Bu proje Avrupa Birliği tarafından finanse edilmektedir.

INTRA

National Programme for Turkey 2014 – 2020

Instrument for Pre-Accession Assistance II

Hâkim ve Savcı Adaylarının Staj Verimliliğinin ve Etkinliğinin Arttırılması Projesi

Sözleşme No.: TR2015/RL/03/A3.5-01

Referans No.: EuropeAid/162288/ID/ACT/TR

SİBER SUÇLAR EĞİTİM MODÜLÜ

Hazırlayan Uzmanlar:

Jose DE LA MATA AMAYA, Kıdemli Hâkim

Pedro BARCELO OBRADOR, Kıdemli Hâkim

Bu proje, Türkiye Cumhuriyeti ve İspanya Krallığı arasında yürütülen bir eşleştirme ortaklığıdır.

Bu proje Avrupa Birliği tarından
finanse edilmektedir.

İÇİNDEKİLER

GİRİŞ

Teknolojik gelişmeler, bilgi ve iletişim teknolojileri kapsamında işlenen veya bunlar tarafından desteklenen suçların ortaya çıkmasına neden olmuştur. Bu suçların, yasal varlıkları çok farklı mahiyetlerde etkileyebilecek önemli ölçüde zararlı bir potansiyeli vardır.

Bilgi ve iletişim teknolojileri, suçun planlanması ve işlenmesinin farklı aşamalarına imkan sağlamakta ve suçun etkilerinin ulusal sınırların içinde veya sınırlarımızın ötesinde farklı ve uzak yerlerde gerçekleştirilebilmesini veya gösterilebilmesini sağlamaktadır.

Bu fiillerin özel mahiyeti, fiillerin araştırılmasına karmaşıklık unsurları eklemektedir. Elektronik deliller bu fiillerin araştırılmasında önemli bir rol oynamaktadır.

Bu olgu sadece bilişim suçlarının kendisiyle değil aynı zamanda bilgisayar sistemlerinde veya dijital ortamlarda saklanmış delilleri olabilecek herhangi bir suçla ilgilidir.

Bu olgunun boyutu bizi fiziki dünyada geliştirilen bir araştırmayı yönetenlerden tamamen farklı yaklaşımlarla ve değişkenlerle karşılaşılan yeni bir senaryoyla karşı karşıya bırakmaktadır.

Bu teknolojik araçların kişisel bilgileri toplayabilmesi ve sistematik hale getirebilmesi ile üçüncü taraflarla iletişime yön verebilmesi ve iletişimi artırabilmesi, haberleşmenin gizliliği hakkının korunmasına ilişkin anayasal yetkiyi belirlemektedir. Özel hayatın gizliliği ve kişisel verilerin korunması, bu cihazlarda saklanan verileri ve içeriği kapsayacak şekilde genişletilmelidir. Bu, söz konusu fiillerin soruşturmasında belirleyici olacaktır. Çünkü spesifik bir davada imkan tanıyan gerekliliklerin temel hakları etkileyen bir tedbirle ilgili mutabakata varılması için gerekli olup olmadığının ağırlıklandırmasını ve verilerin kişisel verilerin korunması düzenlemelerine uygun olarak korunması ve güvenliğinin sağlanması için tedbirler alınmasını gerektirecektir. Bu tür bilgilerin güvenliğinin sağlanmasına ve bu bilgilere orantılılık kriterleri uyarınca ayrı ayrı değerlendirilen vakalarda erişilebilmesinin sağlanmasına yönelik denetim ve tedbirlerin belirlenmesi, özel hayatın gizliliği ve/veya kişisel verilerin korunmasının etkilenmesi riskini büyük ölçüde azaltmaktadır.

Kısaca siber suçlar, küresel bir olguya ortak bir yanıt verme ihtiyacı doğurmaktadır. Bu olguda, bölgesel ve fiziksel sınırlar tamamen önemsizdir ve suç teşkil eden eylemlerin etkisini gösterme hızı ve suçun delilinin kırılganlığı ve hassasiyeti, ilgili Devletler arasında güçlü ve birbiriyle uyumlu hızlı eylemler gerektirmektedir.

Bu yeni senaryoda, iç, maddi ve ceza muhakemesi kanunlarının teknolojik gelişmelerden doğan yeni durumlara uyarlanması yeterli değildir. Aksine, bu soruşturmaların etkililiği ve başarısı için diğer Devletlerle normatif uyumlaştırmayı hedefleyen ek çalışmalar yapılması şarttır. Uluslararası iş birliği, farklı ülkelerin maddi hukuk ve usul hukuklarının uyumlaştırılması ve araştırma araçlarının homojen hale getirilmesi, öncelikli ihtiyaç haline gelmiştir.

Asli ceza açısından suç oluşturan fiilin tanımının yapılması, ceza soruşturmalarında iş birlikçi bağlantılar kurmak ve uluslararası hukuki yardım talep etmek ve almak için gereklidir. Her iki ülkede suç olarak sayma ilkesi, birçok ulus üstü iş birliği belgesinin temelini oluşturmaktadır ve benzer şekilde tipik fiillerin tanımı bunun için gereklidir.

Usul açısından tüm Taraf Devletler tarafından üstlenilecek bir görevle birlikte elektronik verilerin soruşturmanın yürütüldüğü diğer ülkelerin yetkili makamları tarafından kullanımı için tutulması ve naklinin sağlanması için ortak kriterleri belirlemektedir.

23.11.2001 tarihinde yayımlanan ve Budapeşte Sözleşmesi olarak bilinen Siber Suçlar Sözleşmesi, bu alandaki uluslararası referans belgesidir.

Sözleşme, Avrupa Konseyi'ne üye olan 46 ülke tarafından (Rusya Federasyonu hariç tüm ülkeler) imzalanmıştır ve 44 ülke sözleşmeyi onaylamıştır (Rusya Federasyonu'na ek olarak İrlanda ve İsveç de Sözleşmeyi onaylamamıştır). Avrupa Konseyi çerçevesi dışında 21 ülke Sözleşmeyi onaylamıştır.

Ancak bu olgu çok daha kapsamlıdır. Aslında Avrupa Konseyi tarafından sunulan bilgilere göre ("Siber Suçlar Mevzuatının Küresel Durumu"):

"Bu yıl Şubat ayının sonunda Birleşmiş Milletler'in 106 üyesi (veya %55'i) bilişim suçlarını ve bilgisayar aracılığıyla işlenen suçların yasa dışı olduğunu beyan etmek için iç mevzuatlarını büyük ölçüde Siber Suçlara ilişkin Budapeşte Sözleşmesi'yle uyumlu hale getirmiştir. Özellikle Afrika'da iyi bir ilerleme kaydedilmiştir. Gittikçe artan sayıda Devlet, siber suçları soruşturmak ve spesifik ceza soruşturmalarında gerekli verileri toplamak için yetki vermiştir. Bu olumlu gelişmelere rağmen ceza adaleti uygulayıcıları tarafından mevzuatın uygulanmasını sağlamak için daha fazla kapasite geliştirilmesi gerekmektedir".

Burada amaç, siber suçlara karşı Avrupa Konseyi'nin cezai konularda iş birliğine ilişkin çerçevesi kapsamında mevcut Sözleşmeleri destekleyerek hem maddi hukuk hem ceza muhakemesi hukukunu ele alan etkili bir yanıt verilmesini sağlayacak bağlayıcı bir belge hazırlanmasıdır.

Bu, siber suçlara karşı ortak bir ceza politikası belirlenmesi için küresel çağrıda bulunan ve temeli belirleyen yasal belgedir. Budapeşte Sözleşmesi, özellikle Devletler arasındaki yoğunlaşan iş birliğinin ortaya çıkarılmasına dayanarak tasarlanmıştır. Çünkü bu, sanal gerçekliğin küresel olarak yasa dışı amaçlar için kullanılmasıyla ortaya çıkan soruna karşı tek etkili çözümdür.

Sözleşmenin amacı, Girişte vurgulanmaktadır: bilgisayar sistemleri ve verilerle ilgili soruşturmaların ve suçlara ilişkin elektronik delillerin sağlanmasında etkililiğinin sağlanması amacıyla "toplumun siber suçlara karşı korunması için gerekli mevzuatın kabul edilmesi ve uluslararası iş birliğinin geliştirilmesi" için ortak bir cezai politika belirlenmesidir.

Buna üç amaç hedeflenerek ulaşılmaktadır:

1. Her ülkenin maddi ceza hukuku ve bilişim suçlarına ilişkin ilgili hükümleri uyarınca suç unsurlarının uyumlaştırılması,

2. Her ülkenin ceza muhakemesi kanunu uyarınca bu tür suçların ve bilgisayar sistemleri veya elektronik formattaki diğer delillerin kullanılmasıyla işlenen diğer suçların soruşturulması ve kovuşturulması için gerekli yetkilerin belirlenmesi,

3. Hızlı ve etkili bir uluslararası iş birliği rejimi oluşturulması.

BUDAPEŞTE SÖZLEŞMESİ

2.1.- MADDİ CEZA HUKUKU

Mevzuat uyumlaştırması, siber suçlara karşı ortak bir yanıt vermek için gereklidir ve maddi hukuk bağlamında uyumlaştırma, tipik benzer fiillerin tanımlanması ve cezalandırılması yoluyla gerçekleştirilmelidir.

Sözleşmenin 2-13. maddeleri; bilgisayarlarla ilgili suçlar ve taraf devletler tarafından belirlenecek bilgisayar kullanımıyla ilgili suçlar (fakat taraf devletlere basit mahiyetteki kabahatlerin hariç tutulması imkanı sağlamaktadır), yasa dışı erişim suçlarının tanımlanması, yasa dışı müdahale, veri bütünlüğüne saldırılar, sistem bütünlüğüne saldırılar, cihazların kötüye kullanımı, bilgisayarla ilişkili sahtecilik fiilleri, bilgisayarla ilişkili dolandırıcılık, çocuk pornografisiyle ilgili suçlar, telif haklarının

ve benzer hakların ihlaline ilişkin suçlar, yükümlülük ve yaptırım biçimleri ve alınacak tedbirlerle ilgili hükümler içermektedir.

Sözleşme, asgari fikir birliğini temsil eden ayrıntılı bir listedir ve bu listenin, her tarafın ulusal kanunlarında yapılabilecek veya Sözleşmeye yapılacak değişikliklerle kapsamının genişletilmesini hariç tutmamaktadır. Sözleşme yayımlandıktan kısa bir süre sonra Kısım 2'nin birinci bölümünde yer alan davranışların ağlar aracılığıyla işlenen ırkçılık ve yabancı düşmanlığı davranışlarını kapsaması için Ek Protokol hazırlanmıştır.

A) Verilerin ve bilgisayar sistemlerinin gizliliği, bütünlüğü ve mevcudiyetine karşı suçlar

Bu cezai suçlar, bilgisayar sistemlerinin veya verilerin gizliliğinin, bütünlüğünün ve mevcudiyetinin korunmasını ve ağların tasarımında veya meşru ve ortak işletimler veya ticari uygulamalarda var olan meşru ve ortak faaliyetlere suçlu muamele yapılmamasını amaçlamaktadır.

A.1) Yasa Dışı Erişim

"Erişim", bir bilgisayar sisteminin (donanım, parçalar, yüklenen sistemde depolanmış veriler, dizinler, trafik verileri ve içerikle ilgili veriler) tamamına veya bir kısmına girilmesidir.

"Erişim", kamu telekomünikasyon şebekeleri aracılığıyla bağlı olan başka bir bilgisayar sistemine veya LAN (yerel alan ağı) veya bir kurumun kurum içi ağı gibi aynı ağdaki bir bilgisayar sistemine girilmesini içermektedir.

İzinsiz girişin, yani "hackleme", "şifre kırma" veya "bilgisayara izinsiz giriş"in prensipte yasa dışı olması gerekmektedir. Bu, sistemlerin ve verilerin meşru kullanıcıları açısından engel oluşturabilir ve yeniden oluşturma için yüksek masraflarla birlikte değişiklik veya imhaya neden olabilir. Bu tür izinsiz girişler, gizli verilere (şifreler, hedeflenen sistemle ilgili bilgiler dahil olmak üzere) ve sırlara, ödeme yapmadan erişim sağlayabilir veya hatta hackerlerin bilgisayarla ilgili dolandırıcılık veya sahtecilik gibi bilgisayarla ilgili daha tehlikeli suçlar işlemelerini teşvik edebilir.

Suç eyleminin "haksız surette" işlenmesi gerekmektedir. Bu ifadeye ilişkin yukarıda verilen açıklamaya ek olarak, sistemin veya sistemin bir kısmının sahibi veya başka bir hak sahibi tarafından yetki verilen erişimin suç olarak kabul edilmediği anlamına gelmektedir (örneğin, ilgili bilgisayar sisteminin izinli bir şekilde test edilmesi veya korunması amacıyla). Ayrıca kamuoyunun ücretsiz ve açık erişimine izin veren bir bilgisayar sistemine erişim suç olarak kabul edilmemektedir çünkü bu erişim "haklı surette" yapılmaktadır.

Tarafların kendi ulusal mevzuatlarının, ihlalin bilgisayar verilerinin elde edilmesi amacıyla veya sahtekarlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesini veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilgili olarak yapılmasını gerektirebileceği belirtilmektedir (İspanya hukukunda olduğu gibi).

A.2) Yasa Dışı müdahale

Bu hüküm, verilerin iletiminde özel hayatın gizliliğinin korunmasını amaçlamaktadır. Suç, kişiler arasındaki sözlü telefon görüşmelerinin geleneksel olarak dinlenmesi ve kaydedilmesi şeklinde haberleşmenin gizliliğinin ihlal edilmesiyle aynıdır. Haberleşmenin gizliliği hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde güvence altına alınmıştır.

Cezai suç, bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında teknik yöntemler kullanarak bir bilgisayar sistemine, sisteminde veya sistem içinde veri iletimine haksız surette dahil olunmasıdır. Bu suç, bilgisayar verilerinin "kamuya açık olmayan" iletimleri için geçerlidir. "Kamuya açık olmayan" ifadesi, iletilen verilerin değil iletim (haberleşme) sürecinin mahiyetini belirtmektedir.

"Kamuya açık olmayan" ifadesi aslında kamusal ağlar ile gerçekleştirilen haberleşmeleri hariç bırakmamaktadır. İletimler kamusal ağlarla yapılmış olsa bile bunların saklı tutulmasını veya hangi mekanizmaların kurulduğuyla ilgili olarak öyle ya da böyle gizliliğin sağlanması ve üçüncü tarafların bu bilgiye sahip olmasının engellenmesini amaçlamasını içermektedir.

İkinci olarak, işletim sırasında bir bilgisayardan yayılabilecek elektromanyetik dalgaları olan bir bilgi sisteminin elektromanyetik dalgalarından elde edilebilecek bilgisayar verileri de bu hükümde korunmaktadır. Bu tür yayılımlar, "veri" olarak değerlendirilmemektedir. Ancak bu tür yayılımlardan veriler yeniden oluşturulabilmektedir.

"Teknik yöntemler" kullanarak müdahalede bulunulması, haberleşmenin içeriğinin dinlenilmesi, izlenmesi veya gözetimi, bilgisayar sistemine erişim ve sistemin kullanılmasıyla ya doğrudan ya da elektronik gizli dinleme veya dinleme cihazlarının kullanımıyla dolaylı olarak veri içeriğinin tedarikiyle ilgilidir. Müdahale, kaydı da içerebilir. Teknik yöntemler, iletim hatlarına monte edilen teknik cihazları ve kablosuz haberleşmeleri bir araya getirmek ve kaydetmek için kullanılan cihazları içermektedir. Bunlar; yazılım, şifreler ve kodların kullanımını içerebilir. Teknik yöntem kullanımı gerekliliği, aşırı suçlamadan kaçınmaya yönelik kısıtlayıcı bir özelliktir.

Bilgisayar verilerinin iletimi şeklindeki haberleşme, tek bir bilgisayar sistemi içinde (örneğin, merkezi işlem biriminden (CPU) ekrana veya yazıcıya veri akışı), aynı kişiye ait iki bilgisayar sistemi arasında, birbiriyle iletişim kuran iki bilgisayar arasında veya bir bilgisayar ve bir kişi arasında (örneğin, klavye aracılığıyla) gerçekleşebilir.

Cezai yükümlülük olması için yasadışı müdahalenin "kasıtlı olarak" ve "haksız surette" yapılması gerekmektedir. Örneğin, müdahalede bulunan kişinin müdahale etmeye hakkı varsa, iletime katılan kişilerin yönlendirmeleri veya yetkilendirmesiyle hareket ediyorsa (katılımcıların mutabık kaldığı izinli bir şekilde test etme veya koruma faaliyetleri dahil olmak üzere) veya gözetime ulusal güvenliğin veya soruşturmayı yürüten makamların suçları tespit etmesinin yararına yasal olarak izin verilmişse, bu eylem gerekçelendirilebilir. Ayrıca "çerezler"in çalıştırılması gibi ortak ticari uygulamaların kullanılmasının, "haksız surette" bir müdahale olmadığı için bu şekilde suç teşkil etmeyi amaçlamadığı anlaşılmıştır.

A.3) Verilere müdahale

Bu hükmün amacı, maddi mallara karşı kasıtlı zarara karşı sağlanana benzer olarak bilgisayar verileri ve bilgisayar programlarına koruma sağlamaktır. Burada korunan hukuki yarar, saklanan bilgisayar verilerinin veya bilgisayar programlarının bütünlüğü ve doğru bir şekilde işleyişi veya kullanımıdır.

Cezai suç, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınmasıdır.

Örtüşen eylemler olan "tahrip etme" ve "bozma", özellikle verilerin ve programların bütünlüğünün veya bilgi içeriğinin olumsuz bir şekilde değiştirilmesiyle ilgilidir.

Verilerin "silinmesi," maddi bir şeyin imha edilmesiyle eşdeğerdir. Verileri imha etmekte ve tanınmaz hale getirmektedir. Bilgisayar verilerinin erişilemez kılınması, bilgisayara veya verilerin depolandığı veri taşıyıcıya erişimi olan kişinin verilere erişimini önleyen veya yok eden herhangi bir eylem anlamına gelmektedir.

"Değiştirme", mevcut verilerin değiştirilmesi anlamına gelmektedir.

Bu nedenle, virüs ve Truva atı gibi zararlı kod ilave etmek, bu fıkra kapsamında yer almaktadır çünkü bunlar verilerin değiştirilmesiyle sonuçlanmaktadır.

Bu madde, tamamen veya kısmen bilgisayar parçalarının imha edilmesini ve etkilenen parçanın yok edilmesi, silinmesi veya kısmen silinmesiyle ve bu parçaların ilk kapsamının veya içeriğinin değişimini içeren yeni verilerin dahil edilmesiyle meydana gelebilecek bu parçaların değiştirilmesini içerenler dahil olmak üzere bilgisayar parçalarını etkileme olasılığı olan neredeyse bütün fiilleri kapsamaktadır.

Yukarıda belirtilen fiiller ancak "haksız surette" yapılırsa cezalandırılabilir. Buna ek olarak, failin "kasıtlı olarak" fiilde bulunmuş olması gerekmektedir.

Sözleşmenin bu maddesi, Taraflara bu maddede tanımlanan fiili, söz konusu fiilin ciddi zararla sonuçlanması şartına bağlama hakkını saklı tutmasına imkan tanımaktadır. Ciddi zararı neyin oluşturduğunun yorumlanması, her ülkenin yasama organının takdirindedir.

A.4) Sistemlere müdahale

Bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak suretiyle bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilidir. Burada korunan hukuki yarar, bilgisayar veya telekomünikasyon sistemlerinin işletimcileri ve kullanıcılarının bunların doğru bir şekilde işlemesini sağlayabilmesine yönelik yararıdır.

"Engelleme" ifadesi, bilgisayar sisteminin düzgün işleyişini engelleyen fiillere atıfta bulunmaktadır. Engelleme; yeni veriler ilave ederek, verileri başka yerlere ileterek, tahrip ederek, silerek, değiştirerek veya erişilemez kılarak gerçekleşmelidir.

Engelleme fiili ayrıca "ciddi" (örneğin, "hizmeti engelleme" saldırıları, sistemin işleyişini engelleyen veya büyük ölçüde yavaşlatan virüsler gibi zararlı kodlar oluşturan programlar veya sistemin haberleşme işlevlerini engellemek için bir alıcıya çok sayıda elektronik posta gönderen programlar suretiyle) ve "haksız surette" olması ve "kasıtlı olarak" yapılması gerekmektedir.

Taraflar, kendi mevzuatları kapsamında idari veya cezai yaptırımı gerekçelendiren zarar eşiğine ulaşmak için sistemin işleyişinin kısmen veya tamamen, geçici olarak veya daimi olarak ne ölçüde engellenmesi gerektiğini belirlemek zorundadır.

A.5) Cihazların kötüye kullanımı

Bu, bilgisayar sistemleri veya verilerinin gizliliği, bütünlüğü ve erişilebilirliğine karşı yukarıda tanımlanan suçların işlenmesi amacıyla kötüye kullanılacak belli cihazlar veya erişim verileriyle ilgili olarak belli yasa dışı fiillerin kasıtlı olarak işlendiği ayrı ve bağımsız bir cezai suçtur.

Bu suçların işlenmesi genellikle erişim araçlarına ("hacker araçları") veya diğer araçlara sahip olunmasını gerektirdiği için bu araçların üretimi ve dağıtımında bir tür karaborsa oluşturulmasına neden olabilecek cezai suç amaçlarıyla bunların elde edilmesine yönelik güçlü bir güdü vardır. Bu tehlikelerle daha etkili bir şekilde mücadele etmek için ceza kanununda potansiyel olarak tehlikeli fiillerin kaynağında yasaklanması gerekmektedir.

Bu nedenle, taraf devletlerin cezai yükümlülük oluşturması için belli sayıda cihazın elde bulundurulmasını gerektirebileceği öngörülmektedir.

Yasa dışı fiile konu olan cihaz ve araçlar şunlar olabilir:

1) Bilgisayar programı dahil olmak üzere, tanımlanan fiillerden herhangi birinin yapılması amacıyla tasarlanmış veya bu amaca uygun hale getirilmiş cihazlar. Bunların üretimi, satışı, kullanım amacıyla tedariki, dağıtımı veya başka surette elde edilmesi veya elde bulundurulması cezai yükümlülük doğurmaktadır.

"Bilgisayar programı"nın dahil edilmesi, virüs programları veya bilgisayar sistemlerine erişim sağlamak için tasarlanmış veya uyarlanmış programlar gibi verileri değiştirmek veya hatta imha etmek ya da sistemlerin işleyişine müdahale etmek için tasarlanan programlara atıfta bulunmaktadır.

2) Bir bilgisayar sisteminin tamamına veya bir kısmına erişim sağlayan bilgisayar şifreleri, erişim kodları veya benzeri veriler. Bunların üretimi, satışı, kullanım amacıyla tedariki, dağıtımı veya başka surette elde edilmesi veya elde bulundurulması cezai yükümlülük doğurmaktadır.

Bu fiilin kasıtlı olarak ve haksız surette yapılması gerekmektedir.

İzinli bir şekilde test etme veya bir bilgisayar sisteminin korunması için oluşturulan bu araçlar, bu hüküm kapsamında yer almamaktadır. Örneğin, test cihazları ("şifre kırma cihazları") ve bilgi teknolojisi ürünlerinin güvenilirliğini kontrol etmek veya sistem güvenliğini test etmek için endüstri tarafından tasarlanan ağ analizi cihazları, meşru amaçlar için üretilmektedir.

B) Bilgisayarlarla ilişkili suçlar

Bu suçlar, bir bilgisayar sisteminin kullanılması suretiyle sıklıkla işlenen adi suçlardır.

B.1) Bilgisayarlarla ilişkili sahtecilik

Bu maddenin amacı, somut evraklarda sahteciliğe paralel bir suç oluşturmaktır.

Bilgisayarlarla ilişkili sahtecilik, saklanan verilerin hukuki işlemler sırasında verilerde yer alan bilgilerin orijinalliğine bağlı olan farklı bir delil değeri kazanması için söz konusu verilerin izinsiz bir şekilde oluşturulması veya değiştirilmesini içermektedir ve hile yoluyla işlenir. Burada korunan hukuki yarar, hukuki ilişkiler açısından sonuçları olabilecek elektronik verilerin güvenliği ve güvenilirliğidir ve bu fiillerin suç teşkil etmesinin sebebi, delil değeri olan söz konusu verilerin kötüye kullanılmasının, üçüncü bir taraf yanlış yönlendirilirse geleneksel sahtecilik fiillerinde olduğu gibi benzer ciddi sonuçlara neden olabilmesidir.

Taraflar, cezai yükümlülüğün ortaya çıkmasını hile veya benzeri bir dolandırıcılık niyetinin olması şartına bağlayabilirler.

B.2) Bilgisayarlarla ilişkili dolandırıcılık

Bu suçlar büyük ölçüde yanlış verilerin bilgisayara koyulduğu veya veri işleme süresince program işlemeleri ve diğer müdahaleler suretiyle veri eklenmesinden oluşmaktadır. Bu maddenin amacı, bir mülkiyetin yasa dışı olarak devrini gerçekleştirme amacıyla veri işleme süresince usule aykırı herhangi bir fiilin suç teşkil etmesini sağlamaktır.

Dolandırıcılık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla yapılan bu fiil, aşağıda belirtilenler suretiyle bir mülkiyetin kaybına sebep olmaktadır:

(a) bilgisayar verilerine herhangi bir şekilde yeni veriler eklemek, verileri herhangi bir şekilde değiştirmek, silmek veya erişilemez kılmak,
(b) bir bilgisayar veya sistemin işleyişine herhangi bir şekilde müdahale etmek.

Bilgisayarlarla ilişkili dolandırıcılık fiilleri, doğrudan ekonomik kayba veya bir başkasının mülkiyetinin kaybına neden olursa ve fail, kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla fiilde bulunursa suç teşkil eder.

Suçun “kasıtlı olarak” işlenmesi gerekmektedir. Genel kasıt unsuru, bir başkasının mülkiyetinin kaybına neden olan bilgisayarla ilgili kötüye kullanım veya müdahaleye atıfta bulunmaktadır. Bu suç

ayrıca dolandırıcılık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacı içermektedir.

C) İçerikle ilişkili suçlar

C.1) Çocuk pornografisiyle ilişkili suçlar

Bu hükümler, bilgisayar sistemlerinin çocuklara karşı cinsel suçlar işlenmesinde kullanılmasının daha etkili bir şekilde kısıtlanması amacıyla ceza kanunu hükümlerini modern hale getirmek suretiyle, çocukların cinsel istismara karşı korunması dahil olmak üzere, çocuklara yönelik koruyucu tedbirlerin güçlendirilmesini amaçlamaktadır.

Çocuk pornografisinin elektronik ortamda üretimi, elde bulundurulması ve dağıtılmasının çeşitli yönlerini suç olarak tanımlamaktadır. Birçok devlet halihazırda çocuk pornografisinin geleneksel bir şekilde üretimi ve fiziki dağıtımını suç olarak tanımlamaktadır. Ancak bu tür materyallerin ticaretinin yapılması için başlıca araç olarak internetin gittikçe daha fazla kullanılmasıyla birlikte bu yeni cinsel istismar biçimiyle ve çocukların tehlike altında olmasıyla mücadele etmek için uluslararası bir yasal belgede spesifik hükümlerin yer almasının şart olduğu düşünülmüştür.

Çocukların cinsel istismarına karşı tepkilere ilişkin bu uluslararası endişe, 1989 Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme ve 25 Mayıs 2000 tarihli Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisiyle ilgili İhtiyari Protokolünün kabul edilmesiyle Birleşmiş Milletler düzeyinde halihazırda açık hale gelmiştir. Bu Sözleşmede, çocuk pornografisi kavramı, "çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesi" olarak tanımlanmıştır.

Budapeşte Sözleşmesi'nde, aşağıdaki fiiller kasıtlı olarak ve haksız surette yapıldığında cezai suç olarak tanımlanmaktadır:

a. bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek,
b. bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak veya çocuk pornografisine erişim sağlamak. "Sunmak" ifadesi ile çocuk pornografisi almak için başkalarından talepte bulunulmasının kapsanması amaçlanmaktadır. Materyali sunan kişinin bunu gerçekten sunabilmesi anlamına gelmektedir. "Erişim sağlamak" ifadesi ile çocuk pornografisinin başkalarının kullanımı için internet ortamına koyulmasının kapsanması amaçlanmaktadır.

c. bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ya da yaymak. "Dağıtım", materyalin gerçekten dağıtımı anlamına gelmektedir.
d. kişinin bir bilgisayar sistemi üzerinden kendisi ya da başkası için çocuk pornografisi temin etmesi,
e. bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak.

"Çocuk pornografisi" terimi, aşağıdakileri görsel anlamda teşhir eden pornografik malzemeler anlamına gelmektedir:

a. cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı,
b. cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı,
c. cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren görüntüler.

"Cinsel anlamda müstehcen bir eylem", en azından gerçekte veya taklit suretiyle a) aynı cinsiyetten veya karşı cinsiyetten reşit olmayan kişiler arasında veya bir yetişkin ve reşit olmayan bir kişi arasında cinsel uzuv-cinsel uzuv yoluyla, ağız-cinsel uzuv yoluyla veya ağız-anüs yoluyla cinsel birleşme, b) hayvanlarla cinsel ilişki, c) mastürbasyon, d) cinsel bağlamda sadistik veya mazoşistik istismar veya e) reşit olmayan bir kişinin cinsel uzuvlarının veya cinsel uzvunun çevresinin cinsel amaç güden şekilde gösterilmesini içermektedir. Tasvir edilen fiilin gerçekte mi yoksa taklit suretiyle mi olduğu önemli değildir.

Sanatsal, tıbbi, bilimsel veya benzer niteliğe sahip malzemeler, pornografik olarak değerlendirilmeyebilir. Görsel tasvir, bilgisayar disketinde veya görsel resme dönüşebilen diğer elektronik saklama araçlarında saklanan verileri içermektedir.

"Reşit olmayan kişi" terimi, 18 yaşından küçük kişiler anlamına gelmektedir. Ancak taraflardan herhangi biri, daha düşük bir yaş sınırı belirleyebilir. Söz konusu yaş sınırı 16'dan az olmayacaktır.

D) Telif haklarının ve benzer hakların ihlaline ilişkin suçlar

Telif hakları başta olmak üzere, fikri mülkiyet haklarının ihlali, internet üzerinde en yaygın şekilde işlenen suçlar arasındadır. Bu suçlar, hem telif hakkı sahipleri hem de bilgisayar ağlarıyla profesyonel bir şekilde çalışan kişiler için endişeye sebep olmaktadır. Korunan eserlerin, telif hakkı sahibinin onayı olmadan internet üzerinde kopyasının yapılması ve dağıtılması oldukça yaygındır. Bu tür korunan eserler; edebi eserleri, fotoğraf eserlerini, müzik eserlerini, görsel-işitsel eserleri ve diğer

eserleri içermektedir. Dijital teknoloji nedeniyle kopyaların izinsiz bir şekilde kolaylıkla yapılabilmesi ve elektronik ağlar bağlamında eserlerin kopyalanması ve dağıtılmasının düzeyi, ceza kanunu yaptırımlarına hükümler eklenmesini ve bu alandaki uluslararası iş birliğinin genişletilmesini gerekli kılmıştır.

Taraflardan her biri, maddede sayılan anlaşmalardan kaynaklanan ve bazen komşu haklar olarak anılan telif hakları ve benzer hakların ihlallerini, bu ihlaller bir bilgisayar sistemi üzerinden ve ticari ölçekte yapıldığında suç olarak tanımlamak zorundadır.

Taraflardan her birinin bu ihlalleri suç olarak tanımlama yükümlülüğü bulunurken bu ihlallerin kendi ulusal mevzuatlarında nasıl tanımlanacağı devletten devlete değişiklik gösterebilmektedir. Ancak Sözleşme kapsamındaki suçla ilgili yükümlülükler, yalnızca Sözleşmede açık bir şekilde ele alınan (madde 10) fikri mülkiyet ihlallerini kapsamaktadır. Bu nedenle, patent veya ticari marka ihlallerini hariç bırakmaktadır.

Devletler, bu fiilleri, kendi ulusal telif hakları kanunundaki tanım ve bu alanda kabul edilen anlaşmalar uyarınca tanımlamaları için teşvik edilmektedir.

Telif haklarıyla ilgili olarak şu anlaşmalara atıfta bulunulmaktadır: Edebiyat ve Sanat Eserlerinin Korunmasına ilişkin Bern Sözleşmesi'nde Değişiklik Yapan 24 Temmuz 1971 tarihli Paris Metni, Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması ve Dünya Fikri Mülkiyet Örgütü (WIPO) Telif Hakları Antlaşması. 2. fıkrada atıfta bulunulan uluslararası yasal belgeler, İcracı Sanatçılar, Fonogram Yapımcıları ve Yayın Kuruluşlarının Korunmasına Dair Uluslararası Sözleşme (Roma Sözleşmesi), Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması ve WIPO İcralar ve Fonogramlar Antlaşması'dır.

Suç oranlarıyla ilgili olarak Sözleşme yetersiz kalmıştır. Şahit olduğumuz olağandışı teknolojik gelişmeler doğrultusunda, bilişim suçları alanında başka bir öngörülemez fiil ortaya çıkmıştır ve Sözleşme kapsamında yer almamıştır. Aslında bu belge kabul edildikten kısa bir süre sora 28 Ocak 2003 tarihinde Avrupa Konseyi, Sözleşmedeki bu tür fiillere ilişkin hükümlerin kapsamını genişleterek, bilgisayar sistemleri üzerinden yapılan ırkçı veya yabancı düşmanlığı niteliğinde eylemlerin suç olarak tanımlanmasına ilişkin Ek Protokolü hazırlamıştır.

2.2.- USUL TEDBİRLERİ

Elektronik verilerin toplanması, tutulması ve iletilmesinin siber suç alanına giren suçlara karşı diğer ülkelerde yürütülen soruşturmalarda bu verilerin olası kullanımlarını sağlayan kurallar

doğrultusunda yapılmasını sağlamak amacıyla tüm taraf devletler tarafından kabul edilecek ortak kriterler belirlemenin önemi tartışılmazdır.

Sözleşmenin 14. maddesinde, taraflara bu kısımda belirtilen yetki ve usullerin esas alınması suretiyle bazı ceza soruşturmalarında ve işlemlerin yapılabilmesi için gerekli olabilecek yasama tedbirlerinin ve diğer tedbirlerinin alınmasını zorunlu kılan Kısım 1 Bölüm 2'de yer alan usul kurallarının kapsamı tanımlanmaktadır.

Bunlar, bir bilgisayar sistemi üzerinden işlenen herhangi bir suça ve ceza yargılamasında elektronik delil elde edilmesine uygulanan tedbirlerdir. Kısaca, açıklayıcı raporda belirtildiği üzere, dijital formattaki veya başka bir elektronik formattaki bilgilerin, suçun mahiyetine bakılmaksızın, ceza duruşmasında mahkeme nezdinde delil olarak kullanılabilmesi olasılığının tarafların kendi ulusal mevzuatına dahil edilmesi suretiyle, elektronik formattaki delilin Sözleşmede belirtilen kurallar uyarınca alınabilmesinin ve güvence altına alınabilmesinin sağlanması meselesidir.

Sözleşmede yer alan usul kuralları, şu hususlarda uygulanacaktır:

a) Soruşturma altında olan suç, Sözleşmede sıralanan suçlardan biriyse.
b) Suç, bir bilgisayar sistemi üzerinden işlenmişse herhangi bir suçun soruşturmasında.
c) Davadaki delil herhangi bir şekilde dijital kayıtta tutuluyorsa, herhangi bir soruşturmada delil toplarken.

Çoğu durumda, soruşturmanın yürütüldüğü ülkenin yargı yetkisinin dışında bulunan iletişim ağlarının operatörlerine ait sunuculardaki saklanan elektronik delillerin alınmasının şart olduğu bu tür soruşturmaların mahiyeti, farklı devletler arasında ortak eylem kriterleri olmadan teknolojik araştırmaların büyük bir kısmının mümkün olmayacağının belirtilmesini mümkün kılmaktadır. Bu ortak düzenleyici mevzuat, soruşturmanın iyi bir şekilde sonuçlanmasını sağlamanın tek yoludur.

Yeni teknolojiler üzerinden veya yeni teknolojilerin desteğiyle işlenen suçların soruşturması, elektronik delillerin muhafaza edilmesine ve böylece bunlara erişim sağlanmasına dayalı olmak zorundadır. Benzer şekilde, elektronik delillerin talep eden devlette takip edilen usule dahil edilmesi amacıyla da şarttır. Delillerin sağlanması, korunması ve iletilmesi sürecinde, delilin geçerliliğiyle ilgili herhangi bir şüpheye yer bırakmamak için gerekli teminatlar gözlenmektedir.

Sözleşmede atıfta bulunulan tedbirler şu şekildedir:

A. Saklanan bilgisayar verilerinin korunmasının kolaylaştırılması (madde 16)

Geleneksel deliller, olay yerinde uzun bir süre kalır ancak dijital veriler (elektronik deliller), kaybolduğunda veya tahrip edildiğinde geri getirilmesi zordur. Örneğin, trafik verileri bir suçun failinin kimliğinin belirlenmesinde oldukça yardımcı olmaktadır. Ancak bu tür bilgiler, veri saklama mevzuatı uygulanmıyorsa sistematik olarak erişilebilir değildir.

Bu tedbir, ulusal yetkili makamların, belli bir ceza soruşturması veya yargılamasıyla bağlantılı olarak saklanan bilgisayar verilerinin korunmasının kolaylaştırılması yönünde talimat verebilmesini veya söz konusu hususu benzer şekilde temin edebilmesini sağlamayı amaçlamaktadır.

Bu tedbirler, yetkili makamların, özellikle bilgisayar verilerinin kaybedilmesinin ya da değiştirilmesinin söz konusu olabileceğine dair gerekçelerin mevcut bulunduğu durumlarda, trafik verileri dahil olmak üzere, bir bilgisayar sistemi aracılığıyla saklanan bazı bilgisayar verilerinin korunmasının kolaylaştırılması yönünde talimat vermeleri ya da söz konusu hususu benzer şekilde temin etmelerini sağlamak için gerekli tedbirlerdir.

Bu tedbirler, hizmet sağlayıcılar gibi veri sahipleri tarafından halihazırda toplanmış ve saklanan verilere uygulanır. Gelecekteki trafik verilerinin gerçek zamanlı toplanmasına ve saklanmasına veya haberleşmelerin içeriğine gerçek zamanlı erişime uygulanmaz.

“Koruma”, halihazırda saklanan verilerin mevcut niteliğinin veya durumunun değişmesine veya bozulmasına neden olacak herhangi bir şeyden korunmasını gerektirmektedir. Saklanan verilerin, verilerin değiştirilmesinden, bozulmasından veya silinmesinden korunmasını gerektirmektedir. Koruma, verilerin “dondurulması” (yani erişilemez hale getirilmesi) ve verilerin veya verilerin kopyalarının meşru kullanıcılar tarafından kullanılamaması anlamına gelmek zorunda değildir. Talimatın verildiği kişi, talimatın özelliklerine bağlı olarak, verilere erişim sağlamaya devam edebilir.

Tedbirin kendisi özel hayatın gizliliği, haberleşmelerin gizliliği veya verilerin korunması gibi temel hakların ihlal edilmesini belirtmemektedir. Çünkü tedbirin tek etkisi, saklanan verilere erişilmesi ve bu veriler hakkında bilgi sahibi olunması için resmi emir alındığı sürece, spesifik ve belirli soruşturmalarla ilgili soruşturmayı yürüten kişi tarafından tutulan bilgilerin, tahrip edilmesini veya değiştirilmesini önlemek amacıyla saklanmasıdır (dondurulması). Bu yaklaşım uyarınca ve yaklaşımın ihtiyati mahiyeti göz önünde bulundurularak, bu tedbir İspanya mevzuatında (Budapeşte Sözleşmesi’nde olduğu gibi) azami 90 günlük bir süre için alınabilir ve yalnızca bir kez benzer bir süre için uzatılabilir. Hükümde bu husus açık bir şekilde belirtilmemiş olmasına rağmen yetkili makam saklanan verilere erişimi reddederse veya hukuki süre bu hususun lehine bir kararla sonuçlanmadan biterse, spesifik veri koruma görevi, bu bağlamdaki olağan kurallar uygulanarak bozulmalıdır.

Budapeşte Sözleşmesi'nde verilerin korunması yönündeki talimatı kimin verebileceğine ilişkin sınırlamalar yer almamaktadır. Bu nedenle, verilerin korunması yönündeki talimatın, verilere erişmek için vakitlice talep edilmesi gereken hukuki yetkiye halel getirmeksizin sadece mahkemelerden değil aynı zamanda kolluk kuvvetlerinden veya savcılıktan da gelebileceği anlaşılmaktadır.

Bu tedbir ayrıca Budapeşte Sözleşmesi'nin farklı devletler arasında verilerin korunması talebinde bulunma olasılığı sağlayan 29. maddesi uyarınca ulus üstü bir boyutu vardır. Bu amaçla, 29. maddede yerine getirilmesi gereken bazı koşullar yer almaktadır:

a) karşılıklı yardım talebinde bulunulması,
b) soruşturmaya konu olan suç ve ilgili esasların özetinin belirtilmesi,
c) hangi verilerin saklanmasının amaçlandığı ve bunun soruşturmaya konu olan suçla ilişkisi.

B. Trafik verilerinin korunmasının kolaylaştırılması ve kısmen açıklanması (madde 17)

Geçmiş haberleşmelerle ilgili saklanan trafik verilerinin temin edilmesi, örneğin, çocuk pornografisinin dağıtımını yapan, hileli bir planın parçası olarak hileli yanlış beyanların dağıtımını yapan, bilgisayar virüslerini dağıtan, yasa dışı olarak bilgisayar sistemlerine erişme teşebbüsünde bulunan veya başarılı bir şekilde erişen ya da sistemdeki verilere veya sistemin düzgün işleyişine müdahale eden bir bilgisayar sistemine bilgileri ileten kişilerin tespit edilmesinde oldukça önemli olan geçmiş bir haberleşmenin kaynağının veya hedefinin belirlenmesinde önemli olabilmektedir.

Bazen trafik verileri veya en azından bazı trafik verileri, ticari amaçla, güvenlik amacıyla veya teknik amaçla haberleşmenin iletimine dahil olan hizmet sağlayıcılar arasında paylaşılmaktadır. Böyle bir durumda, hizmet sağlayıcılardan herhangi biri, haberleşmenin kaynağının veya hedefinin belirlenmesi için gerekli trafik verilerini elinde bulundurabilmektedir. Ancak genellikle tek bir hizmet sağlayıcı, haberleşmenin gerçek kaynağının veya hedefinin tespit edilebilmesi için yeterli trafik verilerini elinde bulundurmamaktadır. Her bir hizmet sağlayıcı, puzzle'ın bir parçasını elinde bulundurmaktadır ve kaynak veya hedefin tespit edilmesi için bu parçaların her birinin incelenmesi gerekmektedir. 17. madde, bir veya daha fazla hizmet sağlayıcının bilgilerin iletimine dahil olduğu hallerde, trafik verilerinin korunmasının tüm hizmet sağlayıcılar arasında kolaylaştırılabilmesini sağlamaktadır.

C. Üretim talimatı (madde 18)

Yetkili makamın üretim talimatı aracılığıyla talebi üzerine, kişinin mülkiyetinde bulunan bazı verilerin iletilmesidir. Söz konusu veriler, saklanan veriler veya mevcut verilerdir ve trafik verileri veya gelecekteki haberleşmelerle ilgili içerik verileri gibi henüz var olmayan verileri içermemektedir.

"Üretim talimatı", özellikle daha müdahaleci veya daha ağır tedbirler yerine, kolluk kuvvetlerinin birçok durumda uygulayabileceği daha esnek bir tedbir sağlamaktadır. Bu tür bir usul mekanizmasının uygulanması, genellikle kendi kontrollerindeki verileri sağlayarak gönüllü olarak kolluk kuvvetlerine yardımcı olmaya hazır olan fakat bu yardım için kendilerini sözleşmeden doğan veya sözleşmeden doğmayan yükümlülükten kurtaran uygun bir yasal dayanağı tercih eden internet servis sağlayıcılar (İSS) gibi üçüncü taraf veri koruyucuları için de faydalıdır.

Bu maddede aşağıda belirtilen tedbirler öngörülmektedir:

a) Söz konusu tarafın ulusal sınırlar içinde bulunan bir kişinin, söz konusu kişinin mülkiyetinde ya da kontrolünde bulunan ve bir bilgisayar sisteminde veya bilgisayar verilerini saklamak için kullanılan başka bir cihazda saklanan bazı bilgisayar verilerini vermesinin sağlaması.
b) Söz konusu tarafın ulusal sınırlar içinde hizmet veren bir hizmet sağlayıcının, mülkiyetinde ya da kontrolünde bulunan ve sözü geçen hizmete ilişkin abone bilgilerini vermesi yönünde talimat vermesi.

Bu, ulusal bir tedbirdir, uluslararası iş birliği değildir. Çünkü talimat, diğer devletlerde halihazırda kök salmış hizmet sağlayıcıların, talep eden devlette hizmetlerini sunması yönündedir ve hizmet sağlayıcılar, talep eden tarafın ulusal sınırları içinde atılan adımlarla oluşturulan verileri temin etmeye yönlendirilmektedir.

İlk durumda, talep eden ülkenin ulusal sınırları içinde bulunan bir kişinin veya kuruluşun mülkiyetinde veya kontrolünde bulunan ve bir bilgisayar sisteminde saklanan ve soruşturma için gerekli abone bilgileri, trafik verileri veya içerikle ilgili bilgileri talep etme olasılığına atıfta bulunulmaktadır. Hüküm bu bağlamda saklanan verilerle ilgilidir, şu anda oluşturulmakta olan veya gelecekte oluşturulabilecek verilerle ilgili değildir. Bunlarla bağlantılı olarak Sözleşmenin ilgili kurallarının uygulanması gerekecektir. Verilerin, talep edilen sağlayıcının mülkiyetinde bulunması şart değildir, sağlayıcının kontrolünde olması yeterlidir.

İkinci durum, Madde 18.3.3'te belirtildiği üzere, özellikle abone bilgileriyle ilgilidir ve talep eden devletin ulusal sınırlarında fiziksel veya yasal olarak bulunmasa bile bu sınırlarda hizmet sunan hizmet sağlayıcılara yöneliktir. Abone bilgileri, fiziki olarak hizmet sağlayıcının mülkiyetinde veya

kontrolünde olabilir ve diğer devletlerde bulunan sunucularda uzakta saklanabilir. Yani bunlar, hizmet sağlayıcının bir devletin vatandaşına hizmetleri için sözleşme yapma olasılığı sunduğu veya muhatap devletle gerçek ve önemli bir bağlantının olduğu ve verilerin hizmet sağlayıcının mülkiyetinde veya kontrolünde olduğu durumlar olmalıdır.

D. Saklanan bilgisayar verilerinin aranması ve bunlara el koyulması (madde 19)

Bunlar, bilgisayar verilerinin somut bir veri taşıyıcının aranması ve buna el koyulmasıyla eşit düzeyde etkili bir şekilde temin edilebilmesinin sağlanması amacıyla, dijital dünyadaki aramalar ve el koymalarla ilgili spesifik kurallardır.

Bunun birkaç sebebi vardır:

- İlk olarak, veriler elektromanyetik biçimde olduğu gibi elle tutulamaz biçimdedir.
- İkinci olarak, veriler bilgisayar donanımının kullanılmasıyla okunabilirken, bu verilere basılı bir kayıtta olduğu gibi el koyulamaz ve veriler götürülemez. Elle tutulamaz verilerin saklandığı fiziki ortama (örneğin, bilgisayarın hard diski veya disket) el koyulması ve bunun götürülmesi gerekmektedir veya verilerin kopyası ya somut olarak (örneğin, bilgisayar çıktısı) ya da kopyayı içeren somut ortama el koyulup bu götürülmeden önce fiziki bir ortamda (örneğin, disket) elle tutulamaz bir biçimde yapılması gerekmektedir. Verilerin kopyalarının yapıldığı ikinci iki durumda, verinin bir kopyası bilgisayar sisteminde veya saklama cihazında kalmaktadır. Ulusal mevzuat, bu tür kopyaların yapılması için yetki vermelidir.
- Üçüncü olarak, bilgisayar sistemlerinin bağlantısallığı nedeniyle, veriler, aranan belli bir bilgisayarda saklanmayabilir fakat bu tür verilere bu sistemden rahatlıkla erişilebilir. Veriler, bilgisayarla doğrudan bağlantılı olan veya internet gibi iletişim sistemleri aracılığıyla dolaylı olarak bağlantılı olan ek bir veri saklama cihazında saklanabilir. Bu, aramanın, verinin gerçekten saklandığı (veya verinin bu ortamdan aranan bilgisayara çekilmesi) yere genişletilmesine veya geleneksel arama yetkilerinin her iki ortamda daha koordineli ve kolay bir şekilde kullanılmasına izin verecek yeni kanunlar çıkarılmasını gerektirebilir veya gerektirmeyebilir.

Tedbirler şu şekildedir:

a) Kolluk kuvvetlerine, bir bilgisayar sistemi ya da bu sistemin parçasında (ek veri saklama cihazı) veya ayrı bir veri saklama ortamında (örneğin, CD-ROM veya disket) saklanan bilgisayar verilerine erişim sağlamaları ve bunları aramaları için yetki verilmesi.

b) Soruşturmayı yürüten mercilere, gerekli verilerin başka bir bilgisayar sisteminde saklandığına dair gerekçeleri olması halinde başka bir bilgisayar sistemi veya bu sistemin bir parçasında arama yapmaları veya bunlara erişim sağlamaları için izin verilmesi. Ancak diğer bilgisayar sisteminin veya bu sistemin parçasının "kendi ulusal sınırları" içinde olması gerekmektedir.

c) 1. veya 2. fıkra uyarınca erişilen bilgisayar verilerine el koyulması veya bu verilerin koruma altına alınması için yetkili makamlara yetki verilmesi. Bu tedbirler şunları içermektedir: bir bilgisayar sistemi veya bu sistemin parçasına ya da bilgisayar verileri saklama ortamına el koyulması veya bunların korunması, bu bilgisayar verilerinin kopyalanıp bunlara el koyulması, söz konusu saklı bilgisayar verilerinin bütünlüğünün korunması, erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez hale getirilmesi ya da silinmesi.

d) Son olarak, bilgisayar verilerinin aranması ve bunlara el koyulmasının kolaylaştırılması için zorlayıcı tedbir getirilmektedir. İşlenebilecek ve saklanabilecek verilerin miktarı, güvenlik tedbirlerinin uygulanması ve bilgisayar işlemlerinin mahiyeti göz önünde bulundurulduğunda, delil olarak aranan verilere erişim sağlanması ve bunların tespit edilmesini zorlaştırabilecek pratik bir hususu ele almaktadır. Aramanın en iyi nasıl yapılması gerektiğiyle ilgili teknik yöntemlerle ilgili olarak bilgisayar sistemiyle ilgili belli bilgiye sahip sistem yöneticilerine danışılabileceğini kabul etmektedir. Bu nedenle, bu hüküm kolluk görevlilerinin, makul olduğu ölçüde bir sistem yöneticisini arama ve el koymanın gerçekleştirilmesine yardımcı olmak zorunda bırakmasına izin vermektedir.

E. Trafik verilerinin gerçek zamanlı olarak toplanması (madde 20)

Telekomünikasyonla ilgili trafik verilerinin (örneğin, telefon konuşmaları) toplanması, kaynak veya hedefin (örneğin, telefon numaraları) ve çeşitli yasa dışı haberleşme türleriyle (örneğin, suç tehditleri ve taciz, suç komplosu, hileli yanlış beyanlar) ve geçmişteki veya gelecekteki suçlara (örneğin; uyuşturucu kaçakçılığı, cinayet, ekonomik suçlar vs.) delil sağlayan haberleşmelerle ilgili verilerin (örneğin; saat, tarih ve süre) belirlenmesi açısından faydalı bir soruşturma aracı olmuştur.

Bilgisayar haberleşmeleri, aynı suç türleri için delil teşkil edebilir veya delil sunabilir. Ancak bilgisayar teknolojisinin yazılı metin, görsel resimler ve ses dahil olmak üzere büyük miktarlarda veri

iletebilmesi göz önünde bulundurulduğunda, yasa dışı içeriğin dağıtımı (örneğin, çocuk pornografisi) dahil olmak üzere suç işlenmesi için de büyük bir potansiyeli vardır.

Bu soruşturma tekniği, şüphelinin haberleşmelerinin saati, tarihi, kaynağı ve hedefiyle mağdurların sistemlerine girilme zamanları arasında bağlantı kurabilmekte, diğer mağdurları tespit edebilmekte ve suç ortaklarıyla bağlantıları gösterebilmektedir.

Söz konusu trafik verileri, tarafın ulusal sınırları içindeki özel iletişimle ilgili olmak zorundadır. Bu nedenle, Sözleşme genel veya rastgele büyük miktarlarda trafik verilerinin gözetlenmesi ve toplanmasını gerektirmemekte veya buna yetki vermemektedir. Soruşturulan spesifik suç olaylarının aksine, suç faaliyetlerinin keşfedilmesinin beklendiği yerlere "olta atılmasına" yetki vermemektedir. Yargı makamları veya verilerin toplanmasına ilişkin talimat veren diğer merciiler, trafik verilerinin toplanmasının ilgili olduğu haberleşmeleri belirtmek zorundadır.

Bu maddede, taraflardan her birinin, yetkili mercilerinin aşağıdaki hususlarda yetkili olması için gerekli olabilecek yasal işlemleri ve diğer işlemleri yapacağı belirtilmektedir:

Trafik verilerinin gerçek zamanlı olarak, ilgili tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplanması ya da kaydedilmesi ve herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde; trafik verilerini gerçek zamanlı olarak, ilgili tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplaması ya da kaydetmesi veya trafik verilerinin gerçek zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle iş birliği yapması ve onlara bu hususta yardımcı olması.

F. İçerikle ilgili verilere müdahale edilmesi (madde 21)

Telekomünikasyonla ilgili trafik verilerinin (örneğin, telefon konuşmaları) toplanması, kaynak veya hedefin (örneğin, telefon numaraları) ve çeşitli yasa dışı haberleşme türleriyle (örneğin, suç tehditleri ve taciz, suç komplosu, hileli yanlış beyanlar) ve geçmişteki veya gelecekteki suçlara (örneğin; uyuşturucu kaçakçılığı, cinayet, ekonomik suçlar vs.) delil sağlayan haberleşmelerle ilgili verilerin (örneğin; saat, tarih ve süre) belirlenmesi açısından faydalı bir soruşturma aracı olmuştur. Bilgisayar haberleşmeleri, aynı suç türleri için delil teşkil edebilir veya delil sunabilir. Ancak bilgisayar teknolojisinin yazılı metin, görsel resimler ve ses dahil olmak üzere büyük miktarlarda veri iletebilmesi göz önünde bulundurulduğunda, yasa dışı içeriğin dağıtımı (örneğin, çocuk pornografisi) dahil olmak üzere suç işlenmesi için de büyük bir potansiyeli vardır.

"İçerikle ilgili veriler", iletişimin içeriğine yani iletişimin anlamı veya manası ya da iletişimle iletilen mesaj veya bilgiye atıfta bulunmaktadır. İçerikle ilgili veri, trafikle ilgili olmayan veri ve iletişimin bir parçası olarak iletilen her şeydir.

2.3.- ULUSLARARASI HUKUKİ İŞ BİRLİĞİ

Hem cezai-maddi hem de usul açısından normatif uyumlaştırmanın değeri, sanal gerçeklikte yürütülen ceza soruşturması ve kovuşturması faaliyetlerinde uluslararası iş birliği çerçevesinde tam boyutunu kazanmaktadır:

- Siber suçlar, tüm suçlar arasında en ulus üstü olan suçtur.
- Siber suçların soruşturulması, etkili uluslararası iş birliği gerektirmektedir.
- Uluslararası iş birliği olmadan soruşturmaların başarılı olması olası değildir.

Siber suç davalarında uluslararası iş birliğine ilişkin uluslararası kuruluşların en önemli girişimleri şu şekilde olmuştur:

1.- INTERPOL

Interpol'e, dünyanın dört bir yanından, tüm kıtalardan, 190'dan fazla kolluk kuvveti üyedir ve bu kurumun hedefleri şu şekildedir:

- uluslararası polis iş birliğinin artırılması ve kolaylaştırılması,
- küresel bir polis iletişim sistemi kurulması,
- özel veri tabanları ve polis bilgi analizleri hazırlanması.

2.- Avrupa Birliği

Avrupa Birliği, tüm Üye Devletleri Budapeşte Sözleşmesi'ne taraf olması konusunda teşvik etmiştir. Tüm üye devletler sözleşmeyi imzalamıştır.

Avrupa Konseyi'nin 24 Şubat 2005 tarihli 2005/222/JHA sayılı (16.3.2005 tarihli L 69/67 sayılı Avrupa Birliği Resmi Gazetesi) bilişim sistemlerine karşı yapılan saldırılara ilişkin Çerçeve Kararı'nın 11.1 maddesinde, tüm Avrupa Birliği Üye Devletlerinin "yedi gün 24 saat faaliyet gösteren temas noktalarının mevcut ağından faydalanılmasını sağlayacağı" belirtilmektedir.

3.- EUROPOL

EUROPOL, Avrupa Birliği Üye Devletlerindeki kolluk kuvvetleri arasındaki iş birliğinin etkililiğinin artırılmasını amaçlayan bir Avrupa Birliği Kurumudur. 1999 yılından bu yana faaliyet gösteren EUROPOL, suçla ilgili bilgilerin analiz edilmesini kolaylaştırmakta ve Üye Devletler arasında veri paylaşımı yapmaktadır. Bünyesinde Avrupa Siber Suç Merkezi (European Cybercrime Centre, EC3) bulunmaktadır (2013 Ocak ayında açılmıştır).

4.- EUROJUST

Eurojust'ın, Üye Devletlerin yetkili makamları arasındaki iş birliğinin desteklenmesi ve uluslararası karşılıklı hukuki yardım ve suçluların iadesi taleplerinin uygulanmasının kolaylaştırılması görevleri bulunmaktadır.

5.- CEZAİ KONULARDA AVRUPA YARGI AĞI

Cezai Konularda Avrupa Yargı Ağı, yargı temas noktalarından oluşan bir ağdır. Bu ağa bağlı temas noktaları, üye devletler arasında yargı iş birliğinin kolaylaştırılması göreviyle aktif aracılardır.

Atlas, uygulayıcıların karşılıklı hukuki yardım talebi almak ve bunu uygulamak için her üye devletteki yetkili yerel makamın derhal tespit edilmesini sağlamaktadır.

6.- Avrupa Konseyi

1959 tarihli Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi, Budapeşte Sözleşmesi'nin temelini oluşturmaktadır.

7.- Budapeşte Sözleşmesi

Budapeşte Sözleşmesi'nin 3. Bölümü uluslararası iş birliğinin güçlendirilmesine yöneliktir. Sözleşmenin 23. maddesinde, taraflar arasında mümkün olan en geniş biçimde iş birliği uygulanmasına yönelik bir teşvik ifadesi yer almaktadır ve bu madde, suçun bir bilgisayar sistemi kullanılarak işlendiği veya bilgisayar sistemi kullanılmadan işlenen bir suçun (örneğin, cinayet) elektronik delil içerdiği durumlara uygulanabilmektedir.

Bu iş birliğinin alt yapısında, taraflar tarafından hem çok taraflı hem iki taraflı olarak imzalanan Uluslararası Anlaşmalar ve Antlaşmalar vardır. Taraflar arasındaki yardıma ilişkin ikincillik kuralları,

Sözleşmenin 27. maddesinde, ilgili ülkeler arasında uluslararası anlaşma veya antlaşma olmayan durumlar için belirtilmektedir.

Taraflar arasındaki etkili iş birliğini artırmak amacıyla, Sözleşmede, 2-11. maddeler kapsamındaki suçlara yönelik suçluların iadesinin teşvik edilmesini amaçlayan kurallar yer almaktadır.

Dolayısıyla, 25. maddede, Sözleşme kapsamındaki suçlara yönelik soruşturmalar veya yargılamalarda karşılıklı iş birliğinin desteklenmesine ilişkin genel ilkeler yer almaktadır. Bu maddede, acil durumlarda hızlı iletişim yoluyla talebin iletilmesi (e-posta veya faks) ve bilgilerin anında iletilebilme olasılığı (madde 26) belirtilmekte ve uygulanabilir olduğu durumlarda her iki ülkede suç olarak sayma ilkesinde esneklik için çağrıda bulunulmaktadır.

27. madde, karşılıklı yardımlaşmaya ilişkin spesifik kuralların bulunmadığı durumlarda Sözleşmenin kurallarının geçerliliğini beyan ettikten sonra bu tür bir suç için karşılıklı yardımlaşmanın yapıldığı usul ve koşulları (ilave olarak) belirtmektedir (yetkili mercilerin belirlenmesi, reddetme gerekçeleri, gizlilik vs.). Aşağıda belirtilen hususlar özellikle vurgulanmaktadır:

- Acil durumlarda yargı makamları arasında doğrudan iletişim (hem talep edilen hem talep eden Devletin merkezi makamlarına eşzamanlı olarak gönderilmesi).
- Taleplerin veya yazışmaların INTERPOL aracılığıyla gönderilmesi.

Son olarak, Sözleşmede bahsi geçen araçların uluslararası kullanımına ilişkin spesifik kurallar belirtilmektedir. Sözleşmenin 16-21. maddelerinde belirtilen araçların, aynı Ülkede etki oluşturan fiilin açıklığa kavuşturulmasında tamamen geçerli ve etkili olduğu fakat bu ülkenin düzenlemesinin, bu uluslararası araç çerçevesinde, her ülkenin coğrafi sınırlarının ötesinde ulus üstü kullanımına ilişkin nihai bir hedefinin olduğu açıktır.

Başlıca uluslararası iş birliği tedbirleri şu şekildedir:

a. Anında bilgilendirme (madde 26)

Bir tarafın yetkili makamları, bir iç soruşturma kapsamında elde ettiği bazı bilgileri, diğer tarafın yetkili makamlarına iletebilir. Bu bilgilendirme, söz konusu suç eylemi Sözleşme çerçevesinde yer alıyorsa yapılabilir.

Bu bilgi iletimi, gizlilik başta olmak üzere, belli koşullara bağlı olarak yapılır.

b. Bir bilgisayar sisteminde saklanan verilerin korunmasının kolaylaştırılması (madde 29)

Bu, dijital ortamın çok kısa sürelerde silinebilecek bir şeyin korunması ihtiyacına ilişkin özelliği nedeniyle yeni bir uluslararası iş birliği aracıdır.

Bu yalnızca acil sebepler için bir koruma tedbiridir ve korunan tedbirlerin otomatik olarak açıklanması anlamına gelmemektedir. Uygulamada, verilerin korunması kolaylaştırıldıktan sonra bu verilerin talep eden tarafa açıklanmasını gerektirecek herhangi bir durum olmadığı varsayılabilir.

Bu hüküm, paralel bir çerçeve sağlamaktadır:

a. Bir tarafa, başka bir taraftan verilerin korunmasının kolaylaştırılmasını talep etme imkanı sağlamaktadır,
b. Aynı zamanda ilgili tarafa arama veya el koyma ya da benzer bir tedbir için resmi yardım talebini ifade etme imkanı vermektedir.

Talep eden tarafın, kendi ulusal kanununa göre, gerekli itinayla, talep edilen verileri korumak için gerekli eylemde bulunması gerekmektedir.

Talep edilen taraftan, verilerin korunmasının koşulu olarak bir eylemin her iki ülkede de suç sayılması talep edilemez.

c. Trafik verilerinin açıklanması (madde 30)

Özel iletişim sayılan trafik verilerinin korunmasına ilişkin olarak madde 29 çerçevesinde iletilen talebin yerine getirilmesi sırasında, kendisinden yardım talep edilen tarafın başka bir ülkedeki bir hizmet sağlayıcının söz konusu iletişimin sağlanmasında dahli bulunduğunu keşfetmesi halinde, söz konusu taraf, talepte bulunan tarafa, ilgili hizmet sağlayıcının ve verilerin aktarıldığı yolun belirlenmesi için gerekli ölçüde trafik verisini en kısa sürede açıklayacaktır.

d. Saklanan bilgisayar verilerine erişilmesine ilişkin karşılıklı yardımlaşma (madde 31)

Taraflardan herhangi biri, kendisinden talepte bulunulan tarafın ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla saklanan verilerin, bu çerçevede madde 29 uyarınca korunan verilerin, söz konusu tarafça araştırılması, bunlara erişilmesi, el konulması ya da bunların benzer şekilde elde tutulması ya da açıklanması amacıyla söz konusu taraftan talepte bulunabilir.

Sözleşmede açıkça ilgili ülkeler arasındaki mevcut iki taraflı veya çok taraflı iş birliği belgelerinin veya karşılıklılık kriterlerine dayalı anlaşmaların kullanılmasına atıfta bulunulmaktadır.

e. Saklanan bilgisayar verilerine izinli şekilde ya da bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlamak (madde 32)

Taraflar, diğer tarafın iznini almaksızın: kullanıma açık (herkesin ulaşabileceği bir kaynaktan gelen) saklı bilgisayar verilerine, bu verilerin coğrafi konumuna bakılmaksızın erişebilir ya da ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla, başka bir taraf dahilinde bulunan saklı bilgisayar verilerine, bu verileri söz konusu bilgisayar sistemi üzerinden açıklama yetkisine haiz olan kişinin iznini yasal olarak aldıktan sonra erişebilir ya da bunları alabilir.

Bu maddenin yorumlamasından, maddenin iki tür durumda uygulandığı anlaşılmaktadır: 1) içeriğinin başka bir ülkede saklandığı bir e-posta hesabı sahibinin kendi kararıyla veya hizmet sağlayıcının kararıyla, bu içerikleri yetkili makamlara tahsis etmeye veya yetkili makamların içeriklere erişmesine izin vermeye karar verdiği durumlar, 2) soruşturulan kişinin gönüllü olarak polise veya araştırmayı yürüten organlara, bilginin başka bir ülkede bulunup bulunmadığına bakılmaksızın sahibi olduğu hesaplara erişim için rızasını verdiği durumlar. Her iki durumda da Sözleşmede belirtildiği üzere, sınır ötesi erişim sağlamak mümkündür. Yani aşağıdaki hususlara uygun olarak karşılıklı hukuki yardımlaşma tedbirlerine halel getirmeksizin başka bir tarafın ulusal sınırlarında bulunan bilgilere tek taraflı erişim sağlanabilir:

1. Sınır ötesi erişime ilişkin rıza, kanuna uygun ve gönüllü olmalıdır, aldatma veya baskıyla alınmamalıdır. Bu amaçla, çocuk veya engelli olduğu için karar verme yetisi kısıtlı olan kişilerin verdiği rıza, spesifik durumları ışığında geçerli olmayacaktır.
2. Başka bir ülkede saklanan verilere erişmek için yasal olarak izinli olacak kişilerin belirlenmesi, her durumdaki koşullara ve uygulanacak mevzuata bağlı olacaktır. Bu kişiler, gerçek kişiler veya hatta tüzel kişiler olabilir. Ancak hizmet sağlayıcılar, kullanıcılarının verileri açısından prensipte bu yetkiden hariç tutulmaktadır.
3. Genellikle erişim izni olan kişi hem fiziki olarak hem yasal olarak talep eden devletin ulusal sınırları içinde olacaktır fakat bu kişinin verilerin saklandığı veya hatta üçüncü bir ülkede olduğu durumlar gibi başka durumlar da ortaya çıkabilir.
4. Her halükarda, tedbiri uygulayan yetkili makamlar, verilerin ulusal sınırları içinde saklandığı ülkenin bilgisayar sistemi vasıtasıyla verilere erişim veya verilerin açıklanması mümkün değilse, başka bir ülkedeki verilere erişimin de mümkün olmayacağı şekilde bu amaçla oluşturulan ulusal mevzuatı dikkate almalıdır.

5. Bu durumda, karşılıklı hukuki yardım kanallarına başvurmaya gerek yoktur. Erişilen verilerin ulusal sınırları içinde bulunduğu ülkeyi bilgilendirmeye de gerek yoktur. Ancak taraflar uygun görürse ilgili ülke bilgilendirilebilir.

Bu hüküm ancak verilerin ulusal sınırlarında saklandığı ülkenin bilindiği durumlarda uygulanabilir. Ülkenin bilinmediği veya verilerin yerinin değiştirildiği durumlarda uygulanamaz.

f. Trafik verilerinin gerçek zamanlı olarak toplanması konusunda karşılıklı yardımlaşma (madde 33)

Taraflar, kendi ulusal sınırları içinde özel iletişim olarak görülen ve bir bilgisayar sistemi üzerinden aktarılan trafik verilerinin gerçek zamanlı olarak toplanması için birbirilerine yardımcı olacaklardır. Fıkra 2'ye tabi olmak kaydıyla, bu yardım ulusal yasalarda belirtilen şartlar ve usuller çerçevesinde gerçekleşecektir.

Taraflardan her biri, en azından, ulusal sınırlar içinde trafik verilerinin gerçek zamanlı olarak toplanabilmesini mümkün kılanlara benzer nitelikteki cezai suçlar konusunda yardım sağlayacaktır.

g. 7/24 temas noktaları (madde 35)

Sürekli olarak erişilebilir temas noktası oluşturma zorunluluğu: 7/24 temas noktaları ağı. Uluslararası iş birliğinin kolaylaştırılmasına yönelik bu temas noktalarının genel hedefleri şu şekildedir:

- diğer temas noktalarına teknik tavsiyede bulunulması,
- verilerin muhafaza edilmesinin kolaylaştırılmasına yönelik uygun mekanizmanın devreye sokulması,
- verilerin hızlı bir şekilde toplanması,
- sanıkların kimliğinin tespit edilmesi.

1. TEKNOLOJİK SORUŞTURMA TEDBİRLERİ

3.1.- GİRİŞ

"Siber suçlar", sadece bu teknolojilerin kullanıcıları için değil aynı zamanda suç eylemlerinin önlenmesi ve cezalandırılması için çağrıda bulunulan yetkili makamlar için de yeni zorluklar teşkil etmektedir.

Yeni teknolojilerin ortaya çıkışı ve genele yayılması, toplum düzeyinde "bilgi teknolojileri" adını verdiğimiz büyük ve yatay bir değişikliği beraberinde getirmiştir. Bu değişiklikler, inkar edilemez avantajlarına ek olarak, kişileri ve kurumları, diğerlerinin yanı sıra internet, kurum içi ağ, teknolojik gelişme, bilgi yönetimi senaryolarında eşzamanlı olarak tehditler, riskler ve belirsizliklerle karşı karşıya bırakmıştır.

Bu dijital olgunun gölgesinde ve ağın sağladığı anonimlik göz önünde bulundurularak, yeni suç türleri ortaya çıkmıştır. Bu suç türlerinin en düşük ortak paydası, suçlunun lehine ve toplumdaki bireylerin bireysel veya bireysel üstü çıkarlarına karşı donanım veya yazılım düzeyinde bilgisayar sistemlerinin kullanılması ve suiistimal edilmesidir. Bilgisayar suçları birçok biçimde bulunmaktadır ve en yaygın olanları kimlikle ilgili olanlardır. Bu, "şifre avcılığı" (internet kullanıcılarının kişisel bilgilerini vermeleri için kandırılması), "kötü amaçlı yazılım" (kişisel bilgileri toplayan ve farkında olmadan indirilen yazılım) ve "hackleme" (üçüncü tarafın bilgisayarına veya sunucusuna uzaktan yasa dışı olarak erişim sağlanması) yoluyla yapılmaktadır. Suçlular, örneğin, kredi kartı ve para bilgilerine el koymak için bu yöntemleri kullanmaktadır. Öte yandan, internet telif hakkı ve fikri mülkiyet haklarıyla ilgili suçlar ile çocuk pornografisi ve taciz içerikli materyaller gibi suçlar için de bir yer haline gelmiştir.

Ceza yargılamasının soruşturma aşamasının spesifik işlevlerinden biri, olayın ayırt ediciliğinin ve olayın kaynağının daha önceden var olduğunun bulunmasını amaçlayan soruşturma faaliyetlerinin gerçekleştirilmesidir.

Günümüzde birçok ceza soruşturmasında teknolojik destek alınmaktadır. Bu bağlamda, polis tarafından modern teknolojilerin kullanımı, suçla ilgili dijital delillerin temin edilmesi ve organize suç örgütlerinin kullandığı karmaşık araçların ve bu örgütlerin faaliyetlerinin uluslararası yapısının etkisiz hale getirilmesi için önemli bir çalışma aracıdır. Polisin delil niteliğindeki yargısal faaliyetin etkililiğinin dayandığı gerekli araçlara her zaman sahip olması gerekmektedir.

Fakat bu tür bir soruşturma, kamu düzeninin güvence altına alınması ve soruşturulan kişinin özel hayatının gizliliğinin korunması arasında yeterli dengenin sağlanması gibi yeni zorluklar ortaya çıkarmaktadır.

Yakın zamana kadar özel hayatın yaşandığı ve ailenin bulunduğu alanlar temel olarak evle ve yazışmalarla sınırlıydı. Günümüzde yeni teknolojiler özel hayatın birçok yönünün yalnızca fiziki olarak değil aynı zamanda sanal olarak yeni alanlarda geliştirilmesine olanak sağlamıştır ve bunların korunması gerekmektedir. Binlerce kilometre uzaklıkta bulunan bir sunucu, bizimle ilgili kendi evimizdekinden daha fazla bilgi barındırabilmektedir.

Yukarıdaki hususa ek olarak, yeni teknolojilerin ele alınmasına dahil olan teknolojik zorluk nedeniyle bu suçların soruşturmasında karmaşıklık söz konusudur ve bu da adli polis bünyesinde özel araştırma birimlerinin oluşturulmasını gerektirmiştir. Bu, neredeyse sürekli yeniliğe ve değişime tabi bir alandır. Kısa bir sürede, bilgisayarın bulunduğu yerin adresini girerek bilgisayarın hard diskinin kaydının yapılması, internet üzerinden kayıtlar yapılmasına imkan sağlayan programların kullanılması ve bu kayıtların içeriğinin başka bir cihazda kaydedilmesi ve çoğaltılması mümkün olmuştur. Bir diğer örnek, uzaktan kontrol edilen ve açık alanlara neredeyse sınırsız bir izinsiz girme kapasitesi olan dronelardır.

Bu bağlamda ve Avrupa Konseyi kapsamında, bununla ilgili suçları soruşturmak için gerekli yasal tedbirlerin alınması konusunda tarafları teşvik etmek için Budapeşte Sözleşmesi imzalanmıştır. Bu tedbirler, tarafların, 1950 Avrupa Sözleşmesi, Birleşmiş Milletler Medeni ve Siyasi Haklara ilişkin Uluslararası Sözleşmesi (1966) veya insan hakları konusunda uygulanacak diğer yasal belgelerde yer alan insan hakları ve temel özgürlüklerin korunmasını güvence altına alması gereken ve orantılılık ilkesini içermesi gereken ulusal kanunlarında yer alan şartları ve güvenceleri gözetmelidir.

Budapeşte Sözleşmesi'ne dayanan tedbirler, taraf devletler arasında uyumlu bir şekilde uygulanmalı ve böylece tüm üyelerde benzer olmalıdır.

Modülün bu kısmı, İspanya'da kabul edilen genel kavramlara ve tedbirlere dayanmaktadır. Bu nedenle, diğer ülkelerde kabul edilenlerle karşılaştırılabilir. İspanya'daki kanun koyucular, ulusal ve uluslararası mahkemelerin hakları sınırlayan soruşturma tekniklerinin birçoğunun dayandığı doktrini ve önemli araçların bazılarını değerli bir normatif uyumlaştırma çabasıyla bir araya getirmiş ve sistematikleştirmiştir. Aynı şekilde konuyla ilgili normatif hükümleri ve uluslararası sözleşmeleri belirlemiştir.

3.2.- ETKİLENEN TEMEL HAKLAR VE GÜVENCELER

Teknolojik soruşturma tedbirleri, bazı temel hakları etkilemektedir. Bu haklar; mahremiyet hakkı, haberleşmenin gizliliği, konut dokunulmazlığı, kişisel verilerin korunması ve kendisine karşı ifade vermeme ve suçu itiraf etmeme hakkıdır.

Yeni temel hakların tanınması teknolojik gelişmelerle bir bağlantı kurulmasını sağlamıştır. Örneğin, 2007 yılında, Almanya Anayasası'nda, bilgisayar sisteminin fiziki olarak bulunduğu yere fiziki olarak erişim sağlamaya gerek kalmadan bir bilgisayar sisteminde uzaktan bilgi elde edilmesine izin

veren çevrimiçi erişim tekniklerinin ortaya çıkması sonucunda oluşan izinsiz girişlere karşı bilgi sistemlerinin gizliliğinin ve bütünlüğünün korunması temel hakkı tanınmıştır.

a) Mahremiyet hakkı, başkalarının bizim kim olduğumuzu veya ne yaptığımızı bilmemesini güvence altına almaktadır. Bu hak, üçüncü tarafların veya devletin müdahalesi olmadan ve özel hayatın saklanan alanlarını kimsenin ihlal edememesini güvence eden bir haktır. Kişisel mahremiyetin, sınırsız veya mutlak olmadığı düşünülmektedir. Yani anayasal olarak geçerli başka bir çıkar için bu haktan feragat edilebilir. Bu nedenle, özel hayata müdahale öncelikle anayasal olarak meşru bir amacın var olmasını gerektirmektedir (bir suçun soruşturulmasına yönelik kamu yararı ve daha spesifik olarak ceza yargılaması için ilgili esasların belirlenmesi) Özel hayatın gizliliği hakkının var olduğu düşünüldüğünde, bu hakkın sahibi, korumak istediği alanı sınırlayabilir ve sonuç olarak, araştırmacıları bu sınırlamadan muaf tutarak araştırmacıların mesajlarının veya konuşmalarının içeriğine erişimine izin verebilir.

İspanya'da özel hayatın gizliliği hakkının koruma düzeyi haberleşmenin gizliliği hakkından daha düşüktür. Çünkü kişilerin günlük hayatlarıyla ilgili her şey temel korumadan faydalanmamaktadır. Yalnızca ilgili kişinin rızası olmadan kanunun özünü etkileyen hususlar bu korumadan faydalanmaktadır. Ancak haberleşmenin gizliliği, söz konusu haberleşmenin kişisel, samimi veya saklı olmasına bakılmaksızın haberleşmenin tüm içeriğini kapsamaktadır. Bu nedenle, acil durumlarda, polisin mahremiyet alanıyla ilgili verilere erişim hakkı vardır. Bu yetki, örneğin, pedofili, cinsel içerikli vb. arşivlenen görsellerin ağ üzerinden dağıtılabileceği ve mağdurların uğradığı zararı daha da artırabileceği olasılığıyla gerekçelendirilmektedir.

b) Konut dokunulmazlığı hakkı, aleni bir suç durumu hariç olmak üzere, konut sahibinin rızası ve yargı makamının izni olmadan bir adrese girilmesini veya bir adresin kaydedilmesini önleyen bir haktır.

c) Haberleşmenin gizliliği hakkı. Haberleşme ifadesi, kullanılan araçlara ve muhatapların arasındaki mesafeye bakılmaksızın her türlü haberleşmeyi içerir. Aynı zamanda yüz yüze iletişimi de korur.

Geçmiş konuşmalar incelenirken etkilenen hak, haberleşmenin gizliliği değil özel hayatın gizliliği hakkıdır. Çünkü konuşmalar alıcı tarafından sunucudan indirilmiş, okunmuş ve saklanmıştır, haberleşme süreci bitmiştir ve alıcının özel cihazına (bilgisayar, telefon vb.) kaydedilen haberleşmenin gidişatına artık müdahale edilemez veya müdahale edilmeyecektir. Bu da özel hayatın gizliliği kapsamındadır.

d) Kişisel verilerin korunması hakkı. Bu, incelediğimiz tedbirlerden etkilenen temel haklardan bir diğeridir. Bu hakkın içeriği, her kişiyi ilgilendiren bilgi akışını kontrol etme yetkisinden oluşur. Kişisel verilerin korunması hakkını güvence altına alan, verilerin tahrip edilmesine ilişkin yetkidir.

e) Kendisine karşı ifade vermeme ve suçu itiraf etmeme hakkı. Haberleşmelerin kaydedilmesiyle bağlantılı olarak, dinleme ve kayıt cihazlarının kanuna uygun olarak yerleştirilmesinin sağlanması ve soruşturulan veya şüphelenilen kişinin kendisine karşı bir konuşma yürütmesi için zorlandığına veya ikna edildiğine ya da bir tuzak kullanıldığına dair bir gösterge olmamasının sağlanması gerekmektedir.

Ayrıca örneğin bir tutukluyla avukatı arasındaki konuşmaların dinlenilmesine izin verilmemektedir. Çünkü bu konuşmaların gizli olduğu ve bunların dinlenilmesinin savunma hakkını ihlal ettiği düşünülmektedir.

Güvencelerle ilgili olarak öncelikle soruşturma altındakilerin temel haklarını rahatlıkla olumsuz bir şekilde etkileyebilecek teknolojik araştırma merkezlerinin, özellikle etkili adli kontrolle bu olumsuz etkileri azaltan ve anayasal olarak tanınan temel hakları güvence altına alan tedbirleri aldıkları zaman kabul edilmesi gerektiği belirtilmelidir.

VAKA ÇALIŞMALARI

VAKA A – SİBER SUÇ

1.- Jack bir polis memurudur. Uyuşturucu kaçakçılığı yapan bir çeteyle çalışmaktadır. Çete lideri, Jack'e üç plakanın yer aldığı bir liste verir ve bu arabaların kendisini takip ettiğinden şüphelendiğini söyler. Jack, karakola gider, kendi şifresiyle polis veri tabanına giriş yapar ve bu plakaların polis araçlarına ait olduğunu görür. Bu bilgiyi çete liderine verir.

Jack herhangi bir suç işlemiş midir?

2.- Anne, bir boşanma sürecinin ortasındadır. Evdeyken kocasının kendisini aldattığını kanıtlayacak deliller bulmaya çalışır ve fotoğrafların yüklü olduğu bazı CD'ler bulur. CD'lerin içeriğine baktığında bir tanesinin çocuk pornografisi fotoğraflarıyla dolu olduğunu görür. Hemen karakola gider ve CD'yi polis memurlarına vererek cihaza nasıl eriştiğini söyler.

Anne herhangi bir suç işlemiş midir?

3.- Polis, aylık üyelik ücretini ödeyenlere çocuk istismarı resimleri sunan bir internet sitesini fark eder ve IP adresi, kredi kartı numarası, e-posta adresi, fatura adresi ve şifre dahil olmak üzere internet sitesine erişim için para ödeyenlerin verilerini çıkarır.

Müşterilerden biriyle ilgili arama emri çıkarılır. Bu müşterinin bilgisayarı incelenir. Suçlayıcı hiçbir şey bulunamaz çünkü bu kişi bütün içeriği silmiştir.

Bu müşteri herhangi bir suç işlemiş midir?

4.- John, evindeki bilgisayarında gerçekçi banka makbuzları hazırlamak için ticari olarak erişilebilir olan bir fotoğraf yazılımı kullanmaktadır. Bu makbuzu gerçek olarak kabul eden bankasına götürür ve banka parayı John'un hesabına aktarır.

John hangi suçu işlemiştir?

VAKA B – TEKNOLOJİK SORUŞTURMA TEDBİRLERİ

1.- Victor, çocuk pornografisi seven ve bir kreşin mutfağında çalışan biridir. Dost canlısıdır ve çocukların güvenini kazanmıştır.

Bu durumdan faydalanarak on yaşındaki Paul'un soyunup videosunun kaydedilmesine izin vermesi için Paul'u ikna eder ve Paul'a videoyu kimseye göstermeyeceğini söyler. Video kaydedilir ve Victor bu videoyu bilgisayarında pedofili içeriği olan internet sayfalarından aldığı diğer çıplak çocuk görsellerinin kaydedildiği bir dosyaya kaydeder.

Birkaç ay sonra, polis çocuk pornografisiyle ilgili suç işlediğinden şüphelenerek Victor hakkında soruşturma başlatır. Victor ifadesinde suçlamaları reddeder.

Hakim, polise Victor'un evine girmesi ve bilgisayarındaki içeriği incelemesi için izin verir. Daha sonra içeriği silinmiş bir dosya bulunur.

Buna rağmen teknik yöntemler kullanılarak dosyanın içeriği kurtarılır ve yüzlerce çocuğun çıplak fotoğrafı ve Paul'un videosu ortaya çıkar.

Resimlere ne zaman ulaşıldığının ve resimlerin ne zaman silindiğinin belirlenmesi mümkün değildir.

Victor'un internet üzerinden ortak bir indirme sistemine bağlı olup olmadığı bilinmemektedir.

Victor kaç tane suç işlemiştir?

EK ÇALIŞMA MATERYALLERİ

a. Budapeşte Sözleşmesi

https://www.coe.int/en/web/cybercrime/the-budapest-convention

b. Siber Suç Sözleşmesi Ek Protokolü

https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

c. Budapeşte Sözleşmesi Açıklayıcı Rapor

https://rm.coe.int/16800cce5b#:~:text=The%20Convention%20and%20its%20Explanatory,International%20Conference%20on%20Cyber%2Dcrime.

d. Siber Suç Sözleşmesi Ek Protokolü Açıklayıcı Rapor

https://rm.coe.int/16800d37ae

e. Octopus Siber Suç Topluluğu
https://www.coe.int/en/web/octopus/home

EĞİTİM REHBERİ/PLANI

Siber suçlara ilişkin seminer

Seminerin başlıca amaçları ve hedefleri şu şekildedir:

- Cezai konularda yabancı yargı makamlarıyla iş birliği yapmak için yasal dayanakların belirlenmesi,
- Katılımcılara yeni iş birliği türleriyle (Ortak Soruşturma Ekipleri) ilgili bilgi verilmesi,
- İyi uygulamaların belirlenmesi,
- Yurt dışından çıkarılan derslerin açıklanması: Eurojust'ın cezai konularda uluslararası iş birliğindeki faydası ve rolü

Vaka çalışmaları vasıtasıyla öğrenme

- Her vakanın dikkatli bir şekilde okunması
- Vakaların başlıca hususlarına ilişkin genel tartışma
- Eğitici tarafından sunulan fikirler veya sorulara ilişkin spesifik tartışma

Seminer süresi

2 gün:

- 1. Gün: Modülde yer alan konuların açıklanması ve Türkiye'de uygulanabilir olan yasal dayanakların ayrıntılı açıklaması
- 2. Gün: Vaka çalışmaları ve diğer ülkelerde elde edilen deneyimler

Lojistik

Tartışmalara tam katılımın sağlanması için katılımcılar her birinde en fazla 10 katılımcı olacak şekilde 4 gruba ayrılabilir. İki grup, Vaka A'yı incelerken iki grup Vaka B'yi inceler. Bu oturumların sonunda, dört grup bir araya gelir ve her iki vakanın genel değerlendirmesine kendi katkılarını sağlar.

DEĞERLENDİRME FORMU

SİBER SUÇLARA İLİŞKİN SEMİNER

- Faaliyet ne kadar ilginizi çekti ve sizin işiniz ne kadar faydalı oldu? (1 hiç 10 çok yüksek anlamına gelmektedir).

İlgi çekicilik	1	2	3	4	5	6	7	8	9	10
Fayda	1	2	3	4	5	6	7	8	9	10

➢ Lütfen faaliyetin içeriğiyle ilgili olarak aşağıdaki ifadelerden hangisine katıldığınızı işaretleyiniz:

❑ Faaliyet konuları, uygulamadan ziyade daha çok teorik veya doktrin açısından ele alındı.

❑ Faaliyet konularına yönelik yaklaşım teorikten ziyade daha uygulamaya yönelikti.

❑ Faaliyetin konusuna yönelik teorik ve uygulamaya yönelik yaklaşımlar doğru bir şekilde birleştirilmişti.

➢ Lütfen faaliyetin aşağıda belirtilen hususlarıyla ilgili memnuniyet düzeyinizi belirtiniz (1 *hiç* 10 *çok yüksek* anlamına gelmektedir).

Belgelerin seçimi (ele alınan hususlar)	1	2	3	4	5	6	7	8	9	10
Eğiticiler tarafından sunulan belgeler (nicelik)	1	2	3	4	5	6	7	8	9	10
Eğiticiler tarafından sunulan belgeler (nitelik)	1	2	3	4	5	6	7	8	9	10
Faaliyetin uygulanmasında faaliyeti düzenleyenler ve eğiticiler tarafından gösterilen ilgi	1	2	3	4	5	6	7	8	9	10
Katılımcıların faaliyete gösterdiği ilgi	1	2	3	4	5	6	7	8	9	10
Zaman dağılımı	1	2	3	4	5	6	7	8	9	10
Genel olarak organizasyon	1	2	3	4	5	6	7	8	9	10

➢ Faaliyetin süresiyle ilgili olarak aşağıdaki ifadelerden hangisine katıldığınızı işaretleyiniz:

❑ Çok uzundu, daha kısa olabilirdi.

❑ Süre uzatılmalıdır.

❑ Faaliyetin içeriği ve süresi iyi ayarlanmıştı.

➢ Bu konuyla ilgili faydalı sonuçlara ulaşıldı mı?

❑ Evet

❑ Hayır

➢ Sizce, faaliyeti düzenleyenler ve eğiticiler, ilgili konular hakkında deneyim ve görüş paylaşımını teşvik etti mi?

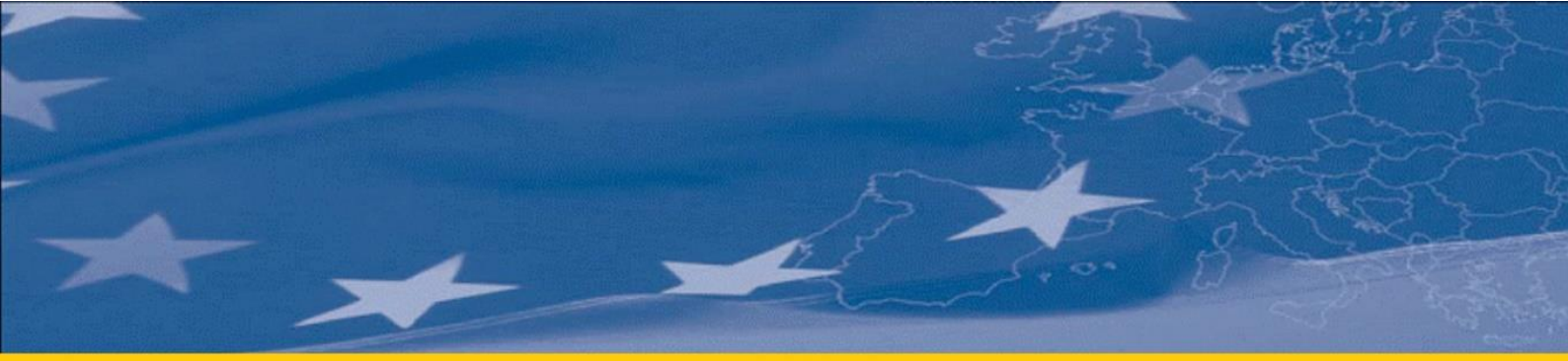
❑ Evet

❑ Hayır

➢ Faaliyetin konusu göz önünde bulundurulduğunda, sizce:

- ❑ Eğiticilerin mesleki arka planı uygun muydu?
- ❑ Farklı bakış açılarına katkıda bulunan diğer meslek gruplarından konuşmacı eksikliği var mıydı?

➢ Faaliyeti genel olarak değerlendirdiğinizde 1 ila 10 arasında kaç puan verirsiniz?:



Bu yayın, Avrupa Birliği'nin maddi desteği ile hazırlanmıştır. İçerik tamamıyla FIIAPP F.S.P.'nin sorumluluğu altındadır ve Avrupa Birliği'nin görüşlerini yansıtmak zorunda değildir.