Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-15

Hukuki Açıdan Bilişim Suçları, Siber Güvenlik, Adli Bilişim Ve Güncel Teknolojiler

https://www.siberportal.org/red-team/cyber-attacks/bilisim-suclari-kategorileri-ve-cesitleri/

Hafta-15

Bilişim Hukuku ve Bilişim Suçu

Temel Kavramlar

- **Bilişim,** elektronik sistemlerin tamamını içeren bir üst terimdir,
- **Bilişim**, bilgi ve teknolojinin birlikte kullanılarak üretilen sonuçladır,
- **Bilişim**, teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve ozellikle elektronik aletler aracılığıyla düzenli bir biçimde işlenmeyi öngören bir bilimdir. Bir diğer tabirle, her türlü bilgi ve verinin elektronik bilgi işlem araçlarıyla işlenmesini ve değerlendirme tekniklerini konu alan bilim şeklinde de tanımlanabilmektedir.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Hafta-15

Bilişim Hukuku ve Bilişim Suçu

Temel Kavramlar

- **Bilişim Hukuku**: bilgi ve teknolojinin kotüye kullanımı ile insanlara zarar verilmesini onlemek amacıyla ortaya çıkmış olan bir hukuk dalı

- **Bilişim Suçları:** bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış ya da, bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlar şekliyle de tanımlanabilir.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

Türkiye'de bilişim alanında gerçekleştirilen yasal düzenlemeler, genel olarak AB direktifleri ile uyumlu olacak şekilde hazırlanmıştır. Bilişim suçları, her suçun kendi alanına ilişkin düzenlemeler içermektedir.

Bilişim suçlarına yönelik Türkiye'de ilk yasal metin, 765 sayılı Türk Ceza Kanununa 1991 yılında eklenen "…bilgileri otomatik işleme tabi tutan sistem…" ibaresidir. Bundan sonra ortaya çıkan ihtiyaçlar neticesince bir çok kanuna bilişim ile ilgili hükümler eklenmiştir.

Bilişim suçları ile ilgili en kapsamlı düzenleme 5237 sayılı Türk Ceza Kanununda yer almaktadır.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

Türk Ceza Kanununun onuncu bölümünde bilişim alanında suçlar başlığı altında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kotüye kullanılması konularında düzenleme getirmiştir.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

- 5237 sayılı Türk Ceza Kanunu'nun Özel Hükümler isimli İkinci Kitap'ının "Topluma Karşı Suçlar" başlıklı Üçüncü Kısım'ının Onuncu Bölümü "Bilişim Alanında Suçlar"a ayrılmıştır.

- Bilişim sistemine girme (Madde 243), Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244), Banka veya kredi kartlarının kötüye kullanılması (Madde 245), Yasak cihaz veya programlar (Madde 245A) ve Tüzel kişiler hakkında güvenlik tedbiri uygulanması (Madde 246) madde başlıklı beş farklı maddeyle bilişim alanını ilgilendiren en önemli fiil ve hareketler suç kapsamına alınmıştır.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

Bu suçların, bilişim sistemlerinin güvenliği, sistemin manipüle edilmeden doğru bir şekilde işlemesi, içerdiği verilerin bütünlüğü, sıhhati, sistem içerisinde kredi kartlarının kullanılma yoğunluğu ve ekonomik sistemdeki rolü nedeniyle; bu sistemlerin kötüye kullanılmasının önlenmesi, toplumdaki herkesin yararına olacağı için "Topluma Karşı Suçlar" kısmında düzenlenmiştir

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

- 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle Türk Ceza Kanunu'na eklenen 245A maddesinde yer alan yasak cihaz veya programlar suçu...

- 6698 sayılı Kanun'un 30. maddesiyle Türk Ceza Kanunu'nun 243. maddesine eklenen dördüncü fıkrada kendine yer bulan veri nakillerini sisteme girmeksizin izleme suçu...

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilişim Suçları

Türk Ceza Kanunu'nun başka bölümlerinde de bilişim sistemlerini ilgilendiren, bilişim sistemlerini kullanarak haksız yarar sağlamayı veya bilişim sistemlerinin bir aracı olarak kullanılmasını farklı şekilde yaptırıma bağlayan hükümler yer almaktadır.

"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümde yer alan Kişisel verilerin kaydedilmesi (Madde 135), Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136), Verileri yok etmeme (Madde 138) suçları dışında, Türk Ceza Kanunu'nun çeşitli bölümlerinde, Haberleşmenin gizliliğinin ihlali suçu (Madde 132), Hakaret (Madde 125), Haberleşmenin engellenmesi suçu (Madde 124), Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (Madde 142/2-e), Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (Madde 158/1-f) gibi bilişim sistemleriyle işlenmesi mümkün çeşitli suçlar da yer almaktadır.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Türkiye'de İnternet Hukuku

Türkiye'de internet ile ilgili en kapsamlı düzenleme 2007 yılında 5628 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile yapılmıştır.

5628 sayılı Kanun ile ilk defa;

- İnternet aktorlerinin (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu aktorlerin hak ve sorumlulukları belirlenmiştir.
- Yasada suçlar bakımından erişimin engellenmesi usul ve esasları düzenlenmiştir.
- İnternet ortamında yayınlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.
- Konusu suç teşkil eden (ve/veya küçükler için zararlı olan) içerik kapsamında filtreleme usulü öngörülmüştür.
- Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği internet bilgi ihbar merkezi (ihbarweb.org.tr) kurulmuştur.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Türkiye'de İnternet Hukuku

5628 sayılı Kanununun 8 inci maddesinde erişimi engellenebilecek suçları katalog halinde saymıştır. İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir. Bunlar:

26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yonlendirme (madde 84),
2) Çocukların cinsel istismarı (madde 103, birinci fıkra),
3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
4) Sağlık için tehlikeli madde temini (madde 194),
5) Müstehcenlik (madde 226)
6) Fuhuş (madde 227)
7) Kumar oynanması için yer ve imkân sağlama (madde 228), suçları ve

25/7/1928 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

SOME Vaka Müdahele Araçları

Vaka Müdahale Araçları

SOME'nin olaylara müdahalede kullanabileceği birçok araç *(tool)* vardır. Aşağıdaki tabloda bu araçlardan bazıları sıralanmıştır. Sıralanan araçların büyük bir kısmı kitabımızın **Üçüncü Bölümünde** kapsamlı bir şekilde ele alınmıştır. Bu nedenle ayrıntılarına inmeden isimlerini ve hangi maksatla kullanılabileceklerini listeleyip, sadece en etkili araçlar arasında gördüğümüz GetData Forensic Imager, AccessData FTK Imager, Binalyze IREC TACTICAL ve IREC AIR hakkında bilgilendirme yapacağız.

Görev	Kullanılan Aygıt/Yazılım
Disk imajları (adli kopya) oluşturma	GetData Forensic Imager, AccessData FTK Imager
Ağ paylaşımını görüntüle	BySoft Network Share Browser, NetShare Watcher
Olaya müdahale ve veri toplama	Binalyze IREC TACTICAL ve IREC AIR
Kullanıcı yetkileri yönetimi	Novell ZENworks Desktop Manager 7, Windows Users and Groups Control Panel
Silinmiş verilerin kurtarılması	Forensic Explorer, RecoverMyFiles, TestDisk, Foremost

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

SOME Vaka Müdahele Araçları

Network koklama (sniffing)/paket analizi	Wireshark, Packetyzer, TCPdump, LiveAction Omnipeek
Şifre/Parola kırma	Cain&Abel, John the Ripper, Passware, Elcomsoft
Aktif port sıralama	Nmap, Netcat

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

Adli Bilişim ve Vaka Araçları

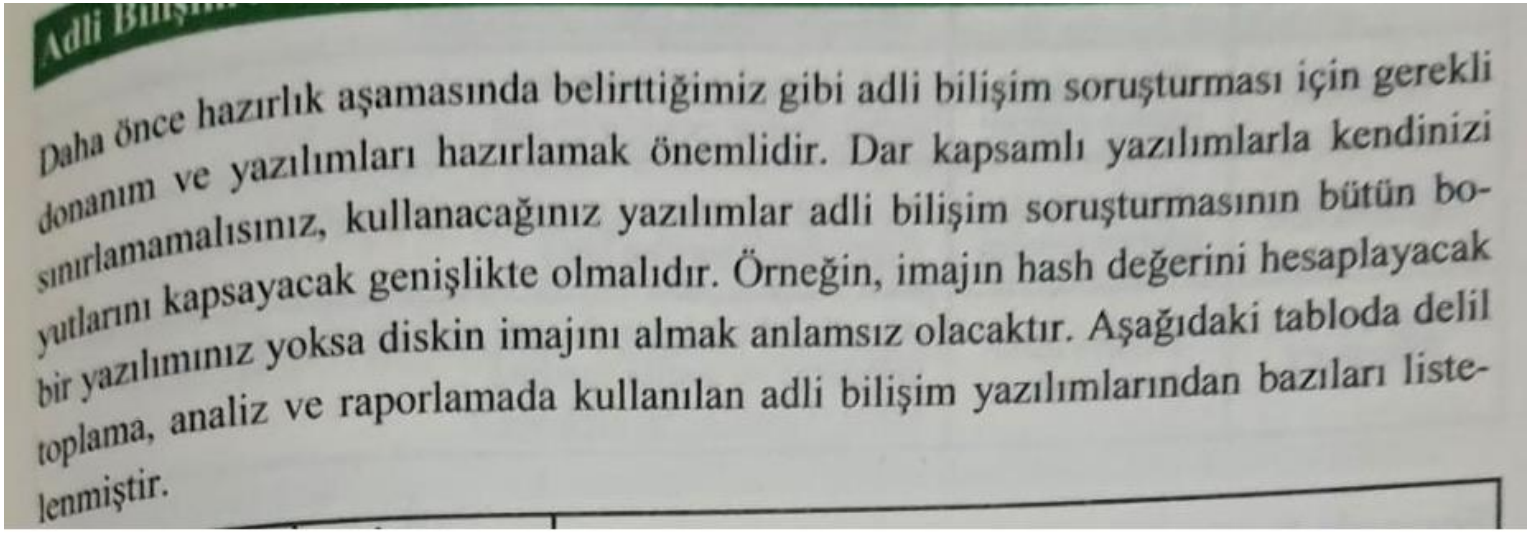
Adli bilişim, bilgisayarlar veya dijital saklama aygıtlarında veya elektronik ortamda bulunan yasal delillerin elde edilmesine ilişkin olan adli bilimler altında sınıfl andıran bir branştır. Bu bilim dalı uluslararası standartlarla şekillenmiştir. ISO tarafından 2012 yılında yayımlanan ve 2018 yılında gözden geçirilen ISO/IEC 27037:2012 bu alandaki en temel belgedir.

Adli Bilişim ve Vaka Araçları

Türk hukukunda **adli bilişimle** ilgili temel düzenleme **5271 sayılı Ceza Muhakemesi Kanunu'nun** "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlıklı **134. maddesi** altında düzenlenmiştir. Söz konusu hükme göre bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surett e delil elde etme imkanının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir.

Hafta-15

Adli Bilişim Vaka Araçları



Daha önce hazırlık aşamasında belirttiğimiz gibi adli bilişim soruşturması için gerekli donanım ve yazılımları hazırlamak önemlidir. Dar kapsamlı yazılımlarla kendinizi sınırlamamalısınız, kullanacağınız yazılımlar adli bilişim soruşturmasının bütün bo-yutlarını kapsayacak genişlikte olmalıdır. Örneğin, imajın hash değerini hesaplayacak bir yazılımınız yoksa diskin imajını almak anlamsız olacaktır. Aşağıdaki tabloda delil toplama, analiz ve raporlamada kullanılan adli bilişim yazılımlarından bazıları liste-lenmiştir.

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

Adli Bilişim Vaka Araçları

Yazılım	İşletim Sistemi	Açıklama
Autopsy-The Sleuth Kit (TSK)	Birden fazla işletim sistemi	Genel maksat açık kaynak adli bilişim yazılımı. Autopsy ismiyle grafiksel arayüzü vardır. (https://www.sleuthkit.org/autopsy//)
Forensic Explorer	Windows	Delil toplama, analiz ve raporlama dâhil geniş yelpazede adli bilişim imkânları sunan özel bir yazılım. (http://www.forensicexplorer.com/)
EnCase	Windows	Delil toplama, analiz ve raporlama dâhil geniş yelpazede adli bilişim imkânları sunan özel bir yazılım. (https://www.guidancesoftware.com/encase-forensic)
CAINE	Linux/ Windows	CAINE (Computer Aided INvestigative Environment) içerisinde adli bilişim yazılımı olan açık kaynak Linux dağıtımı (https://www.caine-live.net/)
Forensic Toolkit (FTK)	Windows	Çok maksatlı bir yazılım olan FTK ile bir disk taranarak önizlemesi yapılabilir. Bu yazılım ile lokal sabit sürücülerin, USB hafıza kartlarının, Zip sürücülerin, CD ve DVD'lerin imajı alınabilir. Aynı zamanda FTK Imager bu ortamlardaki dijital delillerin imajını almadan ön izlenmesine de imkân tanır. (https://accessdata.com/products-services/forensic-toolkit-ftk)

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

Adli Bilişim Vaka Araçları

SIFT	Ubuntu (Linux)	SANS Investigative Forensic Toolkit (SIFT), SANS Institute tarafından geliştirilmiş, adli bilişim soruşturmalarında kullanılabilecek ücretsiz uygulamaları olan bir açık kaynak yazılımdır. *(https://digital-forensics.sans.org/community/downloads)*
DFF	Birden fazla işletim sistemi	Digital Forensics Framework (DFF), gerek uzman olmayanlar gerekse uzmanlar tarafında kullanılabilecek genel maksat açık kaynak adli bilişim yazılımı. *(https://github.com/elthariel/dff)*
COFEE	Windows	Computer Online Forensic Evidence Extractor (COFEE), Microsoft tarafından geliştirilmiş özel bir yazılım. Yazılım hedef bilgisayara takılacak USB belleğe yükleniyor. İnternet geçmişi, silinen dosyalar ve uçucu veriler gibi adli bilişim verilerini topluyor. *(https://www.megaleecher.net/taxonomy/term/8324)*
WindowsSCOPE	Windows	RAM'dekiler gibi uçucu verileri incelemek için geliştirilmiş canlı adli bilişim yapabilen özel bir yazılım. *(http://www.windowsscope.com/)*
Volatility	Windows, Linux	RAM'dekiler gibi uçucu verileri incelemek için geliştirilmiş bir açık kaynak yazılımı. *(http://www.volatilityfoundation.org/)*

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

Adli Bilişim Vaka Araçları

Foremost	Linux	Açık kaynak veri kurtarma ve kazıma yazılımı. *(http://foremost.sourceforge.net/)*
TestDisk	Birden fazla işletim sistemi	Açık kaynak veri kurtarma ve kazıma yazılımı. *(https://www.cgsecurity.org/wiki/TestDisk)*
log2timeline	Birden fazla işletim sistemi	Açık kaynak zaman çizelgesi oluşturma yazılımı. *(http://log2timeline.net/)*
Wireshark	Birden fazla işletim sistemi	Ağ adli bilişimi için faydalı olabilecek açık kaynak paket yakalama ve analiz yazılımı. *(https://www.wireshark.org/)*

Erdal Özkaya, Siber Güvenlik Saldırı ve Savunma Stratejileri, Ekim 2022, Buzdağı Yayınevi

Hafta-15

KVKK nedir ve Sorumluluklarımız

KVKK, kişisel verilerin korunma kanunu anlamına gelmektedir.

https://berqnet.com/blog/kvkk-nedir

KVKK nedir ve Sorumluluklarımız

Veriyi Hangi Ortamda Olursa Olsun Korumak Zorundayız!

Hem kamu hem de özel kurum ve kuruluşlar, bir hizmetin veya ürünün piyasaya sürülebilmesi için uzun bir süredir kişisel veri niteliğindeki bilgileri toplamakta, satmakta veya paylaşmaktaydılar. Ancak kişilerin temel hak ve özgürlükleri kapsamında veri işleme süresince verinin korunması öncelikli olmalıdır.

https://berqnet.com/blog/kvkk-nedir

Hafta-15

KVKK nedir ve Sorumluluklarımız

Veriyi Hangi Ortamda Olursa Olsun Korumak Zorundayız!

Kurumların vermiş oldukları hizmetlerin sürdürülmesi, kamu hizmetlerinin etkin bir şekilde halka arz edilmesi, mal ve hizmetlerin geliştirilmesi, dağıtımı ve pazarlanması için kişisel verilerin toplanması kaçınılmaz bir hale gelmiştir.

Bu veriler toplanırken de kişisel verilerin sınırsız ve gelişigüzel olması sebepleri, yetkisiz kişilerin erişimine açılmasının, ifşasının, amaç dışında ya da kötüye kullanımı sonucunda kişisel hakların ihlal edilmesinin de önüne geçilmesi kişisel hak ve özgürlüklerimiz noktasında zorunlu olmalıdır.

Bu sebeple Avrupa Konseyi tarafından bir süre önce tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme”, 28 Ocak 1981 tarihinde imzaya açılmış ve ülkemiz tarafından da Avrupa Birliği Üyelik Kapsamı dahilinde imzalanmıştır.
Bu sözleşme son olarak 17 Mart 2016 tarihinde Resmî Gazetede yayımlanarak iç hukuka dâhil edilmiştir.

https://berqnet.com/blog/kvkk-nedir

KVKK nedir ve Sorumluluklarımız

Kişisel Verilerin Korunması Hakkı Nedir?

2010 yılında yapılan Anayasa değişikliği ile Anayasanın özel hayatın gizliliğini düzenleyen 20. maddesine belirtildiği gibi temel bir hak olarak düzenlenen kişisel verilerin korunmasını isteme hakkı, Anayasanın kişinin hak ve ödevlerine ilişkin bölümünde yer almıştır. Aynı şekilde kişisel verilerin korunmasına ilişkin hak Anayasada çizilen sınırlar çerçevesinde diğer hak ve özgürlükler lehine sınırlandırılabilir. Avrupa Birliğine uyum kapsamında hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı 18 Ocak 2016 tarihinde TBMM Başkanlığına sevk edildi.

https://berqnet.com/blog/kvkk-nedir

KVKK nedir ve Sorumluluklarımız

KVKK Ne Zaman Yürürlüğe Girdi?

Söz konusu olan KVKK kanun metini 24 Mart 2016 tarihinde TBMM Genel Kurulu tarafından kabul edilerek kanunlaşmış ve 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

KVKK Nedir?

KVKK, Kişisel Verilerin Korunması Kanunudur. Aynı zamanda bu kanunu işletebilmek ve süreçleri sürdürebilmek için KVKK kurumu hayatımıza girmiştir. Bu tarihten sonra denetimler başlayarak kişisel verilerin korunması konusunda ciddi adımlar atılmaya başlanmıştır. Uzun bir süredir tasarı halinde bekleyen KVKK kanunu 7 Nisan 2016 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiştir. Bu sayede kişisel verilerin işlenmesinden tutun da özel hayatın gizliliğine kadar kişilerin temel hak ve özgürlüklerini korumak için kişisel verileri işleyen firmaların yükümlülükleri ile uyacakları kurallar belirlenmiştir.

https://berqnet.com/blog/kvkk-nedir

KVKK nedir ve Sorumluluklarımız

Kişisel Verilerin Korunması 6698 Sayılı Kanununun Amacı Nedir?

Uluslararası belgeler, mukayeseli hukuk uygulamaları ve ülkemizin ihtiyaçları göz önüne alınması için hazırlanan bu kanun ile kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması amaçlanmaktadır.

KVKK Kanununun amacı, kişisel verilerin işlenme şartlarını, kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemekle başlamıştır. Kişinin mahremiyetinin korunması ile veri güvenliğinin sağlanması da bu kapsamda değerlendirilmektedir. KVKK kanunu ile, kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanır.

https://berqnet.com/blog/kvkk-nedir

Hoşcakalın