeyle burada asıl sorun ilkenin bir diğer sonucu olan "kanunsuz ceza olmaz" kuralı bakımından ortaya çıkmaktadır. Bu Kanunun 8. maddesinde; İnternet ortamında yapılan ve içeriği bu maddede sayılan suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verileceği düzenlenmiştir[7]. 8. maddenin ikinci fıkrasına göre bu tedbire; soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından karar verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu bakımdan, erişimin engellenmesi tedbiri bir ceza muhakemesi tedbirinin tipik özelliklerini taşımaktadır.

4 ŞEN, a.g.m., s. 718; AKYÜREK, s. 202.

5 AKYÜREK, s. 202.

6 ŞEN, a.g.m., s. 712.

7 5651 sayılı Kanunun 8/1. Maddesinde bu suçlar; "a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan; 1) İntihara yönlendirme (madde 84), 2) Çocukların cinsel istismarı (madde 103, birinci fıkra), 3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), 4) Sağlık için tehlikeli madde temini (madde 194), 5) Müstehcenlik (madde 226), 6) Fuhuş (madde 227), 7) Kumar oynanması için yer ve imkân sağlama (madde 228) suçları; b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar" olarak sayılmıştır.

Bununla birlikte, yine 8. maddenin 4. fıkrasında; savcılığı ve en önemlisi de hakim kararını devreden çıkaran bir hüküm getirilerek, bir idari birim olan "Telekomünikasyon İletişim Başkanlığı"nın bu tedbiri re'sen uygulamasına imkan veren bir hal öngörülmüştür. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir. 8. maddenin 4. fıkrasında; savcılığı ve en önemlisi de hakim kararını devreden çıkaran bir hüküm getirilerek, bir idari birim olan "Telekomünikasyon İletişim Başkanlığı"nın bu tedbiri re'sen uygulamasına imkan veren bir hal öngörülmüştür. Buna göre; içeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocukların cinsel istismarı veya müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı resen Başkanlık tarafından verilir. Bu hallerde, resen tedbire karar veren Başkanlık, yalnızca yayını yapanların kimliklerinin belirlenmesi halinde, Savcılığa bildirimde bulunur. Yine aynı maddenin, 11. fıkrasına göre; Başkanlık tarafından verilen bir idari tedbir olarak öngörülen "erişimin engellenmesi" kararının yerine getirilmemesi; idari para cezasını, hatta para cezasının ödenmemesi halinde yetkilendirmenin iptalini gerektirebilmektedir.

Bu düzenlemenin yasallık ilkesi bakımından doğurduğu sakınca, bir idari makama maddede sayılan bir takım suçların işlendiği şüphesini değerlendirme yetkisi vermesindedir. Ayrıca, bu tedbirler, çoğunlukla Türkiye'de bulunmayan kişiler hakkındadır ve Türk hukuk uygulamasına göre, tedbirin iptali için başvuru ehliyetine sahip olanlar yalnıza bu kişilerdir.

Söz konusu kişiler, bu tür yasal yollara seyrek olarak başvurduklarından ve kullanıcılar Başkanlığın kararına karşı başvuru hakkına sahip olmadığından, netice çeşitli İnternet sitelerinin belirsiz olarak yasaklanması veya bunlara erişimin engellenmesi olmaktadır. Tedbirin uygulanması bakımından belirli bir sure sınırı bulunmamaktadır ve bir ceza soruşturmasının bulunmasına gerek yoktur. Özellikle şüphelinin kimliği belirlenebilir olmadığında, böyle bir durumla karşılaşılmaktadır. Bu nedenle, Başkanlık tarafından uygulanan erişi-

min engellenmesi kararlarının bir ceza muhakemesi tedbirinin özelliklerini taşımadığı ve "geçicilik" unsurunun eksik olduğu belirtilmelidir[8]. Bu haliyle, daha ziyade tehlikeli bir faaliyetin önlenmesi için başvurulabilecek bir güvenlik tedbirinin söz konusu olduğu ileri sürülebilirse de, güvenlik tedbirleri de yasallık ilkesine tabidir ve bu tedbirlere ancak geçerli bir ceza hükmü neticesinde bir mahkeme kararıyla hükmedilebilir. Bu gerekçelerle, ilgili yasada öngörülen bu idari tedbir, yasallık ilkesi bakımından sıkıntı doğurabilecek niteliktedir.

(2) Yasal düzenlemeler, BİT'in veya İnternet'in hukuka uygun kullanımı üzerindeki yersiz ve aşırı caydırıcı etkilerinden nasıl kaçınmaktadır?

Bugüne kadar, Türk yasa koyucusu çift kullanımlı yazılımı (dual-use software) veya hem yasal hem de yasadışı amaçlar içeren diğer çevrimiçi hareketleri ceza hukuku alanına dahil etmekten kaçınmıştır. Bununla birlikte, Türkiye'de özellikle 5651 sayılı yasanın uygulanması bakımından yasal düzenlemelerin, İnternetin meşru kullanımı üzerindeki aşırı soğutma etkilerinden söz etmek uygun olur.

Bugüne kadar, mahkemeler ve Başkanlık tarafından verilen erişimin engellenmesi kararlarında, içeriği Kanunda öngörülen suçları oluşturan yayınların ya da sakıncalı olduğu kabul edilen içeriklerin yayından kaldırılmasındansa, bu yayınların yer aldığı web sitesinin erişime tamamen kapatılması tercih edilmiştir. "Bu durum ise (...), hukuka aykırı olduğu ileri sürülen içeriğin yanı sıra bunlar aracılığıyla sunulan tamamen hukuka uygun içerikteki milyonlarca İnternet sayfasına erişimin de engellenmesi sonucunu doğurmuştur"[9]. Bu konuda en çarpıcı örnek İstanbul 1. Sulh Ceza Mahkemesi tarafından Mart 2007'de 5651 sayılı Kanun'un 8. maddesi uyarınca, sitede Atatürk'e hakaret niteliği taşıyan bir videonun yer alması nedeniyle "Youtube" isimli İnternet sitesine erişimin engellenmesi yönündeki tedbir uygulamasıdır. Bu tedbir iki yılı aşkın bir süre uygu-

8 AKDENİZ, Yaman; Report of the OSCE Representative on Freedom of the Media on Turkey and İnternet Censorship, p. 32, http://www.osce.org/fom/41091 (Erişim Tarihi: 31.08.2012)

9 AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and İnternet Censorship, p. 28, http://www.osce.org/fom/41091 (Erişim Tarihi: 31.08.2012)

lanmış ve bu süre boyunca İnternet kullanıcılarının bu siteye erişimi tamamen engellenmiştir[10]. Sonuç olarak, bu alanların hukuka uygun kullanımı hukuki başvuru yollarına erişimin yetersizliğinden dolayı engellenmektedir.

Bununla birlikte, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı tarafından 01.03.2010 tarihinde yayınlanan erişim engelleme istatistiklerini içeren bilgi notunda[11], herhangi bir erişimin engellenmesi kararı verilmeden önce suç unsuru içeren kısmi içeriklere konu İnternet siteleriyle, ulaşılabilir iletişim bilgileri çerçevesinde irtibata geçildiği, böylece "uyar-kaldır" yöntemi ile İnternet sitesinin tamamının erişiminin engellenmesi sakıncası giderilmek suretiyle yalnızca suça konu içeriğin erişiminin engellendiği belirtilmektedir. Bu şekilde, yani "uyar-kaldır" yöntemi sayesinde ihbar konusu İnternet sitelerinden 3.521 adet içeriğin çıkarılmasının sağlandığı açıklanmıştır. Bununla birlikte, 5651 sayılı Kanunda ya da bu Kanunun uygulanması amacıyla çıkarılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik"te[12] böyle bir yönteme yer verilmemektedir. Bu konuda, ayrıca altı çizilmesi gerekli bir diğer konu; söz konusu tedbirin uygulanması yoluyla erişimin engellenmesi kararları ile ilgili istatistiki bilgiye ulaşmanın Mayıs 2009'dan itibaren mümkün olmadığıdır. Yukarıda belirtilen bilgi notunda, mahkemeler ve re'sen TİB tarafından verilen erişim engelleme kararları kamuoyu ile ayrıntılı olarak paylaşılmıştı. Ancak Mayıs 2009 tarihinden beri bu konuda herhangi bir güncelleme yapılmamıştır. Hatta bu tarihten itibaren istatistiki bilgiye ulaşmak amacıyla TİB'e yapılan bir bilgi edinme başvurusu "özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek türden bir bilgi" niteliğinde kabul edilerek reddedilmiş ve konu şu anda idari yargıya taşınmıştır[13].

10 http://haber.mynet.com/youtubea-erisim-engellendi-275750-guncel/ (erişim tarihi: 18.08.2012)

11 http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010.pdf (Erişim tarih: 20.08.2012)

12 30.11.2007 tarihli ve 26716 sayılı Resmi Gazete.

13 AKDENİZ, Yaman, "TİB'e Erişim Engelleme İstatistiklerini Gizlemekten Dava", 13 Mayıs 2010, Bianet (http://bianet.org/bianet/ifade-ozgurlugu/121956-tibe-erisim-engelleme-istatistiklerini-gizlemekten-dava) (Erişim tarihi: 26.08.2010)

(3) Ceza yasalarının, hızlı teknolojik yenilikler karşısında geri kalmasından nasıl kaçınılmaktadır? Örn;

- **İnternet ve sosyal ağların kullanımındaki değişiklikler ne şekilde dikkate alınmaktadır?**
- **yasa, teknolojik ilerlemeye nasıl uyarlanmaktadır (örn. idari düzenlemelere atıfta bulunularak)?**

BİT alanındaki cezai düzenlemeler Türk ceza hukuku sistemine 1991 yılında 765 sayılı mülga TCK'na 525a ila 525d maddelerinin eklenmesi suretiyle girmiştir. Suç tanımları; güncelliğini yitirmiş ve kısa zamanda yasal boşluklara neden olan özel teknolojik tabirler ve suçların maddi konuları bakımından muğlak terimler içermekteydi (örn. "verileri otomatik işleme tabi tutulan sistemler"). 2005 yılında 5237 sayılı TCK'nun yürürlüğe girmesiyle bu suç tanımlarında belirgin değişiklikler söz konusu olmuştur. Buna karşın, söz konusu düzenlemelerde az sayıda fiilin suç olarak yer aldığının ve halen teknolojik yeniliklerle birlikte gelişen bütün suç türlerini içermediğinin altı çizilmelidir.

Özel suç düzenlemelerindeki eksikliğin tek sonucu bazı fiillerin cezasız kalması olmamakta, bu durum aynı zamanda bir takım suçların üst üste binmesine veya aşırı cezalandırmaya da neden olmaktadır. Örneğin, kredi kartı hırsızlığı ile kredi kartlarının kötüye kullanılması suçlarını içine alacak tek bir suç tipinin öngörülmemiş olması nedeniyle, böyle bir fiili gerçekleştiren kişi aynı anda birçok suç nedeniyle cezalandırılmaktadır (hırsızlık, sahtekarlık, kredi kartının kötüye kullanılması ve bazı hallerde, bilişim sisteminin işleyişini engelleme).

BT suçlarına ilişkin suç tanımlarında idari düzenlemelere herhangi bir atıfta bulunulmamaktadır. Yasalar ve yönetmeliklerle Bilgi Teknoloji ve İletişim Kurulu'na ve Telekomünikasyon İletişim Başkanlığı'na bir takım yetkiler verilmişse de, bu düzenlemeler cezai alanı içermemekte, belirtilen Kurumlara, daha ziyade izleme, denetleme, düzenleme ve bu faaliyetlerle bağlantılı tedbirlerin ve para cezalarının düzenlenmesi gibi bir takım idari yetkiler tanınmaktadır. Ancak, bu noktada, yukarıda belirtildiği üzere İnternet sitelerine erişimin engellenmesi gibi bazı idari tedbirlerin, neredeyse cezai bir takım sonuçları olduğu da hatırlatılmalıdır.

Sonuç olarak, Türk yasa koyucusunun suçlara ilişkin düzenlemelerin teknolojik yenilikler karşısında geri kalmasını engelleyecek özel bir takım tedbirler almadığı belirtilebilir.

(D) Cezai düzenlemelerin kapsamı

(1) Ceza yasalarında, "hackleme", "e-dolandırıcılık"[14], bilgisayar sahtekarlığı veya download (karşıdan yükleme) korumasının baypas edilmesi için kullanılabilecek yazılımın bulundurulması gibi, yalnızca kötüye kullanımın devam ettirilmesi riskini taşıyan hazırlık hareketlerini ne ölçüde cezalandırılmaktadır? Bu hareketler cezalandırılmaktaysa, bu tür yasaların kabul edilmesi tartışmalara neden olmakta mıdır? Yasa koyucular aşırı cezalandırmanın önüne geçmek için özel bir çaba göstermekte midir?

BT suçları bakımından hazırlık hareketlerini cezalandıran düzenlemelere suç tanımlarında oldukça seyrek olarak rastlanmaktadır. Bununla birlikte, BT sistemlerini içeren suçlarda kullanılabilecek malzemelerin elde edilmesinin ya da bulundurulmasının cezalandırıldığı iki durum söz konusudur.

5846 sayılı FSEK'nun 72. maddesine göre; "bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya **kişisel kullanım amacı dışında elinde bulunduran** kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır".

Bundan başka, TCK'nun 245/2. maddesine göre; "başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır".

TCK'nun 243. maddesinde öngörülen "bir bilişim sistemine hukuka aykırı olarak girmek ve orada kalmak" suçu bir soyut tehlike

14 Sahte e-posta veya web siteleriyle kullanıcıların kredi kartı bilgileri ele geçirilerek yapılan dolandırıcılık.

suçu olarak düzenlenmesine karşın, hukuka aykırı olarak bir bilişim sistemine girme, TCK md. 244 kapsamında "hackleme" suçunun maddi unsurunu oluşturan hareketin bir parçasını teşkil ettiğinden, burada yalnızca hazırlık hareketinin cezalandırıldığını kabul etmek mümkün değildir. Ancak, TCK'nun 243. maddesinde düzenlenen suçun; aşırı muğlak olması ve hareketin mağdur bakımından bir zarar doğurması için herhangi bir ölçütü içermemesi nedeniyle öğretide eleştirilerle karşılaştığı belirtilmelidir.

Suç tanımlarında hazırlık hareketlerinin yer alması bakımından geniş çaplı bir tartışma söz konusu olmamıştır. Bununla birlikte, başka hukuk sistemlerinde hazırlık hareketlerinin artan şekilde cezalandırılmasını "risk ceza hukuku"nun bir örneği olarak eleştiren ve bu eğilime karşı uyarıda bulunan pek çok görüş bulunmaktadır[15].

(2) Bir takım verilerin yalnızca bulundurulması ne ölçüde suç oluşturmaktadır? Hangi alanlarda ve neye dayanarak? Veri "bulundurulması" nasıl tanımlanmaktadır? Bu tanım, geçici olarak bulundurmayı veya yalnızca görüntülemeyi içermekte midir?

TCK'nun 226. maddesinde düzenlenen "müstehcenlik" veya pornografi suçu Alman Ceza Kanunu model alınarak düzenlenmiştir ve pornografik içeriğe sahip (suç tanımındaki ifadeyle "müstehcen") ürünlerin yalnızca bulundurulmasının cezalandırıldığı iki tür hareket öngörülmüştür. Bunlardan biri içeriğinde çocukların kullanıldığı pornografik ürünlerin bulundurulması (iki yıldan beş yıla kadar hapis cezası ile cezalandırılmaktadır), diğer ise şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin pornografik ürünlerin bulundurulmasıdır (bir yıldan dört yıla kadar hapis cezası öngörülmüştür). Kuşkusuz, "doğal olmayan yoldan yapılan cinsel davranış" deyimi fazlasıyla muğlaktır ve homoseksüel ilişkiyi, BDSM'yi veya fetişizmi içerecek şekilde yorumlanabilecektir. Bu tür bir yorum pek çok başka yasal faaliyetin cezalandırılması sonucunu doğuracak ve ayrımcılık yasağının ve sonuç olarak ilgili kişilerin insan haklarının ihlaline neden olacaktır.

15 Bkz., örn. ERMAN, Barış, "Ceza Hukukunun Dönüşümü", Prof. Dr. Duygun Yarsuvat'a Armağan, basılı.

Veri bulundurmanın cezalandırıldığı bir diğer örnek FSEK'nun 71. maddesinde öngörülmektedir. Burada düzenlenen suç tanımına göre; kanunda korunan fikir ve sanat eserlerinin "kişisel kullanım amacı dışında bulundurulması veya depolanması" bir yıldan beş yıla kadar hapis cezasını gerektiren bir fiildir.

Bunlardan başka, "kişisel verilerin hukuka aykırı olarak ele geçirilmesi" (TCK md. 136) ve "verilerin yok edilmemesi" (TCK md. 138) bir takım verilerin bulundurulmasının dolaylı olarak cezalandırıldığı hallere örnek olarak belirtilebilir.

(3) Bir takım verilerin bulundurulması ya da bunlara erişim elde etme suç teşkil ettiği takdirde, ceza sorumluluğu servis sağlayıcıları da içerecek şekilde genişletilmekte midir (örn. yer veya içerik sağlayıcılar)? Bunların sorumluluğunun söz konusu olması için, özellikle kusurluluk yönünden gerekli koşullar nelerdir?

(Servis) Sağlayıcılar, sağladıkları ya da erişime sundukları bilgileri gözlemlemek ya da denetlemekle yükümlü müdür? Sağlayıcılar, kullanıcıların kimliklerine ilişkin bilgi sağlamakla yükümlü müdür? Sağlayıcıların, belirli bilgilere erişimi önlemek zorunluluğu bulunmakta mıdır? Yanıt olumlu ise, hangi koşullarda? Bu tür yükümlülükleri yerine getirmemek ceza sorumluluğuna neden olmakta mıdır?

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 4. maddesine göre içerik sahibi ya da içerik sağlayıcı temelde kendi fiilinden dolayı sorumludur. Bununla birlikte, içerik sağlayıcı tarafından başka İnternet sitelerine sağlanan bağlantılar, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre cezai sorumluluğa neden olabilmektedir.

5651 sayılı Kanun'un 6. maddesine göre erişim sağlayıcı kendi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmek-

le yükümlü değildir, dolayısıyla herhangi bir ceza sorumluluğu da bulunmamaktadır. Ancak erişim sağlayıcı herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten bu kanun hükümlerine göre Telekomünikasyon İletişim Başkanlığınca haberdar edilmesi halinde ve teknik olarak engelleme imkanı bulunduğu ölçüde erişimi engellemekle yükümlüdür. Bu yükümlülüğün yerine getirilmemesi herhangi bir yaptırıma tabi değildir.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Yönetmeliğin 8/b maddesine göre erişim sağlayıcı sağladığı hizmetlere ilişkin trafik bilgilerini bir yıl saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Aksi takdirde erişim sağlayıcısına TİB tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

Aynı Yönetmeliğin 8. maddesine göre faaliyete başlamasından itibaren her ay düzenli olarak, her erişim yöntemine ilişkin kullanacağı erişim numaralarını ve toptan hizmet verdiği abonelere ilişkin bilgileri Telekomünikasyon İletişim Başkanlığı'na göndermekle de yükümlüdür. Ancak bunun yerine getirilmemesinin bir yaptırımı yoktur.

Yer sağlayıcı, bu kanunun 5. maddesine göre yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir, bu nedenle de ceza sorumluluğu bulunmamaktadır. Ancak yer sağlayıcı, yer sağladığı hukuka aykırı içerikten bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi halinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. İçerik sağlayıcı ise bu kanunun 4. maddesine göre İnternet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

(4) BİT ve İnternet suçlarıyla ilgili olarak, belirli hareketlerin suç olarak düzenlenmesi yönünden hangi anayasal sınırlar genel ve özel olarak tartışma konusu olmuştur[16] (örn. ifade özgürlüğü, basın özgürlüğü, örgütlenme özgürlüğü, gizlilik, "başkalarına zarar vermeme ilkesi" (harm principle), (suç oluşturan) bir hareketin bulunması gerekliliği, kusurlu iradenin gerekliliği)?

Türkiye'de bilişim suçları bakımından kaygılara neden olan temel konular ifade özgürlüğü ve İnternet sansürüdür. Bu kaygı esas olarak İnternet sitelerine erişimi engelleyen tedbirlerin düzenlenmesi ve uygulanmasıyla ilgilidir. OSCE Raporuna göre; "erişimin engellenmesi tedbirlerinin düşünce açıklamalarının önüne geçilmesi amacıyla kullanılması sansüre AİHS'nin 10. maddesinin ihlaline neden olur"[17].

Bu uygulama özellikle İnternet basınıyla ilgili olaylarda sansüre yol açabilecek bir "ön kısıtlama" sonucunu doğurur[18].

İnternet sansürü Telekomünikasyon İletişim Başkanlığı tarafından yayınlanan "İnternetin Güvenli Kullanımına İlişkin Usul ve Esaslar"ın 22 Ağustos 2011 tarihinde yürürlüğe girmesiyle birlikte yeniden temel bir tartışma konusu haline gelmiştir. Bu kurallar, İnternet servis sağlayıcılarına; aileler, çocuklar ve okullar için filtreleme seçenekleri sunma yükümlülüğü getirmiştir. Bu filtreler Başkanlık tarafından belirlenen "siyah ve beyaz listeler" ile uyumlu olmak zorundadır. "Çocuk profili" seçeneğini tercih eden kullanıcılar yalnızca beyaz listede yer alan sitelere erişim sağlayabilirler. "Aile profile" seçeneğinde ise "siyah liste"de yer alan sitelere erişim otomatik olarak yasaklanacaktır. Herhangi bir profili tercih etmeyen kullanıcılar için ise, daha önce olduğu gibi Başkanlık tarafından veya mahkeme kararıyla yasaklanmayan herhangi bir siteye erişim mümkündür. Bu listeler tercihe bağlı olarak uygulansa da, listelerin hükümete bağlı bir idari otorite tarafından hazırlanması ifade özgürlü-

16 What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and Internet crime?

17 AKDENİZ, Report of the OSCE Representative on Freedom of the Media on Turkey and İnternet Censorship, p. 30, http://www.osce.org/fom/41091 (Erişim tarihi: 31.08.2012)

18 Ibid, p. 31.

ğü açısından kaygı yaratan bir durum olmuştur. Ayrıca okullara belirli profiller arasında tercih yapma imkanı tanınmamış ve "aile profili"ni seçmeleri zorunlu hale getirilmiştir.

Endişe yaratan bir diğer konu ise, yalnızca zarara ya da muhakkak bir tehlikeye yol açan hareketlerin ceza sorumluluğuna neden olması esasına dayanan "başkalarına zarar vermeme" ilkesiyle ilgilidir. Yukarıda belirtildiği gibi, TCK'da öngörülen suçların çoğunda cezalandırmanın söz konusu olabilmesi için hareketin sonucunda belirli bir zararın ya da somut bir tehlikenin ortaya çıkması aranmaktadır. Ancak, "bilişim sistemine hukuka aykırı olarak grime ve orada kalma" suçunun düzenlendiği 243. madde bu modele uymamakta ve herhangi bir zarar ihtimali veya zarar vermeye yönelik bir irade aranmaksızın her türlü hareket cezalandırılmaktadır. Böylece, bir soyut tehlike suçu düzenlenmekte ve kusurlu iradenin gerekliliğine ilişkin herhangi bir kısıtlama söz konusu olmamaktadır.

Kusurluluk ilkesine ilişkin endişe yaratan diğer haller özellikle mahkemeler tarafından yasal düzenlemelerin uygulandığı somut haller nedeniyle ortaya çıkmaktadır. BT bağlantılı suçların soruşturulmasındaki teknik zorluklar ve mahkemeler ve savcılıkların uyum sağlama sorunları nedeniyle bazı hallerde kusurluluk esasına göre sorumluluk bakımından gerekli ölçülerin karşılanmadığı görülmektedir. Bunun sonucunda, kişiler hakkında yalnızca hukuka aykırı içeriğin İnternete yüklenmesinde kullanılan IP numarasına bağlı telefon hattının sahibi olmak nedeniyle dava açıldığı veya sorumlu tutulduğu örneklere rastlanabilmektedir. Bu tür durumlarda, şüpheli veya sanık bakımından hareketi ya da kastı ispata yönelik olarak başkaca bir araştırma yapılmamaktadır.

Benzer bir sorun geleneksel anlamda "içerik sağlayıcı" veya "yer sağlayıcı" kavramlarının kolaylıkla ayırt edilmesinin mümkün olmadığı web 2.0 uygulamalarıyla ilgili olarak ortaya çıkmaktadır. Bu tür platformlarda faaliyette bulunan kişiler ve bunların, kendi sorumluluk alanları içinde suç teşkil eden hareketlerin önlenmesi konusundaki yükümlülüklerine ilişkin herhangi bir özel düzenleme bulunmamaktadır. Bu durum, söz konusu kişilerin ceza sorumluluklarının kolayca tespit edilemediği bir "gri alan" yaratmaktadır.

(5) Yasada siber suçluları hedef alan ceza yaptırımları öngörülmekte midir (örn. İnternet kullanımının geçici olarak yasaklanması)?

Mevzuatımızda siber suçluları hedef alan bunlara özel ceza yaptırımları bulunmamaktadır. Ancak işlenen suçun cezası bir yıl veya daha az ise (kısa süreli hürriyeti bağlayıcı) TCK'nun 50/1d'e göre mahkum olunan cezanın yarısından bir katına kadar süreyle belirli yerlere girmekten veya belirli etkinlikleri yapmaktan yasaklanmaya çevrilmesi mümkündür. Burada yer alan yaptırımlar sınırlı olarak sayılmamıştır. Bu nedenle, örneğin hakim somut bir olayda bir bilişim sistemine hukuka aykırı olarak giren kişi bakımından bir yıldan az hapis cezasına hükmettiğinde bu kişiye cezanın yarısından bir katına kadar süreyle İnternet kullanımını yasaklamak şeklinde seçenek yaptırıma çevirmek konusunda takdir yetkisi vardır.

(E) Cezalandırmaya Seçenekler

(1) BİT ve İnternet'in kötüye kullanımı ile mücadelede ceza hukuku, diğer yollarla karşılaştırıldığında nasıl bir rol üstlenmektedir? BİT alanında hukuki ve idari yaptırımlar (zararın giderilmesi, işyerinin kapatılması, vb.), ceza hukukuyla nasıl bir ilişki içerisindedir?

Ceza hukuku, BİT ve İnternet'in kötüye kullanımı ile mücadelede her zaman öncü bir rol oynamıştır. Türk kanun koyucusu, ceza hukuku araçlarını daima en etkili hukuki araçlar olarak benimsemiştir; bu açıdan, BİT ve İnternet ile ilgili ortaya çıkan hukuksal sorunların çözümüne ilişkin olarak ceza hukuku araçlarını kullanılmasını esas alan sürekli bir eğilimin varlığından söz edilebilir. Bu nedenle, BİT ve İnternet alanındaki hukuksal düzenlemeler noktasında özel hukuk ve idare hukuku tedbirlerinin ikincil (tâli) bir niteliği olduğunu ifade etmek gerekir.

Bazı hallerde ise, özel hukuk ve idare hukuku tedbirlerinin, ceza hukuku tedbirleri ile birlikte düzenlendiği görülmektedir. Örneğin, 5651 sayılı Kanun her ne kadar esas itibarıyla İnternet sağlayıcıların sorumluluklarını ve İnternet suçlarıyla mücadeleye ilişkin usulü düzenlemekte ise de, bu Kanunun 9. maddesi spesifik olarak özel hu-

kuka ilişkin bir konuyu ele almakta ve "içeriğin yayından çıkarılması" ve "cevap hakkı" gibi cezai olmayan tedbirleri düzenlemektedir.

9. maddeye göre, bir web sitesindeki içerik nedeniyle haklarının ihlal edildiğini ileri süren kişiler içerik sağlayıcıya – eğer içerik sağlayıcıya ulaşılamıyorsa yer sağlayıcıya – başvurarak ihlal teşkil ettiğini ileri sürdükleri içeriğin yayından çıkartılmasını talep edebilirler.

Şikâyetçilerin Kanun'un 9(1) maddesine göre, aynı zamanda "cevap hakkı" da bulunmaktadır ve içerik veya yer sağlayıcıdan, cevaplarının ihlal teşkil ettiğini ileri sürdükleri içeriğin yayınlandığı web sitesinde 1 hafta süreyle yayınlanmasını talep edebilirler.

Eğer içerik veya yer sağlayıcı bu talebin kendilerine ulaşmasından itibaren 48 saat içerisinde talebi yerine getirmezlerse, bu takdirde şikâyetçi 15 gün içerisinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkartılmasına ya da hazırladığı cevabın yayınlanmasına karar verilmesini isteyebilir.

(2) Suç teşkil eden faaliyetler içerisinde olan web siteleriyle mücadelede ceza hukuku alanı dışında ne gibi araçlar kullanılmaktadır / çoğalmaktadır (örn. web sitelerinin kapatılması, bunlara erişimin engellenmesi)?

Ceza hukuku araçları, her ne kadar BİT'le ilgili sorunlarda en fazla tercih edilen tedbirler olsalar da, bu alanda ortaya çıkan tüm sorunların çözmeye uygun değillerdir. Saldırgan web siteleri ve özellikle bu web sitelerinde yer alan yasadışı ve zararlı içeriklerle mücadele, ceza hukuku dışı araçlarla müdahale edilmesi gereken temel bir sorun olarak ortaya çıkmaktadır. Türk hukukunda, bu tarz saldırgan web siteleri ile mücadeleye ilişkin esaslar, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile düzenlenmiştir.

5651 sayılı Kanun'da yer alan web sitelerine "erişimin engellenmesi" hem bir ceza muhakemesi tedbiri hem de bir idari tedbir olarak düzenlenmiştir. Bununla birlikte, özellikle "idari tedbir" şeklinde öngörülen erişimin engellenmesi tedbirine uygulamada ölçüsüz

ve aşırı bir biçimde başvurulması, "İnternet sansürü" kavramını gündeme taşımıştır. Bu durum, medya ve ifade özgürlüğü için ciddi bir tehdit yaratmış bulunmaktadır. Bu nedenle, sansür tartışmalarına sebebiyet veren bu düzenlemenin kaldırılması ya da yeniden kaleme alınması konusunda BİT endüstrisi temsilcileri tarafından halen bir kampanya yürütülmektedir.

(3) BİT kullanıcılarının kendilerini ne ölçüde korumaları beklenmektedir (örn. mesajların şifrelenmesi, şifre kullanımı, koruyucu yazılımların kullanılması)? Kişinin bilgisayarının makul ölçüde korunmaması karşısında yaptırımlar öngörülmekte midir, örn. virüsten koruyucu yazılım kullanılması veya özel ağlara erişimin şifre ile engellenmesi? Makul ölçüde oto-koruma eksikliği, bir başkasının ağına yasadışı girmek ve kötüye kullanmakla ya da bir başkasının verilerini kötüye kullanmakla suçlanan kişiler bakımından bir savunma gerekçesi oluşturmakta mıdır?

Türk hukuk sistemi içerisinde, devlete bağlı kuruluşlar (örneğin Telekomünikasyon İletişim Başkanlığı-*bundan sonra Başkanlık)* çocuklar ve gençler ile ailelerin İnternet ortamındaki yasadışı ve zararlı içeriklere karşı korunması konusunda proaktif bir rol oynamaktadır. Başkanlığın temel kuruluş amacı ise, Türk hukuk sisteminde farklı kanunlarda düzenlenmiş olan teknik araçlarla iletişimin denetlenmesi kararlarının tek bir birim bünyesinde, merkezi bir sistemle uygulanmasının sağlanmasıdır. 5651 sayılı Kanun hükümleri çerçevesinde, Başkanlık, İnternet içeriklerini izlemek ve hâkimler, mahkemeler ve savcılıklar tarafından alınan erişimin engellenmesi kararlarını yerine getirmekle görevli kurum olarak belirlenmiştir.

Bu nedenle, BİT kullanıcılarının korunması noktasındaki yükümlülük büyük ölçüde Başkanlık tarafından üstlenilmiş olup, BİT kullanıcılarının kendilerini korumak üzere şifreleme, koruyucu yazılım kullanma veya benzeri tedbirler alması beklenmemektedir.

Bununla birlikte, kendilerini koruma noktasında BİT kullanıcılarına bir tercih imkânı da tanınmış bulunmaktadır. 2011 yılının Şubat ayında Türk hükümeti aynı yılın Ağustos ayında yürürlüğe girmek üzere tüm yurttaşlar için bir İnternet filtreleme sisteminin

hazırlandığını açıklamıştır. Her ne kadar bu genel filtreleme sisteminin ilk açıklanan orijinal şeklinde tüm kullanıcılar için zorunlu 4 profil bulunmakta ise de; hükümet BİT endüstrisi, sivil toplum örgütleri ve kullanıcılardan gelen şiddetli "sansür" iddiaları karşısında bu sistemi revize etmek durumunda kalmıştır. Bu çerçevede, 2011 yılının Kasım ayında kullanıcılar için gönüllü olarak tercih edilebilecek olan 2 farklı profilden oluşan "revize edilmiş" İnternet filtreleme sistemi yürürlüğe girmiştir. Bu modelde, BİT kullanıcıları küçükleri İnternet ortamındaki yasadışı ve illegal içerikten korumak üzere tasarlanmış olan "aile" veya "çocuk" profillerinden birini seçme hakkına sahip bulunmaktadır.

5651 sayılı Kanun'un 7. maddesi İnternet kafeleri de kapsar anlamda, bilgisayarlarını belirli bir ölçüde korumak üzere belirli yükümlülükleri yerine getirmek durumunda olan toplu kullanım sağlayıcıları düzenlemektedir.5651 sayılı Kanun'un 7/2. Maddesine göre, toplu kullanım sağlayıcılar, Başkanlık tarafından onaylanan filtreleme araçlarını kullanmak suretiyle illegal İnternet içeriklerine erişimi engellemekle yükümlüdürler.

Resmi izin belgesi olmadan faaliyet gösteren toplu kullanım sağlayıcılar 3.000 TL ile 15.000 TL arasında idari para cezası ile cezalandırılırlar.

Bir başkasına ait bilişim ağına/sistemine izinsiz olarak girilmesi ve o ağdaki/sistemdeki verilerin tahrif edilmesi Türk Ceza Kanunu'nun 243. maddesinde suç olarak düzenlenmiş bulunmaktadır. Bu açıdan, bilişim ağına/sistemine izinsiz girilmesi veya verilerin tahrif edilmesi eylemi açısından, o ağda/sistemde makul bir otokorumanın bulunmaması, failler açısından hiçbir şekilde bir hukuka uygunluk nedeni veya mazeret nedeni oluşturamaz

(F) Kimliğin gizlenmesinin sınırlanması

(1) İnternet servis sağlayıcılarını; İnternet kullanım geçmişi de dâhil olmak üzere, kullanıcıların kişisel verilerini depolamakla yükümlü kılan yasalar ya da düzenlemeler bulunmakta mıdır?

Servis sağlayıcılar, kanun uygulayıcı makamlara bu tür verileri sağlamak yükümlülüğü altında tutulabilir mi?

İnternet yer *(hosting)* sağlayıcılarına ilişkin hukukî esaslar, 5651 sayılı Kanun'un 5. maddesinde düzenlenmiştir. Bu düzenleme ile, Avrupa Birliği Elektronik Ticaret Direktifi ile paralel olarak, uyarı bazlı bir sorumluluk rejimi getirilmiştir. Buna göre, yer sağlayıcı şirketlerin sunucularında depolanan verileri izleme gibi bir yükümlülüğü olmadığı gibi, yasadışı faaliyeti ortaya koyan vakıa ve koşulları aktif bir biçimde araştırma yükümlülüğü de bulunmamaktadır.

Bununla birlikte, 5651 sayılı Kanun'un 5/2. maddesi uyarınca, yer sağlayıcı şirketlerin Başkanlık tarafından kendilerine bildirilen bir uyarı veya 5651 sayılı Kanun'un 8. maddesi uyarınca bir yargısal kararın kendilerine ulaşması durumunda, bu yasadışı veya ihlal teşkil eden içeriği yayından çıkartma zorunluluğu söz konusudur.

Erişim sağlayıcılar ise 5651 sayılı Kanun'un 6. maddesinde düzenlenmiştir ve genel olarak bakıldığında, erişim sağlayıcılara yer sağlayıcılar ile benzeri yükümlülükler getirildiği tespit edilebilir.

5651 sayılı Kanun'dan ayrı olarak, hükümete bağlı idari otorite tarafından yer sağlayıcı ve erişim sağlayıcılara faaliyet belgesi verilmesine ilişkin kuralları belirleyen Ekim 2007 tarihli *"Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar hakkında Yönetmelik*" yayınlanmıştır.

Bu Yönetmeliğin 15. ve 26. maddelerinde, trafik verilerinin depolanmasına ilişkin esaslar belirlenmiştir. Buna göre, erişim sağlayıcılar 1 yıl süreyle, yer sağlayıcılar ise 6 ay süreyle trafik verilerini saklamak zorundadır. Buna karşın, erişim ve yer sağlayıcıların kullanıcıların kişisel verilerini saklamalarına veya bu verilerin kolluk güçleri ile paylaşılmasına ilişkin esasları belirleyen bir yasal düzenleme mevcut değildir.

(2) İnternet servis sağlayıcıyı, servis sağlama hizmeti öncesinde kullanıcılara kayıt yaptırma zorunluluğu altında bırakan yasalar ya da düzenlemeler mevcut mudur?

Yukarıda değinildiği üzere, *"Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar hak-*

kında Yönetmelik", gerek erişim gerekse yer sağlayıcılar açısından belirli bir süreyle "trafik verileri"ni saklama yükümlülüğü getirmektedir. İnternet sağlayıcılarının bu yükümlülüğün dışında, sunulan hizmetlerden yararlanan kullanıcıları kaydetme vb. yükümlülükleri bulunmamaktadır.

(3) İnternette dosyalara ve mesajlara şifreleme konulmasını sınırlayan yasalar ya da düzenlemeler bulunmakta mıdır? Şüpheliler, kullandıkları şifreleri ifşa etmeye zorlanabilir mi?

Türk hukuk sisteminde, İnternet ortamındaki dosya veya mesajların şifrelenmesine ilişkin sınırlamalar getiren herhangi bir yasal düzenleme bulunmamaktadır.

(G) Uluslararasılaştırma

(1) Ulusal düzenlemeler, ülke dışında, İnternete girilen veriler bakımından uygulanır mı? Yurt dışından veri girmek yönünden bir "çifte cezalandırma" gerekliliği bulunmakta mıdır?[19]

Türk hukukunda yurtdışından veri girilmesine ilişkin özel bir yasal düzenleme bulunmamaktadır. Şu halde, Türk ceza hukukunun yer bakımından uygulamaya ilişkin genel esasları, bu tarz durumlar için de uygulanmak durumundadır. Bu nedenle aşağıda Türk Ceza Kanunu'nun yurtdışında işlenen suçlara ilişkin kuralları aşağıdaki kısaca özetlenecektir:

Prensip olarak, Türk kanunları Türkiye'de işlenen suçlara uygulanır. (Türk Ceza Kanunu Madde 8). Bu kapsamda, Türk Ceza Kanunu'nun mülkîlik *(ülkesellik)* kavramının son derece geniş bir biçimde tanımlandığını belirtmek gerekir. Türk Ceza Kanunu'nun 8. maddesine göre, fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi hâlinde suç, Türkiye'de işlenmiş sayılır. Böylece, yurtdışında İnternet ortamına veri girilmesine ilişkin herhangi bir fiilin, Türkiye'de işlenmiş sayılmasının önü açılmış bulunmaktadır.

19 Is there a requirement of "double criminality" with respect to entering data from abroad?

Bununla birlikte, Türk kanunlarının yurtdışında işlenmiş suçlara uygulanabilmesine imkân veren belirli istisnalar da bulunmaktadır.

İlk istisnai durum olan, yurtdışında işlenen suçun bir Türk vatandaşı tarafından işlenmesi hususu, Türk Ceza Kanunu'nun 11. maddesinde düzenlenmiştir. Buna göre, bir Türk vatandaşı, Türk Ceza Kanunu'nun 13 üncü maddesinde yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu yabancı ülkede işlediği ve kendisi Türkiye'de bulunduğu takdirde, bu suçtan dolayı yabancı ülkede hüküm verilmemiş olması ve Türkiye'de kovuşturulabilirliğin bulunması koşulu ile Türk kanunlarına göre cezalandırılır. Suç, aşağı sınırı bir yıldan az hapis cezasını gerektirdiğinde yargılama yapılması zarar görenin veya yabancı hükümetin şikâyetine bağlıdır. Bu durumda şikâyet, vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır.

İkinci istisnai durum olan, yurtdışında işlenen suçun bir yabancı tarafından işlenmesi hali ise Türk Ceza Kanunu'nun 12. Maddesinde düzenlenmiştir.

(1) Bir yabancı, Türk Ceza Kanunu'nun 13 üncü maddesinde yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı en az bir yıl hapis cezasını gerektiren bir suçu yabancı ülkede Türkiye'nin zararına işlediği ve kendisi Türkiye'de bulunduğu takdirde, Türk kanunlarına göre cezalandırılır. Yargılama yapılması Adalet Bakanı'nın istemine bağlıdır. (2) Yukarıdaki fıkrada belirtilen suçun bir Türk vatandaşının veya Türk kanunlarına göre kurulmuş özel hukuk tüzel kişisinin zararına işlenmesi ve failin Türkiye'de bulunması hâlinde, bu suçtan dolayı yabancı ülkede hüküm verilmemiş olması koşulu ile suçtan zarar görenin şikâyeti üzerine fail, Türk kanunlarına göre cezalandırılır. (3) Mağdur yabancı ise, aşağıdaki koşulların varlığı hâlinde fail, Adalet Bakanının istemi ile yargılanır: a) Suçun, Türk kanunlarına göre aşağı sınırı üç yıldan az olmayan hapis cezasını gerektirmesi. b) Suçluların geri verilmesi anlaşmasının bulunmaması veya geri verilme isteminin suçun işlendiği ülkenin veya failin uyruğunda bulunduğu devletin hükümeti tarafından kabul edilmemiş olması. (4) Birinci fıkra kapsamına giren suçtan dolayı yabancı mahkemece mahkûm edilen veya herhangi bir nedenle davası veya ce-

zası düşen veya beraat eden yahut suçu kovuşturulabilir olmaktan çıkan yabancı hakkında Adalet Bakanı'nın istemi üzerine Türkiye'de yeniden yargılama yapılır.

Türk kanunları aynı zamanda Türk Ceza Kanunu'nun 13. maddesinde düzenlenmiş olan belirli "katalog suçları"nın yurtdışında bir Türk vatandaşı veya bir yabancı tarafından işlenmesi halinde de uygulanabilir. Bununla birlikte, siber suçlar bu katalog suçlar listesi içerisinde belirlenmiş değildir

Son olarak, Türk Ceza Kanunu Türkiye'de (mülkîlik sistemi çerçevesinde), devletin güvenliğine ya da Türk gerçek veya tüzel kişilerine karşı işlenen suçlar için yönünden bir "çifte cezalandırma" sistemini benimsememiştir.

(2) Ülkenizin BİT ve İnternet alanındaki ceza hukuku düzenlemeleri, uluslararası hukuki belgelerden ne ölçüde etkilenmiştir?

Teknoloji hukukun daima bir adım önünde ilerlediği için, BİT ve İnternet alanında yasal düzenleme faaliyetine girişmek ulusal kanun koyucular için her zaman çok zorlu bir görev olmuştur. Bu nedenle, uluslar arası hukuk enstrümanları (ve karşılaştırmalı hukuktaki yasal mevzuat) BİT ve İnternet alanındaki kanunları ve diğer yasal düzenlemeleri kaleme alırken göz önünde bulundurulan ilk kaynaklar olma özelliği taşımaktadır.

Türk hukukunda, BİT alanındaki ilk cezai düzenleme 1991 yılında 765 sayılı (Eski) Türk Ceza Kanunu'na 525 a-d maddeleri "Bilgisayarlar Aracılığıyla İşlenen Suçlar" şeklinde eklenerek yürürlüğe girmiştir. Gerek bu ilk düzenleme gerekse halen yürürlükteki 5237 sayılı Türk Ceza Kanunu'nun 243-246. maddeleri arasında düzenlenen "bilişim alanında suçlar" şeklindeki düzenleme, büyük ölçüde Avrupa Birliği'nin Direktiflerinden etkilenmiş bulunmaktadır.

Aynı bağlam içinde, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" da yine uluslar arası hukuk enstrümanlarıyla etkileşim içerisinde hazırlanarak yürürlüğe konulmuştur. Bu Kanun'daki bazı özel hükümler (sözgelimi İnternet sağlayıcı-

ların sorumluluğuna ilişkin 4-7. maddeler) Avrupa Birliği Elektronik Ticaret Direktifi'nden alınmış ve bu şekilde Avrupa Birliği mevzuatı ile de uyum sağlanması amaçlanmıştır.

Buna karşın, Türkiye'nin halen Avrupa Konseyi Siber Suç Sözleşmesi'ni imzalamamış olduğunun altı önemle çizilmelidir. Türk mevzuatında bu anlamda ancak bu Sözleşme'nin imzalanması ve onaylanması ile doldurulabilecek bir boşluk halen mevcuttur. Ancak, bu uyumsuzluğun giderilebilmesi yönelik bazı adımlar atılmış ve örneğin 2005 yılında yürürlüğe giren Türk Ceza Kanunu'nun cinsel suçlara ilişkin hükümleri hazırlanırken, bu Sözleşme'nin "içerikle ilişkili suçlar-çocuk pornografisi"ne ilişkin getirdiği esaslar benimsenerek bir yasal düzenleme getirilmiştir.

(3) Ülkeniz, siber-suç yasalarının uyumlaştırılması konusundaki tartışmalara katılmakta mıdır (örn. BM nezdinde oluşturulan, siber-suç konusunda hükümetler-arası uzmanlar grubu)?

Türk hükümeti, siber suçlar alanındaki düzenlemeleri uyumlaştırma tartışmalarını da kapsar anlamda hemen tüm uluslar arası yasal düzenleme faaliyetlerine katılma yönünde sürekli bir irade ortaya koymasına karşın; bu faaliyetler neticesinde hazırlanan düzenli raporları ve diğer çalışmalarını kamuoyuna açıklama noktasında aynı derecede istekli değildir.

Bu nedenle, şu an itibarıyla Türk hükümetinin siber suç mevzuatlarının uyumlaştırılmasına ilişkin katılımı ve ne ölçüde katkı sağladığı hususunda tam olarak bilgilendirilmiş değiliz. Ancak, halihazırda BİT ve İnternet alanında faaliyet gösteren bir çok sivil toplum örgütü gerek uluslar arası gerekse karşılaştırmalı hukukta siber suç alanında yapılan yasal düzenleme faaliyetlerini sürekli olarak takip etmektedir.

(H) Gelecekteki gelişmeler

Lütfen ülkenizde BİT ve İnternet suçları konusundaki mevcut yasama eğilimlerini ve hukuki tartışmaları belirtiniz.

BİT alanındaki düzenlemelere ilişkin olarak Türkiye'deki mevcut eğilim daha ziyade elektronik ticaretin yasal düzenlemesi konusuna odaklanmış bulunmaktadır. Bu kapsamda, e-ticaret faaliyetlerinin modern çağın gereklerine uygun bir şekilde yürütülebilmesini temin etmek üzere çeşitli taslak/tasarı metinler hazırlanmış bulunmaktadır.

Bu noktada değinebileceğimiz ilk tasarı metin, Avrupa Birliği Elektronik Ticaret Direktifi ile tam bir uyumun sağlanabilmesi için hazırlanmış olan "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı"dır. Bu tasarı özel olarak spam e-postaların sınırlandırılmasına ve e-ticaret faaliyetlerinde kişisel verilerin korunmasına ilişkin bulunmaktadır. Tasarıda e-ticaret kapsamındaki bu tarz ihlallerin ceza sorumluluğu ile karşılanması öngörülmüştür.

Bu alandaki diğer bir tasarı ise "Kişisel Verilerin korunması Kanun Tasarısı"dır. Bu Tasarı'da yine uzun bir süredir Türkiye'nin gündemindedir ve tüm kullanıcılar yönünden kişisel verilerin yeterli standartlarda korunmasını sağlamak üzere hazırlanmıştır.

SECTION 2: CONCEPT PAPER AND QUESTIONNAIRE

Prof. Dr. Emilio C. Viano

(A) Scope of questionnaire (see Introduction and Annex)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Emilio C. Viano: emilio.viano@gmail.com

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply

modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

(2) Are there also negligent offenses in this field?

(3) If yes, please, provide a list of those offenses.

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

b. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

2. Data and system interference

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

b. Act – destruction/alteration/rendering inaccessible?

i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program? ***ii.*** Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/ information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under ***a***?

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-diallers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data? ***ii.*** Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;
- Their disclosure practices;
- Their professional ethical obligations;
- And whether patients or clients have any control over the disclosure of their personal data?

ii. Which data are specifically protected, if any?

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

b. Subject – Type of perpetrators?

Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply *for each category listed below* citing the relevant law and its provisions, if available:

1. Illegal collection
2. Illegal use
3. Illegal retention

4. Illegal transfer

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

ii. What standart of need is required for an authorized collection and/or distvibution of personel and private data (compelling, important, reasonable, convenient)?

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

ii. In particular, does your criminal law:

Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:

1. to transmit,
2. make available,
3. export
4. and intentionally access child pornography on the Internet;

Allow judges to order the deletion of child pornography posted on computer systems in your country;

Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;

Criminalize:

1. Knowingly accessing child pornography on the internet
2. Transmitting child pornography on the internet
3. Exporting child pornography on the internet
4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it...?

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

vii. Mens rea: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?
2. cyber-bullying?
3. cyber-stalking?
4. cyber-grooming?

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud
2. Infringement of Intellectual Property IP rights
3. Industrial espionage

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.

(3) Do victimization surveys in your country include questions on cyber-crimes?

(4) What types of computer crime / computer fraud are most often reported in your country?

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)			
Hacking (illegal intrusion into computer systems; theft of information from computer systems)			
Malicious code (worms, viruses, malware and spyware)			
Illegal interception of computer data			
Online commission of intellectual property crimes			
Online trafficking in child pornography			
Intentional damage to computer systems or data			
Others			

(9) In addition, to the above, if there are there any other forms and means of cyber-crime that have occurred (either frequently or infrequently) in your country, please identify them as well as the frequency with which they occur in the following table:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently

Thank you for your valuable collaboration!

Preparatory Colloquium Section II

ANNEX - THE INFORMATION SOCIETY AND RELATED CRIMES

Prof. Dr. Emilio C. Viano

The modern networked society is highly vulnerable to information-age related deviance and criminal behaviors. Globally, in the past few years, concerns have increased sharply over cyber-security, including the issues of cybercrime or high technology crime, "cyber-war," "cyber-defense," "cyber-terrorism," critical infrastructure protection, and information security. At the same time, growing attention is also being paid to how responses to cyber-security may affect and how they should be balanced with human rights values, such as individual autonomy, privacy, anonymous political speech, freedom of expression and freedom of association, human development goals, including access to knowledge, and economic interests, including innovation, competition, and the protection of trade secrets and other proprietary information. These issues of policy and values also present complex technical issues, such as the issue of "attribution," that is, the extent of the ability to determine the true senders of any message or request for information.

There is no question that the technologies that make the information society possible and functional have become essential tools that have significantly affected various aspects of personal and social lives, ranging from education, business, to cultural and leisure activities. With the widespread use of personal computers and of other electronic devices (iPhone, iPad, iPod, iTunes, etc,) and technology (Skype, Google Earth, etc.) and high speed internet, various related deviant and criminal behaviors have increased significantly, such as hacking, illegal downloading of music and software programs, and stealing others' passwords or identity. While the accurate extent and overall cost of cyber deviance is unknown and the estimated cost of it actually varies, there is no question that it is now a global and growing phenomenon.

Consequently, cyber-security has become a major concern of governments and the private sector around the world. There seems to have been a major shift in consciousness, stemming from a variety of sources, including:

- Increased appreciation of how critical the Internet and its resources are in multiple spheres of human endeavor and how many infrastructures and systems are increasingly dependent on Internet connectivity and capacity
- Continuing disclosures of major data breaches at financial institutions, other corporations, government agencies and academic institutions globally
- Continuing releases of malware and the increased sophistication of what is deployed
- Continuing reports of varying levels of governmental accessing, monitoring and filtering (or censorship) Internet use and content
- Unattributed cyber-attacks on key infrastructure, e.g. in Lithuania, Estonia, Georgia and other countries and most recently on a nuclear plant and on a munitions base in Iran. Stuxnet and Duqu used against Iran are considered the world's first 'super weapons' for cyber war.
- Concerns with governmental and corporate espionage
- Increased concern over cybercrime, including online fraud, identity theft, child pornography, theft of intellectual property, and related criminal movement of money and money laundering on the Internet
- Privacy concerns about corporate and governmental data access and the widespread collection, recording and diffusion of private information on practically everyone worldwide

As the reach of the information technology and software continues to grow exponentially among the world's population, and given the apparent lack of adequate user awareness on

implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of entities. These include criminal enterprises, "hackers" (whether for financial gain or as a challenge), cause-based groups, businesses spying on other businesses, proxies for governments, and governments, including their military and intelligence agencies. Motives for the attacks range from financial gain to the advancement of national security interests to the satisfaction of peer recognition.

Any effort to reach international consensus on cyber-security is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the Internet, of human rights, and of economic policy. Some see cyber-security as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block any undesirable content. Others strongly believe that Internet governance (including Internet security) involves an integration and balancing of interests, including not only national security but also human rights and the economic and developmental interests associated with a vibrant, innovative and competitive information society. These differing perspectives manifest themselves in many areas. Even the definition of computer crime is debated and contested.

(A) Cybercrime: Terminology and Definition

A cybercrime is a type of crime that involves the abuse of information technology. The term cybercrime covers a series of crimes which range from cyber terrorism to industrial espionage. Some cybercrimes may involve only limited influence of computers and networks while others rely almost entirely on the use of a computer or other electronic device and a network. First, an individual might use a computer or other electronic device to engage in criminal activity. Second, the evidence needed to prove a criminal case might be stored in computerized or electronic form. The law governing use of a computer or electronic device to commit a crime is substantive electronic crime law, because it concerns the scope of substantive conduct that has been

criminalized. The law governing the collection of computerized evidence is procedural electronic crime law.

Cybercrime is an extensive phenomenon expressed via an intricate ecosystem of operators, victims and instruments. Over the years, in fact, cybercrime has acquired a hierarchical and international organization, with a genuine "black market" for the commerce of data, tools and skills.

As the instruments have become more streamlined, the expertise required to access the world of cybercrime has been lowered: whereas cybercrimes were once perpetrated by groups of "black hats", today almost anyone with some technical skills can download and use instruments in order to carry out some type of attacks, from anywhere in the world. Today's cybercrimes are characterized by these two aspects: on the one hand, crimes can take numerous different forms in terms of expertise and attacks; on the other hand there is a series of well-structured schemes and mechanisms that typically characterize organizations and markets focused on profit.

Cybercrime refers to any crime that involves a computer or electronic device (iPhone, iPad, tablet, Blackberry, etc.) and a network where a computer or an electronic device may or may not have played an instrumental part in the commission of the crime. Many of the techniques involve the use of a computer/electronic device and of a network. However, many other techniques have nothing to do with computers other than information stored in text files on the computer's hard drive. Because of the diversity of computer/electronic-related offenses, a narrower definition would be inadequate. The rapid emergence of electronic technologies and software and the exponential expansion of the Internet have spawned a variety of new, technology-specific criminal behaviors that go beyond the category of "computer crimes." The terms "cybercrime" or high technology crime or information and communication technology crime are umbrella names for all crimes involving certain electronic devices and an information and communication network, mostly known today as "the internet." Debating semantically whether an act is a computer crime versus a

cybercrime versus a high technology or an information and communication technology crime is not that important. Gaining a better grasp of the problem and of its criminal law implications and response is more important. To combat these new criminal behaviors, many countries have indeed passed specialized legislation.

Experts have had difficulty calculating the damage caused by computer and electronic crimes due to the difficulty in adequately defining them; victims' reluctance to report incidents for fear of embarrassment, losing customer confidence and diminished competitiveness; and the lack of detection.

(B) Legal Interests Deserving Criminal Law Protection

The major interests identified in this Section II as deserving of the criminal law protection are:

(1) The integrity and functionality of the cyber-Information & Communication Technology (ICT) system (CIA offenses)

Offenses against the confidentiality, integrity, and availability of computer systems (called the "CIA" offenses) constitute the major threat to this primary interest of the ICT system.

(2) Protection of privacy

The term "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. Philosophical debates concerning definitions of privacy became prominent in the second half of the twentieth century, and are greatly influenced by the development of privacy protection in the law. Some defend privacy as focusing on control over information about oneself ; others see it as a broader concept required for human dignity or essential for intimacy; others consider it the value that accords us the ability to control the access others have to us. The earliest calls for explicit recognition of privacy protection in law were in large part motivated by the expanding communication technology. It is

clear that many people still view privacy is a valuable interest and realize it is now threatened more than ever by technological advances. There are massive databases and Internet records of all sorts of information about anyone of us, from individual financial and credit history to medical records, to purchases and Internet searches and communications. Most people do not know what information is stored about them or who has access to it. The ability for others to access and link the databases, with few controls on how they use, share, or exploit the information, makes individual control over information about oneself very challenging. The questionnaire for Section II in great part covers the major types of offenses against privacy.

(3) Protection of digital personality

Our Digital Personality is the pool of digital information about each one of us available to anyone with the right access, tools and motivation to find it. In the digitized world, it represents each one of us. Increasingly it is the first impression that we make upon others, and first impressions are important.

This phenomenon has grown almost accidentally. There are now many ways through which businesses and ordinary people are creating, using, sharing and storing increasing amounts of personal information.

Business tools are emerging to link the various parts of our Digital Personality together to create comprehensive views of each one of us.

There has been continuing outrage at this invasion of our personal space.Yet we persist in using new digital technologies and willfully post material on ourselves that create even more information for others to find.

Personal information on the internet and social media generally legally belongs to the businesses that hold it. They can manipulate, use, trade and store endless amounts of our personal information and yet we currently have limited legal rights to challenge this situation.

Additionally, as digital technologies become increasingly pervasive, we find ourselves living within ubiquitous intelligent interactive systems. Interacting with them is a complex and time-consuming task that sometimes is difficult for everyone, even Information Technology specialists, and at times impossible for certain groups of people. Although there are many user-centric approaches to deal with this phenomenon, ironically, it seems that the only unnatural part of the digital environment is the real human being. To solve this problem the creation of a context-based digital personality (DP) is being worked on as a proxy between digital surroundings and the final user. DPs will benefit from mobile technologies for context-creation, maintenance and usage; and from semantic technologies for formal decisions and verifications. The DP is conceived as being an electronic alter ego that exists independently of us, having executive powers and carrying our identity when we deal with the electronic world. Using it should simplify everyday interaction between users and digital environments and provide a framework for implementing value-added services for mobile operators.

Pertinent questions in Section II address the major possible violations and exploitation of our digital personality, how to protect it, and how to rebalance this lopsided equation of power over sensitive information about us.

(4) Protection against illegal content

- One could summarize illegal content to be any content, images, code, or software that executes or promotes:
- Malware and malicious code
- Denial-of-service attacks
- Computing viruses
- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare

- Harassment
- Spam, or the unsolicited sending of bulk email for commercial purposes
- Unauthorized access of licensed or protected software, or other intellectual property.
- Drug trafficking
- Terrorism
- Child pornography, child grooming, and some content inappropriate for minors.

Many jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

As a reaction to the actual or potential placement of "illegal" material on the web, government policies concerning censorship of the Internet may be broadly grouped into four categories:

(a) Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies.

In these countries laws of general application apply to illegal Internet content such as child pornography and, in some, incitement to racial hatred.

It is not illegal to make content "unsuitable for minors" available on the Internet, nor must access to it be controlled by a restricted access system. Perhaps all such governments encourage the voluntary use of, and ongoing development of, technologies that enable Internet users to control their own, and their children's, access to content on the Internet (e.g. parental controls).

(b) Criminal law penalties (fines or jail terms) applicable to content providers who make content "unsuitable for minors" available online. Additionally, in these countries, laws of general application forbid other illegal content, like child pornography.

(c) Government ordered blocking of access to content deemed unsuitable for adults. Some countries require Internet Service Providers (ISPs) to block material while others only allow restricted access to the Internet through a government controlled access point.

(d) Government prohibition of public access to the Internet.

A number of countries either prohibit general public access to the Internet, or require Internet users to be registered or licensed by a government authority before permitting them restricted access as in (c) above. In the many countries that have restrictive Internet censorship laws, governmental focus appears to be on prohibiting and/or restricting politically sensitive speech, criticism of the government, etc.

Concerns about access to content on the Internet vary markedly around the world and regulatory policy reflects this. What is illegal in one country is not illegal in others, and what is deemed unsuitable for minors in one country is not in others. However, by and large, child pornography is widely criminalized.

(5) Protection of property (including intellectual property rights)

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.

IP is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs. The innovations and creative expressions of indigenous and local communities are also IP, yet because they are "traditional" they may not be fully protected by existing IP systems. Access to, and

equitable benefit-sharing in, genetic resources also raise IP questions.

Information and Communications Technology is also widely used to commit traditional crimes like fraud. In our very competitive business world, industrial espionage is reportedly conducted frequently to unjustly obtain competitive advantages.

(6) Protection against acts committed exclusively in the virtual world

Crimes, as traditionally thought of, are committed in the so-called real world, in our shared physical reality. The conduct used to commit such crimes, the circumstances involved in their commission, and the harms that result from their commission all occur in "real" places like public streets or private residences. Consequently, existing criminal law imposes liability and penalties for conduct that results in inflicting bodily harms, like injury to persons or property or the unauthorized taking of another person's property. The modern criminal law insists, as a fundamental premise, that liability be predicated upon some conduct—action or inaction in the face of a duty to act—taken in the external, physical world. It fundamentally rejects that liability can be imposed for incorporeal behaviors such as improper or even criminal thoughts.

At the same time, cyberspace exists along with, but distinct from the physical world. It is a shared conceptual reality, a "virtual world," not a shared physical reality. Since it is not a physical domain, some question whether the current principles of criminal law we employ are adequate to address crimes that exploit the unique advantages of cyberspace. This inadequacy cannot exist unless there are material differences between cybercrimes and "real" crimes as to, for example, the conduct used to commit the offenses that fall into both categories, the circumstances surrounding the commission of the offenses, and the harms that result. Naturally, we should not simply assume that criminal conduct that exploits cyberspace represents an entirely new phenomenon called "cybercrime." It may simply be perpetrators using cyberspace to engage in conduct that has long been outlawed

for a long time. The telephone, the telegraph, radio, television etc. have been used to perpetrate frauds, for example. However, fraud has been a crime for centuries. The same is true of homicide, whether committed with a knife, a club, a firearm or poison. Can there be truly virtual crimes that is offenses whose fundamental elements manifest themselves solely or almost solely in cyberspace? There are legal experts who maintain that traditional criminal law principles can be adapted to include most, if not all, the acts considered cybercrimes. Others, nothing especially the considerable difference between the world of the telephone and that of the internet, the fact that criminals can cause a much greater harm through the internet than other means, like the telephone, to defraud others and the advantage that they have on traditional criminals in avoiding detection and successful prosecution, favor developing new principles of criminal liability and new laws of cybercrimes.

The international responses to the questions on this issue contained in the Section II questionnaire will provide us with an assessment of the direction criminal law is taking internationally on this issue.

(7) Protection of enforcement system (non-compliance offences)

Internet Service Providers (ISPs) possess valuable information that can very useful for the investigation of crimes like subscriber information; internet traffic data (log-files, IP-related data); and content data. It is natural for governments, law enforcement, prosecutors to want to access as much information derived from internet use, web surfing and other transactions as possible. This may collide with constitutional notions of privacy, protection from unreasonable searches and seizures, and forbidding governmental "fishing expeditions."

Another situation that often arises is the control that national governments want to have on the content provided by ISPs to their citizens. There are three primary motives for internet censorship:

politics and power, social norms and morals, and security concerns. Protecting intellectual property rights and existing economic interests can also lead to internet censorship. In addition, blocking the networking tools and applications that allow the sharing of information is not infrequent in some countries. Censorship directed at the political opposition is especially frequent in authoritarian and repressive regimes. Some countries block Web sites related to religion and minority groups, often when these movements represent a threat to the ruling regimes. There have been well publicized conflicts and clashes between well known ISPs and the governments of certain countries on this issue. Financial interests related to intellectual property rights can also be a factor justifying drastic governmental intervention.

The questionnaire aims at obtaining information on this wide and complicated issue that reflects different legal traditions (e.g. the concept of Lèse majesté), cultural values, and economic priorities.

(C) International Approaches

Developing an international paradigm for addressing electronic crime is a challenge, given the global nature of the technology. All nations continue to struggle to define these crimes and develop electronic crime legislation applicable to both domestic and international audiences and situations. Purely domestic solutions are inadequate because cyberspace has no geographic or political boundaries and many electronic systems can be easily and surreptitiously accessed from anywhere in the world. International financial institutions are common targets for electronic fraud and embezzlement schemes. In addition, the development of sophisticated electronic technology has enabled organized crime and terrorist groups to bypass government detection and carry out destructive acts of violence. Even when computer-specific criminal statutes are in place, the rules of evidence in several industrialized countries could continue to hinder prosecutions until they adapt them to electronic crimes. Countries that restrict their political

discourse face the problem that the Internet provides a source of "illegal" information that is difficult to regulate. Moreover, what constitutes "acceptable" speech in the various countries on the information super-highway differs greatly, even between Western democracies. Solutions to freedom of expression issues on the Internet have varied widely. Some European countries initially tried to target the Internet service providers (ISPs). Other countries have implemented regulations that criminalize the distribution or consumption via the Internet of "harmful" information, and at times or even permanently limit or disrupt internet access.

Intellectual property crimes are a serious problem in the international arena. International software piracy remains endemic which means that many software applications existing on electronic devices around the world continue to be unpaid-for, illegal copies. In some cases legislation has been enacted to place considerable requirements and consequently to potentially incriminate Internet Service Providers. The problems of data mining, identity fraud, online gambling, child pornography, controlling employees via information technology, privacy violations by social media and search engines, like Facebook and Google, or wireless communications, like iPhones, are attracting considerable attention and concern. Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access, violations of privacy rights and manipulation of data. While a number of differences remain, there are significant areas of convergence in various nations' legislation. By defining specific new offenses and penalties, these codes avoid analytical difficulties that arise when general criminal laws are applied to computer crimes. At the same time, however, electronic governmental access to private or business information, bypassing traditional steps of constitutional protections and procedural criminal law, are raising concerns, new and difficult questions and the need to update substantive and procedural criminal law. International organizations and private corporations are also working to combat ICT crimes by contributing to the drive to harmonize national legislation. Nonetheless, international efforts have been mixed.

(D) The Questionnaire

It is clear that our information society has generated many new problems, challenges and opportunities for criminal law. There is a clear need to expand the frontiers of criminal law and of its application. The protection of privacy and human rights remains a paramount concern. The many areas of intervention mentioned above are appropriate for debate in Section II since they constitute the core of the specific expansion and innovation in substantive criminal law required by the information society that more and more encompasses and even controls not only our lives and activities but also world affairs, international relations and the threat of cyber wars. The accompanying questionnaire for Section II, Special Part, has been designed to collect relevant information on the response of criminal law to cybercrime in various countries worldwide. The questionnaire is organized around the major interests that have been identified as deserving protection (see above Section C). The questions center around the interests to be protected and the classical criminal law requirements of actus reus, mens rea, and the penalty envisioned in the law for different types of perpetrators like private persons, public officials, investigators, etc. The questionnaire limits itself to set major markers in the field and allow the National Reporters to contribute information taking into account different legal traditions and varying stages of development of national cybercrime laws. It is hoped that following this scheme of legal interests will facilitate the work of the National Reporters and elicit valuable information on the status of cyber criminal law worldwide. This should be fertile material for the development of resolutions at the Preparatory Colloquium and at the International Congress of the AIDP.

2. COLLOQUE PRÉPARATOİRE (SECTİON II) RAPPORT NATİONAL TURC PRÉPARÉ PAR

Dr. iur. E. Eylem AKSOY RETORNAZ*
Dr. Sinan ALTUNÇ**

(B) Les pratiques législatives et les concepts juridiques

(1) Comment les lois pénales relatives aux cyber-crimes sont-elles codifiées dans votre pays? Sont-elles contenues dans un titre unique ou un code unique ou sont-elles réparties dans les divers codes ou divers titres? (Veuillez fournir les textes utiles).

Les réglementations pénales relatives aux cyber-crimes se trouvent d'abord dans le Code pénal turc (CPT). Donc il n'y a pas de loi pénale spécifique relative aux cyber-crimes.

Mais dans certaines lois telles que la "Loi sur les œuvres intellectuelles et artistiques" et la "Loi sur la signature électronique", on peut trouver des dispositions sur les cyber-crimes.

Par exemple l'article 72 de la Loi sur les œuvres intellectuelles et artistiques, celui qui produit, offre à la vente, vend ou possède pour l'utilisation personnelle les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, sera puni avec une peine d'emprisonnement de 6 mois à 2 ans.

(2) Quel est l'impact des décisions judiciaires sur la formulation des lois pénales relatives aux cyber-crimes?

Il est très rare que les décisions judiciaires aient l'effet sur la formulation des lois pénales en Turquie. Mais quand même il y a

* Collaboratrice scientifique, Université de Galatasaray, Faculté de droit, Département de droit pénal et de procédure pénale.

** Maître de conférence, Université de Bahçeşehir, Faculté de droit, Département de droit pénal et de procédure pénale.

quelques décisions importantes qui ont influencé l'élaboration de la loi. Une de ces décisions est l'affaire Coşkun Ak. Coşkun Ak était l'administrateur de forum au Superonline [un fournisseur de service (internet service provider - ISP) turc]. Il a été tenu responsable pour un message anonyme publié au forum, en 2001. Il a été puni par les dispositions du CPT, parce qu'il n'y avait pas de normes spécifiques pour les crimes commis par l'intermédiaire de l'internet. Donc on a introduit un article dans la Loi sur la presse et essayé de résoudre les problèmes issus de l'utilisation de l'internet.

Ces dispositions n'ont pas été suffisantes et le besoin d'une loi spécifique s'est montré. Alors en 2007 la "Loi no. 5651 sur la régulation les publications faites dans le domaine d'internet et sur le combat avec les infractions commises par l'intermédiaire de ces publications" a été mise en vigueur.

(3) Pour rattraper l'évolution des besoins et des circonstances ainsi que pour atteindre de nouveaux objectifs, certaines lois sont les sujets de fréquentes modifications. Normalement, ces modifications prennent la forme de nouvelles lois. Dans certains cas, ces nouvelles lois, au lieu de simplement modifier les parties de la loi qui doivent être modifiées, présentent les modifications nécessaires dans un texte consolidé avec tous les amendements passés. Cette technique est appelée "la refonte". Est-ce la façon dont les lois sur la cyber-criminalité sont mises à jour et adaptées aux changements de réalité dans votre pays? Veuillez fournir les références et les citations appropriées.

Comme on en a déjà parlé, jusqu'à la Loi no. 5651, les modifications ont été faites par les articles particuliers dans le lois. Mais la Loi no. 5651 est completement relative à l'internet. Quant aux changements effectués au sein du CPT afin de incriminer les actes commis par l'intermédiaire de l'internet, on a modifié les parties intéressées.

(C) Les infractions spécifiques à la cybercriminalité

(1) En ce qui concerne l'élément moral, les infractions relatives à la cybercriminalité doivent-elles être intentionnelles? Ont-elles besoin d'une intention spécifique?

Les infractions relatives à la cybercriminalité doivent être intentionnelles. Elles n'ont pas besoin d'une intention spécifique.

(2) Y a-t-il également des infractions par négligence dans ce domaine?

Ces infractions ne sont pas l'objet de la négligence. Mais dans l'article 243 alinéa 3 du CPT, il s'agit d'une circonstance aggravante quand les données se perdent ou se changent. Quand même ce résultat peut être réalisé par négligence.

(3) Si oui, veuillez fournir une liste de ces infractions.

(a) L'intégrité et la fonctionnalité du système informatique

1. Accès illégal et interception de la transmission

a. Objet : système ou données?

Votre droit pénal érige-t-il en infraction pénale l'entrave grave et non autorisée faite au fonctionnement d'un ordinateur et/ou d'un système électronique en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant ou supprimant des informations ou des données à partir d'un système informatique, logiciel ou programme?

Dans le CPT, on a deux articles qui incriminent ces infractions. L'article 243, intitulé "entrer dans le système informatique" et l'article 244, intitulé "entraver, détériorer le système, effacer ou changer les données".

L'article 243 incrimine le fait d'entrer dans le système et y rester illégalement. L'article 244 incrimine l'entrave du fonctionnement d'un système informatique.

b. Exigence de la violation des mesures de sécurité?

Est-ce une exigence de votre droit pénal que le pirate effectue le piratage du système informatique en utilisant un ou plusieurs logiciels nécessaires pour vaincre les mesures de sécurité et gagner l'accès au niveau d'entrée ou à un niveau?

Non. Il suffit d'entrer dans le système informatique illégalement.

2. Les interférences de données et du système

a. Objet - la protection du système / matériel / données?

Votre droit pénal définit-il « l'ordinateur et / ou les données électroniques »? Est-ce que cette définition comprend des programmes, des logiciels ou de codage similaires?

Si vous avez une définition, veuillez la fournir accompagnée de la référence aux paragraphes des articles connexes ou de votre code.

"La Loi no. 5651 sur la régulation les publications faites dans le domaine d'internet et sur le combat avec les infractions commises par l'intermédiaire de ces publications" nous donne la définition de la donnée. D'après cette définition la donnée est la valeur sur laquelle il est possible de faire l'opération par l'ordinateur. Mais il n'y a pas de définition de l'ordinateur ou les données électroniques.

b. Acte - Destruction / modification / rendre inaccessible?

i. Votre droit pénal incrimine-t-il l'effacement non-autorisé, la modification, le fait de rendre inaccessible, d'acquérir des informations ou les données à partir d'un ordinateur, d'un système électronique ou un programme ? D'autres interférences similaires avec les informations ou les données à partir d'un ordinateur, d'un système électronique ou un programme sont-elles incriminées?

L'article 244 du CPT incrimine ces actes. L'alinéa 1 incrimine l'acte d'entraver ou de détériorer le fonctionnement du système informatique. L'alinéa 2 prévoit l'incrimination des faits de détériorer, d'effacer, de changer, de rendre inaccessible les données qui se trouvent dans le système. En plus on incrimine les faits d'installer des données dans le système ou d'envoyer les données existantes ailleurs.

ii. Votre droit pénal incrimine-t-il l'interception non autorisée de la transmission de quelque manière que ce soit de données informatiques ou électroniques et / ou d'informations?

D'une part l'article 124 du CPT sanctionne le fait d'entraver illégalement la communication qui se déroule entre les individus. La transmission des données informatiques ou électroniques peut s'entendre comme la communication. Donc «entraver la communication» résulte «entraver la transmission des données».

D'autre part l'article 244 du CPT (susmentionné) peut aussi accepter en tant qu'une disposition qui incrimine l'interception non autorisée parce que l'article parle d'entraver le fonctionnement d'un système informatique.

3. Les fausses données

a. Objet - l'authenticité?

Votre droit pénal définit-il, comme une infraction pénale, la saisie non-autorisée, l'altération, l'effacement ou la suppression des données informatiques ou électroniques résultant de données inauthentiques, afin de protéger l'authenticité des données qui seront utilisées à des fins juridiques? Si vous disposez d'une définition, veuillez la fournir avec les références aux paragraphes pertinents ou articles de votre code et / ou lois spéciales.

La première disposition est l'article 136 du CPT. Cet article incrimine le fait de «donner, diffuser ou obtenir illégalement les

données». Parmi les articles qui régularisent les infractions informatiques il n'y a pas de disposition qui sanctionne clairement ce type de faits.

En plus dans la Loi sur la signature électronique, l'article 17 incrimine le fait de former un certificat électronique faux ou bien d'imiter ou d'abimer les certificats qui ont été créés légalement.

b. Acte - modification / suppression

Votre droit pénal incrimine-t-il la saisie non autorisée, le changement, l'effacement ou la suppression de données informatiques ou électroniques aboutissant à des données inauthentiques avec l'intention qu'elles soient considérées comme ou agissent sur des buts légaux, comme si elles étaient authentiques? Si oui, veuillez fournir la référence des paragraphes pertinents ou des articles de votre code.

La Loi sur la signature électronique, l'article 17 incrimine le fait de former un certificat électronique faux ou bien d'imiter ou d'abimer les certificats qui ont été crées légalement.

4. Les abus de dispositifs

a. Objet - type de dispositif?

Votre droit pénal incrimine-t-il le développement de la «boîte à outils » d'un hacker ou d'une partie de celle-ci (par exemple, les cartes d'acquisition de mots de passe et les enregistreurs de frappe, programmes blue-box, les war-dialers, les logiciels de cryptage, les programmes qui craquent les mots de passe, les scanners de vulnérabilité de la sécurité, des packet sniffers, etc) pour l'accès non autorisé à un ordinateur ou à des systèmes électroniques ou de transmissions?

Dans le domaine des cyber-crimes, on rencontre peu aux dispositions qui incriminent les actes préparatoires. Mais il y a deux cas où l'obtention ou la possession incriminent.

Selon l'article 72 de la Loi sur les œuvres intellectuelles et artistiques, celui qui produit, offre à la vente, vend ou **possède**

pour l'utilisation personnelle les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, sera puni avec une peine d'emprisonnement de 6 mois à 2 ans.

Selon l'article 245 alinéa 2 du CPT, celui qui produit, vend, transfert, achète ou accepte des faux cartes bancaires ou cartes de crédit seront punis avec la peine d'emprisonnement de 3 à 7 ans.

b. Acte - distribution publique / transfert à une autre personne?

i. Votre droit pénal incrimine-t-il l'utilisation non-autorisée de l'un des outils du hacker énumérés ci-dessus?

Pour incriminer l'utilisation non-autorisée de l'un des outils du hacker énumérés ci-dessus, cette utilisation doit être atteindre au niveau d'entrer non-autorisé au système informatique.

ii. Votre droit pénal incrimine-t-il la distribution publique et / ou le transfert à d'autres parties de l'information électronique piratée?

Dans l'article 244 alinéa 2, le fait de transférer les données qui se trouvent dans un système informatique à d'autres parties.

En outre, si l'information est en forme de la communication entre les individus, il s'agit de l'infraction de la divulgation illégale du contenu de la communication. Si cette infraction est commise par la voie de la presse ou la media, la peine sera augmentée.

Si ces informations sont en forme des voix ou des images relatives à la vie privée des individus, l'article 134 alinéa 2 du CPT sera applicable. L'article 134 alinéa 2 incrimine le fait de divulguer les voix ou les images relatifs a la vie privée des individus et prévoit une peine d'emprisonnement de 1 à 3 ans.

Enfin, selon l'article 136, le fait de donner, de diffuser ou d'obtenir illégalement les données personnelles est passible d'une peine d'emprisonnement de 1 à 4 ans.

c. Possession?

Votre droit pénal incrimine-t-il la possession de «boîte à outils» d'un hacker ou d'une partie de celle-ci (par exemple, les cartes d'acquisition de mots de passe et les enregistreurs de frappe, programmes blue-box, les war-dialers, les logiciels de cryptage, les programmes qui craquent les mots de passe, les scanners de vulnérabilité de la sécurité, des packet sniffers, etc) pour l'accès non autorisé à un ordinateur ou à des systèmes électroniques ou de transmissions?

Dans le domaine des cyber-crimes, on rencontre peu aux dispositions qui incriminent les actes préparatoires. Mais il y a deux cas où l'obtention ou la possession incriminent.

Selon l'article 72 de la Loi sur les œuvres intellectuelles et d'art, celui qui produit, offre à la vente, vend ou **possède pour l'utilisation personnelle** les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, seront punis avec une peine d'emprisonnement de 6 mois à 2 ans.

Selon l'article 245 alinéa 2 du CPT, celui qui produit, vend, transfert, achète ou accepte des faux cartes bancaires ou cartes de crédit seront punis avec la peine d'emprisonnement de 3 à 7 ans.

(b) La vie privée

1. La violation du secret des données privées

a. Objet - type de données privées?

(Remarque: les données privées sont des données qui appartiennent à la vie privée des gens, mais n'identifient pas ou ne permettent pas d'identifier une personne, par exemple, l'état civil, l'orientation sexuelle, l'état de santé, les habitudes d'achat ou de préférences)

i. Les lois de votre pays exigent-elles que les collecteurs de données divulguent leurs pratiques d'information avant de recueillir des informations privées auprès des

consommateurs comme, par exemple, la façon dont l'information est utilisée, la manière dont elle est recueillie et le but de cette collecte? Si elle est partagée avec d'autres et si les consommateurs ont un contrôle sur la divulgation de leurs données privées?

Selon l'article 20 alinéa 3 de la Constitution turque, «tout le monde a le droit de demander la protection de ses données personnelles. Ce droit inclut être informe de l'avoir accès à et de demander la correction et l'effacement de ses données personnelles et être informe si ces données sont utilisées les objectives envisagées. Les données personnelles ne peuvent être allé en procession que aux cas ou il est prévu dans la loi ou quand l'individu donne son consentement. Les principes et les procédures relatifs à la protection des données personnelles sont prévus pas la loi.» Il n'y a pas encore une telle loi en Turquie. Mais les travaux continuent sur le Projet de Loi sur la protection des données personnelles.

Dans les lois qui sont en vigueur, on rencontre des dispositions sur l'interdiction de collecte des données personnelles sans autorisation préalable ou sans consentement de l'individu. Par exemple on peut parler de la Loi sur la signature électronique. L'article 12 de cette loi règlemente la protection des informations. Selon cet article, quand on demande le certificat électronique d'un individu, les informations nécessaires ne peuvent être pris qu'avec son consentement et les informations obtenues ne peuvent pas être partagées avec les tierces personnes sans l'autorisation de celui-ci.

Dans l'article 73 de la Loi sur la banque, on parle de garder les informations apprises pendant les activités bancaires. La Loi sur les cartes bancaire et les cartes de crédit aussi prévoit une règle similaire dans l'article 23.

ii. Les lois de votre pays exigent-elles que les sociétés et les entités qui font des affaires sur internet, informent les consommateurs de l'identité de celui qui collecte des données, du fait du caractère volontaire ou obligatoire

de la fourniture des données demandées ainsi que les mesures prises par le collecteur de données pour assurer la confidentialité, l'intégrité et la qualité des données?

Le Projet de Loi sur la régulation du commerce électronique est important. Ce projet de loi prévoit que, avant la signature du contrat, le fournisseur des services offre les informations sur la confidentialité aux consommateurs. Il doit expliquer s'il sera possible d'accéder au contrat suivant la signature et combien de temps cet accès sera possible. Le fournisseur des services sera responsable de la protection et de la sécurité des données personnelles.

iii. Les lois de votre pays exigent-elles des sites Web d'afficher leur politique de confidentialité et d'expliquer comment les renseignements personnels seront utilisés avant que les consommateurs entrent dans le processus d'achat ou de toute autre opération pour laquelle ils doivent fournir des informations sensibles?

Dans l'article 9/A de la Loi sur la protection du consommateur, on a fait une disposition sur les contrats à distance. La conclusion d'un contrat à distance peut se faire par tout moyen utile (par téléphone, courrier électronique, catalogue, etc.) sans qu'il y ait présence physique et simultanée des parties au contrat. Avant conclure un contrat à distance, quelques informations doivent être données aux consommateurs.

iv. Le droit pénal de votre pays incrimine-t-il l'omission de fournir les informations mentionnées ci-dessus (Cf : a.ii et a.iii)?

Le droit pénal turc accepte ce type d'omissions en tant que contravention et prévoit des sanctions administratives.

b. Acte - L'utilisation illégale et le transfert / distribution?

i. Le droit pénal de votre pays définit-il le transfert et la distribution illégale des données privées?

Le droit pénal turc définit les données. Dans l'article 2 de la Loi sur la réglementation des diffusions d'internet et contre les

infractions commises par la voie d'internet, la donnée est définie comme toutes sortes de valeurs sur lesquelles on peut faire des opérations par ordinateur.

Le Projet de loi sur la protection des données personnelles définit la donnée personnelle en tant que toutes informations relatives aux personnes déterminées ou déterminables.

Mais le droit pénal turc n'a pas fait la définition le transfert et la distribution illégale des données privées.

ii. Le droit pénal de votre pays incrimine-t-il l'utilisation illégale, le transfert et /ou la distribution des données privées?

L'article 136 du CPT incrimine le transfert, la diffusion ou l'obtention illégale des données personnelles.

c. Justification?

i. Dans quelles conditions les lois de votre pays autorisent-elles la collecte, le traitement autorisé, le transfert et la distribution de données privées?

Premièrement, le droit turc autorise la collecte, le traitement autorisé, le transfert et la distribution de données privées/ personnelles, quand il y a le consentement de l'intéressé. En fait, le consentement de l'intéressé est un fait justificatif général réglementé dans l'article 26 du CPT. Donc on peut appliquer cette justification dans ces cas-là.

Deuxièmement on parler de la légalité d'enregistrement des données personnelles. Un autre fait justificatif est l'ordre de la loi, réglemente dans l'article 24 du CPT. Donc si l'enregistrement est effectué à l'issue de l'ordre de la loi, il sera justifié. Par exemple, le Code de procédure pénale (CPP) nous montre les conditions qui autorisent la collecte ou la saisie.

ii. Quelle règle de nécessité est requise pour autoriser une collecte et /ou une distribution (convaincante, importante, raisonnable, pratique)?

Pour autoriser une collecte ou une distribution, la règle de nécessité doit être convaincante.

2. Violation du secret professionnel

a. Objet - type de données privées?

i. Les lois de votre pays exigent-elles des professionnels de divulguer :

- **Les informations collectées et les pratiques de gestion avant la collecte d'informations personnelles de leurs patients ou clients;**
- **Leurs pratiques de divulgation;**
- **Leurs obligations éthiques professionnelles;**
- **Et si les patients ou les clients ont un contrôle sur la divulgation de leurs données personnelles?**

Dans les lois turques, on prévoit que les personnes mentionnées ci-dessus, doivent garder les informations personnelles qu'ils sont informées au cours de leurs professions. Par exemple, les avocats ne peuvent pas divulguer les informations que leurs clients leur ont données. En plus selon l'article 46 du CPP, les avocats ne peuvent pas faire témoignage sur ces informations sans qu'il y ait l'autorisation de leurs clients.

Selon l'article 258 du CPT, il est interdit pour les fonctionnaires de divulguer les informations dont ils sont informés au cours de leur fonction.

Quant aux médecins, l'article 134 du CPT peut être appliqué. Dans cet article, la divulgation des voix et des images relatifs à la vie privée des individus est incriminée. En plus, le décret sur la déontologie médicale parle de la même interdiction dans son article 4, alinéa 1. L'interdiction similaire pour le témoignage des médecins est réglementée le même article 46 du CPP.

ii. Quelles sont les données spécifiquement protégées, le cas échéant?

Les données dont ils sont informés au cours de leur profession sont protégées.

iii. La législation pénale de votre pays autorise-t-elle ou même exige-t-elle de la part des médecins, des avocats, des prêtres, etc… de violer la confidentialité dans certaines situations ou pour certaines raisons prévues par la loi? Dans quels cas serait-ce possible? (Exemples de cas : croire raisonnablement qu'il y a des abus voire un cas de maltraitance à l'égard d'un enfant, des femmes ou des personnes âgées)?

Dans l'article 278 on incrimine le fait de ne pas dénoncer l'infraction. A l'alinéa 4 de cet article, on parle des personnes qui ont le droit de ne pas témoigner. Ces personnes ne seront pas sanctionnées sauf si ils ont la charge d'éviter la commission d'une infraction.

En plus de cela, les articles 279 et 280 réglementent des infractions similaires. L'article 279 incrimine la non-dénonciation des fonctionnaires, et l'article 280 celle des membres de la profession de la santé. Donc ces gens là sont tenus de violer la confidentialité dans les situations susmentionnées.

En outre, la Loi de la protection de la santé générale prévoit de dénonciation des maladies vénériennes.

b. Sujets - Type d'auteurs?

Le droit pénal de votre pays identifie-t-il les catégories de professionnels qui sont liées par des règles spécifiques de confidentialité?

L'article 46 du CPP réglemente l'abstention du témoignage à cause de la profession. Dans cet article quelques professionnels sont mentionnés. Ce sont les avocats, les médecins, les pharmaciens, les dentistes, les accoucheuses, tous les autres membres de la professions de santé, les conseillers financiers et les notaires.

A part, l'article 239 du CPT le fait de donner ou de divulguer les informations à caractère secret commercial, bancaire ou de client.

En dernier, l'article 258 punit les fonctionnaires qui divulguent les informations qui doivent rester secrètes.

c. Acte - l'utilisation illégale et le transfert / distribution?

Quels sont les actes (par exemple la collecte illégale, l'utilisation, le transfert et la distribution) qui sont spécifiquement punis par le droit pénal de votre pays?

Dans le cas où la collecte des informations est considérée légale, la divulgation et le transfert illégaux des informations secrètes peuvent être punis. Ici celui qui collecte les informations le fait parce que c'est sa profession. Par exemple, la police a le pouvoir de collecter des informations si elle a un ordre de l'autorité légitime. Mais si la collecte est illégale, alors cette fois-ci celui qui collecte sera responsable.

3. Traitement illégal de données personnelles et privées

a. Objet?

Votre droit pénal incrimine-t-il l'acquisition illégale et non autorisée, la transformation, le stockage, l'analyse, la manipulation, l'utilisation, la vente, le transfert etc, de données personnelles et privées?

L'article 135 du CPT punit l'enregistrement des données personnelles et l'article 136 du CPT punit la délivrance ou l'obtention illégale des données.

b. Sujet?

Votre droit pénal identifie-t-il particulièrement les catégories de personnes et les entités qui sont concernées par cette interdiction pénale et ses sanctions?

Si les infractions contre la vie privée et le domaine secret de la vie sont commises (1) par les fonctionnaires en abusant leurs pouvoirs

ou (2) en profitant de la facilité fournie par une profession, la peine sera augmentée. En outre l'article 140 du CPT prévoit la punition des personnes morales en cas de commission ces infractions.

c. Acte?

i. Votre droit pénal sanctionne-t-il les actes spécifiques qui constituent tout ou partie du traitement illégal des données personnelles et privées? Répondre pour chaque catégorie ci-dessous en citant la législation pertinente et, le cas échéant, les dispositions:

1. La collecte illégale

L'article 136 du CPT : «Celui qui donne les données personnelles à l'autrui, les diffusent ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans.» On peut considérer l'obtention illégale des données comme la collecte illégale.

2. L'utilisation illégale

L'article 136 du CPT : «Celui qui donne les données personnelles à l'autrui, les diffuse ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans.» Donner ou diffuser les données personnelles exige les utiliser. Donc ces actes définis dans cet article signifient en même temps l'utilisation illégale.

3. La rétention illégale

L'article 138 du CPT : «Celui qui s'abstient de supprimer les données qui se trouvent dans le système après un délai déterminé par la loi, sera puni par l'emprisonnement de six mois à un an.»

4. Le transfert illégal

L'article 136 du CPT : «Celui qui donne les données personnelles à l'autrui, les diffusent ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans.»

ii. Existe-t-il une différence si ces données personnelles et privées sont utilisées, transférées etc, pour des enquêtes de police ou à des fins judiciaires?

Quand les données personnelles et privées sont utilisées, transférées, etc. pour des enquêtes de police ou à fins judiciaires, cette utilisation, ce transfert, etc. ne seront plus illégaux. Il y a des dispositions dans le CPP qui rendent ces actes légaux. Par exemple l'article 135 du CPP réglemente le constat, l'interception, l'enregistrement de la télécommunication du suspect ou de l'inculpé afin d'obtenir la preuve. En plus, l'article 134 du CPP donne le pouvoir de faire la perquisition, la transcription et la saisie sur les ordinateurs. Ces interceptions peuvent être effectuées suivant la décision du juge ou l'ordre écrite du procureur. La police est tenue d'appliquer cette interception. Donc s'il y a une telle décision ou un tel ordre, le fait de la police sera légal.

d. Justification?

i. Dans quelles conditions la loi de votre pays permet-elle la collecte, le traitement autorisé, le transfert et la distribution de données personnelles et privées?

Premièrement, le droit turc autorise la collecte, le traitement autorisé, le transfert et la distribution de données privées/personnelles, quand il y a le consentement de l'intéressé. En fait, le consentement de l'intéressé est un fait justificatif général réglementé dans l'article 26 du CPT. Donc on peut appliquer cette justification dans ces cas-là.

Deuxièmement on parler de la légalité d'enregistrement des données personnelles. Un autre fait justificatif est l'ordre de la loi, réglemente dans l'article 24 du CPT. Donc si l'enregistrement est effectué a l'issue de l'ordre de la loi, il sera justifié. Par exemple, le CPP nous montre les conditions qui autorisent la collecte ou la saisie.

ii. Quel cas de nécessité est requis pour une collecte autorisée et/ou la distribution de données à caractère personnel et privé (Convaincante, importante, raisonnable, pratique)?

Pour autoriser une collecte ou une distribution, la règle de nécessité doit être convaincante.

4. Le vol d'identité

(Remarque: le vol d'identité se produit lorsque quelqu'un s'approprie les renseignements personnels d'autrui, sans que ce dernier en ait connaissance, pour commettre un vol ou une fraude. Le vol d'identité est un moyen pour perpétrer des fraudes. En règle générale, la victime est amenée à croire qu'elle doit divulguer des renseignements personnels à une entreprise ou une entité légitime, parfois comme une réponse à une sollicitation d'e-mail de mettre à jour la facturation ou les renseignements sur l'adhésion ou comme une application frauduleuse d'affichage sur internet pour un emploi ou pour un prêt.)

a. Objet

i. Votre droit pénal incrimine-t-il le vol d'identité? Veuillez citer le texte légal pertinent.

L'identité doit être considérée comme une donnée personnelle. Donc l'article 136 du CPT qui réglemente l'obtention illégale des données personnelles peut être appliqué pour le vol d'identité.

A part cela, dans l'article 142 alinéa 2, la sanction du vol est augmentée si cet acte est commis par l'utilisation des systèmes informatiques. Aussi dans l'article 158 alinéa 1, la sanction de l'escroquerie est augmentée, si elle est commise par l'utilisation des systèmes informatiques.

ii. Votre droit pénal proscrit-il les formes spécifiques de vol d'identité, comme le phishing, par exemple? Le phishing est défini comme une forme de vol d'identité en ligne qui utilise des emails usurpés conçus pour attirer les destinataires vers des sites frauduleux qui tentent de les

inciter à divulguer des données financières personnelles telles que les numéros de cartes de crédit, les noms d'utilisateur et les mots de passe pour accéder aux comptes, les numéros de sécurité sociale etc…

Il n'y a pas en droit turc une disposition qui incrimine clairement ce type d'actes. Mais la Cour de cassation turque, applique les règles relatives à l'escroquerie.[1]

b. Sujet

Votre droit pénal contient-il une responsabilité pénale liée à la personnalité numérique d'une personne, ou à son Avatar, ou à son personnage numérique dans un jeu de simulation basé sur internet (par exemple Cityville, Farmville, etc)? Veuillez citer la loi pertinente.

Le droit pénal turc ne contient pas une responsabilité pénale liée à la personnalité numérique d'une personne, ou à son avatar, ou à son personnage numérique dans un jeu de simulation basé sur internet. On accepte que le droit pénal doive être *ultima ratio.* Donc si on incrimine ces types de faits, alors on élargit énormément le domaine d'intervention du droit pénal.

(c) La protection contre les contenus illicites: les TIC connexes

1. Objet

a. La pornographie infantile - des images d'enfants réels ou virtuels?

i. Votre droit pénal incrimine-t-il l'utilisation d'internet dans le but de stocker, d'accéder et de diffuser de la pédopornographie? Si c'est le cas, veuillez citer les textes légaux pertinants.

1 Dans une de ces decisions, la Cour de cassation applique les regles relatives à l'escroquerie. Selon le fait, l'inculpé a obtenu le code de MSN de la plaignante et apres lui demande d'envoyer de l'argent par la voie de MSN. La Chambre criminelle numéro 11 de la Cour de cassation applique l'article 158 dans cette affaire. (C. Cass. 11. chambre crim., 18.03.2010, 2007/5408, 2010/3253).

Le droit turc n'adopte pas une définition de la pédopornographie. Néanmoins, l'article 226 al. 3 du Code pénal turc (CPT) intitulé « l'obscénité» incrimine le fait d'utiliser des enfants afin de fabriquer des images, des sons et des textes de caractère obscène. Cette infraction est passible d'une peine privative de liberté de cinq ans à dix ans d'emprisonnement et de cinq mille jours de jours-amendes. Au titre du même alinéa de l'art. 226 CPT, «Celui qui aura importé, mis en circulation, vendu, diffusé, transféré, possédé, pris en dépôt, ou mise à disposition d'un tiers sera puni d'une peine privative de liberté de deux à cinq ans et de cinq mille jours de jours-amendes.»

Il convient de noter qu'en droit turc, à défaut d'une définition claire de ce qu'est l'obscénité, toute image, son et texte, même de nature érotique, peut être considéré comme obscène Cela constitue, à nos yeux, une violation de la légalité des délits et des peines.

La diffusion par voie de presse ou médias est prévue comme une circonstance aggravante dans l'art. 226 al. 5 CPT.

ii. En particulier, votre droit pénal :

Crée-t-il une nouvelle infraction qui cible les criminels qui utilisent internet pour leurrer et exploiter les enfants à des fins sexuelles?

Incrimine-t-il:

1. **la transmission,**
2. **la mise à disposition,**
3. **l'exportation**
4. **et l'accès intentionnel à de la pédopornographie sur internet;**

Le fait de diffuser, de servir d'intermédiaire pour la diffusion, de mettre à disposition d'un tiers par voie de presse ou de publications constitue une circonstance aggravante de l'infraction d'obscénité au terme de l'art 226 al. 5.

Les termes «par voie de la presse et des publications»signifie «la diffusion d'informations par l'intermédiaire de moyens

d'information de masse écrits, audiovisuels et électroniques» selon l'article 6 CPT consacré aux «définitions».

Se pose la question de savoir si l'internet pourrait être considéré comme un moyen écrits, audiovisuels et électroniques au sens de l'art 6 CPT.

Conformément à l'article 2 du Code sur internet une plate-forme Web signifie «une plateforme publique installée sur internet en dehors des logiciels de communication ou des systèmes informatiques personnelles ou organisationnelles». Ni la diffusion du contenu obscène par le biais des logiciels de communication ni des systèmes personnels ou organisationnels n'entrent donc dans le champ d'application de la loi. Pour invoquer la responsabilité pénale au sens de l'art 226 al. 3 et la responsabilité des acteurs d'internet au sens de la loi 5651 sur internet, le contenu obscène doit donc être diffusé sur des sites Web accessibles à tout le monde.

Dans le même sens, la Cour de cassation turque, dans un arrêt rendu en 2007, considère que «*vu les dispositions en vigueur le transfère d'information ou de document par le courrier électronique ne peut être considéré une diffusion par voie de presse et des médias*».

Permet-il aux juges d'ordonner la suppression de la pédopornographie affichée sur des systèmes informatiques dans votre pays;

La législation turque ne permet pas au juge d'ordonner la pédopornographie affichée sur des systèmes informatiques.

Cependant l'art. 8 de la loi 5651 permet au juge d'interdire l'accès à un site Web si des raisons suffisantes permettent de soupçonner que certaines infractions sont commises par l'intermédiaire d'un site Web. Ces infractions sont les suivantes : (i) l'incitation au suicide, (ii) les violences sexuelles faites aux enfants, (iii) le fait de faciliter la toxicomanie, (iv) la fourniture de produits dangereux pour la santé, (v) l'obscénité, (vi) la prostitution, (vii) les jeux d'argent, ainsi que (viii) les infractions régies par le Code turc 5816, qui incrimine les actes portant atteinte à la mémoire d'Atatürk.

Lorsqu'il est saisi d'une plainte ou par suite de ses propres constatations, le parquet peut demander à un juge d'ordonner l'interdiction d'accès au site Web concerné dans un délai de vingt-quatre heures. Le parquet peut, en cas d'urgence ordonner lui-même cette interdiction, qui doit ensuite être approuvée par un magistrat dans un délai de vingt-quatre heures (la décision du juge doit par conséquent suivre dans ce délai de vingt-quatre heures). L'interdiction donnée doit être appliquée dès que possible et exécutée par le fournisseur d'accès Internet dans un délai de vingt-quatre heures à compter de l'ordonnance judiciaire. En cas de rejet de l'interdiction par le juge, le parquet est tenu de rétablir intégralement l'accès au site Web en question.

Lorsque le parquet conclut à l'absence de contenu incriminé sur le site Web concerné ou si le tribunal estime que ce contenu n'est pas constitutif d'une infraction, l'interdiction est levée et l'accès au site Web est rétabli.

Si le fournisseur d'accès Internet ou le fournisseur d'hébergement ne bloque pas intégralement l'accès au site Web en question, le personnel responsable est passible d'une peine de deux à six mois d'emprisonnement.

De plus, la Présidence des télécommunications et des transmissions, instituée par ladite loi et placée sous la tutelle du Conseil turc des télécommunications, est habilitée à interdire un site Web sans l'approbation d'un juge lorsque celui-ci est constitutif de l'infraction d'obscénité et que son contenu et son fournisseur d'hébergement réside hors du territoire turc ou lorsqu'un site Web comporte un contenu constitutif de violences sexuelles faites aux enfants ou obscène et que son contenu et le fournisseur d'hébergement réside en Turquie. Cette interdiction doit ensuite être appliquée par le fournisseur d'accès Internet. Chaque fois que l'auteur de l'infraction et son lieu de résidence sont identifiés, la présidence est tenue d'en informer le parquet, afin que ce dernier engage des poursuites.

Le particulier qui estime qu'un site Web porte atteinte à ses droits subjectifs (l'enfant victime, les parents qui ont l'autorité parentale ou son tuteur dans le cas d'obscenité) peut demander au fournisseur d'accès Internet ou au fournisseur d'hébergement la suppression de ce contenu et la publication d'un droit de réponse pendant une période de sept jours et sur un espace aussi étendu que le contenu initialement présenté, à l'endroit même de sa présentation. Les fournisseurs d'accès Internet ou le fournisseur d'hébergement sont tenus de répondre favorablement à cette demande dans un délai de deux jours. Passé ce délai, la demande est présumée rejetée. Dans ce cas, le juge de paix local peut en être saisi dans un délai de quinze jours. Il lui incombe alors de statuer dans un délai de trois jours sans procès. Sa décision est susceptible d'appel devant les juridictions supérieures.

Lorsque le juge de paix fait droit à la demande, le fournisseur d'accès Internet ou le fournisseur d'hébergement à l'obligation de supprimer le contenu en question et de publier un droit de réponse du plaignant dans un délai de deux jours. En cas de refus d'exécuter la décision du juge de paix, le personnel responsable du fournisseur d'accès Internet ou du fournisseur d'hébergement est passible d'une peine de six mois à deux ans d'emprisonnement.

Permet-il à un juge d'ordonner la confiscation de tout matériel ou équipement utilisé dans la perpétration d'une infraction de pédopornographie;

En droit turc, le juge peut prononcer la confiscation des objets qui ont servi ou devaient servir à commettre une infraction ou qui sont le produit d'une infraction à condition que ces objets n'appartiennent pas à des tiers en vertu de l'art. 54 al. 1 CPT. Les objets dont la production, le stockage, l'utilisation, le transport, l'achat ou la vente constitue une infraction fait l'objet de la confiscation selon l'art 54 al. 4.

La confiscation est une mesure de sûreté selon le CPT donc le juge peut confisquer les valeurs patrimoniales alors même qu'aucune personne déterminée n'est punissable.

Le juge peut donc ordonner la confiscation de tout matériel ou équipement utilisé dans la perpétration d'une infraction de pédopornographie en vertu de l'art 54 al.1 et 4 du CPT.

Criminalise-t-il:

1. **l'accès en connaissance de cause à la pornographie infantile sur internet**
2. **la transmission de pornographie infantile sur Internet**
3. **l'exportation de pornographie juvénile sur Internet**
4. **La possession de pornographie juvénile sur internet dans le but, par exemple, de transmettre, d'exporter ...?**

L'art 226 CPT punit la simple possession, de la pornographie infantile. Selon la Cour de cassation turque, l'auteur est punissable même s'il ne possède pas la pornographie infantile à des fins commerciales mais à usage personnel.

Aux yeux de la Cour de cassation, la pornographie enfantine téléchargée et stocké de manière systématique et continue entraîne sa possession. Cependant, le seul fait d'accéder à un site Web et de visionner les images, en connaissance de cause ne suffit pas à caractériser l'infraction prévu par l'article 226-23, alinéa 3, du Code pénal.

iii. Votre droit pénal incrimine-t-il la sollicitation en ligne des enfants à des fins sexuelles via des sites Web de réseaux sociaux et des chats?

L'art. 103/1 CPT incrimine l'abus sexuel sur mineur. Selon cette disposition «l'auteur de tout acte à caractère sexuel sur un mineur de moins de 15ans, ou sur une personne de 15 ans ou plus incapable de comprendre les conséquences juridiques d'un tel acte, est passible de trois à huit ans d'emprisonnement. Le code ne définit pas les actes à caractère sexuel.

Par «*acte à caractère sexuel*», la jurisprudence entend, en effet, un contact physique sans nécessairement une relation sexuelle.

Nonobstant la jurisprudence, d'aucuns considère que l'infraction peut être constitué sans contact même en l'absence de contact de physique. Cela étant les propos, gestes et mimiques d'ordre sexuels adressé au mineur sur les réseaux sociaux sur internet suffit à caractériser l'infraction d'abus sexuel sur mineur.

L'incitation à la prostitution d'un mineur peut être commise par le biais d'internet.

iv. La définition de la pornographie juvénile dans votre code pénal est-elle proche de celle contenue dans les instruments internationaux (par exemple directives de l'UE)?

La Turquie a signé le Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants et l'a ratifié par la loi n°4755 de 2002. Elle signé la Convention sur la cybercriminalité du Conseil de l'Europe en 2010 mais ne l'a pas encore ratifié. Elle fait partie aussi de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

Même si la Turquie a érigé en infractions pénales la plupart des actes que les États membres sont invités à interdire conformément aux dispositions du Protocole, aucune définition de la pornographie enfantine n'est adoptée.

Certaines modifications ont été apportées dans la législation turque afin de se conformer notamment à l'art. 8 du Protocole facultatif. L'art. 52/3 et 226 du CPP s'inscrivent dans cette ligne. L'audition d'un mineur victime d'une infraction sexuelle devra faire l'objet d'un enregistrement sonore ou audiovisuel. Un tel enregistrement est en effet de nature à limiter le nombre des auditions de la victime, mais aussi à faciliter l'expression de l'enfant tout en permettant d'y déceler les éléments non verbalisés et de les mémoriser pour la suite de la procédure. Cet enregistrement, est, aux termes de la loi, obligatoire dans toutes les procédures où des mineurs victimes doivent être entendues. L'enfant victime doit être accompagné par des spécialistes lors de son audition.

v. La victimisation secondaire est-elle évitée pour les victimes de pornographie infantile dans votre droit pénal? Dans des États où la prostitution ou l'apparition dans la pornographie sont punissables sous couvert du droit pénal national, il devrait être possible de ne pas poursuivre ou de ne pas imposer de peines conformément aux lois dans le cas où l'enfant concerné a commis ces actes car il est victime d'exploitation sexuelle ou a été contraint à participer à la pornographie d'enfant. Ceci est-il envisagé par votre droit pénal?

La prostitution n'est pas incriminée en droit turc. Cependant, l'incitation à la prostitution constitue une infraction en vertu de l'art 227 al. 1 CPT. Toute personne qui incite un enfant à la prostitution, facilite la prostitution d'un enfant, procure le matériel nécessaire ou sert d'intermédiaire en vue de la prostitution d'un enfant encourt de 4 à 10 ans d'emprisonnement assortis de 5 000 jours-amende. La personne incitée à la prostitution considérée comme victime n'est ni poursuivie, ni punie.

vi. Votre droit pénal incrimine-t-il la pornographie d' « enfant virtuel»? La pornographie d'«enfant virtuel » n'utilise pas de vrais enfants ou d'images d'enfants réellement identifiables. Lorsque l'image n'est pas celle d'un enfant réel mais une combinaison de millions de pixels informatiques fabriqués par un artiste, le gouvernement peut-il interdire cette création dont votre pays est prétendument victime? Veuillez citer la loi applicable et / ou les décisions judiciaires.

Le code pénal turc, en mentionnant expressément, l'utilisation de mineurs, empêche la prise en compte des représentations virtuelles.

Selon l'art 226 al. 7, les dispositions de l'article 226 ne s'appliquent pas aux ouvrages scientifiques et aux œuvres ayant valeur artistique et littéraire à condition que les mineurs ne puissent y avoir accès et n'y figurent pas.

vii. Elément moral: Pour être responsable, la personne doit à la fois avoir l'intention d'entrer dans un site où la pornographie juvénile est disponible et savoir que ce genre d'images peut être trouvé ici. Les sanctions ne devraient pas être appliquées à des personnes qui entrent par inadvertance sur des sites proposant des images pédopornographiques. Est-ce le cas dans le droit pénal de votre pays?

L'infraction d'obscénité (art. 226 CPT) ne peut être commise que de manière intentionnelle.

b. Tout autre objet où la criminalisation dépend de l'utilisation des technologies de l'information et des communications (TIC)

Votre droit pénal incrimine-t-il les situations suivantes? Veuillez citer les lois pertinentes:

1. **la création et l'utilisation de l'envoi anonyme et/ou la réception des documents sur les TIC?**
2. **la cyber-intimidation?**
3. **le cyber-harcèlement?**
4. **le cyber-toilettage?**

Le cyber intimidation, le cyber harcèlement et le cyber toilettage ne constitue pas une infraction en soi en droit turc. Cependant, il est possible de poursuivre les auteurs desdits actes par les infractions du Code pénal qui correspondent à tels actes : harcèlement sexuel (art. 105 CPT), menace (art.106 CPT), chantage (art.107 CPT),violation du secret de la correspondance (art. 132 CPT), violation de la vie privée (art.134 CPT), enregistrement des données personnelles (art.135 CPT), acquisition illégale des données personnelles (art. 136 CPT).

2. Acte - création / adhésion / possession / transfert / distribution publique par les TIC (donner des exemples)

Citer des lois spécifiques qui criminalisent la création (même si elles ne sont jamais utilisées), l'adhésion, la

possession (même si elle est seulement privée), le transfert et la distribution publique par internet et par d'autres moyens électroniques de matériaux à côté de ceux déjà mentionnés ci-dessus et ce, en raison précisément d'internet / de l'utilisation de la technologie électronique.

L'art. 226 CPT, calqué sur l'infraction disposé dans le Code pénal allemand incrimine la possession de la pornographie enfantine (le contenu obscène en vertu du texte de la loi).

La possession personnelle ou le stockage des œuvres intellectuelles et artistiques protégées par la loi constitue une infarction en vertu de l'art. 71 de la lois sur la protection de la propriété intellectuelle.

La possession des données est punie indirectement dans les infractions d'acquisition illégale des données personnelles (art. 136 CPT) et le fait de ne pas détruire des données (art. 138 CPT).

(d) La violation des droits de propriété en matière de TIC, y compris la propriété intellectuelle.

Votre droit pénal incrimine-t-il spécifiquement les comportements suivants commis grâce à l'utilisation des TIC?

Veuillez citer les textes légaux de référence.

1. La fraude

L'art. 158 CPT incrimine l'acte d'escroquerie commise en utilisant les systèmes informatiques. Utiliser les systèmes informatiques constitue une circonstance aggravante.

2. La violation de droits de propriété intellectuelle

En outre l'art. 71 de la Loi sur les œuvres intellectuelles et artistiques incrimine l'acte de propager, de changer, de diffuser les œuvres sans la permission préalables de son auteur.

3. L'espionnage industriel

L'art. 239 CPT incrimine la divulgation des secrets commerciaux, bancaires et secrets des clients. L'acte incriminé est de donner aux personnes non-autorisées ou de divulguer les secrets. L'alinéa 2 de cet article prévoit que les informations relatives à l'industrie aussi sont incluses à la protection de cet article.

(e) La criminalisation des actes commis dans le monde virtuel

Votre droit pénal incrimine-t-il la perpétration de crimes commis dans le monde virtuel comme, par exemple, la pédopornographie virtuelle, la violence virtuelle, les graffitis virtuels, la cyber-diffamation, le harcèlement sexuel, le harcèlement au travail lorsqu'ils sont commis sans aucune implication de personnes réelles mais, seulement par des représentations virtuelles? Veuillez citer les textes légaux de référence et fournir des détails.

Le droit pénal turc n'incrimine pas ces types d'actes.

(f) La non-conformité aux infractions

Votre droit pénal incrimine-t-il le refus de coopérer avec les organismes d'application de la loi dans le domaine de la cybercriminalité? L'obligation de coopérer peut-elle avoir pour fonction de retenir et de stocker des informations, pour produire / fournir des informations telles que requis par une ordonnance de production, de donner accès au cyber-systèmes, d'installer des filtres ou des dispositifs etc. Est-ce que l'obligation de coopération peut également être forcée au moyen de sanctions administratives? Citer la législation pertinente et fournir plus de détails.

(D)Les informations complémentaires facultatives concernant le droit et la pratique (y compris les statistiques)

(1) Les cyber-crimes sont-ils inclus dans la collecte de données sur la criminalité dans votre pays?

À statistiques officielles de l'Institution de statistique turque, on ne peut pas rencontrer l'information sur les cyber-crimes.

(2) Y a-t-il dans votre pays un site Web qui fournit des données et des informations sur l'apparition, la gravité, le coût et plus généralement l'impact de cyber-crimes dans votre pays? Si oui, veuillez fournir l'adresse du site internet.

On peut donner comme exemple les sites d'internet de la police. Les departments sur les infractions informatiques de la police nous donne des informations importantes. (http://www.eskisehir.pol.tr/subeler/kacakcilik/bilisim.asp, http://www.gaziantep.pol.tr/birimdetayoku.aspx?Bid=176&masaadi=Asayis)

A part, on a le site d'internet de l'Association contre les crimes informatiques (www.bsm.org.tr).

Aussi il y a un autre site comme http://privacy.cyber-rights.org.tr.

(3) Les enquêtes sur les victimes dans votre pays comprennent-elles des questions sur les cyber-crimes?

On n'a pas d'information sur ce sujet.

(4) Quel type de criminalité informatique/fraude informatique est le plus souvent recensé dans votre pays?

Le fait d'entrer dans le système informatique est plus souvent recensé en Turquie.

(5) Les services d'application de la loi et des poursuites dans votre pays ont-t-ils une unité spécialisée dans les crimes informatiques? Si oui, combien d'agents et des procureurs compte-t-elle?

A part des départements établis au sein de la police sur les cyber-crimes, il y a des départements au sein du parquet.

(6) Est-ce que vous ou une autre faculté de droit dans le pays offre des cours sur la cyber-criminalité? S'il vous plaît, veuillez fournir une adresse de site Web.

Dans l'Université Bahçeşehir on a des cours intitulés «Internet Law». Dans l'Université Galatasaray et aussi Bahçeşehir, aux cours de droit pénal on traite «les crimes au domaine de l'informatique».

(7) L'étude de la cybercriminalité est-elle incluse dans la formation et/ou la formation continue des juges, des procureurs et la police?

Dans la formation et/ou la formation continue des juges, des procureurs et de la police inclut aussi l'étude de la cybercriminalité.

BÖLÜM 2: KAVRAM AÇIKLAMASI VE SORULAR

Prof. Dr. Emilio C. Viano

(A) Soruların Kapsamı (bkz. Giriş ve Ek)

Bu Bölümdeki sorular, genel olarak "siber suç" ile ilgilidir. Bu terim; bilgisayar sistemlerinin ve internetin düzgün işleyişi, bilgi ve iletişim teknolojilerine (BİT) veya bunlar aracılığıyla transfer edilen veya saklanan verilerin bütünlüğü ve gizliliği, ya da internet kullanıcılarının sanal kimlikleri gibi BİT kullanımıyla bağlantılı menfaatleri etkileyen suç oluşturan eylemleri kapsayacak şekilde kullanılmaktadır. Siber suçluluk alanına giren bütün suçların ve siber suç soruşturmalarının ortak paydası ve karakteristik özelliği; bunların, bir taraftan bilgisayar sistemleri, bilgisayar ağları ve bilgisayar verileri ile ve diğer taraftan siber sistemler, siber ağlar ve siber verilerle olan ilişkilerinde bulunabilir. Siber suç alanı, geleneksel bilgisayarların yanında çevrim içi bilgi dağıtımı ve siber veri tabanlarıyla ilgili suçları da içine alır.

Ulusal raportörler, daha fazla bilgi almak ya da soru sormak için genel raportör ile bağlantıya geçebilirler: Prof. Dr. Emilio C. Viano: emilio.viano@gmail.com

(B) Yasama Faaliyetleri ve Hukuki Kavramlar

(1) Siber suçlara ilişkin konular, ülkenizin ceza yasalarında nasıl düzenlenmiştir? Tek bir başlık veya yasa kapsamında mı yoksa çeşitli yasalarda ve başlıklarda mı düzenlenmiştir? (Lütfen, ilgili alıntıları belirtiniz).

(2) Yargı kararlarının, siber suçlara ilişkin ceza hukuku düzenlemelerine etkisi nedir?

(3) Değişen ihtiyaçlara ve koşullara yetişmek ve yeni hedeflere ulaşmak için bazı yasalarda sık sık değişiklik yapılmaktadır. Normalde, bu değişiklikler yeni yasa şeklini almaktadır. Bazı durumlarda bu yeni yasalar, değiştirilmesi gereken yasanın

sadece belli kısımlarını değiştirmek yerine; gerekli değişiklikleri, önceden yapılmış tüm değişikliklerle birlikte konsolide bir metin halinde göstermektedir. Bu yöntem, yeniden şekillendirme olarak adlandırılmaktadır. Sizin ülkenizde de siber suçlara ilişkin yasaların güncellenmesi ve değişen gerçeklere uyarlanması bu şekilde mi yapılmaktadır? Lütfen ilgili referanslar ve alıntıları belirtiniz.

(C) Özel Siber Suçlar

(1) Manevi unsura ilişkin olarak, bilişim suçlarının kasten mi işlenmiş olması gerekmektedir? Bu suçların gerçekleşmesinde özel kast gerekli midir?

(2) Bu alanda, taksirli suçlar da söz konusu olabilir mi?

(3) Eğer öyleyse, lütfen, bu suçları listeleyiniz.

(a) Bilişim Sisteminin Bütünlüğü ve İşlevselliği

1. Yasadışı Giriş ve İletimin Engellenmesi

a. Konu – sistem ya da veriler

Ceza hukukunuz, bilgiyi veya veriyi; giriş yapmak, iletmek, silmek, bozmak, değiştirmek ya da bir bilgisayar sistemi, yazılım veya programdan kaldırmak veya onlara zarar vermek suretiyle; bilgisayarın ve/veya elektronik sistemin işleyişinin ciddi şekilde, haklı bir sebep olmaksızın, engellenmesini suç olarak kabul etmekte midir?

b. Güvenlik Önlemlerinin İhlali Gereği

Hacker'ın haksız bir şekilde bilişim sistemine girme hareketini (hack), güvenlik önlemlerini aşmak ve giriş düzeyinde ya da yüksek düzeyde erişim elde etmek için gerekli olan bir ya da birden fazla yazılım aracılığıyla gerçekleştirmesi, ceza hukukunuzda aranan bir şart mıdır?

2. Verilere ve Sisteme Müdahale

a. Konu – sistemin/yazılımın/verilerin korunması

Ceza hukukunuz "bilgisayar verilerini ve/veya elektronik verileri" tanımlamakta mıdır? Bu tanım, programları veya yazılımları veya benzer programlamaları da içermekte midir? Eğer bir tanım söz konusuysa, lütfen tanımı ve bununla ilgili yasanızdaki paragraf ve maddelerin atıflarını belirtiniz.

b. Eylem – yok etme/değiştirme/erişilmez kılma

i. Ceza hukukunuz, bilgisayar, elektronik sistem veya program bilgi veya verilerini izinsiz silme, değiştirme, erişilmez kılma, elde etme veya bunlara diğer benzer şekillerde müdahalede bulunmayı cezalandırmakta mıdır?

ii. Ceza hukukunuz, bilgisayar veri ve/veya bilgisinin veya elektronik veri ve/veya bilginin herhangi bir biçimde veya araçla gönderilmesine izinsiz müdahaleyi cezalandırmakta mıdır?

3. Veri sahteciliği

a. Konu – gerçeklik

Ceza hukukunuz, hukuki amaçlarla kullanılan veya işlenen verilerin gerçekliğini korumak için, sahte verilerin yaratılmasına yol açacak şekilde, bilgisayar verilerine ve elektronik verilere izinsiz erişimi, bunların değiştirilmesi, silinmesi ve ortadan kaldırılması eylemlerini suç olarak tanımlamakta mıdır? Eğer, bir tanım söz konusu ise, lütfen tanımı ve bununla ilgili ceza yasanızdaki ve/veya özel yasalardaki paragraf ve maddeleri belirtiniz.

b. Eylem – değiştirme/silme

Ceza hukukunuz, hukuki sebeplerle gerçek kabul edilmesi veya işlenmesi amacıyla, sahte verilerin/bilgilerin yaratılmasına yol açacak şekilde, bilgisayar verileri/bilgilerine veya elektronik verilere/bilgilere izinsiz erişimi, bunların değiştirilmesi, silinmesi ve ortadan kaldırılması eylemlerini cezalandırmakta mıdır? Öyleyse, lütfen yasanızdaki uygulanabilir paragraf ve maddeleri belirtiniz.

4. Cihazların Kötüye Kullanılması

a. Konu – cihazın türü

Ceza hukukunuz, bilgisayar veya elektronik sistem ya da yayınlara izinsiz erişim amacıyla hacker'ların "araç kitleri" veya bunların herhangi bir bölümünün (örneğin, parola çalıcı ve klavye kaydedici (keylogger), blueboxing programları, bilgisayar modemine başarılı bir şekilde bağlanan kullanıcıların numaralarını tespit eden programlar (wardialer programları), şifreleme yazılımları, program şifre kırıcıları, güvenlik açığı tarayıcıları, veri paketlerinin izlenmesi (packetsniffers) ve benzeri programlar) geliştirilmesini cezalandırmakta mıdır?

b. Eylem – kamuya dağıtılması/üçüncü bir kişiye aktarımı

i. Ceza hukukunuz, a'da sayılan araçlardan herhangi birinin izinsiz kullanımını cezalandırmakta mıdır?

ii. Ceza hukukunuz, hack'lenmiş elektronik bilgilerin kamuya dağıtılmasını ve/veya üçüncü kişilere aktarımını cezalandırmakta mıdır?

c. Bulundurma

Ceza hukukunuz, bilgisayar veya elektronik sistem ya da yayınlara izinsiz erişim amacıyla hacker'ların "araç kitleri" veya bunların herhangi bir bölümünün (örneğin, parola çalıcı ve klavye kaydedici (keylogger), blueboxing programları, bilgisayar modemine başarılı bir şekilde bağlanan kullanıcıların numaralarını tespit eden programlar (wardialer programları), şifreleme yazılımları, program şifre kırıcıları, güvenlik açığı tarayıcıları, veri paketlerinin izlenmesi (packetsniffers) ve benzeri programlar) bulundurulmasını cezalandırmakta mıdır?

(b) Özel Hayatın Gizliliği

1. Özel Verilerin Güvenliğinin İhlali

a. Konu – özel veri türü

(Not: özel veri, kişilerin özel hayatlarına ilişkin verilerdir; fakat kişileri tanımlayan veya tanımlamayı sağlayacak verilerden, örneğin

medeni halleri, cinsel yönelimleri, sağlık durumları, satın alma alışkanlıkları ve tercihleri vb. değildir)

i. Ülkenizin yasaları, veri toplayıcılarının, tüketicilerden özel verileri toplamadan önce, örneğin, hangi bilginin kullanıldığı, nasıl ve hangi amaçla elde edildiği, başkalarıyla paylaşıp paylaşılmadığı ve tüketicilerin özel bilgilerin paylaşılmasında herhangi bir kontrolleri olup olmadığı gibi bilgiye ilişkin faaliyetlerini bildirmelerini zorunlu kılmakta mıdır?

ii. Ülkenizin yasaları, internet üzerinden iş yapan şirket ve tüzel kişilerin, tüketicilere; verileri toplayanların kimliği, istenen veriye ilişkin düzenlemenin ihtiyari mi yoksa zorunlu mu olduğu, verinin gizliliği, bütünlüğü ve veri kalitesinin sağlanması için atılması gereken adımlar konularında bilgilendirme yapmasını gerektirmekte midir?

iii. Ülkenizin yasaları, internet sitelerini; gizlilik politikalarını göstermeye ve tüketiciler, satın alma işlemine daha başlamadan ya da hassas bilgilerini açıklamalarını gerektirecek diğer tüm işlemleri gerçekleştirmeden önce, kişisel bilgilerinin nasıl kullanılacağını bildirmeye zorunlu kılmakta mıdır?

iv. Ülkenizin ceza hukuku, önceki maddelerde bahsedilen açıklığın sağlanmamasını cezalandırmakta mıdır?

b. Eylem – izinsiz kullanım ve aktarım/dağıtım

i. Ülkenizin ceza hukuku, özel verinin izinsiz aktarımını ve dağıtılmasını tanımlamakta mıdır?

ii. Ülkenizin ceza hukuku, özel verinin izinsiz kullanımı, aktarımı ve/veya dağıtılmasını cezalandırmakta mıdır?

c. Hukuka uygunluk nedenleri

i. Ülkenizin yasaları hangi koşullar altında, özel verilerin hukuka uygun bir şekilde toplanması, kullanımı, aktarımı ve dağıtımına izin vermektedir?

ii. Hukuka uygun bir şekilde toplama ve/veya dağıtma için ne gibi gereklilikler (zorlayıcı, önemli, mantıklı, uygun) aranmaktadır?

2. Mesleki gizliliğin İhlali

a. Konu – özel verinin türü

i. Ülkenizin yasaları, uzmanların;

- Hasta ve müşterilere ait kişisel bilgileri toplamadan önce, bilgi toplama ve yönetim faaliyetlerini;
- İfşa yöntemlerini;
- Mesleki etik yükümlüklerini;
- Hastaların veya müşterilerin verilerin açıklanması üzerinde herhangi bir denetim imkanının olup olmadığını

konularını açıklamalarını zorunlu kılmakta mıdır?

ii. Eğer varsa, hangi veriler özellikle korunmaktadır?

iii. Ülkenizin ceza hukuku, gizlilik ilkelerinin; hekimler, avukatlar, din adamları ve benzeri meslek gruplarında çalışan kişiler tarafından, hukukça belirlenmiş bazı durumlarda veya kimi sebeplerle ihlal edilmesine izin vermekte veya hatta bu ihlali zorunlu kılmakta mıdır? Bu hangi şartlar altında yapılabilmektedir? (Örneğin ortada bir çocuğa, kadına veya yaşlıya karşı kötü muamele olduğuna dair makul bir gerekçe varsa)

b. Özne– faillerin türü

Ülkenizin ceza hukuku, özel gizlilik kurallarıyla bağlı mesleki gruplar belirlemekte midir?

c. Eylem – yasa dışı kullanım ve aktarım/dağıtım

Hangi eylemler (örneğin yasa dışı toplama, kullanım, aktarım ve dağıtım), ülkenizin ceza hukuku tarafından özellikle cezalandırılmaktadır?

3. Kişisel ve özel verilerin yasa dışı şekilde işlenmesi

a. Konu

Ceza hukukunuz kişisel ve özel verilerine izinsiz ve yasa dışı bir şekilde yapılan; edinim, işleme, saklama, analiz, manipülasyon, kullanım, satış, aktarım vb. hareketleri cezalandırmakta mıdır?

b. Özne

Ceza hukukunuz cezai yasak ve yatırımlara tabi olan gerçek ve tüzel kişilerin kategorilerini özel olarak belirtmekte midir?

c. Eylem

i. Ceza hukukunuz, kişisel ve özel verilerin yasa dışı yollardan işlenmesinin bir kısmını ya da tamamını oluşturan belirli eylemleri cezalandırmakta mıdır? Aşağıda listelenen her kategori için, eğer mümkünse, ilgili yasa ve düzenlemeleri belirtiniz.

1. Yasa dışı toplama
2. Yasa dışı kullanım
3. Yasa dışı saklama
4. Yasa dışı aktarım

ii. Kişisel ve özel verilerin polis veya yasa uygulayıcı mercilerin amaçları doğrultusunda kullanılması, aktarılması vb. bir değişiklik yaratmakta mıdır?

d. Hukuka uygunluk nedenleri

i. Hangi şartlar altında ülkenizin yasaları, kişisel ve özel verilerin hukuka uygun bir şekilde toplanması, işlenmesi, aktarılması ve dağıtılmasına izin vermektedir?

ii. Kişisel ve özel verilerin hukuka uygun bir şekilde toplanması ve/veya dağıtımı için ne gibi gereklilikler (zorlayıcı, önemli, mantıklı, uygun) aranmaktadır?

4. Kimlik hırsızlığı

(Not: kimlik hırsızlığı, kişinin bir başkasının kişisel bilgilerini onun bilgisi dışında hırsızlık ve dolandırıcılık eylemlerini işlemek maksadıyla kullanmasıdır. Kimlik hırsızlığı, dolandırıcılık suçlarını işlemede kullanılan bir araçtır. Genellikle, mağdura e-posta yoluyla fatura veya üyelik bilgilerini güncellemesi talebinde bulunularak, ya da internet üzerinden hileli bir iş veya kira ilanına başvuru yaptırılarak, hassas kişisel bilgilerini yasal bir işletme ya da tüzel kişiye verdiği düşündürülür.)

a. Konu

i. Ceza hukukunuz kimlik hırsızlığını cezalandırmakta mıdır? Lütfen, ilgili yasayı belirtiniz.

ii. Ceza hukukunuz kimlik hırsızlığının "yemleme" (phishing) gibi özel şekillerini yasaklamakta mıdır? Yemleme, tüketicileri sahte e-postalar aracılığıyla hileli sitelere çekerek kredi kartı numarası, kullanıcı adları ve şifreleri, sosyal güvenlik numaraları gibi finansal verileri tüketicileri tuzağa düşürerek vermelerini sağlayan çevrimiçi kimlik hırsızlığı olarak tanımlanmaktadır.

b. Özne

Ceza hukukunuz kişinin dijital kişiliğine, Avatar'ına (sanal karakter), ya da internet temelli simülasyon oyunlarındaki (Cityville, Farmville gibi) dijital rolüne bağlı cezai sorumluluk içermekte midir? Lütfen ilgili yasayı belirtiniz.

(c) Yasadışı içeriğe karşı koruma: BİT'e ilişkin

1. Konu

a. Çocuk pornografisi - gerçek ya da sanal çocuk görüntüleri

i. Ceza hukukunuz internetin çocuk pornografisine erişim, onu depolama ve dağıtma amacıyla kullanılmasını cezalandırmakta mıdır? Öyleyse, ilgili yasayı belirtiniz.

ii. Özellikle, ceza hukukunuz:

- İnterneti çocukları cinsel amaçlarla kandırıp onlardan faydalanmak için kullanan suçluları hedef alan yeni bir suç tanımı yaratmakta mıdır? Çocuk pornografisini,

  1. internet üzerinden yaymak,
  2. erişilebilir hale getirmek,
  3. dışarıya aktarmak
  4. ve çocuk pornografisine kasıtlı olarak internet üzerinden ulaşmak

  eylemlerini suç haline getirmekte midir?

- Yargıçların çocuk pornografisinin ülkenizde yayınlandığı bilgisayar sistemlerinden silinmesi kararını vermesine imkân vermekte midir?
- Bir yargıcın çocuk pornografisi suçunun işlenmesinde kullanılan her türlü donanım ve materyale el konulması kararını vermesine imkân vermekte midir?

1. İnternet üzerinden çocuk pornografisine bilinçli ulaşımı,
2. İnternet üzerinden çocuk pornografisinin iletimini,
3. İnternet üzerinden çocuk pornografisini dışarıya aktarmayı,
4. İnternette iletmek, dışarıya aktarmak amacıyla çocuk pornografisi bulundurmayı,

suç haline getirmekte midir?

iii. Ceza hukukunuz sosyal paylaşım siteleri ve sohbet odaları aracılığıyla çocukların çevrimiçi ortamda kandırılmalarını cezalandırmakta mıdır?

iv. Ceza hukukunuzdaki çocuk pornografisi tanımı uluslararası belgelerdekilere yakınlık göstermekte midir? (Örneğin AB yönergeleri)

v. Ceza hukukunuzda çocuk pornografisi mağdurlarına karşı ikincil mağdurlaştırmadan kaçınılmakta mıdır? Para karşılığı cinsel ilişki veya pornografide gözükmenin ulusal ceza hukukuna göre cezalandırıldığı devletlerde, ilgili çocuk, ona yapılan cinsel istismarın veya çocuk pornografisine katılmaya zorlanmasının sonucunda o eylemleri işlemişse, bu hukuk sistemlerine göre kovuşturma yapılmaması veya ceza verilmemesi söz konusu olabilmektedir. Sizin ceza hukukunuzun kanaati de bu yönde midir?

vi. Ceza hukukunuz "sanal çocuk pornografisini" cezalandırmakta mıdır? "Sanal çocuk pornografisi" gerçek çocukları veya kimliği belirlenebilecek çocuk görüntülerini kullanmamaktadır. Görüntü gerçek bir çocuğa ait değil de, bir sanatçı tarafından milyonlarca bilgisayar pikselinin bir araya getirilmesiyle oluşturulan bir kombinasyonla ortaya çıkıyorsa, ülkenizdeki hükümet bu gibi sözde mağdursuz yaratımları yasaklayabilmekte midir? Lütfen uygun yasaları ve/veya mahkeme kararlarını belirtiniz.

vii. Manevi unsur: Sorumlu olmak için, kişi çocuk pornografisi içeren bir siteye girmeye yönelik kastı olmalı ve bu tip görüntülerin orada bulunduğunu bilmelidir. Kast olmadan çocuk pornografisi içeren sitelere giren kişilere ceza verilmemelidir. Sizin ceza hukukunuzdaki koşullar da bu şekilde midir?

b. Suç niteliği taşımanın, Bilgi ve İletişim Teknolojilerinin (BİT) kullanımına bağlı olduğu başka durumlar var mıdır?

Ceza hukukunuz aşağıdaki eylemleri cezalandırmakta mıdır? Lütfen ilgili yasayı belirtiniz.

1. Bilgi ve iletişim teknolojileri üzerinden materyal gönderme veya almada "gerçek anonimliğin" yaratılması ve kullanılması

2. Siber zorbalık

3. Siber takipçilik

4. Siber istismar

2. Eylem – BİT aracılığıyla yaratım/erişim/bulundurma/aktarma/halka dağıtma (örnekler veriniz)

Yukarıda sayılanlar dışında internet ve elektronik materyaller aracılığıyla, özellikle internet ve teknoloji kullanımı nedeniyle yaratımını (hiç kullanılmasa dahi), erişimini, bulundurmayı,(sadece özel hayatta olsa dahi), aktarmayı ve halka dağıtmayı suç haline getiren yasaları belirtiniz.

(d) BİT ile İlişkili – Fikri Mülkiyet de Dahil Olmak Üzere –Mülkiyet Hakkının İhlali

Ceza hukukunuz özel olarak BİT aracılığıyla işlenen aşağıdaki eylemleri yasaklamakta ve cezalandırmakta mıdır? Lütfen ilgili yasayı belirtiniz.

1. Dolandırıcılık

2. Fikri mülkiyet haklarının ihlali

3. Endüstriyel casusluk

(e) Sanal Dünyada Gerçekleştirilen Eylemlerin Suç Haline Getirilmesi

Ceza hukukunuz gerçek insanların katılmadığı, sadece sanal temsilin olduğu durumda; sanal çocuk pornografisi, sanal şiddet, sanal grafiti, siber itibarsızlaştırma, cinsel taciz, iş yerinde taciz gibi sanal dünyada gerçekleştirilen suçları cezalandırmakta mıdır? Lütfen ilgili yasayı belirtip detay veriniz.

(f) İtaatsizlik Suçları

Ceza hukukunuz siber suçlar alanında resmi makamlarla işbirliği yapmamayı cezalandırmakta mıdır? İşbirliği görevleri; bilgi edinme ve depolama, üretim emrinin gereklerine göre bilgi üretme/teslim etme, filtre ve aygıtlar yüklenmesi için siber sistemlere giriş izni verilmesi gibi görevler olabilir. İşbirliği yapma yükümlülüğünün ihlali, idari yaptırımlar aracılığıyla da cezalandırılmakta mıdır? İlgili yasayı belirtip detay veriniz.

(D) Hukuk ve uygulamaya ilişkin tamamlayıcı seçimlik bilgiler (istatistikler de dahil)

(1) Ülkenizde siber suçlar, suça ilişkin verilerde yer almakta mıdır?

(2) Ülkenizde, siber suçların meydana gelmesi, ağırlığı, maliyeti, etkileri vb. konularında veri ve bilgi sağlayan bir internet sitesi var mıdır? Eğer varsa, sitelerin elektronik adreslerini temin ediniz.

(3) Ülkenizdeki viktimizasyon araştırmalarında, siber suçlara ilişkin sorular var mıdır?

(4) Ülkenizde hangi tipte bilgisayar suçu/bilgisayar dolandırıcılığı daha sık bildirilmektedir?

(5) Ülkenizde kolluk ve savcılık makamlarının bilgisayar suçları birimi bulunmakta mıdır? Öyleyse, kaç memur/savcı, bu birimde çalışmaktadır?

(6) Üniversitenizde veya ülkenizdeki herhangi bir hukuk fakültesinde, siber suçlarla ilgili ders verilmekte midir? Lütfen bir internet sitesi veriniz.

(7) Yargıçlar, savcılar ve polislerin; aldıkları ve/veya devam etmekte oldukları eğitimler, siber suçlara ilişkin konuları da kapsamakta mıdır?

(8) Ülkenizde siber suçların aşağıdaki şekil ve yöntemlerinin hangi sıklıkla (sıklıkla meydana gelmektedir, nadiren meydana gelmektedir, meydana gelmemiştir) meydana geldiğini tablodaki uygun boşluklara "X" koyarak gösteriniz.

Siber Suçun Şekil ve Yöntemleri	Sıklıkla Meydana Gelmektedir	Nadiren Meydana Gelmektedir	Meydana Gelmemiştir
Çevrimiçi (online) kimlik hırsızlığı (yemleme ve sahte kimlik bilgilerinin çevrimiçi ticareti de dahil olmak üzere)			
Hack'leme (bilgisayar sistemlerine izinsiz giriş; bilgisayar sitemlerinden bilginin çalınması)			
Kötücül kodlar (solucanlar – worms-, virüsler, kötücül ve casus yazılımlar)			
Bilgisayar verisine yapılan yasa dışı müdahale			
Fikri mülkiyet haklarının ihlaline ilişkin suçların çevrimiçi olarak işlenmesi			
Çevrimiçi çocuk pornografisi ticareti			
Bilgisayar sistemlerine ve verilerine kasten zarar verme			
Diğerleri			

(9) Yukarıdakine ek olarak, ülkenizde (sıklıkla veya nadiren) meydana gelmiş farklı siber suç şekil ve yöntemleri var ise, lütfen bunları sıklıklarıyla birlikte aşağıdaki tabloda belirtiniz.

Suç Eylemlerinin Şekil ve Yöntemleri	Sıklıkla Meydana Gelmektedir	Nadiren Meydana Gelmektedir

Değerli katkınız için teşekkürler!

Ek

BİLGİ TOPLUMU VE İLGİLİ SUÇLAR

Prof. Dr. Emilio C. Viano

Modern ağ toplumu, bilgi çağına ilişkin sapkınlık ve suçlu davranışlara karşı son derece savunmasızdır. Küresel olarak, son birkaç yıl içinde, siber suç ya da yüksek teknoloji suçları, "siber savaş", "siber savunma", "siber terörizm", kritik altyapının korunması ve bilgi güvenliğini de kapsayacak şekilde siber güvenlik üzerine endişeler oldukça artmıştır. Aynı zamanda, siber güvenliğe karşı verilen tepkilerin insan hakları değerlerini nasıl etkileyeceğine ve bunlarla aralarında nasıl bir denge sağlanması gerektiğine gittikçe daha çok dikkat gösterilmektedir. Bu değerler, bireysel özerklik, özel hayatın gizliliği, isimsiz siyasi söylem, ifade özgürlüğü ve örgütlenme özgürlüğü, insani gelişme hedefleridir. Bu hedefler arasında da bilgiye ulaşma ve inovasyon, rekabet ve ticari sırların ve mal sahibine ait diğer bilgilerin korunması gibi ekonomik menfaatler yer alır. Bu ilke ve değer meseleleri ayrıca "isnat" sorunu gibi, yani herhangi bir mesaj veya bilgi isteminin gerçek göndericilerini belirleyebilme kapsamında, teknik sorunlar da yaratmaktadır.

Şüphesiz ki bilgi toplumunu mümkün ve işler hale getiren teknolojiler, kişisel ve toplumsal yaşantıların, eğitim ve iş alanından kültürel ve gündelik faaliyetlere, birçok farklı yönünü ciddi şekilde etkileyen önemli araçlar haline gelmiştir. Kişisel bilgisayarların ve diğer elektronik cihazların (iPhone, iPad, iPod, iTunes vs.) geniş kullanımı ve yüksek hızlı internet ile, birçok çeşitli sapkın davranışlar ve suç hareketleri ciddi ölçüde artış göstermiştir. Bunlara örnek olarak bilgisayar korsanlığı (hacking), yasa dışı müzik ve yazılım programları indirme ve başkalarının şifre veya kimliklerini çalma gösterilebilir.

Siber sapkınlığın tam kapsamı ve toplam maliyeti bilinmiyor ve tahmini maliyeti aslında değişkenlik gösteriyor ise de, bunun küresel ve büyüyen bir fenomen olduğu tartışılmaz bir gerçektir.

Bu nedenle, siber güvenlik tüm dünyada, hükümetler ve özel sektör açısından önemli bir sorun haline gelmiştir. Zihinlerde, birçok değişik kaynaktan ileri gelen, ciddi bir değişim olduğu görülmektedir. Şöyle ki:

- İnternet ve kaynaklarının, insan gayretinin çeşitli alanlarında ne kadar kritik bir konuma sahip olduğu ve ne kadar altyapı ve sistemlerin internet bağlantısı ve kapasitesine daha da bağımlı hale geldiği algısının gelişmesi
- Küresel anlamda; finansal kuruluşlar, diğer işletmeler, kamu kuruluşları ve akademik kurumlarda gerçekleşen büyük veri ihlallerinin açığa çıkmaya devam etmesi
- Kötücül yazılımların (malware) yayımına devam edilmesi ve bu yayılan yazılımların kapsamının genişlemesi
- Hükümetin çeşitli düzeylerde internet kullanımı ve içeriğine erişimi, gözetimi ve filtrelemesi veya sansürlemesi üzerine devam eden raporlar
- Kilit öneme sahip altyapılara karşı isnat edilemeyen siber saldırılar, örneğin Litvanya, Estonya, Gürcistan ve diğer ülkelerde ve en son İran'da bir nükleer santrale ve bir cephanelik üssüne yapılan saldırılar. İran aleyhine kullanılan Stuxnet ve Duqu, dünyanın siber savaşta ilk 'süper silahları' olarak nitelendirilmektedir.
- Hükümetin casusluk faaliyetlerine ve kurumsal casusluğa ilişkin endişeler
- Siber suç – internet üzerinden dolandırıcılık, kimlik hırsızlığı, çocuk pornografisi, fikri mülkiyet hırsızlığı ve internet üzerinden suç oluşturan para hareketleri ve kara para aklamayı da içerecek şekilde – üzerine artan endişe
- Kurumsal ve hükümetin veri erişimi hakkında gizlilik endişeleri ve neredeyse dünya üzerindeki her bireye ilişkin yaygın bir şekilde gerçekleştirilen özel bilgileri toplama, kaydetme ve yayma faaliyetleri

Bilgi teknolojisi ve yazılımlarına erişim dünya nüfusu arasında katlanarak çoğalmaya devam ettikçe ve güvenlik protokollerinin uygulanması konusunda yeterli kullanıcı bilinçliliği eksikliği de göz önüne alındığında, internet üzerinden çalışan sistemler, çeşitli kuruluşlar gözünde sıklıkla kolay hedef olarak algılanmaktadır. Bu kuruluşlar arasında suç örgütleri, hacker'lar (ekonomik kazanç veya başarıp başaramayacaklarını görmek amacıyla), ideolojik gruplar, başka işletmeler üzerine casusluk yapan işletmeler, hükümet temsilcileri ve hükümetler – orduları ve istihbarat teşkilatlarını da içerecek şekilde – bulunmaktadır. Saldırı amaçları, maddi kazançtan, eşit olarak tanınma isteğinin tatminine yönelik milli güvenlik çıkarlarını geliştirmeye kadar uzanmaktadır.

Siber güvenlik konusunda uluslararası konsensüse ulaşma yolunda gösterilen her çaba; ulusal güvenliğe ilişkin çeşitli görüşlerden, internetin rolü ve değerinden, insan haklarından ve ekonomi politikalarından kısmen kaynaklanan çeşitli endişeler açığa çıkarabilir. Bazıları siber güvenliği, devlet güvenliğinin özü olarak görmektedir. Bu durum da iletileri görüntüleme ve kaynağına dayandırma ve istenmeyen herhangi bir içeriği engelleme imkanını vurgulamaktadır. Diğerleri ise internet yönetişiminin (internet güvenliği de dahil olmak üzere) menfaatlerin birleştirilmesi ve dengelenmesi konularını içerdiğine inanmaktadır. Bu da sadece ulusal güvenliği değil; bunun yanı sıra insan hakları ve canlı, yenilikçi ve rekabetçi bir bilişim toplumu ile ilgili ekonomik ve gelişimsel çıkarları da içine almaktadır. Bu farklı bakış açıları kendilerini birçok farklı alanda göstermektedirler. Bilgisayar suçları terimi dahi tartışma ve itiraz konusu olmaktadır.

(A) Siber suç: Terminoloji ve Tanım

Siber suç, bilgi teknolojisinin kötüye kullanılmasını içeren bir suç tipidir. Siber suç terimi, siber terörizmden sanayi casusluğuna kadar bir dizi suç hareketini kapsamaktadır. Bazı siber suçlar bilgisayarların ve bilişim ağlarının sınırlı bir etkisini içerirken, diğerleri neredeyse tamamen bilgisayar veya başka bir elektronik cihaz ve ağın kullanımına bağlıdır. Öncelikle, birey suç faaliyetinde bulunmak

için bilgisayar veya başka bir elektronik cihaz kullanmalıdır. İkinci olarak, bir ceza davasında ispatı gereken deliller, bilgisayarlı veya elektronik ortamda depolanmış olmalıdır. Bir suçun işlenmesinde bilgisayar veya elektronik bir cihaz kullanımını düzenleyen hukuk alanı, maddi elektronik ceza hukuku olarak adlandırılır; çünkü bu alan cezalandırılan maddi eylemin kapsamına ilişkindir. Bilgisayarlı delil toplamayı düzenleyen hukuk alanı ise usulî elektronik ceza hukukudur.

Siber suç, karmaşık bir operatörler, mağdurlar ve cihazlar ekosistemi aracılığıyla ifade edilen kapsamlı bir olgudur. Yıllar içinde, aslında, siber suç; veriler, araçlar ve beceriler ticareti için gerçek bir «karaborsa» ile, hiyerarşik ve uluslararası bir organizasyon edindi. Cihazların daha da gelişmiş hale gelmesiyle, siber suç dünyasına erişim için gereken uzmanlık seviyesi düşürülmüştür. Bir zamanlar siber suçlar yalnızca "siyah şapkalı" gruplar tarafından işlenebiliyorken, bugün biraz teknik becerisi olan hemen herkes, dünyanın her yerinden, bazı saldırıları gerçekleştirmek amacıyla araçlar yükleyip kullanabilmektedir.

Günümüz siber suçları iki açıdan nitelendirilmektedir: bir yandan, suçlar uzmanlık ve saldırılar anlamında birçok farklı şekil alabilmektedir; diğer yandan ise, genellikle kâr odaklı kuruluşları ve pazarları niteleyen, iyi yapılandırılmış birçok proje ve mekanizma vardır. Siber suç bir bilgisayar veya elektronik cihaz (iPhone, iPad, tablet, Blackberry, vs.) ve bir bilgisayar veya elektronik cihazın suçun işlenmesinde araçsal bir rol oynadığı veya oynamadığı bir bilişim ağını içeren her türlü suçu ifade etmektedir. Tekniklerin birçoğu bilgisayar/elektronik cihaz ve bilişim ağı kullanımını içermektedir. Ancak, başka birçok tekniğin, bilgisayarın sabit disk sürücüsünde metin dosyası olarak kayıtlı bilgi dışında bilgisayarlarla hiçbir ilişkisi bulunmamaktadır. Bilgisayar/elektronik ile ilgili suçların çeşitliliğinden ötürü, daha dar bir tanım elverişsiz olacaktır. Elektronik teknolojilerin ve yazılımların hızla ortaya çıkışı ve internetin hızla yayılması; çeşitli yeni, teknolojiye özgü suç teşkil eden davranışlar ortaya çıkarmış, bu durum da "bilgisayar suçları" kategorisinin ötesine geçmiştir. "Siber suç", yüksek teknoloji suçu veya iletişim teknolojisi suçu terimleri, belli elektronik cihazlar ve bir bilgi ve iletişim

ağına – bugün çoğunlukla bilinen şekliyle "internet" – ilişkin bütün suçlar için kapsayıcı terimlerdir. Bir hareketin bilgisayar suçu mu, siber suç mu, yüksek teknoloji suçu mu yoksa bilgi ve iletişim teknolojisi suçu mu teşkil ettiğini anlamsal olarak tartışmak çok önemli değildir. Sorunu ve onun ceza hukukundaki etkilerini ve yansımasını tam anlamıyla kavramak daha önemlidir. Bu yeni suç teşkil eden davranışlarla mücadele etmek için birçok ülkede özel yasal düzenlemeler getirilmiştir.

Uzmanlar, bilgisayar suçları ve elektronik suçlardan kaynaklanan zararın hesaplanmasında güçlük çekmişlerdir. Bunun sebebi, bu kavramların uygun şekilde tanımlanmasının zor olması; mağdurların utanç, müşteri güveni kaybı ve rekabetin azalması korkusundan, olayları bildirmek konusunda isteksiz olmaları; ve suçları ortaya çıkarmadaki yetersizliktir.

(B) Ceza Hukuku Korumasını Hak Eden Hukuki Menfaatler

Bölüm II'de ceza hukuku korumasını hak ettiği saptanan esas menfaatler:

(1) Siber Bilgi ve İletişim Teknolojileri (BİT) sisteminin bütünlüğü ve işlevselliği (CIA suçları)

Bilgisayar sistemlerinin gizliliği, bütünlüğü ve erişilebilirliğine karşı işlenen suçlar (bunlara "CIA" suçları da denir), BİT sisteminin bu öncelikli menfaatine karşı büyük bir tehdit oluşturmaktadır.

(2) Özel hayatın gizliliğinin korunması

"Özel hayatın gizliliği" terimi, gündelik dilin yanı sıra, felsefi, siyasi ve hukuki tartışmalarda sıkça kullanmaktadır; buna karşın terimin tek bir tanımı veya analizi ya da anlamı dahi yoktur. Tanımlar ile ilgili felsefi tartışmalar yirminci yüzyılın ikinci yarısında öne çıkmış ve büyük ölçüde hukuktaki gizlilik korumasının gelişmesinden etkilenmiştir. Bazıları özel hayatın gizliliğini kişinin kendisi hakkındaki bilgiler üzerinde hakimiyet kurması olarak savunmaktadır; diğerleri bunu insan onuru için gerekli veya mahremiyet için asli öneme sahip, daha geniş bir kavram olarak görmektedir; başkaları ise üçüncü kişilerin bize olan erişimlerini kontrol edebilme yeteneği veren bir

değer olarak görmektedir. Hukukta özel hayatın gizliliğinin korumasının açıkça tanınmaya başlaması için yapılan ilk çağrılar, geniş ölçüde, gelişen iletişim teknolojileri tarafından harekete geçirilmiştir. Birçok insan hala özel hayatın gizliliğini değerli bir menfaat olarak görmekte ve teknolojik gelişmeler göz önüne alındığında, şimdi hiç olmadığı kadar tehdit altında olduğunu söylemektedir. Aramızdan herhangi biri hakkında, bireysel finansal ve kredi geçmişinden tıbbi kayıtlara, alımlar ve internet araştırmaları ve iletişimlerine kadar her türlü bilgiye ilişkin internet kayıtları ve muazzam veri tabanları mevcuttur. Çoğu kişi kendileri hakkında hangi bilgilerin saklandığını veya onlara kimlerin erişimi olduğunu bilmemektedir.

Başkalarının veri tabanlarına erişme ve onları birleştirme yeteneği, onların bilgiyi nasıl kullandıkları, paylaştıkları veya bilgiden nasıl yararlandıkları üzerine yapılan bazı kontroller ile, kişinin kendisi hakkındaki bilgiler üzerinde bireysel denetimi çok zor hale getirmektedir. 2. Bölüm'deki soruların büyük bir kısmında özel hayatın gizliliğine karşı önemli suç tipleri incelenmektedir.

(3) Dijital kişiliğin korunması

Dijital Kişiliğimiz, her birimiz hakkında, hukuka uygun erişimi, araçları ve bulmak için motivasyonu olan herkesin erişebileceği dijital bilgi havuzudur. Dijitalleşmiş dünyada, bu kişilikler bizleri temsil eder. Gittikçe ilk izlenimler üzerinden başkaları hakkında fikir oluşturmak yaygınlaşmakta ve ilk izlenimler önemli hale gelmektedir. Bu olgu neredeyse kazayla gelişmiştir. Şimdi, işletmeler ve sıradan insanların gittikçe artan miktarda kişisel bilgi yaratması, kullanması, paylaşması ve saklaması aracılığıyla birçok yolu vardır.

İş araçları, her birimiz hakkında kapsamlı görünümler oluşturmak amacıyla, Dijital Kişiliğimizin çeşitli bölümlerini birbirine bağlamak üzere ortaya çıkmaktadır. Kişisel alanımıza yapılan bu saldırıda, ihlal devam etmektedir. Ancak biz yine de yeni dijital teknolojileri kullanmakta ısrar etmekte ve kasten kendi hakkımızdaki malzemeyi paylaşmaktayız. Bu da başkalarının hakkımızda ulaşabileceği daha fazla bilginin var olmasına yol açmaktadır.

İnternet ve sosyal medya üzerindeki kişisel bilgiler, genellikle hukuki anlamda bu bilgileri elinde tutan işletmelere aittir. Onlar, son-

suz miktardaki kişisel bilgilerimizi değiştirebilmekte, kullanabilmekte, saklayabilmekte ve bunların ticaretini yapabilmektedir ve bizim buna rağmen, bu durum karşısında sınırlı yasal hakkımız bulunmaktadır. Buna ek olarak, dijital teknolojiler giderek daha yaygın hale geldiğinden, kendimizi aynı anda her yerde bulunabilen akıllı interaktif sistemlerin içinde yaşar bulmaktayız. Bunlarla etkileşim içinde olmak, bazen herkes için – Bilgi Teknolojileri uzmanları için dahi – zor ve kimi grup insanlar için zaman zaman imkansız olan; karmaşık ve zaman alıcı bir iştir. Bu olgu ile başa çıkmak için birçok kullanıcı odaklı yaklaşımlar olmasına rağmen, ironik bir şekilde, dijital ortamın doğal olmayan tek parçasının gerçek insan olduğu görülmektedir. Bu sorunu çözmek için, dijital çevreler ve son kullanıcı arasında bir temsilci olacak, içerik tabanlı bir dijital kişilik (DK) yaratılması üzerinde çalışılmaktadır. DKler içerik oluşturma, bakım ve kullanımı için mobil teknolojilerden; ve resmi karar ve kanıtlamalar içinse anlamsal teknolojilerden yararlanacaktır. DK, bizden bağımsız olarak var olan, icra kuvveti olan ve elektronik dünyada iş yaparken kimliğimizi taşıyan elektronik bir ikinci kişilik olarak tasarlanmıştır. Bunu kullanmak, kullanıcılar ve dijital ortamlar arası günlük etkileşimi kolaylaştırmalı ve mobil operatörler için katma değerli hizmetler uygulanması yönünde bir çerçeve sağlamalıdır.

Bölüm 2'de yer alan ilgili sorular; dijital kişiliğimize karşı olası temel ihlaller ve haksız çıkar sağlamalar, dijital kişiliğimizin nasıl korunacağı ve hassas bilgilerimiz üzerindeki orantısız güç denkleminin yeniden nasıl dengeleneceği sorunları üzerine eğilmektedir.

(4) Yasal olmayan içeriğe karşı korunma

Yasa dışı içerik; aşağıdaki içerik, görüntü, kod veya yazılımlardan herhangi birini gerçekleştiren ya da destekleyen her türlü içerik olarak özetlenebilir:

- Kötücül yazılım ve kodlar
- Hizmeti engelleme saldırıları
- Bilgisayar virüsleri
- Siber takipçilik

- Dolandırıcılık ve kimlik hırsızlığı
- Yemleme
- Bilgi savaşı
- Taciz
- Spam ya da ticari amaçlar sebebiyle istenmeyen toplu e-posta gönderimi
- Lisanlı veya güvenlikli yazılım veya diğer fikri mülkiyetler haklarına yetkisiz erişim
- Uyuşturucu kaçakçılığı
- Terörizm
- Çocuk pornografisi, çocuk istismarı ve küçükler için uygun olmayan bazı içerikler

Birçok yargı sistemi, bazı ifadelere sınırlamalar getirmekte ve nefret söylemi yaratma eğiliminde olan ırkçı, dine hakaret teşkil eden, siyasi anlamda yıkıcı, sözlü veya yazılı olarak hakaret niteliği taşıyan, tahrik edici, kışkırtıcı ifadeleri yasaklamaktadır.

"Yasa dışı" ifadelerin, internet ağına gerçekten veya potansiyel olarak konulmasına tepki olarak, internet sansürüne ilişkin hükümet politikaları genel olarak dört kategoride incelenebilir:

(a) İnternet sektöründe öz düzenlemeyi ve filtreleme/engelleme teknolojilerinin son kullanıcı tarafından gönüllü kullanımını teşvik eden hükümet politikaları.

Bu ülkelerde, çocuk pornografisi ve bazılarında da ırkçı nefreti tahrik gibi yasa dışı internet içeriklerine genel hükümler uygulanır.

"Küçükler için uygunsuz" içeriği internet üzerinde erişilir kılmak hukuka aykırı değildir; ona erişim de sınırlandırılmış bir erişim sistemi tarafından kontrol edilmemelidir. Belki de tüm bu hükümetler, internet kullanıcılarının kendilerinin ve çocuklarının internet içeriğine erişimini denetlemeye imkan veren teknolojilerin gönüllü kullanımını ve devam eden gelişmelerini teşvik etmektedir (örneğin ebeveyn kontrolü).

(b) İnternette 'Küçükler için uygunsuz' içeriği erişilir kılan içerik sağlayıcılarına uygulanabilecek ceza hukuku yaptırımları (para veya hapis cezası).

Ek olarak bu ülkelerde, genel hükümler diğer yasa dışı içeriği yasaklamaktadır (örneğin çocuk pornografisi).

(c) Hükümetin yetişkinler için uygunsuz kabul edilen içeriği engellenme kararı.

Bazı ülkeler engelleme için İnternet Servis Sağlayıcılarına (İSSleri) gerek duymaktayken; bazıları ise devlet kontrollü erişim noktaları aracılığıyla kısıtlı internet erişimine izin vermektedir.

(d) Hükümetin internete kamu erişimini yasaklaması.

Bazı ülkeler ya internete kamu erişimini yasaklamakta ya da internet kullanıcılarına – (c)'deki gibi – kısıtlı erişime izin vermeden önce, onların idari bir makam tarafından kayıtlı ya da lisanslı olmasını aramaktadır.

Kısıtlayıcı internet sansürü yasalarına sahip pek çok ülkede, hükümet odağının, siyasi anlamda hassas söylemler, hükümet eleştirileri vb.'ni yasaklamak ve/veya kısıtlamaya yönelik olduğu görülmektedir.

İnternette yer alan içeriğe erişim hakkındaki endişeler tüm dünyada değişiklik göstermekte ve düzenleyici politikalar da bunu yansıtmaktadır. Bir ülkede yasalara aykırı olan, diğerlerinde olmayabilmekte ve bir ülkede küçükler için uygunsuz kabul edilen, diğerlerinde uygun kabul edilebilmektedir. Bununla birlikte, genel anlamda, çocuk pornografisi yaygın bir şekilde suç teşkil etmektedir.

(5) Mülkiyetin korunması (fikri mülkiyet hakları da dahil olmak üzere)

Fikri mülkiyet (FM), aklın yaratılarını (buluşlar, edebiyat ve sanat eserleri, ticaret alanında kullanılan semboller, unvan ve adlar, resimler ve tasarımlar) ifade etmektedir. FM iki kategoriye ayrılmaktadır: buluşlar (patent), markalar, endüstriyel tasarımlar ve coğrafi işaretleri içine alan sınai mülkiyet; roman, şiir ve oyunlar, filmler, müzik eserleri, güzel sanatlar eserleri (çizim, resim, fotoğraf ve heykeller)

ve mimari tasarımları gibi edebiyat ve sanat eserlerini kapsayan telif hakkı. Telif hakları, performansları esnasında sanatçıların haklarını, fonogram yapımcıların kayıtlar üzerindeki haklarını ve radyo ve televizyon programı yayıncılarının haklarını içermektedir. Yenilikler ve yerli ve yerel toplulukların yaratıcı ifadeleri de ayrıca fikri mülkiyete konu olmakla birlikte, sadece "geleneksel" niteliklerinden ötürü, var olan FM sistemleri tarafından tamamen korunmayabilmektedir. Genetik kaynaklara erişim – ve bunların eşitlikçi yarar paylaşımı – de FM'ye ilişkin sorunlar ortaya çıkarmaktadır.

Bilgi ve İletişim Teknolojileri, ayrıca dolandırıcılık gibi klasik suçların işlenmesinde de yaygın şekilde kullanılmaktadır. Rekabetçi iş dünyamızda, söylentilere göre endüstriyel casusluk, haksız bir şekilde rekabet avantajı elde etmek amacıyla sıkça işlenmektedir.

(6) Sadece sanal ortamda gerçekleştirilebilen eylemlere karşı korunma

Suçlar, geleneksel olarak düşünülürse, sözüm ona gerçek dünyada, paylaştığımız fiziksel gerçeklikte, işlenmektedir. Bu tür suçları işlemek üzere yapılan hareketler, bunların işlenmesi esnasında var olan koşullar ve işlenmeleri sonucu doğan zararların tamamı; herkese açık cadde veya özel konut gibi "gerçek" yerlerde oluşmaktadır. Sonuç olarak, var olan ceza hukuku, fiziksel zarara uğratacak şekilde sonuç veren hareketler (kişilere ya da mala zarar verme ya da başkasının malını izinsiz şekilde alma) için, sorumluluk ve ceza yüklemektedir. Modern ceza hukuku, esaslı bir öncül olarak, sorumluluğun dış, fiziksel dünyada alınmış kimi kararlar – eylem veya hareket etme yükümlülüğü karşısında eylemsizlik – üzerine kurulması konusunda ısrar etmektedir. Bu, temelde sorumluluğun, maddi varlığı olmayan hareketlere – uygunsuz ve hatta suç niteliği taşıyan düşünceler – ilişkin uygulanmasını reddetmektedir.

Aynı zamanda siber alan, fiziksel dünya ile birlikte; ama bundan ayrı olarak varlığını sürdürmektedir. Bu ortak kavramsal bir gerçeklik, bir "sanal dünya"dır; ancak ortak fiziksel bir gerçeklik değildir. Fiziksel bir alan olmadığından, kullandığımız güncel ceza hukuku ilkelerinin siber alanın benzersiz avantajlarından faydalanan suçlara hitap etmede yeterli olup olmadığı sorunları ortaya çıkmaktadır.

Siber suçlar ve "gerçek" suçlar arasında maddi farklar olmadığı takdirde, bu yetersizlik varlığını sürdüremez. Buna ilişkin, her iki kategorinin de kapsamına giren suçları oluşturan hareketler, suçların işlenmesini çevreleyen koşullar ve sonuçlanan zararlar gibi örnekler verilebilir. Doğal olarak, siber alandan faydalanmaya yönelik suç hareketlerinin "siber suç" adlı yeni bir olguyu temsil ettiği sonucuna kolayca varılmamalıdır. Failler yalnızca uzun zamandır yasa dışı ilan edilmiş hareketleri, siber alanı kullanarak icra ediyor olabilir. Örneğin telefon, telgraf, radyo, televizyon vs. dolandırıcılık suçunu işlemek amacıyla kullanılmaktadır. Ancak, dolandırıcılık yüzyıllardır bir suçtur. Aynı şey; bıçak, sopa, ateşli silah veya zehirle olduğu fark etmeden, adam öldürme suçu için de geçerlidir.

Temel unsurları, sadece veya neredeyse sadece siber alanda gösterilen suçlar olarak, gerçekten sanal suçlardan bahsedilebilir mi? Hukuk alanındaki bazı uzmanlar, klasik ceza hukuku ilkelerinin, siber suç teşkil eden eylemlere, tamamını olmasa da çoğunu kapsamak üzere, uyarlanabileceğini savunmaktadır. Diğerleri, telefon ile internet dünyası arasındaki hatırı sayılır ölçüde değişiklik anlamında özel bir şey olmaksızın, dolandırıcılık suçu İnternet aracılığıyla işlendiğinde diğer araçlara – telefon gibi – nazaran suçluların daha büyük bir zarara yol açabileceği gerçeği ve klasik suçlular üzerinde sahip oldukları, suçun ortaya çıkarılması ve başarılı bir soruşturmadan kaçınılması avantajı; siber suçta ceza sorumluluğuna ilişkin yeni ilkelere ve yeni yasalar geliştirilmesini desteklemektedir.

2. Bölüm sorularında konuya ilişkin sorulara verilen uluslararası cevaplar, ceza hukukunun uluslararası anlamda bu konuda aldığı yön hakkında bir değerlendirme sağlayacaktır.

(7) Uygulama sisteminin korunması (itaatsizlik suçları)

İnternet Servis Sağlayıcıları (İSSler); abone bilgileri, internet trafiği verileri (günlük kütüğü, FM'e ilişkin veri) ve içerik verileri gibi; suçların soruşturulmasında faydalı olabilecek değerli bilgilere sahiptir. Devletlerin, idari makamların, savcıların; internet kullanımı, internette gezinme ve diğer veri alışverişlerinden elde edilen mümkün olduğu kadar çok bilgiye ulaşmak istemesi doğaldır. Bu durum özel hayatın gizliliğine ilişkin anayasal kavramlar, sebepsiz

arama ve yakalamalardan korunma ve hükümetin amaçsız bir şekilde gerçekleştirdiği incelemelere getirilen yasaklama gibi ilkelerle çatışabilmektedir.

Ortaya çıkan bir başka durum da ulusal yönetimlerin, İSSler tarafından vatandaşlara sağlanan içerik üzerinde sahip olmak istediği denetimdir. İnternet sansürü için üç ana sebep vardır: siyaset ve iktidar, toplumsal kurallar ve ahlak ve güvenlik kaygıları. Fikri mülkiyet haklarının ve var olan ekonomik çıkarların korunması da internet sansürüne yol açabilmektedir. Buna ek olarak, bazı ülkelerde, bilgi paylaşımına izin veren ağ oluşturma araçlarını ve uygulamalarını engellemek de az rastlanan bir durum değildir. Siyasi muhalefete yöneltilen sansüre, özellikle otoriter ve baskıcı rejimlerde sık rastlanmaktadır. Bazı ülkeler din ve azınlık gruplarına ilişkin web sitelerini, özellikle bu hareketler iktidar rejimine yönelik bir tehdit teşkil ettiklerinde, engellemektedir. Belli başlı İSSları ve bazı ülkelerin hükümetleri arasında, bu konuda, aleniyete dökülmüş pek çok çatışma ve mücadele yaşanmıştır. Fikri mülkiyet haklarına ilişkin finansal çıkarlar da hükümetin esaslı müdahalesini haklı kılan faktörlerden biri olabilmektedir.

Sorular; farklı hukuki gelenekleri (örneğin Lèse majesté kavramı), kültürel değerleri ve ekonomik öncelikleri yansıtan; bu geniş ve karmaşık konu üzerinde bilgi sahibi olmayı amaçlamaktadır.

(C) Uluslararası Yaklaşımlar

Elektronik suçlar hakkında uluslararası bir paradigma oluşturmak, teknolojinin küresel niteliği nedeniyle zorlu bir çaba halini almaktadır. Tüm uluslar bu suçları tanımlamaya ve hem ulusal hem de uluslararası muhatap ve durumlara uygulanabilir hukuki düzenlemeler yapmaya çalışmaktadırlar. Sanal gerçekliğin coğrafi veya siyasi sınırları olmadığından ve çok sayıda elektronik sisteme dünyanın herhangi bir yerinden kolayca ve gizlice ulaşılabildiğinden sadece ulusal boyutta kalan çözümler yetersiz kalmaktadır. Uluslararası finansal kuruluşlar elektronik dolandırıcılık ve zimmet girişimlerinin yaygın hedefleridir. Buna ek olarak, karmaşık elektronik teknolojiler örgütlü suçların ve terörist grupların devlet tarafından ortaya çıkarılmaktan kurtulmalarına ve yıkıcı şiddet eylemlerinin gerçekleştiril-

mesine imkan tanımıştır. Birçok sanayileşmiş ülkedeki ispat kuralları, bilgisayarlara özel cezai hükümler mevcut olduğunda bile, bunlar elektronik suçlara uyarlanana kadar kovuşturmayı aksatmaya devam edebilecektir. Siyasi söylemleri sınırlandıran ülkeler, internetin düzenlenmesi zor bir "yasa dışı" bilgi kaynağı teşkil etmesi sorunu ile karşılaşmaktadırlar. Dahası, neyin "kabul edilebilir" bir söylem olduğu, bilginin hızla aktarım ortamındaki çeşitli ülkeler arasında, hatta Batılı demokrasiler arasında bile, farklılık göstermektedir. İnternetteki ifade özgürlüğü sorunlarına getirilen çözümler büyük oranda birbirinden ayrılmaktadır. Bazı Avrupa ülkeleri ilk olarak internet servis sağlayıcıları (İSS) hedef almışlardır. Diğerleri ise, "zararlı" bilginin internet üzerinden kullanım veya dağıtımını suç haline getiren ve bazı zamanlarda ya da kalıcı olarak internet erişimini sınırlandıran veya engelleyen düzenlemeler getirmiştir.

Fikri mülkiyet suçları uluslararası düzlemde ciddi bir sorundur. Uluslararası yazılım korsanlığı bölgesel niteliğini korumaktadır ki bu da bütün dünyadaki elektronik araçlarda bulunan birçok yazılım uygulamasının ücreti ödenmemiş, yasadışı kopyalar olduğu anlamına gelmektedir. Bazı hallerde, ciddi zorunluluklar getiren ve böylece potansiyel olarak internet servis sağlayıcılarını suçlayabilecek yasal düzenlemeler yapılmıştır. Veri madenciliği, kimlik dolandırıcılığı, çevrimiçi kumar, çocuk pornosu, işçilerin bilgi teknolojileri üzerinden kontrol edilmesi, Facebook ve Google gibi sosyal medya ve arama motorlarındaki ve iPhone gibi kablosuz iletişimdeki özel hayatın gizliliğinin ihlalleri ile ilgili sorunlar hatırı sayılır bir dikkat ve endişe uyandırmaktadır. Tüm dünyada ulusal makamlar, izinsiz erişim, özel hayatın gizliliğine aykırılık, bilgi manipülasyonu konularının yer aldığı, bilgisayarlara özel ceza yasaları oluşturmaktadır. Hala bir takım farklılıklar bulunmakla birlikte, birçok ulusal yasal düzenleme arasında ciddi yakınlaşmalar vardır. Bu düzenlemeler, belirli yeni suç ve cezalar getirerek, genel ceza hukuku kurallarının bilgisayar suçlarına uygulanması durumunda ortaya çıkan analitik sorunların önüne geçmektedir. Ancak bu sırada, hükümetlerin geleneksel anayasal korumaları ve ceza muhakemesi hukuku kurallarını atlayarak özel veya ticari bilgilere elektronik yollardan ulaşmaları endişelere neden olmakta, yeni ve zor bir takım soruları akla getirmekte ve maddi ve usulî ceza hukukunun güncellenmesi ihtiyacını doğurmaktadır.

Uluslararası örgütler ve özel şirketler de ulusal düzenlemelerin uyumlaştırılması çabalarına katılarak BİT suçlarına karşı mücadeleye katkıda bulunmaktadır. Bununla birlikte, uluslararası çabalar birbirine karışmıştır.

(D) Sorular

Bilgi toplumumuzun ceza hukuku açısından birçok yeni sorun, zorluk ve fırsat yarattığı açıktır. Ceza hukuku ve uygulamasının sınırlarının genişletilmesine belirgin bir ihtiyaç duyulmaktadır. Özel hayatın gizliliğinin ve insan haklarının korunması çok önemli bir endişe kaynağı olarak varlığını sürdürmektedir. Yukarıda bahsedilen birçok müdahale alanı, 2. Bölümdeki tartışma için uygundur; çünkü bilgi toplumu – ki o da gittikçe yalnızca hayatlarımızı ve aktivitelerimizi değil; dünya meselelerini, uluslararası ilişkileri ve siber savaş tehditlerini de kapsamakta ve hatta kontrol etmektedir – tarafından gereksinim duyulan, maddi ceza hukukundaki özel genişleme ve yenilenmenin özünü oluşturmaktadır. İlişikteki 2. Bölüm soruları, Özel Kısım, dünya genelinde çeşitli ülkelerde, ceza hukukunun siber suça verdiği tepki üzerine, ilgili bilgileri toplamak üzere tasarlanmıştır. Sorular, korunmaya değer olduğu saptanan temel çıkarların etrafında organize edilmiştir (bkz. Bölüm C). Sorular, korunacak çıkarlar ve maddi unsur; manevi unsur ve özel kişiler, kamu görevlileri, soruşturmacılar gibi farklı tür faillere uygulanacak yasada öngörülen ceza gibi klasik ceza hukuku gerekleri çevresinde yoğunlaşmaktadır. Sorular, alanda önemli belirteçler belirlemek ve Ulusal Raportörlerin, farklı hukuk geleneklerini ve ulusal siber suç hukukunda değişken gelişmişlik düzeylerini göz önüne alarak bilgi vermelerine olanak sağlamakla sınırlandırılmaktadır. Bu hukuki menfaatler sisteminin ardından, Ulusal Raportörlerin çalışmalarını kolaylaştırması ve dünya çapında, siber ceza hukukunun statüsü üzerine değerli bilgiler sağlanması umulmaktadır. Bu, Hazırlık Kolokyumu ve AIDP Uluslararası Kongresinde, kararların geliştirilmesinde verimli bir malzeme olmalıdır.