ham haldeki veridir.
TCK 244/2'de tanımlanan diğer bir eylem ise "verileri yok etmek"tir. Bilişim sistemindeki verilerin yok edilmesinden, verilere ulaşılmasının tamamen engellenmesi anlaşılmalıdır. Bu durumda, bilişim sistemindeki veriler, yukarıda harddiskin kırılması örneğinde olduğunun aksine, somut olarak değil, soyut (mantıksal) olarak ortadan kaldırılmaktadır. Bu tür verilerin yeniden ortaya çıkarılması , bazen uzun uğraşlar sonucunda bazen de kolaylıkla mümkün olabilmektedir. Verilerin yok edilmesine örnek olarak, bilişim sisteminin belleğindeki verilerin geri dönüşümü olanaksız biçimde silinmesi (format edilmesi) verilebilir.

TCK 244/2'de tanımlanan diğer bir eylem ise, verilerin değiştirilmesidir. Bundan kasıt, bilişim sistemindeki bir verinin silinerek yerine başka bir verinin konması ya da sistemdeki veriyle başka bir verinin değiştirilmesidir. Bir başka deyişle, verilerin değiştirilmesinde verilerin orijinal halinden başka bir hale dönüştürülmesi söz konusu olmaktadır. Bu dönüştürmenin kısmen veya tamamen oluşu ya da dönüştürme ile çıkar sağlama ya da zarar verme kastı güdülmüş olması arasında, suçun oluşması bakımından fark yoktur.

244/2'de belirtilen diğer bir hareket ise **"verilere erişilmez kılmak"**tır. Verilere erişilmez kılmak kavramından, verileri kullanan ya da bu verilere malik olan kişinin dilediği zaman verilere ulaşmasının engellenmesi anlaşılmalıdır. Sözgelimi, sisteme giden elektiriğin kesilmesi, verilerin bulunduğu sistemin bozulması, verilerin sistemden silinmesi, verilerin veri taşıma aygıtından silinmesi durumunda verilere erişilmez kılmak eylemi oluşacaktır. Verilerin, mutlaka bu verilerin malikine ait olması gerekmez. Suçun oluşması için önemli olan bu verilere erişme olanağının ortadan kaldırılmasıdır. Verilere erişilmez kılınması eyleminden, bu verilere ulaşmaya yarayan anahtar sözcüğün değiştirilmesi yoluyla veriyi kullanmakla yetkili olan kimsenin bunları kullanamaması da anlaşılabilir. Örneğin bir bilişim sisteminin açılması için gerekli olan giriş şifresinin değiştirilmesi verilere erişilmez kılınması suçunu oluşturacaktır. Sistemde şifre olmadığı halde sisteme şifre yerleştirmekle de bu suç işlenebilecektir. Bu durumda, sisteme erişme yetkisi olan kimse, konulan şifre nedeniyle verilere ulaşamayacak ve verilere erişilmez kılmak suçu oluşacaktır.

TCK 244/2'de belirtilen suçun diğer maddi unsuru ise **"sisteme veri yerleştirmek"**tir. Sisteme veri yerleştirmek, bilişim sistemini kullanmakla yetkili olan kimsenin (veya sistemin malikinin) bilgisi ve onayı dışında, dışarıdan herhangi bir verinin bilişim sistemine yerleştirilmesidir. Yerleştirme işlemi, kaydetme, ekleme veya yükleme şeklinde gerçekleştirilebilir. Veri yüklenirken kullanılan yöntem de bu eylemin oluşması bakımından önem taşımaz. Sözgelimi, taşınabilir bellek, CD, disket ya da internet aracılığı ile de verinin yüklenebilmesi mümkündür. Failde, sisteme zarar verme kastı aranmaz. Bu kasıt olmasa da yalnızca sisteme girilerek verilerin değiştirilmesi bile başlıbaşına suçtur.

TCK 244/2'de belirtilen suçun diğer maddi unsurlarından biri de **"verilerin başka yere gönderilmesi"**dir. Veri göndermeden anlaşılması gereken, veri göndermeye ya da kopyalamaya yarayan bir araçla verilerin kopyasının çıkarılarak başka bir bilişim sistemine veri aktarılması ya da internet yoluyla (örneğin e-posta) bir sistemdeki verilerin başka bir sisteme aktarılmasıdır. Burada da herhangi bir zarar doğmasa dahi yalnızca veri gönderme eylemi nedeniyle fail cezalandırılacaktır. Ancak, burada veriler tamamen yok olmamıştır. Zira, tamamen yok olması durumunda, biraz yukarıda incelemiş olduğumuz verileri yok etme suçu oluşacaktır. Belirtmemiz gerekir ki TCK 244/2'de tanımlanan suç seçimlik hareketli bir suçtur ve maddede sayılan (yukarıda incelenen) sistemin işleyişini engellemek, işleyişini bozmak, sisteme veri yerleştirmek, var olan verileri başka yere göndermek, verileri erişilmez kılmak, verileri değiştirmek veya verileri yok etmek hareketlerinden herhangi birinin gerçekleşmesi ile suç işlenmiş olacaktır.
TCK 244'te tanımlanan suçun banka ve kredi kurumları ya da kamu kurum ve kuruluşlarına ait bilişim sistemleri aleyhine işlenmesi suçtaki ağırlaştırıcı nedendir. TCK 244/1 ve 2. fıkralarındaki suçun manevi unsuru ise genel suç işleme kastıdır. Bundan anlaşılması gereken, failin eylemin suç olduğunun bilinceinde olması ve buna rağmen eylemi gerçekleştirmesidir. (Bilme+ isteme)

3.) Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu: TCK 245. maddesinde düzenlenen "Banka ve Kredi Kartlarının Kötüye Kullanılması" suçu bakımından da bir değerlendirmeye gitmek gerekecektir. TCK'nın 245. maddesinde üç ayrı suç düzenlenmiştir. Maddenin ilk fıkrasında, başkasına ait bir banka veya kredi kartını, bu kartı ne şekilde ele geçirmiş olursa olsun, elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanarak veya kullandırtarak kendisinin ya da bir başkasının adına çıkar sağlaması suç olarak düzenlenmiştir.

İkinci fıkrada ise, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satın alınması, satılması, devredilmesi, kabul edilmesi suç olarak düzenlenmiştir.
Üçüncü fıkrada, sahte olarak üretilmiş olan ya da üzerinde sahtecilik yapılan bir kredi kartını kullanmak yoluyla kendisine veya bir başkasına yarar sağlama fiili suç olarak düzenlenmiştir.

TCK 245/1'deki suçu kısaca **"başkasının kartıyla yarar sağlama suçu"** olarak tanımlayabiliriz. Bu suçun oluşması için, failin kartı ne şekilde elde ettiği önem taşımaz. Buluntu, çalıntı (ya da hatta belki de rızaen teslim) yoluyla kart elde edilmiş olsa da suç oluşacaktır. Kartın ne şekilde elde edildiğinin önem taşımaması, maddedeki "her ne surette olursa olsun" deyiminden yola çıkılarak söylenebilir.
Suçun oluşumu için önemli olan en temel nokta, kartı kullanan kimsenin, **bir başkasına ait kredi kartını kullanarak** kendisinin veya bir başkasının adına bir çıkar elde etmesidir. Bu çıkar, kartın bizatihi kullanılması yoluyla ya da kart bilgilerinin veri iletim ağlarında (internet) kullanılması yoluyla ya da karttan alışveriş yapılması yoluyla olabilir.
Suçun oluşması için gereken ikinci koşul, maddedeki deyişle, "kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın" kartın üçüncü kişi tarafından kullanılmış olmasıdır.
Belirtmemiz gerekir ki bu suçlardan hiçbiri şikayete tabi değildir. Savcılıklar tarafından re'sen koğuşturulur veya mağdurun ihbarı üzerine yargılama kamu davası şeklinde yürür.

TCK'daki Diğer Bilişim Suçları

Yukarıda incelediğimiz suçların yanı sıra, diğer bazı suçlar da bilişim alanında suçlar başlığında düzenlenmemiş olmasına rağmen, bilişim sistemleri aracılığıyla işlenebilecektir.
Bu suçları da iki başlık altında incelemek mümkündür. İlk başlıkta, kişilerin özel hayatına karşı işlenen suçlar olan ve TCK 132'deki "Haberleşmenin Gizliliğini İhlal Suçu", TCK 135'teki "Kişisel Verilerin Kaydedilmesi Suçu"; TCK 136'da düzenlenmiş olan "Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" suçu ile TCK 138'de düzenlenen "Verilerin Yok Edilmemesi" suçları ile TCK 226. maddesinde düzenlenen "Müstehcenlik" suçlarıdır.

İkinci başlıktaki suçlar ise, kişilerin özel yaşamının korunması ile doğrudan doğruya bağlantılı olmamakla birlikte, bilişim sistemleri aracılığı ile de işlenebilen TCK 106'daki tehdit, TCK 124'teki "Haberleşmenin Engellenmesi"; TCK 125'teki "Hakaret"; TCK 142/2.e'deki "Bilişim Sistemlerinin Kullanılması Yoluyla Hırsızlık" ile TCK 158/1.f'deki "Bilişim Sistemlerinin Kullanılması Yoluyla Dolandırıcılık" suçlarıdır. Bunlardan en yaygın olarak görülenleri hakaret, tehdit ve hırsızlıktır. Dolayısıyla, bu suçlara kısaca değinilecektir.
Hakaret suçu, TCK 125'te düzenlenmiştir ve bilişim suçu bakımından maddenin ikinci fıkrası önem taşımaktadır. Buna göre, mağduru hedef alan sesli, yazılı veya görüntülü bir ileti suçun oluşması için yeterli olacaktır. Örneğin, mağdura yönelik hakaret ya da sövem içeren bri e-posta gönderilmesi sonucunda suç oluşacaktır. TCK 106'daki tehdit suçu bakımından da aynısını söylemek mümkündür.
TCK 142.2'e'de hırsızlık suçunun bilişim sistemleri aracılığı ile işlenmesi nitelikli hırsızlık olarak kabul edilmiş ve bu fiil basit hırsızlığa göre daha ağır bir yaptırıma bağlanmıştır. Bu suça örnek olarak, uygulamada sıklıkla karşılaşılan ve "internet hırsızlığı" olarak da adlandırılan suç verilebilir. Bu durumda, bir başkasının hesabına girilerek o hesaptaki paraları kendi hesabına aktaran fail, aslında mağdur olan kimsenin parasını çalmaktadır. Bir başka şekilde belirtilecek olursa, bu eylem nedeniyle, fail bir başkasının malvarlığına zarar vermektedir.