DİN ÖĞRETİMİ
GENEL MÜDÜRLÜĞÜ

DİJİTAL GÜVENLİK VE HUKUK

AİLE ÇOCUK EĞİTİM PROGRAMI 2024

PSK. DAN. FADİME MANSIZ

ŞİRAN ŞEHİT HAKAN AYDOĞAN ANADOLU İMAM HATİP LİSESİ / PSİKOLOJİK DANIŞMA VE REHBERLİK SERVİSİ

KONU BAŞLIKLARI:

- İNTERNETTE HAK & HUKUK VE SORUMLULUKLAR
- KIŞISEL VERILERIN KORUNUMU
- WEB GÜVENLIĞI
- DİJİTAL DÜNYADA KİMLİK HIRSIZLIĞINA DİKKAT
- ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER
-
- KAYNAKÇA

İnternette Hak & Hukuk ve Sorumluluklar

İnternet ortamı insanların gerçek hayatta olduğu gibi kendilerini diledikleri gibi ifade edebilecekleri, istedikleri bilgiye istedikleri anda ulaşabilecekleri özgür bir alandır. İnsanlar iletişim özgürlüğüne sahip olduğu gibi erişim özgürlüğüne de sahiptirler ve bu anayasamızda güvence altına alınmıştır. Bu alanı kullanırken aynen gerçek hayatta olduğu gibi birtakım kişilik haklarına riayet edilmesi ve çevrimiçi ortamın bu hak ve sorumluluklara göre kullanılması için birtakım hukuki düzenlemeler yapılmıştır.

ÇEVRİMİÇİ ORTAMDA VAR OLAN BAZI BİLİŞİM SUÇLARI ŞUNLARDIR:

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
2. Bilgisayar Sabotajı
3. Bilgisayar Yoluyla Dolandırıcılık
4. Bilgisayar Yoluyla Sahtecilik

5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı
6. Kişisel Verilerin Kötüye Kullanılması
7. Sahte Kişilik Oluşturma ve Kişilik Taklidi
8. Yasadışı Yayınlar

9. Ticari Sırların Çalınması
“10. Terörist Faaliyetler
11. Çocuk Pornografisi

12. THacking
13. Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.)

İnternette Hak & Hukuk ve Sorumluluklar

Türk Ceza Kanunu'nun 243, 244 ve 245. maddeleri bilişim vasıtasıyla işlenen suçlara düzenleme getirmiştir. 243. madde ile bir bilişim sisteminin bütününe ve bir kısmına hukuka aykırı, olarak girilmesi ve orada kalmaya devam edilmesi suç olarak düzenlenmiştir. 244. madde ile bir bilişim sisteminin işleyişini engelleyen veya bozan bir kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır hükmü ile bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren var olan verileri başka bir yere gönderen kişi altı aydan üç yıla kadar hapis cezası ile cezalandırılır hükmü getirilmiştir. 245. madde ile de banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. Kredi kartı veya banka kartıyla gerçekleştirilen her türkü hukuka aykırı yarar sağlama eylemi bu suç tipini oluşturmaktadır.

Bilişim suçları yanı sıra internet içerik düzememelerine birden fazla kanunda yer verilmekle birlikte bunlardan en önemlisi olan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 2007 yılında yürürlüğe girmiştir. Kanun ile ilk defa internet ortamındaki katalog suçlar kapsamındaki yasadışı içerik ile ilgili erişimin engellenmesi usul ve esasları düzenlenmiş ve internet hizmeti veren internet aktörlerine de bir takım yükümlülük ve sorumluluklar getirilmiştir. Kanunda tanımlanmış katalog suçlara ilişkin; Bilgi Teknolojileri ve İletişim Kurumu Bilgi ve İhbar Merkezi; vatandaşların bu suçlara ilişkin şikâyetlerini bildirebilecekleri müracaat merkezi olarak kurulmuştur. 23.11.2007 tarihinde faaliyete geçen bu merkeze **http://www.ihbarweb.org.tr** adlı web adresinden yasadışı içeriğe ilişkin ihbarda bulunabilmektedir. Kanun kapsamında ayrıca vatandaşlara internet ortamında kişilik haklarının ihlali ve özel hayatın gizliliği ile ilgili olarak başvuru süreçleri tanımlanmıştır.
5651 Sayılı Kanun'daki hak ve sorumluluklarınız ile ilgili detaylı bilgiye aşağıdaki linkten ulaşabilirsiniz: **http://internet.btk.gov.tr/**

KIŞISEL VERILERIN KORUNUMU

Dünyada ve ülkemizde giderek artan internet kullanımı, birçok kolaylığı beraberinde getirirken kişisel verilerin korunumu konusu da daha önemli hale gelmiştir.

İnternet kullanan bireylerin %82,4'ünün sosyal medya kullanıcısı olduğu günümüzde, Yapılan her paylaşım, internet ortamına girilen her veri size ve bilgilerinize ulaşmak isteyen kötü niyetli kişiler tarafından kullanılabilmektedir. Özellikle sosyal paylaşım ağları kötü niyetli kişilerin bilgilerinize ulaşabileceği en kestirme yoldur. Paylaşım yapmadan önce, yapacağınız paylaşımın ne gibi sonuçlar ve riskler doğurabileceğini detaylı bir şekilde düşünmeniz gerekir.

Akıllı telefonunuza indirdiğiniz ve oynamak için sabırsızlandığınız bir oyun bile küçük bir pop-up ile sizin rızanızı basit bir onaylama yöntemi ile aldıktan sonra siz oyunu oynarken rehberinizdeki kontakları kendi veri tabanına aktarabilmekte ve sonrasında da bunları ne iş yaptığını bilmediğiniz şirketlerle paylaşabilmektedir. Bu bağlamda, uzun zamandır devletler ve ilgili sektör paydaşları veri paylaşımında kullanıcının kontrolünü arttıracak teknik çözümler üretmeye çalışırlarken öte yandan internet kullanıcılarının da dikkat etmesi gereken birtakım noktalar bulunmaktadır.

1. İnternet web tarayıcınızın 'do not track (izlememe)' seçeneğini aktif hale getirmenizi öneririz. Konu ile ilgili daha detaylı bilgiye web güvenliği bölümünden ulaşabilirsiniz.
2. İşlem yapmak istediğiniz web sayfalarının kullanım politikası ve gizlilik sözleşmelerini okuyunuz. Ayrıca ilgili sayfanın iletişim, hakkımızda bölümlerinden sayfa hakkında bilgi alınız.
3. Mobil platformlardan indirdiğiniz uygulamaların sizlerden ne gibi bilgiler toplandığını hususunu iyi analiz ediniz. Gerekirse çok fazla kullanmayacağınız uygulamaları telefonunuza indirmeyiniz.
4. İndirdiğiniz mobil uygulamaların nelerle senkronize olduğuna dikkat edin. Senkronize olmasını istemediğiniz bilgileri devre dışı bırakın. Bunun için telefon ayarlarınızdan hesaplarınızı, uygulama yönetiminizi, konum servislerinizi ve güvenliğinizi tekrar gözden geçirmenizi tavsiye ederiz.

KIŞISEL VERILERIN KORUNMASI KANUNUNA GÖRE HAKLARINIZ NELER?

Kişisel veri sahipleri olarak Anayasanın 6698 sayılı “Kişisel Verilerin Korunması Kanunu” artık yasallaşmıştır. Bu Kanuna göre sahip olduğumuz haklardan bazıları şunlardır:

- Kişisel verilerinizin işlenip işlenmediğini öğrenme.
- Kişisel verileriniz işlenmişse buna ilişkin bilgi talep etme.
- Kişisel verilerinizin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme.
- Kişisel verilerin silinmesini veya yok edilmesini isteme.
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme.
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde, zararın giderilmesini talep etme haklarına sahipsiniz.
- Kanunun tam metnine ve diğer haklarınızı öğrenmek için aşağıdaki linkten ulaşabilirsiniz:

http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

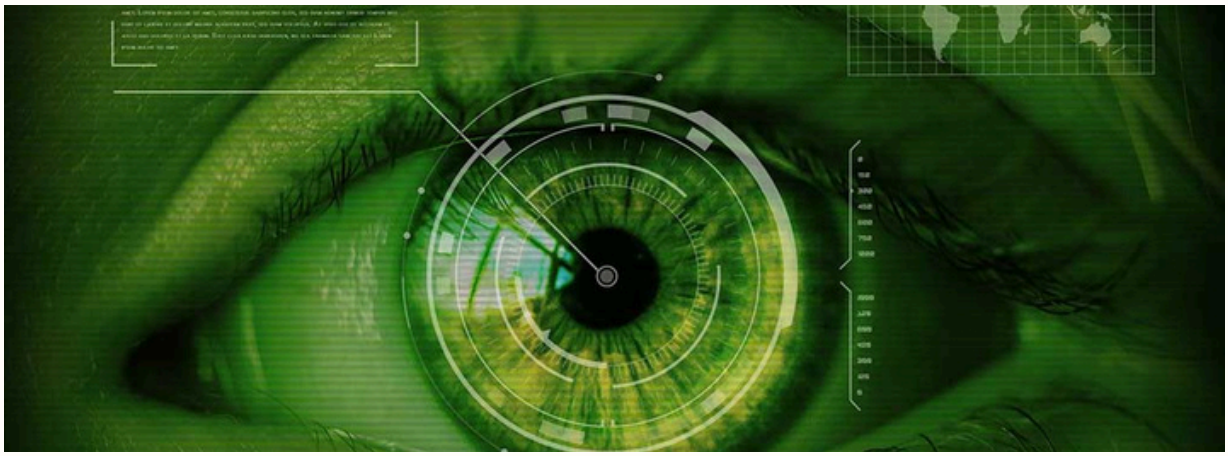
WEB GÜVENLİĞİ

Web güvenliğine öncelikle web tarayıcınızın güvenliğiyle başlamak doğru olacaktır. Bunun için hangi web tarayıcısını kullanıyorsanız kullanın tarayıcı gizlilik ve güvenlik ayarlarını yapmakla başlamalısınız. Örneğin; Firefox Mozilla'yı kullanıyorsanız Araçlar – Seçenekler Gizlilik sekmelerinden ayarlarınızı dilediğiniz gibi ayarlayabilirsiniz.

İzleme seçeneği, web sitelerinin sizin web platformunda dolaştığınız mecraların tarayıcı aracılığıyla takibinin yapılmasına olanak tanıyan bir seçenektir. Geçmişi hatırlama seçeneklerinde ise geçmişinizin asla hatırlanmamasını veya özel ayarların kullanılmasını tavsiye ederiz.

Özel ayarları yaptığınız takdirde çerez yönetimi karşınıza çıkacaktır. Çerez, herhangi bir internet sitesi tarafından bilgisayarınıza bırakılan bir hatırlama dosyasıdır. Çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır. Burada; güvendiğiniz sitelere, örneğin otomatik olarak oturum açmasına olanak sağlamak üzere, sürekli çerez bırakma yetkisi verebilirsiniz. Hiçbir sitenin bilgisayarınıza çerez bırakmasını istemiyorsanız bu seçeneği işaretlemeyin. Yalnız, kimi sitelerin çerezler devre dışıyken düzgün işlemeyeceğini de unutmayın. Bununla birlikte, bir siteyi ziyaret ederken başka bir site tarafından bırakılan "üçüncü kişilere ait çerezler" ya da "yabancı çerezler"i kapalı tutmanızı öneririz.

WEB GÜVENLİĞİ



Yapılan çalışmaların sonuçlarında, internet sitelerinde gezinti yaparken bilgisayarımıza virüs ve tehlikeli yazılım bulaştırma ihtimali yüksek olan siteler genellikle şunlardır:

1. çok fazla bilinmeyen siteler,
2. bahis siteleri,
3. pornografik siteler,
4. korsan yazılım indirilen siteler.

Bilmediğimiz web sayfalarında dolaşmamanız ve çok dikkatli olmanız gerekmektedir. Birçok web sitesi çeşitli tuzaklar barındırıyor olabilir. Bu yüzden güvendiğiniz, bildiğiniz web sayfalarını tercih etmeniz, bilmediğiniz web sayfalarının hakkında/iletişim gibi bölümlerinden web sayfaları hakkında bilgi edinmemiz gerekmektedir. Ayrıca sık kullandığımız web siteleri için tarayıcımızda sık kullanılanlar listesi oluşturmanız, Tuzak sitelerden korunmak adına önem teşkil etmektedir. Bunun için web güvenliğinde öncelikli olarak:

- Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek,
- E-posta mesajları ile gönderilen bağlantılara dikkat etmek,
- Sık kullanılanlar listesi oluşturmak,
- Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak (Yukarıda bahsedilen ayarlar),
- Arama motorlarını kullanırken özellikle çocuklu ailelerin yüksek düzeyli filtreleme araçları sayesinde özellikle müstehcen sitelerin arama sonuçlarında engellenmesini ve bu sayede güvenli arama sağlamaları gerekmektedir. Örneğin Google için **https://www.google.com.tr/preferences** linkinden güvenli arama seçeneğini değiştirebilirsiniz.

WEB GÜVENLIĞI

Benzer şekilde Araçlar-Seçenekler-İçerik sekmesinden ve Araçlar-Seçenekler-Güvenlik sekmesinden Firefox ayarlarınızı aşağıdaki tablolarda gösterildiği şekilde yapmanızı öneririz.
FireFox ile daha fazla bilgiye FireFox'un yardım sayfasından ulaşabilirsiniz:

https://support.mozilla.org/tr/

Benzer ayarlara Internet Explorer'da Araçlar-İnternet Seçenekleri'nden ve Google Chrome için Chrome menüsü (sağ üstte yer alan 3 noktadan ulaşılıyor) - Ayarlar - (Gelişmiş) Gizlilik bölümünden ulaşabilirsiniz.
Daha fazla bilgiye Chrome için:

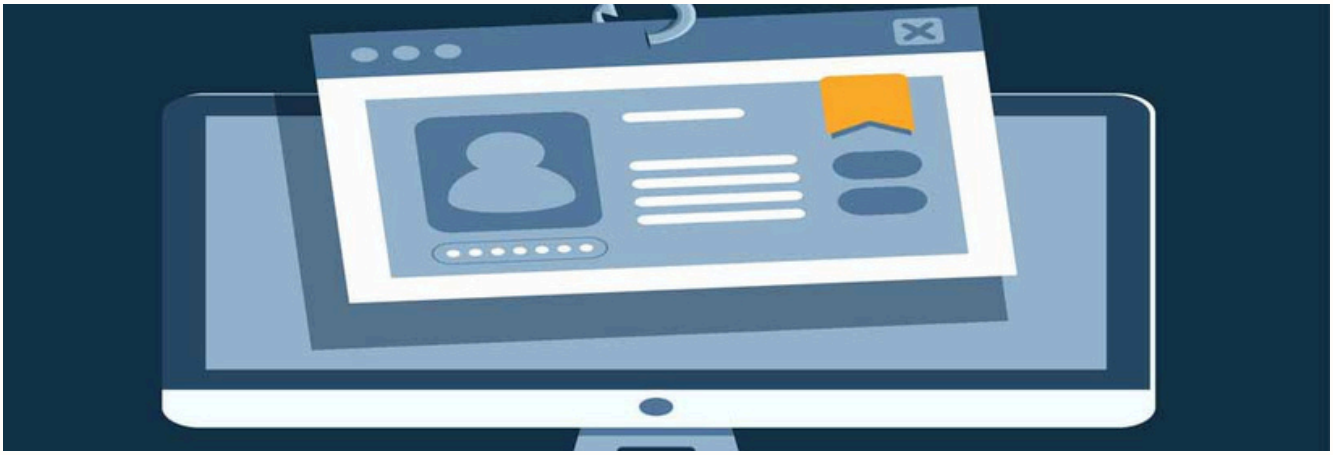
https://support.google.com/chrome/#topic=3227046

Internet Explorer için

https://support.microsoft.com/tr-tr/products/internet-explorer adreslerinden ulaşabilirsiniz.

Tarayıcı ayarlarını kendi bilgisayarınızdan ve/veya tanımadığınız bir bilgisayardan internete bağlanırken yaptıktan sonra internette gezinmeye başlayabiliriz.

DİJİTAL DÜNYADA KİMLİK HIRSIZLIĞINA DİKKAT



Son dönemde sıkça karşılaşılan internet zararlarından bir tanesi de kimlik hırsızlığı. Günümüzde internet kullanıcılarının kimlik bilgilerini ele geçirmek için internette pek çok tuzak bulunuyor. Kimlik hırsızlığı kısaca başkalarının izniniz olmadan kişisel bilgilerinizi kullanması anlamına geliyor.

Çalıntı veya sahte kimlik yöntemiyle veya kimlik avı ve sosyal mühendislik teknikleri ile TC Kimlik Numaranız, sosyal sigorta numaranız, parolanız, adresiniz, anne kızlık soyadınız, kredi kartı numaranız gibi kişisel bilgileriniz bilginiz dışında kullanılabiliyor ve bu durum beraberinde birçok maddi ve manevi tehlikeli sonucu doğuruyor. Örneğin kimlik bilgilerinizi ele geçiren bir kişi, sizin adınıza bankalarda ve kimlik onayı gerektiren internet sitelerinde işlemler yapabilir, Sizin adınıza telefon hattı veya banka hesabı açabilir, kefil olabilir hatta şirket kurabilir.

Nitekim TC kimlikleri fiziksel olarak çalınan veya TC kimlik numarası, anne kızlık soyadı vb kişisel bilgileri bilgisi dışında sosyal mühendislik teknikleri ile ele geçirilen kişilerin üzerlerine bir şirket açılması, bir şirkete ortak/yönetici yapılması ile yaşanan mağduriyetlere dair birçok haber medyada yer alıyor.

Birçok vatandaşın bu yolla mağdur edilmesinin önüne geçmek için internet yoluyla kolay ve etkili bir çözüm bulunuyor. Daha önce ticaret sicili müdürlüklerine başvuru yapılarak gerçekleştirilen kimlik numarası kısıtlaması e-Devlet üzerinden gerçekleştirilebiliyor.

DİJİTAL DÜNYADA KİMLİK HIRSIZLIĞINA DİKKAT

e-Devlet üzerinden birkaç dokunuşla gerçekleştirilen kimlik numara kısıtlaması ile vatandaşların farkında bile olmadan bir şirkete ortak ya da yönetici olmasını engellenebiliyor.
T.C. kimlik numaranızı nasıl kısıtlarsınız?

- e-Devlet adresine giriş yapın.
- "Kurumlar" menüsünden Ticaret Bakanlığı'na ulaşın.
- "Ortak / Yetkili Olunmasına Yönelik Kısıtlama İşlemleri (MERSİS)" seçeneğini seçin.
- "Yeni Başvuru" butonuna tıklayın.
- Bilgileri doldurun ve onaylayın.

Peki, internet ortamında kimlik avı ve sosyal mühendislik teknikleri ile TC Kimlik Numaranız, sosyal sigorta numaranız, parolanız, adresiniz, anne kızlık soyadınız, kredi kartı numaranız gibi kişisel bilgileriniz bilginiz dışında kullanılmaması kısaca kimlik hırsızlığından korunabilmek için hangi önlemler alınmalı?

- **Cihazlarınızı koruyun:** Akıllı telefonunuzu, dizüstü bilgisayarınızı, tabletinizi güvenliği artırılmış, güncel virüs yazılımları kullanarak zararlı yazılımlardan ve saldırganlardan koruyun.
- **Şüpheli sitelerden ve mesajlardan uzak durun:** Kişisel bilgilerinizin nasıl ele geçirileceği konusunda bilgi sahibi olun ve kimlik bilgilerini çalmak amacı ile istenmeyen e-posta veya açılır pencere yoluyla yapılan aldatma yöntemlerine karşı dikkatli olun.

DİJİTAL DÜNYADA KİMLİK HIRSIZLIĞINA DİKKAT

Güvenli bağlantılara tıklayın: Kişisel bilgilerinizi sadece bağlantınız güvenli olduğunda çevrimiçi kullanın. Kamuya açık Wi-Fi ağlarından kaçının, tercihen ev veya iş yeri ağını tercih edin. Mecbur kaldığınızda kişisel bilgilerinizi şifreleyecek sanal özel ağ (VPN) kullanın.

• **Güçlü şifre oluşturun:** Tahmin edilemeyecek, uzun, güçlü ve basit saldırı yöntemleri karşısında kırılması güç şifreler oluşturun. Bütün şifrelerinizi bir şifre yöneticisinde saklayın. Şifrelerinizi daha güçlü koruyabilmek için iki faktörlü kimlik doğrulaması kullanın. Unutmayın birkaç farklı hesap için aynı şifreyi asla kullanmayın ve şifrenizi sakın paylaşmayın veya kaydetmeyin.

• **Kişisel verilerin bulunduğu cihazlara dikkat edin:** İçinde dijital kişisel bilgilerinizi sakladığınız elektronik cihazlarınızdaki verileri sildiğinizden emin olun. Örneğin; eski akıllı telefonunuzu ya da tabletinizi satarken; telefonunuzu, tabletinizi yedekleyin, hesaplarınızı devre dışı bırakın, verilerinizi silmeden önce şifreleyin, telefonunuzu fabrika ayarlarına sıfırlayın.

• **Banka hesaplarınızı sürekli izleyin ve denetleyin:** Çevrimiçi olarak kullandığınız banka hesabınızı düzenli olarak sürekli kontrol etmeniz izinsiz bir müdahaleyi fark etmenizi sağlayabilir. Banka hesabınızın izniniz dışında kullanılmasını önlemek için işlem limitleri belirleyin.
• **Paylaşımlarınızı sınırlandırın:** Sosyal medya hesaplarınızdan kimliğiniz, uçak biletleriniz vb. bilgi ve belgelerinizi sakın paylaşmayın. Kişisel bilgilerinizle ilgili ayrıntı veren paylaşımlarınızı kötü niyetli kişilerin yerinize geçmek için kullanabileceğini unutmayın.

ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER

Özel hayat kavramına ilk defa İnsan Hakları Evrensel Beyannamesinde yer verilmiştir. 10 Aralık 1948 tarihinde ilan edilen beyannamenin 12.maddesine göre;

“Hiç kimse özel hayatı ailesi, meskeni ve yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.”

T.C. Anayasasında özel hayatın gizliliği; özel hayatın korunması başlığı altında ilk kez 1961 Anayasasında yer almıştır. Mevcut Anayasamız olan 1982 Anayasasında; Kişinin Hakları ve Ödevleri başlığı altında 20. madde ile özel hayatın gizliliği düzenleme alanı bulmuştur. 5237 sayılı Tük Ceza Kanununda özel hükümler ikinci kısım dokuzuncu bölüm, Özel Hayata ve Hayatın Gizli Alanına karşı suçlar başlığı altında 134. Madde ile, Özel Hayatın Gizliliğini İhlal suçu düzenleme alanı bularak yaptırıma bağlanmıştır.

Bu nedenle de 5651 sayılı Kanun kapsamında özel hayatın gizliliğinin ihlaliyle ilgili düzenleme yapılmıştır. Kanunun 9/A maddesinde internet üzerinden gerçekleşen ihlallerde, Özel Hayatın Gizliliğinin ihlal edildiği İçeriğe Erişimin Engellenmesi şeklinde yer almaktadır. Kanunun 9/A maddesinde; internet ortamında işlenen suçlarla mücadele etmek ve bu ortamda ortaya çıkan ihlalleri gidermek amacıyla kullanılan temel araçlar niteliğindeki erişimin engellenmesi ve ihlal konusu içeriğin yayından çıkarılması yöntemleri düzenlenmiştir.

ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER

Özel hayatın gizliliğini ihlal suçunun ceza hukuku açısından kısa bir değerlendirmesi:

Türk Ceza Kanunun 134. maddesini de ihtiva eden kişilere karşı suçlar kısmının dokuzuncu bölümünde ana başlık olarak hayatın gizli alanının ihlalinden söz edilmektedir. Burada koruma altına alınmak istenen kişinin aile hayatı, sırları gibi kavramlardır. Kişinin gizli alanı hiç kimseyle paylaşmadığı kendine ait alanı ifade etmektedir.

TCK 134. madde ile Özel Hayatın Gizliliğini İhlal suçu iki fıkra halinde düzenlenmiştir:

- İlk fıkrada özel hayatın gizliliğini ihlal eden kimsenin cezasının bir yıldan üç yıla kadar hapis cezası olacağı belirtilmiştir. Gizliliğin görüntü ve seslerin kayda alınması suretiyle ihlal edilmesi halinde ise ceza bir kat artırılır.
- İkinci fıkrada ise kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimsenin iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağı ve ifşa edilen bu verilerin basın yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunacağı belirtilmiştir.
- Bu suçun faili herkes olabilir. Kanunun 137. maddesinde sayılan kimseler tarafından işlenmesi hali kanun koyucu tarafından nitelikli hal sayılmış olup bu kişiler tarafından işlenmesi halinde ceza artırımına gidilir. Yani kişiye özgü bir suç değildir. Herkes bu suçun mağduru olabilir.
- Bu kanunla korunan hukuki değer, kişilerin mahremiyet alanıdır. Suç serbest hareketli bir suçtur. Buradan anlamamız gereken neticenin meydana gelmesi bu suçun oluşması için yeterlidir. Hareketin meydana geliş biçimi önem arz etmez. Örneğin bir kişinin çantasının karıştırılmasıyla suç oluşmuştur.

ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER

Örneğin;

Kendinize ait herkese açık olan platformlardan birinde paylaşmış olmadığınız ve kimseyle paylaşmak istemediğiniz cep telefonunuzda bulunan bir fotoğrafınız üçüncü bir kişi tarafından ele geçirilip internet ortamında paylaşıldı. Yani ifşa edildi. İfşa kelimesi sözlükte herhangi gizli bir şeyi açığa çıkarma, yayma anlamına gelir. Örnek olayda TCK 134/2 suçu oluşmuştur.

internet ortamında özel hayatın gizliliği ihlal edilmesi halinde – nasıl bir hukuki süreç izlememiz gerekir?

Bu husus, 5651 sayılı Kanunun 9/A maddesinde düzenlenmiştir.

Buna göre:

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Bilgi Teknolojileri ve İletişim Kurumuna doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Kurum, kendisine gelen bu talebi uygulanmak üzere derhâl Erişim Sağlayıcıları Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Bilgi Teknolojileri ve İletişim Kurumuna gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.”

ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER

Bu başvuru **İnternet Bilgi İhbar Merkezi** üzerinden e-devlet ile kimliğin doğrulanmasından sonra veya e-devlete giriş yapıldıktan sonra adım adım diğer işlemler tamamlanıp başvuru gerçekleştirilir.

5651 sayılı kanunun 9/A maddesi 8.fıkrası gereği, gecikmesinde sakınca bulunan bir hal olduğu durumlarda doğrudan Başkanın emri üzerine erişim engellemesi kurum tarafından yapılır. Bu fıkra kapsamında Başkan tarafından verilen erişim engellenmesi kararı 24 saat içinde sulh ceza hâkiminin onayına sunulur ve hâkim de kararını 48 saat içinde açıklar.

Özel hayatın gizliliğinin korunması aynı zamanda bir kişilik hakkı olduğu için böyle bir duruma maruz kalan kişi, 5651 sayılı kanunun 9. Maddesinde yer alan korumadan da yararlanabilir. Böyle bir durumda kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de talep edebilirler.

ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET: TAKİP EDİLMESİ GEREKEN SÜREÇLER

Peki, böyle bir durumla karşılaştığımızda neler yapılabilir?
Youtube, Facebook, Instagram platformlarında siber zorbalığa maruz kalındığında şikâyet etmek için oluşturulmuş yardım merkezleri bulunmaktadır. Böyle bir durumla karşılaşıldığında geldiğinde başvurabileceğimiz yöntemlerden biri budur. Yukarıda bahsedilen kanuni yöntemlerden önce, aşağıdaki adreslere göz atmak faydalı olacaktır:

- **İnternet İçerik Şikâyet Süreçleri**
- **Sosyal Medya Rehberi**

Adli kurumlara başvurmadan önce dikkat edilmesi gereken en önemli hususlardan biri:
Size yapılan tehdit ve hakaret; e-posta yolu ile yapılmış ise içeriklerinin çıktısını alınarak, bir site üzerinde yapılmış ise ayrıntılı hakaret veya tehdit metnini, yazan kişinin ismi veya takma adı, hakaret veya tehdit yapılan tarih ve saat görünecek şekilde ekran görüntüsü alınarak süreç hızlandırılabilir. Bunlar delil olarak kullanılabileceği için yargılama sürecinde fayda sağlayacaktır. Daha sonra da şikâyet usulüyle adli süreci devam ettirilebilir.

KAYNAKÇA

https://www.guvenliweb.org.tr/dokuman-detay/kisisel-verilerin-korunumu

https://www.guvenliweb.org.tr/dokuman-detay/internette-hak-hukuk-ve-sorumluluklar

https://www.guvenliweb.org.tr/haber-detay/dijital-dunyada-kimlik-hirsizligina-dikkat

https://www.guvenliweb.org.tr/blog-detay/ozel-hayatin-gizliligi-ve-mahremiyet-takip-edilmesi-gereken-surecler