Journal of History Culture and Art Research (ISSN: 2147-0626)

Tarih Kültür ve Sanat Araştırmaları Dergisi

Vol. 8, No. 2, June 2019

DOI: 10.7596/taksad.v8i2.1949

Citation: Dolunay, A. & Sağsan, M. (2019). Kişilik Haklarını İhlal Eden Siber Suçlar: KKTC Örneği. Journal of History Culture and Art Research, 8(2), 433-449. doi:http://dx.doi.org/10.7596/taksad.v8i2.1949

Kişilik Haklarını İhlal Eden Siber Suçlar: KKTC Örneği[*] [**]

Cyber Crimes Related to Violation of Personal Rights: TRNC Example

Ayhan Dolunay[1], Mustafa Sağsan[2]

Abstract

Although the digital era allows us to understand irregular human behaviours, jurisprudence attempts to organize and adapt those behaviours into societal rules and regulations. In the frame of technological improvements, knowledge which is used, collected, stored, protected by technical, economic and social fields have been moved onto electronic environments. Information Technology (IT) law plays a very important role to legalize data, information and knowledge within the digital platforms. At this point, Lege Lata (positive law) has a strong relationship between the problems which occurs within the digital era and providing opportunities to prevent regulations for a long time in society. IT law includes specific topics which are directly relevant to some fields such as copyrights, trademarks, criminal sanctions, etc. within the Internet environment. Although most of the countries have already constituted IT Laws in order to solve the digital problems and to prevent or reduce cybercrimes, North Cyprus IT Law improvements are still constitution stage because of some bureaucratic reasons and have seen as a hugely problematic issue for solving the digital problems in the country. For this reason, this study briefly attempts to investigate the constitution of IT Law in North Cyprus. Specifically, IT Law in the context of adaptation process to EU countries will be considered according to rules and regulations of EU IT Law from the two perspectives, called common law and civil law. Literature review will be used by this research to understand whether there are similarities between Turkey-EU countries and North Cyprus based on IT Law and cybercrime or not. The findings which will be relying on literature review will be discussed as a county case studies in the research.

Keywords: IT law, Cyber crimes, Sociological problems, Personal rights, North Cyprus.

---

[*] Bu çalışma Yakın Doğu Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimince desteklenmiştir. Proje Numarası: SOS-2017-01-004

[**] Bu çalışma, yazarların, Oxford Üniversitesi'nde, 13-15 Ağustos 2018 tarihleri arasında gerçekleştirilen 9th Academic International Conference on Interdiciplinary Legal Studies'e kabul alan çalışmasının geliştirilmesi ile yayına hazırlanmıştır.

[1] Near East University (Yakın Doğu Üniversitesi), Yrd. Doç. Dr., Hukuk Danışmanı, İletişim Fakültesi Öğretim Üyesi, İletişim Araştırmaları Merkezi Üyesi. E-mail: ayhan.dolunay@neu.edu.tr

[2] Near East University (Yakın Doğu Üniversitesi), Prof. Dr., Sosyal Bilimler Enstitüsü Müdürü, İktisadi ve İdari Bilimler Fakültesi, Bilgi ve Belge Yönetimi Bölüm Başkanı. E-mail: mustafa.sagsan@neu.edu.tr

Öz

İnternetin, ortaya çıkışı ve değişimi evreleri ardından, içerisinde bulunduğumuz "dijital çağ" olarak adlandırılan dönemdeki yüksek önemine istinaden; bu ortamda gerçekleştirilen faaliyetlerin, fonksiyonel olarak düzensiz insan davranışlarını inceleyen hukuk bilimi tarafından düzenleme altına alınması gerekliliği ortaya çıkmıştır. Teknolojik gelişmeler çerçevesinde insanoğlunun teknik, ekonomik ve toplumsal alanlarda kullandığı bilginin, elektronik ve benzeri makineler aracılığıyla toplanması, işlenmesi, saklanması ve korunması ile, bunlardan doğan ihtilafların çözümünü konu alan bilişim hukuku, pek çok ülkede, başta bilişim yasaları olmak üzere, çeşitli hukuki düzenlemeler ile Lege Lata (pozitif hukuk) olarak, varlık göstermiştir. Gerek internet ortamında yayınlanan eserler üzerindeki telif haklarına aykırı içerikler hususunda cezai müeyyideler getiren; gerekse, internet ortamında gerçekleşen dar ve geniş anlamdaki cezai sonuç doğurucu faaliyetleri kapsamı altına alan bilişim yasaları, belirtildiği gibi pek çok ülkede yürürlüğe girmiş ve gelişen teknoloji ışığında, daha yerinde düzenlemeler için revize edilmeye devam ediyor olsa da, Kuzey Kıbrıs'ta, henüz yürürlükte bir bilişim yasası bulunmamaktadır. Taslak halinde olan Bilişim Yasa Tasarısı ise, uzun yıllardır duyulan ihtiyaca ve sürdürülen çalışmalara rağmen yasalaştırılamamıştır. Bu kapsamda, çalışmada, literatür taraması çerçevesinde, hukuk düzeni olarak yakın bağlantısı nedeniyle örnek oluşturabilecek Türk Hukuku'nun ve yine Kuzey Kıbrıs'ın, Kıbrıs sorununda olası bir çözüm durumunda, katılma hedefi söz konusu olan Avrupa Birliği'nin çeşitli bilişim hukuku düzenlemelerine başlık ve genel amaçları ile değinilmekte; yasal boşluk nedeniyle Kuzey Kıbrıs'ta söz konusu olan mevcut sosyolojik sorunların tespitine ve ilgili sorunların aşılması için somut çözüm önerilerine yer verilmektedir.

Anahtar Sözcükler: Bilişim hukuku, Siber suçlar, Sosyolojik problemler, Kişilik hakları, KKTC.

Giriş

Birleşmiş Milletler (BM)'in 2017 Dünya Nüfus Artışı Raporu'na göre, 7.6 milyara ulaşan dünyadaki insan nüfusu, yine aynı rapordaki öngörülere göre, hızla artışını sürdürecek ve 2030 yılında 8.6 milyara; 2050 yılında ise, 11.2 milyara yükselecektir (World Population Prospects: The 2017 Revision, 2017).

Giderek artan nüfus, bir yönüyle, temel yaşam hakkı, beslenme ve konaklama hakkından başlayarak, hak ve özgürlüklere ilişkin tartışmaları beraberinde getirirken; teknolojik gelişmeler ile birlikte söz konusu olan bir takım önemli diğer yasal düzenlemelerin de gerekliliğini ortaya koymaktadır. Söz konusu teknolojiler her ne kadar bilgiye erişimde özgürlük sağlasa da, olumsuz sonuçları denetim altına alabilecek hukuksal düzenlemelerin yapılması da kaçınılmazdır.

Bahsi geçen hukuksal düzenlemelerin başında, özgürlüklerin, başkalarının özgürlüklerini zedeleyecek ölçüde geniş kullanımı hallerinden kaynaklanan suçların nasıl denetim altında tutulacağı gelmektedir. Bu bağlamda gelişen teknoloji ile birlikte, internet ortamında söz konusu olan siber suçların cezalandırılabilmesi için bir gereklilik olan bilişim hukuku ve bilişim yasalarının önemi ortaya çıkmaktadır.

Çalışmada, KKTC'de bilişim hukukuna ilişkin yasal düzenlemenin/düzenlemelerin yürürlüğe henüz girmemiş olmasının doğurduğu sosyolojik sorunlar ele alınmakta, KKTC'ye bu hususta örnek oluşturabilecek Türk Hukuku ve AB Hukuku'ndaki ilgili düzenlemelerine başlıkları ve düzenleme amaçları ile kısaca değinilmekte ve bahse konu boşluğun doldurulabilmesi için somut çözüm önerilerine yer verilmektedir.

I. Kuramsal Çerçeve

Çalışmanın temel amacı, temel olarak, hayatın pek çok alanında olduğu gibi, bilişim ortamları ile ilgili de yasal düzenlemelere duyulan ihtiyaç üzerine ortaya çıkan bilişim hukukunun önemi yinelenerek; KKTC'ye ilişkin siber suçlar kapsamındaki kişilik hakları ihlallerinin tespiti ve bu hususlara ilişkin somut çözüm önerilerine yer verilmesidir.

Çalışmanın girişinde de ifade edildiği şekilde, insan unsurunun olduğu her yerde karşılaşılması muhtemel "suç" unsurunun, *hukuki açıdan* suç teşkil edebilmesinin temel şartlarının başında, işlenen fiilin önceden kanunlar aracılığı ile suç olarak tanımlanması ve cezai sınırlarının yine ilgili kanunda/kanunlarda belirtilmesi gelmektedir.

Bu çerçevede, yürürlükte bir bilişim yasası bulunmayan KKTC, çalışmanın kapsam açısından odak noktasını oluşturmakta; KKTC'de söz konusu olan ilgili yasal boşluk çerçevesinde yaşanan sorunların tespiti ve bahse konu sorunlara ilişkin çözüm yöntemleri sunma arayışı, çalışmanın temel problemini oluşturmaktadır.

KKTC'ye ilişkin bilişim hukuku sorunlarını tespit eden ve çözüm önerileri sunan başka bir akademik çalışma yapılmamış olması, çalışmanın, konu açısından özgünlüğünü ortaya koymaktadır.

Çalışmada, literatür taraması kapsamında, bilişim, hukuk, bilişim hukuku, bilişim etiği gibi temel kavramlara ilişkin tanımlamalara yer verilmekte; yine çalışmanın odak noktası KKTC'ye ilişkin belirtildiği gibi ilgili yasal boşluğun tespiti yapılarak, bahse konu boşluğun doldurulması için somut çözüm önerilerine ver verilmektedir.

A. "Bilişim" ve "Hukuk" Kavramları

Çalışmanın temel konusu olan bilişim hukukunun tam olarak anlaşılabilmesi için öncelikle, "bilişim" ve "hukuk" kavramlarının tanımlanmasında fayda bulunmaktadır.

Fransızca kökenli *informatique* sözcüğünden gelen ve İngilizce karşılığı *informatics* olan bilişim terimi, kelime anlamı itibarıyla, "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi, enformatik bilimi"ni ifade etmektedir (Köksal, 1981: 191; Pamukoğlu & Ocak, t.y.: 56).

Bilişim terimi, karşılıklı olma olgusuna dayanır; insanların karşılıklı olarak etkileşimde bulunabildiği ortamlar bilişimin temel alanını oluşturmaktadır. Buna verilebilecek en bilinen örnek internettir. İnternet ağında insanlar diledikleri kişilerle iletişime geçebilmekte, bilgi alışverişinde bulunabilmekte, internet üzerinden özel ya da tüzel kişilerin mağazalarından alışveriş yapabilmektedir (Denizci, 2009: 51; Bilişim, t.y.; Bilişim ve Sosyal Medya Hukuku, t.y.).

Diğer yandan hukuk ise; ms. 533 yılında yürürlüğe girmiş temel hukuk metni Corpus Juris Civilis'de yer alan Ulpianus'un tanımına göre, *"hukuk bilimi tanrısal ve beşeri olanın bilgisi, haklı ve haksızın bilimi"*dir (Işıktaç, 1998).

Başka bir tanıma göre; *"İnsan topluluklarında, kişiler arasında ya da kişiler ile devlet arasındaki ilişkileri düzenleyen ve kendilerine uyulması, devletin zorlayıcı gücü (müeyyide) ile sağlanmış bulunan, düzenleyici, yasaklayıcı ve izin verici davranış kurallarının bütününe hukuk denilmektedir"* (Özsunay, 1979: 5).

Diğer bir tanıma göre hukuk, "tasarlanan, emredilen veya kurulan; hangi olgu ya da eylemlerin birbirleriyle bir arada ya da birbirine uyduğuna göre bir kural ya da yöntem"dir. (What is Law?, t.y.)

Bir başka ve bu çalışmanın yazarlarının da hemfikir olduğu görüşe göre ise, dilimizdeki kullanımı açısından hukuk, önüne "sıfatlar" konularak tanımlanmalıdır. "Pozitif hukuk", "yazılı hukuk" vb. Bu açıdan ele alınacak olursa hukuk, iki başlığa ayrılmaktadır: "Pozitif (Olan – *Lege Lata*) Hukuk" ve İdeal (Olması Gereken – *lege ferenda*) Hukuk (Aybay, vd.: 64).

Açık ifadelerinden de anlaşılacağı üzere, pozitif hukuk açısından yer ve zaman önem arz etmekte; belli bir ülkede, belli bir zamanda bulunan hukuk, o ülkenin pozitif hukuku olarak adlandırılmaktadır (Aybay, vd.: 64). Diğer yandan, bu tanımlamadan bağımsız/farklı olarak ideal hukuk, "soyut düzeyde", toplumun gereksinimlerini en uygun şekilde karşılayacak "adalete" en uygun hukuk sistemi olarak tanımlanmaktadır (Aybay, vd.: 65). Bu çalışmanın, lege ferenda'nın, Lege Lata'ya dönüşmesini hedefleyen bir niteliği bulunmaktadır.

B. "Bilişim Hukuku" Kavramı

Bilişim hukuku, teknolojik gelişmeler çerçevesinde insanoğlunun teknik, ekonomik ve toplumsal alanlarda kullandığı bilginin, elektronik ve benzeri makineler aracılığıyla toplanması, işlenmesi, saklanması ve korunması ile bunlardan doğan ihtilafların çözümü ile ilgilenen hukuk dalıdır. Bilişim hukuku, bilgi ve teknolojinin kötü amaçlı kullanım ile, bireylere zarar vermesinin önüne geçilmesi amacını taşımaktadır (Bilişim Hukuku ve Bilişim Suçu, t.y.).

Bilişim Hukuku, iki temel başlığı kapsamı altına almaktadır: "İnternet ortamında telif hakkı ihlalleri" ve "internet ortamında işlenen suçlar" (siber suçlar). Bazı yazarlara göreyse bilişim suçları, üç başlık altında toplanmaktadır (Arora, 2016: 541):

1. Bireylere karşı bilişim suçları,

2. Fikri mülkiyet haklarına karşı bilişim suçları,

3. Devlet, kurum-kuruluş ve topluma karşı bilişim suçları.

Bireylere karşı işlenen bilişim suçlarına örnek olarak, bireylerin kişilik haklarını zedeleyici şekilde, diğer bir ifade ile onur kırıcı şekilde, haklarında yapılan yayın ve paylaşımlar verilebilirken; fikri mülkiyet haklarına karşı işlenen bilişim suçlarına, çevrimiçi ortamda telif haklarını zedeleyecek şekilde sanatsal üretimlerin yayınlanması (Sağsan, 2002: 25); devlet, kurum-kuruluş ve topluma karşı işlenen suçlara ise, devletin bütünlüğünü zedelemeye veya toplumun düzen ve sağlığını bozmaya yönelik gerçekleştirilen çevrimiçi yayınlar verilebilmektedir.

Bir başka görüşe (Birleşmiş Milletler 10. Kongresi'nde kabul gören görüş) göre ise, bilişim suçları; "dar anlamda", bilişim sistemi güvenliği veya veri işlemini hedef alan girişimler (yetkisiz ve izinsiz erişim, verilere yönelik suçlar, ağlara yönelik suçlar, sanal tecavüz vs.) ve "geniş anlamda", bilişim sistemleri aracılığıyla veya bu sistemlerden faydalanarak, işlenen "klasik suç" kabul edilen eylemler (bilişim ortamı aracılığıyla cinayet, tehdit ve şantaj, hakaret, taciz, pornografi, dolandırıcılık, hırsızlık, siber terör vs.) şeklinde ikiye ayrılır (Avşar ve Öngören, 2010: 123; Gönen, Ulus ve Yılmaz, 2016: 230).

İlgili görüşler, farklı unsurlar içerse de, temelde, "telif hakları" ve "siber suçlar" başlıkları altında toplanabilmektedir. Belirtilmelidir ki, bilişim hukukunda başat faktör olan ve hukuki boyutu ön plana çıkan, toplumsal düzenin artan sosyal medya uygulamalarıyla bozulabilme riski için bunu minimize edecek önemli konu siber suçlardır. Bu yüzden çalışmada, bilişim hukukunun siber suçlara yönelik boyutu ele alınıp teorik olarak tartışılacak ve akabinde siber suçların Kuzey Kıbrıs uygulaması açısından irdelemesi gerçekleştirilecektir. Ancak öncesinde, bilişim etiği ve kişilik hakkı hususları ele alınıp, tanımlamaları yapılacaktır.

C. "Bilişim Etiği" Kavramı

Çalışmanın odak noktası siber suçlar ve KKTC'deki yasal boşluk çerçevesinde sosyolojik sorunlar olmakla birlikte; bilişim alanındaki etik ilkelere de değinmekte fayda bulunmaktadır. Çünkü etik değerlere uyulması halinde, yasal boşluk bulunan hallerde bile, temel bir çözüm olmamakla birlikte, sorun kısmen hafifletilebilecektir.

Etik kelimesi, Fransızca *éthique*, (ahlak, ahlaki) sözcüğünden alıntıdır. Fransızca sözcük, Eski Yunanca *ethikós* (ahlaka ilişkin) sözcüğünden alıntıdır. Bu sözcük de, Eski Yunanca *éthos* (örf, adap, ahlak, töre) sözcüğünden türetilmiştir ("Etik Kelime Kökeni", t.y.; Dolunay, 2018: 26).

Etik, oldukça geniş ve sınırları belirlenmesi güç bir kavram olmakla birlikte; ahlaki durumun betimlendiği, gözlem araçlarının geliştirildiği, bir araştırma disiplini; belli bir grup veyahut toplum için geçerli olan, hatta evrensellik iddiası taşıyan kuralların ve yaptırımların üreticisi; iyi ve kötünün veyahut doğru ve yanlışın ne olduğu temelinde kriterler inşa ettiğimiz ve onları doğruladığımız bir eleştirel talep olarak tanımlanabilmektedir (Moressi, 2006: 23; Girgin, 2000: 144).

Bilim ve teknolojinin, küreselleşen dünya yapısında devletlere/kurumlara evrensel bir güç kazandırması, etik ilkelerin oluşturulması ve benimsenmesini kaçınılmaz hale getirmiştir. Etik değerler, belirli meslek gruplarının kendi iç denetimlerini oluşturmasını zorunlu kılmış ve hak - hukuk, ahlaki sorumlulukların belirlenmesini sağlamıştır (Dolunay & Keçeci, 2017: 1397; Dolunay, 2018: 27)

"İlk önce batı dünyasında bilgi ve gücü iç denetime kavuşturmak için etik kurallar uygulanmaya başlanmıştır. Bu etik kuralları, bazen yasa gücünde bazen de bir meslek grubunun iç denetim ilkeleri olarak ortaya çıkmaktadır. Her iki durumda da, etik değerler/kurallar bir başka insana ve topluma karşı iç sorumlulukları içermektedir." (Dolunay & Keçeci, 2017: 1398; Dolunay, 2018: 27).

Diğer yandan belirtilmelidir ki, etik ve ahlak kavramları, bağlantılı olmak ile birlikte; nitelik olarak bir birinden ayrılmaktadır. Örneğin etik hususunda evrensel değerler olmak ile birlikte; ahlak hususunda, coğrafi kriterler ön plana çıkmaktadır. Bu kapsamda da, etik değerler konusunda, evrensel geçerlilik söz konusu olurken, ahlaki değerler, coğrafyalara göre değişebilmektedir. Söz gelimi, Kıbrıs Türk toplum yapısındaki ahlak anlayışı ile, Alman toplumundaki ahlak anlayışı farklılaşabilmektedir.

Badiou (2004: 41), aslında, etik diye bir şeyin olmadığını; sadece bir şeyin etiği (siyaset, bilim, sanat) olduğunu ileri sürmektedir. Pieper ise, etiğin sadece kuramsal bir bilimsel done olarak değil; pratikte de bilimsel olarak yapılabildiğini, genel etiğin, kaidelerinin belirli bir yaşam ve eylem üzerinde uygulama bulması ile, özel, somut hal aldığını ifade eder (Uzun, 2007: 26).

Diğer alanlar ile ilgili etik meselesi bir yana; çalışma konusu kapsamında bilişim etiğine değinilecek olursa, bilişim ortamları aracılığı ile yapılan tüm girişimlerde, uyulması gereken temel ilkeler bulunmaktadır. Bilgisayar Etik Enstitüsü (Computer Ethics Institute) tarafından belirlenen bilişim etiği ilkeleri şunlardır (İşman, 2016: 78; Okmeydan, 2017: 358-359):

1. Bilgisayar, insanlara zarar vermek için kullanılamaz,
2. Başka insanların bilgisayar çalışmaları karıştırılamaz,
3. Bilgisayar ortamında başka insanların dosyaları karıştırılamaz,
4. Bilgisayar, hırsızlık yapmak için kullanılamaz,
5. Bilgisayar, yalan bilgiyi yaymak için kullanılamaz,
6. Bedeli ödenmeyen (lisanssız) yazılım kopyalanamaz ve kullanılamaz,
7. Başka insanların bilgisayar kaynakları izin almadan kullanılamaz,
8. Başka insanların entelektüel bilgileri başkasına mal edilemez,
9. Kişi yazdığı programın sosyal hayata etkilerini dikkate almalıdır,
10. Kişi bilgisayarı, diğer insanları dikkate alarak ve saygı göstererek kullanmalıdır.

Bilişim etiği kuralları, bilişim hukuku kuralları gibi, riayet edilmesi zorunlu, yani, riayet edilmemesi halinde maddi yaptırım uygulanabilmesine olanak sağlayan kurallar olmamasına karşın; evrensel arenada, bahse konu ilkelere uyumlu hareket edilmesi gerektiği benimsenmiştir. Bu çerçevede, bilişim ortamlarındaki kullanıcıların, bu ilkeleri göz ardı etmemesi gerekmektedir.

D. Kişilik Hakları Kavramı

Kişilik hakları, maddi bedensel değerleri (kişinin hayatı, sağlığı ve vücut bütünlüğü), manevi hakları (dış hayatla, toplumla kurulan ilişkiler ile oluşan, kişinin onur ve saygınlığı, adı, fotoğrafı, özel hayatı) ve meslekiticari değerleri (profesyonel becerileri ile ilgili olarak söz konusu olan bilgilerini, faaliyetlerini) kapsamı altına almaktadır (Dolunay, 2018: 43).

Bilişim ortamları aracılığı ile, bireylerin vücut bütünlüğüne veya yaşamlarına karşı saldırıların gerçekleşmesi yönünde teşvik edici haber veyahut bilgilerin paylaşılması, bu duruma örnek gösterilebilmekte ve bu alanda önlem alınması gereken hususların başında gelmektedir.

İnfial yaratacak ve ilgili kişiye karşı önemli bir tepki doğuracak şekilde haberler/paylaşımlar yapılması, ilgili kişilerin onur ve saygınlığını zedelediği gibi; daha da öncelikli olarak, ilgili kişilerin yaşam hakkına aykırı girişimlerin oluşması için zemin hazırlayabilmektedir (Dolunay, 2018: 43).

Türk Hukukunda, 5237 sayılı Türk Ceza Kanunu md. 125 uyarınca, *"Bir kimseye, onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi…cezalandırılır…"*

Kıbrıs Türk Hukuku'nda ise, onur ve saygınlığa karşı işlenen suçlar "Zem ve Kadih" olarak adlandırılmakta; Fasıl 154, Ceza Yasası, "Zem ve Kadih" başlıklı altıncı bölüm kapsamında, md. 195/1'de, "*Bir kişiye herhangi ağır bir suç isnadında bulunmak ve onu genel nefrete, hakarete veya tiksindirilen duruma düşüren somut bir isnatta bulunulması zemmedici malzeme sayılır."* hükmüne yer verilmektedir.

Fasıl 154 md. 196 uyarınca, md. 195'de belirtilen türden bir yayını gerçekleştiren veyahut gerçekleştirme tehdidi ile, haksız kazanım elde etmeye çalışanlar cezalandırılır.

Diğer yandan, özel hayatın gizliliğini ihlal eden paylaşımlar düşünüldüğünde, belirtmek gerekir ki, özgürlükler gibi, özel hayatın gizliliği de ulusal ve uluslararası kapsamda koruma altına alınmaktadır. Buna istinaden özgür paylaşımlar ve özel hayatın gizliliği arasında denge kurulması gerekmektedir (Dolunay, 2018: 44).

Özel hayatın gizliliğini ihlal konusunda, bireyin en önemli manevi varlıkları, adı ve resmi olarak kabul edilmektedir. Kişinin izni olmaksızın resminin çekilmesi ve yayınlanması, adının haksız şekilde kullanılması, bu hususa örnek olarak gösterilebilir. AİHM kararlarında, kişi adı ve resmine yönelik saldırılar özel hayatın gizliliği hakkı kapsamında değerlendirilmektedir.

AİHS, "Özel ve aile hayatına saygı hakkı" başlıklı, 8. maddesi şu şekildedir:

"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir

Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

KKTC Anayasası'nın, "Özel Hayatın Gizliliği" başlıklı, 19. maddesi ise, şu şekildedir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli kovuşturmanın gerektirdiği istisnalar saklıdır."

Özel hayatın korunması, *kişinin giz alanı* ve *özel alanının* korunması üzerine kurulmaktadır.

Bu kavramın genel tanımının verilmekten kaçınıldığı görülmekte ve bu durumun, gelişen teknoloji ve değişim karşısında; bireyin korunabilmesini sağlamak hedefli olduğu kabul edilmektedir.

Özel hayatın gizliliğine bir istisna oluşturan örnek ise, *kamu yararıdır*. AİHS md. 8'de de belirtildiği gibi, kamu yararı söz konusu olması halinde, özel hayatın gizliliği sınırlı ölçüde ihlal edilebilmektedir. Kamuoyunun devamlı olarak dikkatini çeken kişiler ve geçici olarak dikkatini çeken kişiler arası bir ayrım söz konusudur (Dolunay, 2018: 45). Ancak her iki grup için de, özel hayatın gizliliği ile üstün kamu yararı kavramları arası denge kurulması gerekmektedir.

II. Siber Suçlar ve Kategorileri

Siber suçlar, *"bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış ya da, bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlar"* olarak tanımlanabilir (Bilişim Hukuku ve Bilişim Suçu, t.y.).

Bir başka tanıma göre siber suç, *"bilişim sistemlerinin yasadışı kullanımlarını tanımlamak için kullanılan ortak bir terim"*dir (Parker, 1980; Aydın, 1992).

Bilgisayar veya bilişim suçları hususunda genel kabul görmüş bir tanımlama söz konusu olmamakla birlikte; en geniş kabul gören tanımlama, Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris toplantısında yapılan tanımlamadır. Bu kapsamda bilişim suçları; *"bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde, gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"*tır (Özdemir vd., 2013: 17).

1960'lı yılların sonlarına kadar henüz yaygınlaşmamış bir kavram olan "siber suçlar"; gelişmeye başlayan bilgisayar teknolojileri ile birlikte, ilk kez 1966 yılında Minneapolis Tribune'da yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlığını taşıyan makale ile toplumsal olarak öğrenilmeye başlanmıştır (Aydın, 1992: 25).

Bu yayın ardından konuyu araştırmaya başlayan D. B. Parker tarafından, ilgili diğer olaylar da ortaya çıkarılmış (Parker, 1968) ve 1970 yılında, "Bilgisayar'ın Kötüye Kullanılması" adlı proje başlatılmıştır (Aydın, 1992: 113). Bu kapsamda, bilişim suçları, ilgili tarihten sonra, sıklıkla ele alınan bir husus olma niteliği kazanmıştır.

Siber suç tanımında; suçun nesnesi bir bilgisayardır (hack, kimlik avı, spam) ya da suç işlemek için bilgisayar bir araç olarak nitelendirilebilir (çocuk pornografisi, nefret suçları). Siber suçlular (cyber criminals), kişisel bilgilere, ticari sırlara erişmek veya interneti başka kötü niyetli amaçlarla bilgisayar teknolojisini kullanabilmektedir. Suçlular ayrıca bilgisayarları iletişim ve belge veya veri depolama için de kullanabilirler. Bu yasadışı faaliyetleri gerçekleştiren suçlular genellikle "hacker"lar olarak ifade edilirken; siber suç, bilgisayar suçu olarak da adlandırılabilmektedir (Siber suç, t.y.).

Siber suçlar, sayısı çok önemli olmayan ancak ona verilen tepki konusundaki fikir birlikteliğinin öneminin ortaya çıktığı hukuk temelli suçlardır (Shipley et al, 2014). Siber suçların sınıflanmasına ilişkin farklı yaklaşımlar söz konusudur. Bunlardan birincisi, "bilgisayar sistemleri vasıtasıyla işlenen klasik suçlar" ve "bilgisayar sistemlerine yönelik suçlar" (Karagülmez, 2011) yönündeyken; "kimlik hırsızlığı," "çevrim içi taciz", "yetkisiz erişim," "dolandırıcılık" ve "erişim gerektirmeyen siber suçlar" (Easttom ve Taylor, 2011) yönünde daha detaylı sınıflandırılmalar da yapılabilmektedir. Sınıflandırmalardaki farklılık, teknolojinin sürekli gelişiminin etkisi ile de yakından ilişkilidir (Hekim ve Başıbüyük, 2013: 137).

Elektronik ortamda gerçekleştirilen siber suçlara örnek olarak terörizm, kredi kartı saldırıları veyahut pornografi verilebilmektedir. Bu kapsamda, en yaygın siber suç "korsan erişim"ken; müstehcenlik ve pornografi başlığı altında yer alan "çocuk pornografisi", bir diğer yaygın siber suç kategorisidir.

Siber suçlara yönelik en bilinen örneklerden biri, ABD'den verilebilmektedir. ABD Dışişleri Eski Bakanı ve 2008 ile 2016 yıllarında yapılan seçimlerde başkan adayı olan Hillary Clinton gibi önemli siyasi isimler de dahil olmak üzere, pek çok kişinin şahsi e-mail postalarına gönderilen kötü amaçlı e-postalar aracılığıyla, bilgisayarlarına ve dolayısıyla da, özel bilgilerine izinsiz erişim sağlanmaya çalışılmıştır/çalışılmaktadır (Katz, 2017, Şubat 9).

Yine, bilgi hırsızlığı gibi özellikle toplumda belirli bir üne kavuşmuş bireylerin, "müstehcen" fotoğraflarının, video kayıtlarının, akıllı telefonlarından, bilgisayarlarından, "veri hırsızlığı" ile çalındığı ve yayınlandığı örnekler de mevcuttur (Strawser, 2015: 1102). Bu hususta mağduriyet yaşayanlar arasında, uluslararası ün sahibi ve ulusal ün sahibi pek çok sanatçı, siyasetçi bulunmaktadır. Aynı risk, belirtilen oranda üne kavuşmamış pek çok birey için de söz konusu olmaktadır.

Diğer yandan, gerek internet siteleri gerekse sosyal medya platformları aracılığı ile yapılan yayınlar/paylaşımlar da, hukuki ve etik yönden sorunlara neden olabilmektedir. Suçlayıcı, küçük düşürücü, eleştiri sınırını aşan çeşitli ifade kullanımları, bu hususta en çok göze çarpan durumların başında gelmektedir.

Örnekler artırılabilecekken; siber suçlar ile ilgili yapılan farklı gruplandırmalara da değinmek yerinde olacaktır. Bu kapsamda, ABD doktrinindeki görüş; ABD menşeli bir kurum olan McConnel International'ın görüşü; BM'nin yayınladığı ilgili rapor kapsamındaki görüş; AB ve BM Komisyonu'nun ortak raporundaki görüş; Avrupa Konseyi Siber Suç Sözleşmesi'ndeki yaklaşım ve İnternet Üst Kurulu'nun görüşü kısaca şu şekilde belirtilebilmektedir:

ABD doktrinindeki görüşe göre, suçlar 12 başlıkta ele alınmaktadır (Avşar & Öngören, 2009: 96; Altunok & Vural, 2011: 76):

1. Veriler veyahut hizmetlere yönelik hırsızlık,
2. Mülkiyete yönelik hırsızlık,
3. Giriş ihlali,
4. Veri sahtekârlığı,
5. Kişi hataları nedeniyle oluşan ihlal,
6. Gasp,
7. Sır aleyhine ihlal,
8. Sabotaj,
9. Maddi değerlere yönelik hırsızlık,
10. Vakalarda gerçekleştirilen sahtekârlık,
11. Bankamatik kartlarına ilişkin hırsızlık,
12. Manyetik kart şifreleri ile ilgili ihlal.

ABD menşeli bir kurum olan McConnel International'a göre ise, ilgili sınıflarlandırma şu şekildedir (Turhan, 2006: 39-42):

1. Veri suçları (Verilere müdahale, verilerin değiştirilmesi, veri hırsızlığı),
2. Ağ suçları (Ağ Engellemesi, ağ sabotajı),
3. Yetkisiz erişim suçları (Yetkisiz erişim, virüs yayılması),
4. İlgili suçlar (Bilgisayarla sahtekârlık, bilgisayarla dolandırıcılık).

1997 yılında Birleşmiş Milletler'in yayınladığı bir raporda ise siber suçlar şu şekildedir:

1. Bilgi İletişim Sistemleri (BİS)'ne veya BİS'ler üzerinden sunulan hizmetlere yetkisiz erişim,
2. Bilgisayar programlarını veya verilerini tahrip etme,
3. Bilgisayar yoluyla dolandırıcılık,
4. Bilgisayar yoluyla sahtecilik,
5. Yasayla korunmuş bilgisayar programlarını izinsiz olarak çoğaltma,
6. Diğer suçlar (Pornografik yayınlar, hakaret vb.).

AB ve BM Komisyonu ortak raporunda, husus şu şekilde ele alınmıştır (Altunok & Vural, 2011: 76-77):

1. Bilgisayar sistemleri ve servislerine yetkisiz erişim ve dinleme,
2. Bilgisayarların sabote edilmesi,
3. Bilgisayar kullanılarak dolandırıcılık,
4. Bilgisayar kullanılarak sahtecilik,
5. Kanunca korunan bir yazılımı izin almadan kullanma,
6. Kanuna aykırı yayınlar.

2004 yılında yürürlüğe giren Avrupa Konseyi (AK) Siber Suç Sözleşmesinde, siber suçlar;

1. Bilgisayar sistemlerine ve bu sistemlerde saklanan verilere yasa dışı erişim ve müdahale,
2. Bilgisayarların kötüye kullanımı,
3. Sahtecilik,
4. Dolandırıcılık,
5. Telif ve benzeri hakların ihlali,
6. Çocuk pornografisi olarak tanımlanmaktadır.

İnternet Üst Kurulu'nun yaklaşıma göre ise, siber suçlar şu başlıklar altında toplanmaktadır (Turhan, 2016: 42-46; Yıldız, 2015: 5-8):

1. BİS'lere Yetkisiz Erişim (Yetkisiz erişim; dinleme, hesap ihlali),
2. Bilgisayar sabotajı (Mantıksal; fiziksel bilgisayar sabotajı, bilgisayar yoluyla dolandırıcılık, banka kartı dolandırıcılığı, girdi/çıktı/program hileleri, iletişim servislerini haksız ve yetkisiz kullanım),
3. Bilgisayar yoluyla sahtecilik,
4. Bilgisayar yazılımlarının izinsiz kullanımı (Lisans sözleşmesine aykırı kullanım; çoğaltma; kiralama),
5. Diğer suçlar (Kişisel verilerin suiistimali, sahte kişilik oluşturma ve kişilik taklidi, yasadışı yayınlar).

Siber suçlarla ilgili, yukarıda hukuksal çerçevesi çizilen örgütlenme biçimlerine koşut olarak, geleneksel suçlar ile siber suçlar arasındaki farkların ele alınması; *dijital çağ* olarak adlandırılan çağımızda, bu konu üzerine ne kadar hassasiyetle eğinilmesi gerektiğini açıkça ortaya koymaktadır. Bu noktada, geleneksel yapı ile siber yapının genel bir karşılaştırmasına değinmek yerinde olacaktır.

Özellikler	**Geleneksel**	**Siber**
Oluşum Biçimi Açısından:	Aile İlişkilerine ve Ahlaki Değerlere Bağlı	Teknik Yetenek Gerektiren Uzmanlık Alanlarına Bağlı
Teknik Beceriler:	-	Çok Yüksek
İletişim:	Yüz yüze (ör. Tel)	Çevrimiçi (Web)
İtibar:	Kulaktan Kulağa	Çevrimiçi İnternet Forumları ile
Coğrafik Bölge:	Yerel Bölgeler	Uluslararası
Örgütlenme Yapısı:	Hiyerarşik	Belli Türden Yeteneklere Dayalı Yatay Yapı
Emir Yapısı:	Emir Zinciri	Esnek
Yapıdaki Değişiklik:	Yavaş Değişim	Olaylara Bağlı Olarak Gelişen Değişim
Güdü:	Kâra Bağlı	Kâr ve Kaynaklara Bağlı
Becerilerin Bilginin ve Yeteneklerin Kaynağı:	Çıraklık İlişkisine Bağlı	Kendi Kendine Öğrenmeye Bağlı

Tablo 1. Geleneksel Gruplarla Siber Grupların Karşılaştırması (Smith, 2015: 106)

Geleneksel yapıda, oluşum açısından, aile ilişkileri ve ahlaki değerler ön plana çıkarken; siber yapıda teknik yetenek gerektiren uzmanlık alanları ön plana çıkmaktadır. Yine iletişimsel açıdan geleneksel yapı daha ziyade yüz yüze iletişim temeline dayanırken; siber yapıda, çevrimiçi niteliği bulunmaktadır. Yapısal değişiklikler geleneksel yapıda yavaşken; siber yapıda, olaylara bağlı olarak daha hızlı bir değişim sergilemektedir (Bkz. Tablo 1).

Öte yandan, siber suçların insanı makineleştirdiği ve kimi özelliklerini yitirdiği yönündeki iddialar da, özellikle Nijerya temelinde ele aldıkları çalışmalarında tartışılmış olup; Adomi ve Igun (2008)'a göre, söz konusu makineleşmenin altı faktörü vardır:

1. internete kolay erişim,

2. internet tarafından sunulan anonimlik,

3. internet üzerinden e-posta yazılımlarının/sitelerinin kullanılabilirliği (bireysel e-posta adresi edinmek için),

4. yasayı çiğnemenin ağırlığının cehaleti,

5. insanların zor ekonomik koşulları,

6. yetersiz kolluk-hukuki uygulama.

Bu altı maddeye kısaca değinilecek olursa; günümüzde, internete oldukça kolay bir şekilde, her yerden ve herkes tarafından erişim sağlanabilmektedir. İnternet, anonimleşen bir yapı özelliği taşımakta; herkes bireysel e-posta adresleri edinebilmektedir. Diğer yandan, ekonomik krizlerin giderek arttığı günümüz koşullarında, bireyler daha zor ekonomik koşullarda yaşamakta; yine yasalar ihlal edilirken söz konusu olması beklenen "ağırlık" (bu durumdan kaçınılması beklentisi), cehalet perdesinin ardında kalmakta ve tüm bunlara yetersiz kalan kolluk denetimi ve yine yeterli olmayan hukuki uygulama eklenince, durum içerisinden çıkılmaz bir hal almaktadır.

Farklı alt başlıklara ayrılabilen ve farklı sonuçlar doğurabilen bir husus olan siber suçların, kategorileri ve etkileri, tüm coğrafyalar gibi, çalışmanın coğrafik olarak odağı olan KKTC açısından da, yüksek önem arz ettiğini vurgulamak yerinde olacaktır. Çünkü "insan" unsurunun olduğu her coğrafyada, "suç" ve buna bağlı sorunlar ve bu sorunların doğurabileceği sonuçlar söz konusu olmaktadır. Hukuk, düzensiz insan davranışlarını konu ve düzenleme altına aldığı için; bilişim alanındaki düzensiz insan davranışlarının da, yine hukuk – bilişim hukuku tarafından denetim altına alınması gerekliliği önemli bir gerçektir.

III. Türk ve AB Hukukunun Bilişim Düzenlemelerine Genel Bakış

Çalışmanın temel sorunsalı ışığında, KKTC'deki bilişim yasasının henüz tasarı aşamasında olması nedeniyle hem Türk hem de Avrupa Birliği Hukuku'nun bilişim düzenlemeleri ile ilgili gelişmeleri başlıkları ve amaçları ile dahi ortaya koymanın, bu konuda ciddi katkılar sağlayacağı açıktır.

Kara Avrupası hukuk sisteminde olmasına karşın, Türk Hukuku, gerek Türkiye ile olan yakın ilişkiler, gerekse, hukuk sistemi açısından benzerlikler çerçevesinde örnek gösterilebilmektedir. Diğer yandan, Kıbrıs sorununda, nihai bir çözüme ulaşılması durumunda, Kıbrıs'ta kurulacak bir ortak devlette kurucu ortak olacak Kıbrıs Türk toplumu için, AB hukuki düzenlemeleri de örnek teşkil etmektedir.

KKTC açısından husus temelde kişilik hakkı ihlalleri kapsamında ele alınacak olmasına karşın, gelecekte artabilecek tüm siber suçların önlenmesine ve/veya cezalandırılmasına ilişkin yürürlüğe girecek bilişim yasası için örnek teşkil edebilecek AB Hukuku'nun ilgili düzenlemelerinin temelleri, aşağıdaki kaynaklara dayanmaktadır:

1. Yeşil Kitap (1987): Telekomünikasyon ve Bilişim hizmet ve araçları ile ilgili olarak, ortak iç pazar oluşturulmasını sağlamak,

2. Avrupa Birliği Düzenleyici Çerçevesi (1998): Bilişim alanına ilişkin, sektörel bazda eşitlik ve liberalleşmeyi sağlamak,

3. Avrupa Parlamentosu ve Konsey'in İlgili Direktifi (1999): E-imza ile ilgili olarak, Avrupa Topluluğu'nun genel yaklaşımının düzenleme altına alınmasını sağlamak,

4. E-Avrupa Hareketi (2000): Lizbon Zirvesi'nden hareketle, ucuz, hızlı, güvenli ve insan becerilerine yatırım yapılmasını sağlamak,

5. “E-Avrupa+ Hareket Planı” (2001): 2001 Göteborg Zirvesinde gerçekleşen onaydan hareketle, önceki E-Avrupa Hareketi’nin ışığında, AB’ye üye ve AB üyeliğine aday ülkeler bilişim alanındaki “oyuncuların” işbirliğini sağlamak,

6. “Avrupa Siber Suçlar Konvansiyonu” (2001): Strasbourg’ta onayı ile birlikte,

a. Toplumsal bazda, siber suçlara yönelik koruma sağlanması amacı ile gerekli görülen yasal düzenlemelerin kabul edilmesi ve uluslararası ölçüde ortak çalışmaların arttırılması yöntemiyle, ortak bir müeyyide uygulama politikasının öncelikli şekilde onaylanması,

b. Bilgisayar ağları ve elektronik bilgilerin, müeyyide gerektiren suç nitelikli davranışlarda kullanımını ve bu nevi hususlara ilişkin delillerin söz konusu ağlarda gizlenmesini ve/veya aktarılmasını engellemek,

c. Bilgisayar sistemleri, ağlar ve verilere ilişkin gizlilik, doğruluk ve ulaşılabilirliğe dair zarar verecek girişimlerin; diğer yandan, tüm bunların art niyetle kullanımının engellenmesi,

d. (c) bendinden sayılan suç niteliğindeki girişimlerin engellenmesi için, cezai yaptırımların sağlanması ve bu girişimlerin, gerek ulusal, gerekse uluslararası çapta, soruşturulması ve yargı organlarına taşınmasını daha kolay bir şekle getirmek amaçlarını taşımaktadır (Nizam, t.y.).

Temel olarak Common Law (Ortak Hukuk) Sisteminin etkisindeki KKTC’ye, son dönem yasalaşma hareketleri hususunda örnek teşkil eden Kara Avrupası Hukuk Sistemi etkisindeki Türk Hukuku’nda ise, bilişim ve bilişim suçları ile ilgili önem arz eden düzenlemelerin başlıkları ve amaçları şu şekildedir:

1. 5237 sayılı Türk Ceza Kanunu (2004): “Kişi hak ve özgürlükleri ile kamu düzen ve güvenliğini, hukuk devletini korumayı…suç işlenmesini önlemeyi…”,

2. 5070 sayılı elektronik imza kanunu (2004): “Elektronik imzanın, hukukî ve teknik yönleri ile kullanımına ilişkin esaslarını düzenleme altına alınmasını sağlamak”,

3. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007): “İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenleme altına almak”,

4. 5809 sayılı Elektronik Haberleşme Kanunu (2008): “elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesini sağlamak”.

5. 6698 sayılı Kişisel Verilerin Korunması Kanunu (2016): “kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek”.

IV. Kişilik Haklarını İhlal Eden Siber Suçlar Bağlamında KKTC

Çalışmada, bilişim suçları, tüm alt kategorileri ile birlikte ele alınarak, genel olarak açıklanmaya çalışılmıştır. Çünkü tüm alt kategoriler konunun önemini vurgulayıcı niteliktedir. Ancak, KKTC örneği açısından, siber suçlar, temelde, kişilik haklarını zedeleyici girişimler yönünden ele alınacaktır.

Bu yaklaşımın temel nedeni, Türkiye ve Avrupa ülkelerine oranla küçük ve devletin tanınmaması çerçevesinde nispeten kapalı bir topluma sahip olduğu söylenebilecek KKTC’de, siber suçlar bağlamında, kişilik hakkı ihlalleri dışındaki kategorilerin, henüz anlamlı ölçüde örneğe sahip olmamasıdır.

Bu çerçevede, öncelikli olarak, bilişim hukuku bağlamında, KKTC’de söz konusu olan yasal boşluğa değinilecek, ardından ise, uygulamadaki durum ele alınacaktır.

A. Yasal Boşluk ve Diğer Çekinceler

Araştırmanın temel problematiği ışığında, yinelemekte fayda vardır ki, KKTC'de henüz yürürlüğe girmiş bir bilişim yasası bulunmamaktadır. Bilişim yasasına uzun bir dönemden beri duyulan gereklilik çerçevesinde, KKTC Cumhuriyet Meclisi'nin Hukuk ve Siyasi İşler Komitesi tarafından Bilişim Suçları Yasa Tasarısı (Bilişim Suçları Yasa Tasarısı, 2018) hazırlığına başlanmış ve bir taslak metin ortaya çıkarılmıştır.

Ancak, duyulan acil ihtiyaç nedeniyle ilgili taslak metnin KKTC Cumhuriyet Meclisi Genel Kurulu'nda ivedilikle görüşülmesi kararı alınmasına rağmen, tasarı uzun süredir bekletilmekte; Meclis Genel Kurulu'nun gündemine alınmamaktadır.

AB'ye üye ülkelerde, Türkiye'de ve dünyanın pek çok ülkesinde yukarıdaki veya yukarıdaki benzeri hukuki düzenlemeler/girişimler söz konusuyken ve hatta teknolojideki sürekli değişimler karşısında sık sık geliştirilirken; ileride birleşik Kıbrıs'ın kurucu üyesi olarak Avrupa Birliği'ne girme çabasını sürdüren KKTC'de, uluslararası standartlarda bir bilişim yasasının yürürlüğe girmesi gerekliliği yadsınamaz bir gerçektir.

KKTC'nin mevcut sosyal yoğunlaşma içerisinde artan bilişim suçları hala tasarı halinde olan düzenlemenin ivedilikle sonuçlandırılması gerekliliğini ortaya koymaktadır. Ancak, bilhassa hukukçular tarafından getirilen eleştirilerin başında, "yasanın bir araç olarak kullanılarak, bireylerin 'fişleneceği'" gelmektedir (Bilişim Suçlarının Önüne Geçmek İçin Yasalar Şart, 2017, Mart 19).

Bu eleştiriler arasında, devletin ve polisin "orantısız" bir güce sahip olacağı, yargıç denetiminin ortadan kaldırılacağı, özel fotoğraf, mesaj ve girilen sitelerin suçla ilgisi olmasa dahi, depolanacağı şeklindekiler, oldukça dikkat çekicidir. Bu noktada önemle hatırlatılması gerekir ki, *"İnternet sanayi devrimi boyutlarında bir gelişmeyi temsil etmektedir. Bütün dünya, internetin başı çektiği bilgi toplumuna geçişin sancılarını çekiyor... İnternet yaşamın tüm boyutlarını etkilemekte, sınırları yok etmektedir... İnternet tüm dünyaya açılan bir pencere bir sokaktır"* (Akgül, 2011).

İletişim alanında "büyük sıçrayış" olarak nitelendirilebilecek internet ile birlikte; insan ilişkileri hususunda yasal düzenlemeler getiren hukukun, insanlar arası iletişim araçlarını ve dolayısıyla da interneti, bir takım normlar ile düzenleme altına almaması düşünülemez bir husustur. Gerek düzen sağlanması, gerekse, internet kullanıcılarının güvenliğinin sağlanması açısından önemli hukuki düzenlemeler yapılmak ile birlikte; diğer yandan da, yasalar eliyle, internet kullanımının, daha geniş bir ifadeyle, internet kullanımı ile ilgili iletişim özgürlüğünün "kısıtlanmaması" gerekliliğini vurgulamakta fayda bulunmaktadır. Bu kapsamda, yasa tasarısının, "siber-güvenlik" sağlama amacından sapma ihtimali göz ardı edilmemelidir:

Bilişim Suçları Yasa Tasarısı, 26 madde ve md. 24 altında yer alan 4 geçici maddeden oluşmaktadır. Bu çerçevede, md. 1 ile yasanın kısa adı, md. 2 ile yasada yer alan ifadelerin tefsiri (tanımlanması), md. 3 ile de yasanın amaç ve kapsamına yer verilmektedir.

Buna göre, yasanın temel amacı ve kapsamı: *"bilişim sistemlerinin, ağlarının ve verilerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetler ile bu sistem, ağ ve verilerin kötü amaçlı kullanımının ve suç işlenmesinin engellenmesi için uygulanacak usul ve esasların düzenlenmesi; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarının düzenlenmesi; tüm bu faaliyetler kapsamında suç oluşturan eylemler ve cezai niteliklerinin belirlenmesi, söz konusu suçlarla etkili biçimde mücadele edilmesine ve suçların kovuşturulmasına ilişkin usul ve esasların düzenlenmesidir."*.

Tasarı'nın 2. kısmında, "bilişim sistemlerinin ve verilerinin gizliliğine, bütünlüğüne ve kullanımına ilişkin suç ve cezalar"a düzenleme altına alınmakta; bu çerçevede, bilişim sistemine veya bilişim verisine hukuka aykırı erişim, bilişim sistemine veya bilişim verisinin iletimine hukuka aykırı müdahale, bilişim sistemini engelleme, bilişim sistemini veya verisini bozma, yok etme veya değiştirme, cihazların ve verinin kötüye kullanımına ilişkin hususlara yer verilmekte; 3. kısımda ise, "bilişim sistemleriyle bağlantılı suçlar" düzenleme altına alınarak, bilişim verisi üzerinde sahtecilik, bilişim sistemi üzerinden dolandırıcılık, bilişim sistemleri

kullanılarak kredi kartları ve/veya banka kartlarında sahtecilik yapma, çocuk pornografisi ile bağlantılı suçlar'a ilişkin hususlara yer verilmektedir.

Tasarının 4. kısmında "fikri haklara; yazılım ve veri tabanı üzerindeki haklara yönelik ihlaller" ile ilgili kurallara, 5. kısmında "bilişim sistemlerinde ve yazılımlarda arama, kopyalama ve el koyma" ile ilgili kurallara, 6. kısmında ise, "elektronik haberleşme ortamında yapılan yayınların düzenlenmesi içerik, yer, erişim ve toplu kullanım sağlayıcılarının yükümlülük ve sorumlulukları"na yer verilmektedir.

Yasa tasarısının detaylarına değinilmeden önce ifade edilen, "siber güvenlik sağlama amacından sapma" tehlikesi ise, tasarının 7. kısmında düzenleme altına alınan "erişimin engellenmesi kararı ve yerine getirilmesi ile içeriğin yayından kaldırılmasına ilişkin kurallar"a istinaden söz konusu olabilecektir. "Erişimin engellenmesi kararı ve yerine getirilmesi", "erişimin engellenmesi kararının içeriği, yerine getirilmesi ve sonuçları", ve "içeriğin yayından kaldırılması" yan başlıklarının yer aldığı maddeler (20-22) olumlu bir bakış açısıyla değerlendirildiğinde, çalışmada ifade edilen sosyolojik sorun niteliğindeki hususlara, *bir nebze de olsa* karşılık çözüm üretmeye çalışıldığı düşünülebilecek olsa da; daha ziyade, "keyfi olarak" erişimin engellenmesi ve içeriğin yayından kaldırılmasının söz konusu olabileceği şüphesi ön plana çıkmaktadır. Yine, sonraki kısımda (kısım 8) yer alan, idari para cezaları, idari yaptırımlar ve tüzük yapma yetkisi hususlarından, özellikle ceza ve yaptırımlar içerisindeki, *24 saat içerisinde içeriği kaldırmayan yer sağlayıcıların yetkilerini 'iptal edebilme'* hususu, oldukça geniş kapsamlı ve 'tehlikeli' boyutlara ulaşabilecek sonuçlar doğurma potansiyeli taşıyan yapıdadır.

Diğer yandan, erişimin engellenmesi ve yayının kaldırılması hususları düzenleme altına alınırken; yinelemek yerinde olacak ki, çalışmada odaklanıldığı üzere, sosyolojik bir sorun haline gelen, kişilik hakları ihlal edilerek yapılan yayınlara istinaden, "kişilik hakkı", "özel hayatın gizliliği" gibi yüksek önemi olan hak ve ilkelere, detaylı olarak düzenlenmesi bir yana, *kavram olarak dahi* yasa tasarısında yer verilmemesi, önemli eksiklikler bulunduğunun somut örneği olarak kabul edilebilecektir.

Tasarı henüz yürürlüğe girmeden, diğer bir ifade ile yasalaşmadan önce, gerekli değişikliklerin ve eklemelerin, akademisyenler ve alan uzmanlarınca yapılacak öneriler ışığında gerçekleştirilmesi veyahut yeni bir bilişim yasa tasarısının hazırlanması yerinde olacaktır.

B. Uygulamadaki Durum

Yasal boşluğun varlığı çerçevesinde, KKTC'de bilişim ortamlarındaki kullanıcılar, cezalandırılma korkusu ya da diğer bir ifade ile caydırıcılık olmaksızın, başka kişilerin kişisel bilgilerini yayınlayabilmekte, kişilik haklarını zedeleyici küçük düşürücü ifadeler kullanabilmekte, gerçeği yansıtmayan paylaşım ve yayınlar yapabilmektedir. Bu durum, kabul edilebilir ve sürdürebilir bir yapıya işaret etmemektedir.

Diğer yandan, henüz Bilişim Suçları Yasa Tasarısı KKTC Cumhuriyet Meclisi Genel Kurulu'nda oylanıp yürürlüğe girmemiş olmasına karşın; yakın tarihte de yargı kararı ile yegane örneği söz konusu olan bir hususta bahsetmek yerinde olacaktır. Cumhuriyetçi Türk Partisi Milletvekili Doğuş Derya'nın, 2014 yılının Aralık ayı sonlarında gerçekleşen KKTC Cumhuriyet Meclisi Genel Kurulu'ndaki bütçe görüşmeleri sırasında sarf ettiği bir takım sözlere istinaden, Bertan Zaroğlu (bir sonraki dönemde Yeniden Doğuş Partisi Milletvekili olmuştur) sosyal medya (kişisel Facebook hesabı) üzerinden, Derya'ya yönelik *"Doğuş'um Bebeğim…"* ifadesi ile başlayan ve cinsel içerikte bir takım argo ifadeler ile devam eden bir durum güncellemesi paylaşmıştır. Buna karşın Derya, 2015 yılında, Zaroğlu aleyhine davacı olurken; yargılama süreci yaklaşık olarak iki yıl sürmüştür (Cinsel Tacizden Yargılanacaklar, 2017, Ekim 30).

Dava neticesinde mahkeme, yürürlükte bir bilişim yasası olmaması nedeniyle, ilgili sosyal medya paylaşımını, Fasıl 148 Haksız Fiiller Yasası kapsamında ele almış; Zemmedici Malzemenin Yayımlanması yan başlıklı md. 18 kapsamında, sosyal medya/internet aracılığı ile yapılan yayınlar sınırlayıcı olarak sayılmamış olsa da, ilgili paylaşımı "herhangi bir kişi tarafından bir diğer kişiye yönelik zarar verici yayın yapma" olarak

değerlendirmiş ve bu çerçevede de ilgili fiili Zem ve Kadih (Sövme ve Hakaret Etme) olarak nitelendirerek, Zaroğlu'nun suçlu olduğuna hükmetmiştir ('Hakaret' Cezasız Kalmadı, 2017, Kasım 7).

Bu karar, emsal niteliğinde olup; aynı zamanda, KKTC'de bu hususta verilmiş ilk mahkeme kararı olma niteliğini bulunmaktadır. İlgili alanda bu önemli karar sonrasında, bu çalışmanın yayına hazırlandığı sürece değin, KKTC'de mahkemelerce benzer nitelikte bir karar verilmemiştir.

Ancak belirtmek gerekir ki, bu durum, ilgili karar ardından sosyal medya ortamında suçlayıcı ve/veya küçük düşürücü paylaşımlarda bulunulmadığına ve/veya örneğin bazı internet haber siteleri gibi iletişim etiği ile bağlı olmasına karşın kişilik haklarına aykırı şekilde bireyleri henüz şüpheliyken hükümlü ilan eden platformlarda, "zem ve kadih" içeren yayınlar yapılmadığına değil; ilgili girişimlerin, maalesef ki halen cezasız kaldığına işaret etmektedir.

Sonuç ve Öneriler

KKTC'nin küçük bir toplum olmasından mütevellit, özellikle bireylere yönelik oluşan bilişim suçları, fikri mülkiyet ve devlet ile kurum-kuruluşlara yönelik gerçekleşen bilişim suçlarına oranla daha egemen bir noktada yer almaktadır. Sosyal medya hesaplarının da bireyciliği destekleyen ve tetikleyen yapısı, bu yöndeki suçların giderek artacağı ve bilişim yasası ivedilikle yürürlüğe girmezse, bu hususların kontrol altında tutulamayacağı gerçeğini açıkça ortaya koymaktadır.

Bu konuda en büyük sorumluluk KKTC Cumhuriyet Meclisi'ne düşmektedir. Her ne kadar tasarı halkla paylaşılsa da; yasa tasarısının bilişim alanındaki suçları cezalandırıcı değil, önleyici ve caydırıcı bir nitelikte olması büyük önem taşımaktadır. Özellikle AB Hukuku açısından yaklaşıldığında, sivil hak ve özgürlükler bağlamında gerekli görülen yasal düzenlemelerin dikkate alınması önem arz etmekle birlikte; söz konusu hak ve özgürlüklerin devletin çıkarını ve bütünlüğünü de tehlikeye düşürmeyecek şekilde tanzim edilmesi gerekmektedir.

Hızla artan bilişim kullanımının ve bilgisayar okur yazarlığının, bilgi okuryazarlığına dönüştürülmesinde bilişim suçları yasasının önleyici bir rol alması değil, tetikleyici bir güç olması gerekmektedir. Bunun için gözetim toplumu öncül ve argümanlarından uzak, lakin, bilginin etkin ve verimli bir şekilde teknoloji aracılığıyla bireyler tarafından kullanımını da destekleyen bir şekilde düzenleme yapılması, tasarının yasallaşmasında büyük önemi taşımaktadır.

Çalışmada değinilen AB Hukuku düzenlemeleri ve Türk Hukuku düzenlemeleri çerçevesinde, AB Hukuku'nun özgürleştirici potansiyeli çerçevesinde göz ardı edilmemesi gerekliliği ile birlikte, Türk Hukuku'na ilişkin düzenlemelerin örnek alınması gerektiği sonucuna ulaşılmıştır. Bu durumun temel sebebi olarak, KKTC'de son dönem yürürlüğe giren kanunların, Türk Hukuku'ndaki düzenlemelere daha benzer nitelik taşımasından kaynaklanmaktadır.

KKTC'de, yürürlükte bir bilişim yasasının olmaması; iletişimde dijital çağ olarak adlandırılan içerisinde bulunduğumuz dönemde, önemli sorunlara yol açmaktadır. Bilişim ortamında işlenen suçlar, "kanunsuz suç ve ceza olmaz" prensibi çerçevesinde cezasız kalmakta; suçlulara cezai yaptırım uygulanamamaktadır.

Bu hususta yegane istisnai örnek, çalışmada ele alınan Doğuş Derya-Bertan Zaroğlu davasına ilişkin olsa da, bu durum yasal açıdan sürdürülebilir değildir. Bu kapsamda da, bilişim ortamında işlenen siber suçların her zaman cezalandırılabileceğini ifade etmek mümkün görülememekte, diğer bir ifade ile, caydırıcı bir yapının söz konusu olmadığını ortaya koymaktadır. Bahse konu sorunların temel çözümü, ilgili yasal boşluğun doldurulmasından geçmektedir.

Yasal boşluğun doldurulmasındaki temel görev, belirtildiği üzere KKTC Cumhuriyet Meclisi'nin olmak ile birlikte; bu süreç içerisinde, ilgisi açısından, üniversitelerin iletişim, bilgi-belge yönetimi ve hukuk fakülte ve bölümlerinde görev alan uzmanlardan destek alınması önem arz etmektedir.

Yine, çeşitli sivil toplum ve meslek kuruluşları da, bu noktada sorumluluk alarak aktif görev üstlenmeli; ilgili yasa tasarısı ile, toplumsal ve bireysel bazda özgürlükler ve sınırları arasındaki hassas dengenin sağlanması noktasında denetleyici olmalıdır.

Kaynakça / References

'Hakaret' Cezasız Kalmadı, (2017, Kasım 7). Erişim adresi: http://www.yeniduzen.com/hakaret-cezasiz-kalmadi-95748h.html

Adomi, E. E. & Igun, E. S. (2008) "Combating cyber crime in Nigeria", The Electronic Library, 26(5), 716-725.

Akgül, M. (2011, Temmuz 19). İnternet Yasakları, Bilgi Toplumu ve Demokrasi. Erişim adresi: http://blog.akgul.web.tr/

Altunok, E. & Vural, F. A. (2011). Bilişim Suçları, Denetişim, 8, 74-84.

Arora, Bhavna, A. (2016). Exploring and analyzing Internet Crimes and Their Behaviours, Perspectives in Science, 8, 540-542.

Avşar, B. Z. & Öngören, G. (2009). Bilişim Hukuku. İstanbul: Türkiye Bankalar Birliği.

Aybay, A. vd. (2013). Hukuka Giriş, İstanbul: Bilgi Üniversitesi Yayınları.

Aydın, E. (1992). Bilişim Suçları ve Hukukuna Giriş, Ankara: Doruk Yayınevi

Badiou, A. (2004). Etik: Kötülük Kavrayışı Üzerine Bir Deneme (Çev. Tuncay Birkan). İstanbul: Metis.

Bilişim (t.y.). Erişim Adresi: http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.58d149d2501ed3.78053307

Bilişim (t.y.). Erişim Adresi: http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.58d149d2501ed3.78053307

Bilişim Hukuku ve Bilişim Suçu (t.y.). http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html

Bilişim Suçlarının Önüne Geçmek İçin Yasalar Şart (2017, Mart 19). Erişim Adresi: http://www.kibrisgazeteci.com/bilisim-suclarinin-onune-gecmek-icin-yasalar-sart-h6506.html

Bilişim Suçları Yasa Tasarısı (2018, Haziran 6). Erişim adresi: http://www.cm.gov.nc.tr/Yasalar/bilisim.pdf

Bilişim ve Soyal Medya Hukuku (t.y.). Erişim Adresi: https://www.batur.av.tr/calisma-alanlari/bilisim-hukuku/page/10?lang=kn

Cinsel Tacizden Yargılanacaklar (2017, Ekim 30). Erişim adresi: http://www.kibris724.com/cinsel-tacizden-yargilanacaklar-95674h.htm

Cybercrime, (ty). Erişim adresi: https://www.techopedia.com/definition/2387/cybercrime

Denizci, Ö. M. (2009). Bilişim Toplumu Bağlamında İnternet Olgusu ve Sosyopsikolojik Etkileri, Marmara İletişim Dergisi, 15, 47-63.

Dolunay, A. (2018). Dijital Çağda Yasal ve Etik Kodlar Çerçevesinde Basın Hak ve Özgürlükleri: KKTC Örneği. İstanbul: On İki Levha Yayıncılık.

Dolunay, A. & Keçeci, G. (2017). Kıbrıs Türk Hukukunda İletişim Etiği Çerçevesinde Telif Hakkı Sorunları, Journal of Historty Culture and Art Research, 6(4), 1396-1409.

Easttom, C. & Taylor, J. (2011). Computer crime investigation and the law. Course Technology.

Girgin, A. (2000). Yazılı Basında Haber ve Habercilik Etik'i. İstanbul: İnkılâp.

Gönen, S.; Ulus, U. İ. & Yılmaz, Y. N. (2016). Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, International Journal of Informatics Technologies, 9(3), 229-236.

Hekim, H. & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158.

Işıktaç, Y. (1998). Bir Hukuk Tanımı Vermenin Zorunluluğu, Prof.Dr.Vecdi ARAL'a Armağan, Kocaeli Üniversitesi Hukuk Fakültesi Yayını, 127-132.

İşman, A. (2016). Bilgisayar Destekli Eğitim Etiği, (Edit: Aytekin İşman, Hatice Ferhan Odabaşı ve Buket Akkoyunlu). Eğitim Teknolojileri Okumaları 2016, Ankara: Salmat Basım Yayıncılık.

Karagülmez, A. (2011). Bilişim suçları ve soruşturma-kovuşturma evreleri, Ankara: Seçkin.

Katz, M. David, (2017, Şubat 9). The Corporatization of Cyber Crime. Erişim Adresi: http://ww2.cfo.com/cyber-security-technology/2017/02/corporatization-cyber-crime/

Köksal, A. (1981). Bilişim Terimleri Sözlüğü, S. 476, Ankara: Türk Dil Kurumu Yayınları.

Moressi, E. (2006). Haber Etiği Ahlaki Gazeteciliğin Kuruluşu ve Eleştirisi (Çev. Fırat Genç). Ankara: Dost Kitabevi.

Nizam, F. (t.y.). Avrupa Birliği Bilişim Politikası ve Türkiye'nin Uyumu. Erişim Adresi: https://goo.gl/BmSj4Q

Okmedyan-Bitirim, S. (2017). Yeni İletişim Teknolojilerini Sorgulamak: Etik, Güvenlik ve Mahremiyetin Kesiştiği Nokta, Gümüşhane Üniversitesi İletişim Fakültesi Dergisi, 5(1), 347-372.

Özdemir, S. (2013). Elazığ'da Üniversite ve Lisede Öğrenim Gören Bilgisayar Bölümü Öğrencilerinin Adli Bilişim Suçlarına Yaklaşımları, E-Journal of New World Sciences Academy, 8(3), 16-25.

Özsunay, E. (1979). Medeni Hukuka Giriş. İstanbul: Güryay Yayıncılık.

Pamukoğlu, K & Ocak, M. (t.y.). Bilişim Teknolojilerinin Devletin Etkinliğindeki Rolü

ve İnternet Üzerinden Satış Uygulaması, Erişim Adresi: https://s3.amazonaws.com/academia.edu.documents/34271953/bilisim_teknolojilerinin_devlet_etkinligindeki_rolu.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1546683973&Signature=SrThvmuSlbUSyAyIR60ttF5dcM4%3D&response-content-disposition=inline%3B%20filename%3DBilisim_teknolojilerinin_devlet_etkinlig.pdf

Parker, D. B. (1976). Crime by Computer. New York: Charles Scribner's Sons

Sağsan, M. (2002). Sanal Alemde Hak Arayışları: İnternet'te Telif Hakkı Sorununun Boyutlarına Kısa Bir Bakış, Düşünceler, 58, 23-31.

Shipley, T. G.; Bowker, A. & Selsy, N. (2014). Investigating Internet Crimes. Elsevier, New York, NY.

Smith, G. S. (2015). Management models for international cybercrimes, Journal of Financial Crime, 22(1), 104-125.

Strawser, J. B. & Donald, J. J. (2015). Cyber Security and User Responsibility: Surprising Normative Differences, Procedia Manufacturing, 3, 1101-1108.

Turhan, O. (2016). Bilgisayar Ağları ile ilgili Suçlar (Siber Suçlar), T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara.

Uzun, R. (2007). İletişim Etiği Sorunlar ve Sorumluluklar, Ankara: Gazi Universitesi İletişim Fakültesi Kütüphanesi 40. Yıl Yayınları.

What is Law? (t.y.). Black's Law Dictionary, Online 2.nd Edt. Erişim Adresi: http://thelawdictionary.org/law/

World Population Prospects: The 2017 Revision (2017, Haziran 21). Erişim Adresi: https://www.un.org/development/desa/publications/world-population-prospects-the-2017-revision.html

Yıldız, M. (2015). Siber Suçlar ve Kurum Güvenliği, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ankara.