www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:5 Sayı:1

Geliş:02.05.2023
Kabul:23.06.2023

AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi

Nur Sena SEVİNDİ
Juris Avukatlık Ortaklığı, Avukat, Fikri Mülkiyet ve Bilgi Teknolojileri
s.sevindi@jurishukuk.com
ORCID: 0000-0003-1461-9309

Muhammet Emin ORDU
Juris Avukatlık Ortaklığı, Avukat, Fikri Mülkiyet ve Bilgi Teknolojileri
e.ordu@jurishukuk.com,
0009-0002-3599-9881

ÖZ

Veri ihlal bildirimi, kişisel veri ihlalinin gerçekleşmesini takiben veri koruma otoritelerine yapılmak üzere; veri sorumlularına getirilmiş olan bir yükümlülüktür. Bildirimin yapılması otoritelerin kendi formatlarına ve yasal süreye tâbidir. Ancak hem bildirim kaynaklarının hem de sürenin başlangıcının tayini için, veri ihlalinin doğru tespit edilmesi ve kategorilendirilmesi önem arz etmektedir. Veri ihlal türlerinin belirli olmaması ve somut olaya göre değişkenliği sebebiyle, veri ihlal bildirim yükümlülüğü ve süresi; veri sorumluları nezdinde soru işareti uyandırmaktadır. Veri ihlalinin tespitine ilişkin çözüm önerilerinin tartışıldığı bu çalışmada, veri ihlal bildirimi ve veri koruma otoritelerine yapılacak bildirim süreleri; 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Avrupa Birliği Genel Veri Koruma Tüzüğü düzenlemeleri kapsamında karşılaştırmalı olarak ele alınacaktır.
Anahtar Sözcükler: veri ihlal bildirimi, veri güvenliği, veri ihlal bildirim süresi

Comparative Evaluation of Data Breach Detection and Notification Period in the EU and Turkish Law

ABSTRACT

Data breach notification to data protection authorities is a legal obligation of data processors which starts from the occurrence of a data breach. The notification is subjected to the legal time period and format of the authorities. However; it is crucial to detect and categorize the data breach correctly in order to identify the beginning of the notification documents and time period. Due to the fact that the types of data breach are not specific and vary according to the concrete case, the data breach notification obligation and its duration raise a question mark among data controllers. In this study, in which the solutions for the detection of data breach will be discussed, data breach notification and notification periods to data protection authorities will be evaluated comparatively within the scope of the Personal Data Protection Law No. 6698 and the European Union General Data Protection Regulation.
Keywords: data breach notification, data security, data breach notification period

Atıf Gösterme	Sevindi N. S., Ordu., M. E., (2023). AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi, *Kişisel Verileri Koruma Dergisi*. 5(1), 12-22. DOI:

GİRİŞ

Veri ihlal bildirimi, kişisel veri ihlalinin gerçekleşmesinden sonra veri koruma otoritelerinin gecikmeksizin haberdar edilmesi, gerekli önlemlerin alınması ve ilgili kişilerin bilgilendirilmesi amacıyla, veri sorumlularına getirilmiş olan bir yükümlülüktür. Bu yükümlülüğün yerine getirilebilmesi için, veri sorumlularının veri ihlalinin mevcudiyetini ve başlangıcını doğru tespit etmesi gerekmektedir. Mevzuatta veri ihlal türlerinin açıkça düzenlenmemiş olması ve ihlal bildirimi için öngörülen yasal sürenin ihlalin boyutu veya teknik gerekliliklerine her durumda uymaması; veri sorumlularının alacağı önleyici aksiyonlarda karışıklığa neden olmaktadır.

Veri ihlali kavramı, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ("GVKT") 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") hükümlerine kıyasla daha detaylı düzenlenmiş olmasına karşın; veri ihlal bildirimine ilişkin usul ve süre büyük oranda örtüşmektedir. Nitekim, iki mevzuatta da ihlal türlerinin detaylandırılmamış ve bildirim süresinin somut olaya ilişkin kararlarda esnetilmesine rağmen değerlendirmedeki kriterlerin listelenmemiş olması, veri ihlal bildiriminin nihai amacına ulaşmasına engel olabilmektedir.

Bu makalede, veri ihlali kavramı KVKK ve GVKT uyarınca karşılaştırılmalı olarak ele alınacak, ikinci bölümde ise veri ihlalinin farklı senaryolarda tespitine ilişkin değerlendirmelerde bulunulacaktır. Veri ihlalinin tespitini takiben, veri koruma otoritesine bildirim şekli ve bildirim süresi incelenecektir.

VERİ İHLALİ KAVRAMI

Veri sorumlusunun KVKK ve GVKT kapsamında en temel yükümlülüklerinden biri, işlediği kişisel verilerin idari ve teknik boyutta güvenliğini ve gizliliğini temin etmektir. Yasal yükümlülük olarak düzenlenen ve ihlali halinde yüksek yaptırımlar öngörülen bu yükümlülüğün ihlali halinde, veri ihlali ortaya çıkmaktadır. Bu nedenle, veri ihlalini tanımlamak için, ilk önce veri güvenliğini incelemek gerekir.

KVKK'nın veri güvenliğini düzenleyen 12.maddesi kapsamında, veri sorumlusu; veri işleme faaliyetlerinde gerekli güvenliği sağlamakla yükümlüdür. Veri sorumlusu tarafından işlenen kişisel verilerin kanuni olmayan yollarla üçüncü kişilerce ele geçirilmesi halinde, veri güvenliği yükümlülüğü ihlal edilmiş sayılmaktadır. Bu durumda, veri sorumlusu ihlali en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurul'una ("Kurul") bildirmelidir. Bu haliyle düzenleme, veri ihlalinin meydan getireceği zararı bir an önce önlemeyi amaçlamaktadır. İşbu hükümdeki "kanuni olmayan" yollardan anlaşılması gerekenin ne olduğu, üçüncü kişilerin kimi ifade ettiği ve veri ihlalinin yalnızca elde edilme halinde mi gerçekleşeceği hususu; KVKK ve GVKT kapsamında karşılaştırılmalı olarak değerlendirilecektir.

KVKK'nın 12. maddesinde bahsi geçen "kanuni olmayan yollarla" ibaresinden kasıt hukuka uygun olmayan tüm durumları kapsamaktadır. Bu bakımdan; kişisel veriler ile ilgili düzenlemeler yalnızca KVKK kapsamında yorumlanmamalı; aksine Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Sosyal Yardım Verilerinin Kaydedilmesi ve Paylaşılmasına İlişkin Yönetmelik gibi düzenlemelere aykırılık halleri de kanuni olmayan yollara tâbi kılınmalıdır. Dolayısıyla veri ihlali yürürlükteki tüm düzenlemelere aykırı davranışlar sonucunda da meydana gelebilecektir (Dülger, 2019).

KVKK kapsamında veri ihlalinin ne olduğu ve türleri hakkında açık bir düzenleme bulunmamaktadır. Herhangi bir sayma veya örneklendirme yoluna gidilmemiştir. Bu kapsamda küçük ya da büyük ölçekli, önemli ya da önemsiz boyutta olması fark etmeksizin; amaçsal yorum ile her türlü veri ihlalinin Kurul'a ve ilgili kişilere bildirilmesi gerekecektir. (Çekin, 2020).

Kaldı ki, KVKK kapsamında sayılan diğer veri güvenliği tedbirleri; kişisel verilerin muhafazasını sağlamakla birlikte uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri de içermektedir. Dolayısıyla bu yükümlülüklerin ihlali halinde de veri ihlali gündeme gelebilecektir. Bu sebeple, kişisel verilerin mahremiyetinin ihlal edilmesi veya ihlal edilme tehlikesi ile karşı karşıya kalması hallerinde Kurul ve ilgili kişinin bilgilendirilmesi gereklilik arz edecektir.

Öte yandan, ilgili düzenlemenin lafzına bakıldığında; KVKK uyarınca veri ihlalinin mevcudiyeti için, kişisel verilerin başkaları tarafından elde edilmesi gerekliliği arandığı görülmektedir. Düzenlemenin bu haliyle GVKT'ye nazaran oldukça dar yorumlandığı söylenebilecektir. Öyle ki, GVKT'nin Tanımlar başlıklı 4. maddesinde veri ihlalinin tanımı yapılmakta ve veri ihlal türleri dört kategoride sayılmaktadır. Bu kategoriler aşağıdaki gibidir (Veri Koruma Komisyonu, 2019):

- Kişisel verilerin kasten veya kasıt olmaksızın imha edilmesi,
- Değiştirilmesi,
- Yetkisiz şekilde açıklanması
- Kişisel verilere erişim imkanı sağlanması

Görüldüğü üzere, GVKT kapsamında veri ihlalinin somut olaya uyarlanabilir biçimde alt kırılımlara ayrıldığı görülmektedir. Öyle ki, KVKK açısından veri ihlalinin meydana gelebilmesi için üçüncü kişiler tarafından kişisel verilerin elde edilmiş olması gerekliyken, GVKT kapsamında veri sorumlusunun kasten veya sehven yaptığı değiştirilme, imha edilme, kendisi ya da bünyesindeki kişiler tarafından yetkisiz olarak açıklanma ve üçüncü kişilerin kişisel verilere erişmesinin önünün açılması hususu da veri ihlali olarak sayılmaktadır.

Devamla, GVKT kapsamında sayılan ihlal türleri; gizlilik ihlalleri, bütünlük ihlalleri ve erişilebilirlik ihlalleri olmak üzere üç kategoride toplanmaktadır. İlk olarak, gizlilik ihlali; kişisel verilerin kasıt olmadan veya yetkisiz şekilde ifşa edilmesi ya da erişime açılmasını ifade ederken bütünlük ihlali kişisel verilerin yetkisiz veya kasıt olmadan değiştirilmesini ifade eder. Erişilebilirlik ihlali ise, söz konusu kişisel verilerin imha edilmesi veya kaybedilmesini kapsamaktadır. (Tosoni, 2020).

Gizlilik ihlalleri ve bütünlük ihlallerini saptamak somut olay bazında erişilebilirlik ihlallerine nazaran daha kolay olmakla beraber, bir uyuşmazlıkta kalıcı olarak bir kişisel veri imhası ya da kaybı söz konusu ise, bu durumda erişilebilirlik ihlalinin gündeme gelme ihtimalinden genel olarak bahsedilebilir. Ancak söz konusu ihlal türü her ne kadar genellikle kalıcı kayıp veya imhalarda gündeme gelse dahi, hastane gibi özel nitelikli kişisel verilerin bulunduğu işletmelerde kişisel verilere erişimin geçici süreliğine engellenmesi durumu da veri ihlaline sebebiyet verebilecektir. Bu noktada kalıcı olarak erişim engeli olmasını aranmamaktadır. (Avrupa Veri Koruma Kurulu, 2022)

Erişilebilirlik ihlaline örnek olarak, bir şirkete yapılan siber saldırı sonucunda şirkette yer alan kişisel verilere veri sorumlusu tarafından ulaşım sağlanamaması durumu verilebilir. Bu şekilde gerçekleşen bir saldırı akabinde kişisel veriler üçüncü kişilerin eline geçmemiş olsa dahi, bu durum veri sorumlusu bakımından GVKT kapsamında erişilebilirlik ihlali olup, veri sorumlusunun veri ihlal bildirim yükümlülüğünün doğmasına sebebiyet verebilecektir. Somut olay, ilgili KVKK hükmünün dar yorumuyla birlikte değerlendirildiğinde, herhangi bir kişisel veri üçüncü kişilerin eline geçmediği için ve sadece veriye erişim engellediği için, veri sorumlusunun Kurul'a ve ilgili kişiye veri ihlal bildiriminde bulunması gerekmeyecektir. Zira, KVKK hükmü dar yorumlanır ise, GVKT'de yer alan kategorilerden yalnızca gizlilik ihlalini kapsamakta, diğer ihlal türlerini kapsamamaktadır. Bu hususta doktrinde kabul edilen genel görüşe göre, KVKK uyarınca veri ihlali gizlilik, bütünlük ve erişilebilirlik ihlallerini kapsayacak şekilde geniş yorumlanmalıdır.

Aynı şekilde, KVKK'daki veri ihlalinin dar şekilde tanzim edilmiş olmasına karşın, geniş yorumlanma zorunluluğu ticari hayatın gerekliliği haline de gelmiştir. Öyle ki, Avrupa düzenlemelerine uygun şekilde hareket etmek isteyen ve ticari itibarını düşünen veri sorumlularının sadece başkaları tarafından elde edilen kişisel veri ihlallerinde değil; aynı zamanda GVKT kapsamında sayılan kategorilerde de Kurul'a veri ihlal bildiriminde bulunması gerekecektir (Dülger, 2019).

VERİ İHLALİNİN TESPİTİ

Veri ihlali, bir önceki bölümde ele alındığı üzere, somut olaya özgü olarak tanımlanmamış veya tek tek listelenmemiş olup hem KVKK hem de GVKT uyarınca kategorilere dayandırılmıştır. Bu nedenle, veri ihlalinin tanımının geniş, kapsamlı ve kısmen belirsiz olması sebebiyle; kişisel veri üzerinde veya kişisel veriyle ilgili bir işlem veya olayın ihlal teşkil edip etmediği hususu önem arz etmektedir.

Benzer olarak, veri ihlali bildirim yükümlülüğünün de tespitten itibaren başladığı düşünüldüğünde, ihlalin tür ve zaman bakımından tespiti üzerinde durulması gerekmektedir. Öyle ki, somut olayın herhangi bir kategoriye dahil olması halinde; örneğin verilerin dışarıdan erişilebilir hale gelmesi halinde, bu sefer de ihlalin kim tarafından tespit edildiği, ne zaman ve hangi noktada gerçekleştiği sorunu gündeme gelecektir.

KVKK'nın 12. maddesinin 5. fıkrası gereğince, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bildirim yükümlülüğü mevcuttur. 24.01.2019 tarih ve 2019/10 sayılı Kurul kararında ise bu yükümlülüğün başlangıcı, ihlalden *haberdar olma* hali olarak belirlenmiştir. Kişisel Veri İhlali Bildirim Formu Kılavuzu'nda ise ihlalin başlangıç tarihi, "veri sorumlusu tarafından yapılan incelemeler sonucunda veri ihlalinin başladığı tarih" olarak ifade edilmiştir. Bu nedenle potansiyel ihlalin incelenmesi sonucunda ulaşılacak tespit, veri ihlalinin tespitidir. Ancak bu tespitin nasıl yapılacağına ilişkin çerçevesi belirli bir kılavuz veya kontrol listesi bulunmamaktadır.

GVKT'nin 33. maddesi uyarınca, yine *haberdar olma* hali bildirimde esas alınmıştır. Buna göre, veri sorumlusu; veri ihlalinden haberdar olmasını takiben gecikmeksizin ve en geç 72 saat içinde veri ihlal bildirimi gerçekleştirmelidir. Ancak bir veri ihlalinin tespiti için, öncelikle somut olayın veri ihlali teşkil edip etmediğine karar verilmelidir. Yukarıda izah edildiği üzere, kişisel verilerin hukuka aykırı veya kazara imhası, kaybı, değiştirilmesi, yetkisiz kişilere erişilebilir kılınması halleri veri ihlali sayılmaktadır. Dolayısıyla veri sorumlusu, somut olayın hangi kategoriye dahil olduğuna karar vermek suretiyle ihlali tespit etmelidir. Bu kategorilerden herhangi birinin gerçekleştiğine ilişkin *makul bir kanı* bulunması halinde veri ihlali gerçekleşmiş sayılır. Bu kanının oluşması ise haberdar olma kriterinin sağlandığının ve ihlalin tespit edildiğinin göstergesidir (Room, 2019).

Bir başka ifadeyle, GVKT'da veri ihlalinin tespiti; potansiyel ihlalin somut olay bazında incelenmesi, kategorilendirilmesi ve tespiti olmak üzere üç adımda gerçekleştirilmektedir. KVKK'da ise yine potansiyel ihlalin incelenmesi ve tespiti mevcut iken, GVKT'deki gibi sınırları belli bir kategorilendirme mevcut değildir.

Avrupa Veri Koruma Kurumu'nun rehberi ("WP29") uyarınca, veri ihlalinin tespiti; ihlalin veri sorumlusu tarafından doğrudan tespiti, üçüncü kişilerin bildirimi üzerine öğrenilmesi veya veri işleyen tarafından tespiti şeklinde farklı türlerde gerçekleşebilir (Avrupa Veri Koruma Kurumu, 2022).

İhlalin Veri Sorumlusu Tarafından Doğrudan Tespiti

Potansiyel ihlalin üçüncü kişiler, medya, kurumlar gibi dış kaynaktan bilgilendirilme dışında, veri sorumlusu tarafından doğrudan fark edilmesi, keşfedilmesi veya tespiti halinde, öncelikle ihlalin mevcut

olup olmadığının, somut olay özelinde değerlendirilmesi gerekmektedir. WP29 uyarınca, somut olayın ihlal tanımındaki hallerden sayılıp sayılmayacağına bakılmalıdır. Örneğin, bir e-ticaret platformunda müşteri verilerinin erişilebilir hale gelmesi; kişisel verilerin yetkisiz kişilere erişilebilir kılınması anlamına gelmektedir. Bu nedenle somut olay ile ihlal tanımı örtüşmektedir.

Ek olarak, söz konusu ihlalin neticesi, büyüklüğü, ilgili kişilerin temel hak ve özgürlüklerini etkileyip etkilememesi gibi faktörlerin, değerlendirmede önem arz ettiği vurgulanmıştır. Öyle ki, bildirim aşamasında ihlale ilişkin bilgi ve belgeler derlenip raporlanacağından, ihlalin çerçevesinin çizilmesi gerekmektedir.

Veri ihlali bildirim yükümlülüğü, ihlalin tespitinden itibaren başlamaktadır. Nitekim, tespit edilemeyen ihlaller bildirim konusu yapılamayacağından; tespit edilememe veya haberdar olmama gerekçeleriyle bildirim yükümlülüğünün veri sorumluları tarafından göz ardı edilme riski mevcuttur. Bu riski engellemek adına hem GVKT hem de WP29 kapsamında, veri sorumluları ihlal tespit prosedürleri geliştirmekle ve kullanmakla yükümlü kılınmıştır.

Özellikle WP29 metninde örneklendirilen ihlal tespit prosedürlerinde, veri ihlal tespit programları kullanımı, şirket içi raporlama ve loglama gibi örnekler veri sorumlularına yol göstermektedir. Bu nedenle, vuku bulmuş bir veri ihlalinin bildirilmemesi halinde, ilgili teknik veri güvenliği tedbirlerinin alınmaması; bildirim yükümlülüğünün ihlalinde gösterge olacaktır (Burton, 2020).

Benzer olarak, KVKK'nın 12. maddesinde düzenlenen veri sorumlusunun yükümlülüklerinde, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önleme, kişisel verilerin muhafazasını sağlama yükümlülükleri; veri ihlalinin engellenmesi için teknik ve idari tedbirlerin alınması gerekliliğinin göstergesidir. Bu nedenle KVKK kapsamında da bildirim yükümlülüğünün yanı sıra ihlali vuku bulmadan engellemeye yönelik tedbirleri alınması yükümlülüğü mevcuttur.

İhlalin Dış Kaynaktan Öğrenilme Yoluyla Tespiti

Potansiyel ihlalin üçüncü kişiler, medya, kurumlar gibi dış kaynaktan bildirim veya tesadüfi yolla öğrenilmesi hali de ihlalin tespitinde önemli rol oynamaktadır. Özellikle veri sızıntısı ile sonuçlanan veri ihlallerinde ihlalin doğrudan tespitinden önce öğrenilmesi muhtemeldir. Öğrenme halinde somut olayın nitelendirilmesi ve değerlendirilmesi, doğrudan tespit haline göre daha detaylı olabilmektedir.

Öyle ki, dış kaynaktan öğrenilen ihlalin, gerçekten mevcut olup olmadığı ve ihlal teşkil edip etmediği hususunun veri sorumlusu tarafından teyit edilmesi gerekir. Bu nedenle kapsamlı bir araştırma gerekecektir. WP29 uyarınca, veri sorumlusu; ihlalin teyit edilmesi halinde ihlalden haberdar olmuş sayılır. Dolayısıyla bildirim süresi de teyitten itibaren başlayacağından, otoriteye yapılacak bildirimde ihlalin teyidi için yapılacak olan araştırmalar da kapsama dahil edilmelidir.

KVKK tarafından yayımlanan Kişisel Veri İhlali Bildirim Formu Kılavuzu'nda, veri ihlalinin tespit tarihi, ihlalden *haberdar olma* tarihi olarak tanımlanmıştır. Bu tanımdan çıkarımla, dış kaynaktan öğrenilme yoluyla ihlalden haberdar olma hali, veri ihlalinin tespit edildiği ve bildirim yükümlülüğünün başladığı anlamına gelebilecektir. (KVKK, Kişisel Veri İhlali Bildirim Kılavuzu)

İhlalin Veri İşleyen Nezdinde Gerçekleşmesi

KVKK uyarınca veri işleyen, veri sorumlusunun verdiği talimatlar doğrultusunda kişisel verileri işleyen kişiyi ifade eder. Veri işleyen, veri sorumlusu adına hareket etmekte; veri sorumlusu veri işleme faaliyetlerine ilişkin işlem ve yetkilerinin tamamını veya bir kısmını veri işleyene devretmektedir.

Nitekim, veri işleyen ve veri sorumlusu arasındaki hukuki ilişki sebebiyle, veri sorumlusunun kanundan kaynaklanan yükümlülükleri devam etmektedir (Dülger, 2019).

Benzer olarak, GVKT uyarınca veri işleyen, veri sorumlusu adına hareket eden kişiyi ifade eder. Fakat bu tanım KVKK'ya kıyasla daha geniş yükümlülüklerle desteklenmiştir. Öyle ki, veri işleyen ve veri sorumlusu arasında sözleşmesel ilişki bulunması, veri işleyenin yalnızca talimata dayalı olarak veri işlemesi ve gerekli veri güvenliği tedbirlerini alması zorunludur. Veri sorumlusunun ise gözetim ve denetim yükümlülüğü devam etmektedir (Article 29 Data Protection Working Party, 2010).

Veri işleyenin faaliyetleri esnasında veri ihlalinin gerçekleşmesi mümkündür. Veri ihlalinin veri işleyen nezdinde gerçekleşmesi halinde, veri işleyenin söz konusu ihlali tespit ettiği an, ihlalin başladığı andır. Nitekim yukarıda ifade edildiği üzere, KVKK uyarınca esas olan *haberdar olma* kriteri olduğundan, veri işleyenin veri sorumlusuna ihlal hakkında bildirimde bulunduğu tarih haberdar olmanın gerçekleştiği tarih sayılacaktır (Room, 2019).

Veri ihlalinin veri işleyen nezdinde gerçekleşmiş olması halinde, Kurul'a yapılacak bildirimlerde, veri işleyenin ihlali tespit tarihi ve veri sorumlusuna bildirim tarihi formda ayrı ayrı yer almaktadır. Sonraki bölümde incelenecek olan bildirim süresinde bu farklılığın önem arz ettiği görülecektir. Zira veri ihlalinin ilk gerçekleştiği tarih ile veri sorumlusuna bildirim tarihi arasında ciddi bir zaman farkı bulunabilir. Bu da bildirimin 72 saatlik süre içinde yapılıp yapılmadığı hususunda kritik bir konudur (Bakırel, 2021).

GVKT'nin 33. maddesi uyarınca, veri işleyen; veri ihlalini tespit etmesi halinde, veri sorumlusuna derhal bildirimde bulunmakla yükümlüdür. Veri işleyen ve veri sorumlusu arasındaki sözleşmesel ilişki kapsamında, bildirimin nasıl ve ne zaman yapılacağı belirlenmekte, bildirimin yapılmaması halinde yaptırımların cezai şart veya rücu ilişkisine bağlandığı görülmektedir (Carey, 2020).

Veri ihlalin tespitinden hemen sonra; ihlale ilişkin bilgi ve belgelerin kayıt altına alınması, ihlal veri işleyen nezdinde gerçekleştiyse bilgi ve belgelerin temin edilmesi gerekmektedir. İlgili kayıtların Kurul incelemesine hazır tutulması gerekmektedir. Mevcut idari ve teknik veri güvenliği tedbirleri de raporlanmak suretiyle, önleyici ve geciktirici tedbirler hayata geçirilmelidir.

Bir sonraki bölümde, veri ihlalinin tespit edilmesini takiben gerçekleştirilmesi yasal yükümlülük olan ihlal bildirim usulü incelenecektir. Bildirim yükümlülüğünün başlaması ile, KVKK ve GVKT kapsamında belirlenen bildirim süresi ve sürenin uygulanma biçimi karşılaştırmalı olarak ele alınacaktır.

VERİ İHLAL BİLDİRİMİ

KVKK ve GVKT uyarınca, veri ihlal bildiriminin amacı birbiriyle paraleldir. Buna göre, yukarıda açıklanmış bulunan veri ihlal türlerinden herhangi birinin meydana gelmiş olması dolayısıyla ortaya çıkan veya çıkabilecek zararın bir an önce engellenmesi ya da artmasını engelleyecek önlemlerin alınması esas amaçtır. Öyle ki, kişisel verilerin başka kişilerce elde edilmesi ya da GVKT kapsamında veri ihlaline sebebiyet verecek fiillere maruz kalması neticesinde, ilgili kişiler gerek ekonomik gerek sosyal gerekse de fiziksel zararlara maruz kalabileceklerdir. Örneğin, Cambridge Üniversitesi çalışanlarının kişisel verilerinin bir platformda yayınlanması neticesinde üniversite çalışanları hayvan hakları savunucularının hedefi haline gelmiş ve zarar görmüşlerdir. (Küzeci, 2010)

KVKK ve GVKT açısından yukarıda anlatıldığı üzere, veri ihlalinin tespit edilmesi üzerine, ilgili veri koruma otoritesine ve ilgili kişilere mevcut olan en kısa sürede bildirimde bulunulması gerekmektedir. Bu kapsamda GVKT ile karşılaştırmalı olarak KVKK düzenlemesini incelemekte fayda olacağı düşüncesindeyiz. KVKK'nın 12. maddesi uyarınca, veri ihlali gerçekleştirince bu ihlalden hem Kurul

hem de ilgili kişinin bilgilendirilmesi gerekmektedir. Kanun lafzında Kurul'a ve veri sahibi olan ilgili kişiye bildirilecek olan veri ihlalleri açısından bir farklılık aranmamış olup, her türlü veri ihlalinin hem Kurul'a hem de ilgili kişiye bildirilmesi gerekmektedir. Bu hüküm işbu haliyle eleştiriye açıktır. Örneğin, bir şirkette yer alan müşteri verilerini bir çalışanın yanlışlıkla silmesi durumunda, silinen verilerin geri getirilme ihtimali olsa dahi KVKK gereğince hem Kurul'a hem de ilgili kişiye bildirimin yapılması gerekecektir (Avcı, 2019).

GVKT açısından ise, bildirimin kapsamı farklılık arz etmektedir. Bu farklılığı ortaya koymak için, GVKT'nin veri ihlalini düzenleyen 33 ve 34. maddelerinin incelenmesi gerekmektedir. Bu hükümlere göre, GVKT'de temel hak ve özgürlüklere zarar veren veri ihlalleri sebep olacağı zarar boyutu bakımından riskli ve yüksek riskli olarak iki kısma ayrılmaktadır. Bu ayrım, esasen otoriteye ve ilgili kişiye bildirilecek olan veri ihlallerinin ayrışmasını sağlamaktadır. Bu sebeple GVKT, KVKK'nın aksine, her veri ihlalinin otoriteye ve ilgili kişiye bildirilmesini zorunlu kılmamaktadır. GVKT kapsamında veri ihlalinin mevcudiyeti halinde, sadece veri koruma otoritesine bildiriminin yapılacağını düzenlenmekteyken, temel hak ve özgürlüklere zarar verme olasılığı yüksek olan veri ihlali durumlarında ilgili kişiye bildirim yapılması zorunluluğu getirilmemiştir. Bu nedenle, GVKT'nin 34. maddesi uyarınca bildirimin; veri ihlalinin temel hak ve özgürlükler bakımından yüksek riske yol açtığı ya da açacağı durumlarda yapılacağı düzenlemesi, KVKK'ya göre farklılık arz etmektedir (Yörük, 2019).

Bildirim yükümlülükleri arasındaki farkı daha detaylı incelemek gerekirse; GVKT'nin 33. maddesi ise, bir kişisel veri ihlalinin hangi şartlarda ve hangi usulde denetim makamına bildirileceği hususunu düzenleyen hükümdür. İşbu madde hükmünce bir veri ihlali temel hak ve özgürlüklere zarar verecek nitelikte ve riskli ise, veri sorumlusu; veri koruma otoritesine veri ihlalinden haberdar olma anından itibaren gecikmeksizin ve eğer uygunsa en geç 72 saat içerisinde bildirimde bulunmakla yükümlüdür. GVKT'nin 34. maddesi ise, ilgili kişinin veri ihlali hakkında bilgilendirilmesini düzenleyen bir hükümdür. Bu iki hüküm arasındaki en temel farklılık ise, veri ihlalinin meydana getireceği ya da getirebileceği zarar tehlike seviyesidir. GVKT'nin 34. maddesi uyarınca, temel hak ve özgürlüklere zarar veren veri ihlalinin meydana getirebileceği zarar seviyesi yüksek riskli olarak değerlendirildiği durumlarda veri sahibi durumdan haberdar edilmelidir. Bu nedenle aksi durumlarda ilgili kişiye veri ihlal bildirimi yapılmayacağı hususu da ilgili maddede düzenlenmiştir. (Avrupa Veri Koruma Kurulu, 2022) Bu düzenleme ile ulaşılmak istenen nihai amaç, veri ihlallerinden temel hak ve özgürlükleri zarar gören ilgili kişilerin kendi önlemlerini alarak zararı ya da artmasını alacakları önlemlerle engellemelerini sağlamaktır.

Veri ihlal bildirimi hususunda sonuç olarak, KVKK kapsamındaki düzenlemeler, GVKT'ye kıyasla daha yüzeysel olup her türlü veri ihlalinin Kurul'a ve ilgili kişiye bildirilmesi gerektiğini düzenlemektedir. Ancak GVKT kapsamında veri koruma otoritesine ilgili kişiye bildirilecek veri ihlalleri açısından net bir ayrıma gidilmiş olup, temel hak ve özgürlüklere zarar verecek mahiyette olan veri ihlallerinin sebep olacağı tehlike boyutu riskli olarak nitelendiriliyor ise otoriteye; çok riskli olarak nitelendiriliyor ise, hem otoriteye hem de ilgili kişiye bildirim yapılması gerektiği hususları düzenlenmektedir.

VERİ İHLAL BİLDİRİMİNİN SÜRESİ

Önceki bölümlerde açıklandığı üzere, veri ihlallerinin tespit edilmesi ve gerekli koşulların oluşması halinde, veri ihlal bildiriminin yapılması yasal bir yükümlülüktür. Zira gerek KVKK kapsamında gerekse de GVKT kapsamında veri ihlal bildiriminin amacı ve önemi vurgulanmış, gerçekleşmeden engellenmesi veya gerçekleştikten sonra etkisinin azaltılması amacıyla mümkün olan en kısa süre Kurul'a ve ilgili kişiye veri ihlal bildirimde bulunulması gerektiğinden bahsedilmiştir. Bu bildirim ile gerek veri sorumlusu gerek ilgili kişi gerekse de Kurul veri ihlalinden haberdar olacak ve alınması

gereken önlemler alınarak zararın ya da zararın artmasının önüne geçilmeye çalışılacaktır. Dolayısıyla bildirimin yapıldığı an ve süre kritik öneme sahiptir. Bu bölümde, KVKK ve GVKT kapsamında bildirim süresine ilişkin inceleme yapılacaktır.

KVKK'nın 12. maddesinin 5. fıkrası uyarınca, "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir." düzenlemesi ile, bildirimin *en kısa sürede* yapılmasına kanaat edilmiştir. Bu süre, Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarih ve 2019/10 sayılı kararı ile Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Duyuru vasıtasıyla 72 saat olarak belirlenmiştir (Kişisel Veri İhlali Usul ve Esasları Hakkında Duyuru, 2019).

Bu açıdan hem kanun hükmü hem de kararın yorumlanması ile, veri ihlalinin gerçekleşmesi durumunda, veri sorumlusu veri ihlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saatte veri ihlal bildiriminde bulunmalıdır. Nitekim, 72 saatlik bildirim süresi Kurul'a yapılacak bildirime has olup ilgili kişiye yapılacak olan bildirimde makul olan en kısa sürenin dikkate alınması gerekmektedir. Ancak 72 saat kuralı somut olaya göre esnetilebilmekte olup, mutlak algılanmamalıdır. Öyle ki, veri sorumlusunun veri işleme faaliyetlerinin hacmi ve ihlalden etkilenen kişi sayısı gibi unsurları da göz önüne alınarak sürenin uzayabileceği uygulamada kabul edilmektedir. Aşağıda sürenin değerlendirildiği kararlar incelenecektir.

İlk olarak, Kurul'un 08.12.2020 tarih ve 2020/934 sayılı kararında sürenin somut olaya göre değerlendirilmesine hükmedilmiştir. İlgili kararda özetle; bir şirkette yer alan eğitim sorumlusu gerçek kişi, şirket bünyesinde bazı belgelere ulaşım sağlayacak kişileri gösteren bir irtibat listesi oluşturmaktadır. İşbu irtibat listesinin yer aldığı klasör ise şirkette görev alan sınırlı sayıdaki üst düzey yöneticinin erişimine açık olarak oluşturulmuştur. Şirket üst düzey yetkililerinden biri işbu klasöre girdiğinde irtibat listesinde yanlışlıkla platform kullanıcılarının açık bir şekilde şifrelerinin, isimlerinin ve e-posta adres bilgilerinin yer aldığını fark etmektedir. Kurul tarafından yapılan incelemede, ihlalden etkilenen kişi sayısının iki olduğu ve en fazla sekiz şirket üst düzey yöneticisinin kişisel verilere ulaşmış olabileceği saptamasında bulunulmaktadır. Söz konusu veri ihlali 16.09.2019 tarihinde tespit edilip 24.10.2019 tarihinde Kurul'a veri ihlal bildiriminde bulunulmuştur.

Kurul vermiş olduğu kararda, veri sorumlusu şirket her ne kadar 72 saatlik veri ihlal bildirim süresine uymamış olsa dahi veri sorumlusunun çok uluslu bir şirket olması, ihlalden etkilenen iki kişinin tabi oldukları ülke tespiti ve ilgili ülkedeki kişisel veri koruma yükümlülüklerinin tespit edilmesi zaman alabileceğinden kaynaklı olarak 72 saati aşan ve veri ihlalinden yaklaşık bir buçuk ay sonra gerçekleşen veri ihlal bildirimini hukuka aykırı olarak kabul edilmemesi gerektiğine hükmetmektedir. Dolayısıyla hacim ve çok ulusluluk halleri, 72 saatlik veri ihlal bildirim süresinin esnek değerlendirilmesinde rol oynamaktadır.

GVKT'de ise, veri ihlal bildirimi süresi GVKT'nin 33. maddesinde düzenlenmiştir. İşbu düzenlemeye göre, ilgili kişinin temel hak ve özgürlüklerine zarar verecek ölçüde riskli olan bir durumdan veri sorumlusu gecikmeye mahal vermeden ve durumu uygunsa veri ihlalinden haberdar olunmasından itibaren en geç 72 saat içerisinde veri koruma otoritesini veri ihlali hakkında bilgilendirmekle yükümlüdür. İlgili hükümdeki *haberdar olma* kavramı, veri sorumlusu nezdinde *makul bir kanı* bulunması anlamına gelmektedir (Burton, 2020).

Veri ihlaline ilişkin kanının oluşması ise somut olaya göre değişebilmekte ve veri ihlalinin tespiti zorlaşabilmektedir. Örneğin, şirket içerisinde içinde kişisel verilerin olduğu bir taşınabilir belleğin kaybolduğu durumda, taşınabilir belleğin kimin eline geçtiği ve içerisinde yer alan kişisel verilerin başka kişilerce elde edilip edilmediği hususunun belirlenmesi zor olabileceğinden, USB belleğin kaybedildiği

an haberdar olma anı olarak kabul edilmelidir. Bu sebeple her somut olay kendi özelinde incelenmeli ve 72 saatlik süre *haberdar olma* anından başlatılmalıdır. (Avrupa Veri Koruma Kurulu, 2022).
KVKK'ya benzer olarak, GVKT kapsamında da 72 saatlik süre mutlak bildirim süresi değildir. GVKT uyarınca, bildirimin 72 saat dolduktan sonra yapılması, makul bir gerekçeye dayanması halinde ihlal sayılmayacaktır. Örneğin veri ihlalinin çok karmaşık bir yapıda işlenmesi ve tespitinin zor olduğu durumlarda, makul bir gerekçe varlığına kanaat edilebilecektir.
Yukarıda detaylı olarak incelendiği üzere, GVKT kapsamında veri ihlal bildirimlerinde otoriteye yapılan bildirimler ile ilgili kişiye yapılan bildirimler farklı maddelerde düzenlenmektedir. Bu kapsamda ilgili kişiye yapılacak olan veri ihlal bildirimi hakkında GVKT'nın 34 hükmünde KVKK'ya benzer şekilde herhangi bir süre ismi zikredilmemiş olup, *makul süre*den bahsedilmektedir. Makul sürenin belirlenmesinde veri ihlalinin nasıl gerçekleştiği, kimleri etkilediği, sebep olduğu ya da olacağı zararın büyüklüğü unsurlarının göz önünde bulundurulması gerekmektedir. (Avrupa Veri Koruma Kurlu, 2022).
Bildirime esas bilgi ve belgelerin sunulması gerekli için süre için KVKK ve GVKT düzenlemeleri paralellik göstermektedir. Zira hem KVKK hem de GVKT uyarınca veri sorumlusu veri ihlal bildiriminde bulunurken, veri ihlalini tam olarak analiz etmesi kendisinden beklenmemektedir. Veri sorumlusunun yükümlülüğü, veri ihlaline yönelik toplayabileceği bilgi ve belgeleri otorite ile paylaşıp, sonradan edindiği bilgi ve belgeleri de ileri tarihte bildirim konusu yapabilecektir.
Yukarıdaki açıklamalar ışığında, KVKK ve GVKT'deki veri ihlal bildirim süreleri benzerlik göstermektedir. Aynı şekilde, belirlenen 72 saatlik süre kesin bir süre olmayıp, makul bir süre içerisinde ve makul bir gerekçe ile yapılan bildirimlerin de bildirim yükümlülüğünün süresi içinde gerçekleştirildiği manasına gelebileceği görülmektedir.

SONUÇ

Veri ihlali kavramı, KVKK kapsamında ilgili kişilerin kişisel verilerinin başka kişilerce hukuka aykırı yollardan elde edilmesi iken, GVKT kapsamında daha geniş kapsamlı düzenlenmekte ve kişisel verilerin kasten veya sehven imha edilmesi, değiştirilmesi, yetkisiz şekilde açıklanması, kişisel verilere erişim imkânı sağlanması durumları da veri ihlali olarak nitelendirilmektedir. Öte yandan, veri sorumlusunun veri güvenliği yükümlülüğünün kapsamı göz önünde bulundurulduğunda; KVKK uyarınca doğrudan veri ihlali sayılmayan bu hallerin de ilgili kişi ve Kurul'a yapılacak veri ihlal bildirimlerine esas teşkil etmesi gerektiği değerlendirilmelidir.
Kişisel verilerin önemi ve mahiyeti düşünüldüğünde, veri ihlali gerek ilgili kişi, gerek veri sorumlusu, gerekse ekonomik bakımdan birçok farklı zararın doğmasına neden olabilecektir. Bu sebeple, KVKK uyarınca en kısa sürede ve 72 saat içinde bildirim yükümlülüğü düzenlenmiş iken; GVKT uyarınca ise, veri sorumlularının veri ihlali meydana geldikten sonra ilgili kişiye en kısa sürede, veri koruma otoritesine veya Kurul'a ise 72 saat içerisinde veri ihlal bildiriminde bulunulması düzenlenmiştir. Bu sürelerin başlangıcında esas ise veri ihlalinden haberdar olma halidir. Nitekim, her veri ihlalinin farklı biçim ve mahiyette olduğu değerlendirildiğinde, haberdar olma halinin yeknesak bir biçiminin bulunmaması, bildirim yükümlülüğünün başlangıcı ve dolayısıyla da sürenin belirlenmesi bakımından belirsizliğe neden olmaktadır.
Benzer olarak, bildirim yükümlülüğüne ilişkin en kısa süre ve 72 saatlik süre kesin süre olmayıp, bildirimin gecikmesinde makul süre bulunması halinde, Kurul ve veri koruma otoriteleri tarafından esnek değerlendirilebilmektedir. Ancak bu durum veri sorumlularının yükümlülüğünü belirsiz kılmakta ve yapılan bildirimin geçerliliğine istinaden şüpheye mahal vermektedir. Bu nedenle, Türk hukukunun, AB mevzuatı ile uyumlu hale getirilerek, Kurul'a yapılacak veri ihlal bildirimi ile ilgili kişiye yapılacak veri ihlal bildirimi arasında ayrıma gidilmesi gerekmekte olup, her iki mevzuatta da makul gerekçelere ilişkin kriterlerin tayini sürenin belirlenmesinde önem arz etmektedir.

KAYNAKLAR

Article 29 Data Protection Working Party (Çalışma Grubu), Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169, Şubat 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf adresinden erişilmiştir. (13.04.2023)

Avcı, Y. (2019). Kişisel Verilerin Korunması. (Yüksek Lisans Tezi, Selçuk Üniversitesi), Konya.

Bakırel, N.B. (2021). Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı. Ankara: Seçkin.

Burton, C. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. *Article 33 Notification of a personal data breach to the supervisory authority*. New York: Oxford Academic.

Carey, P. (2020). *Data Protection: A Practical Guide to UK and EU Law*. 5th Edition. Oxford University Press.

Çekin, M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. İstanbul: On İki Levha Yayıncılık.

Veri Koruma Komisyonu, (2019). Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR, Ekim 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf web sitesinden edinilmiştir. (22.04.2023)

Dülger, M. V. (2019). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi.

Avrupa Veri Koruma Kurulu, (2022). Guidelines 9/2022 on personal data breach notification under GDPR, Ekim 2022, https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf adresinden erişilmiştir. (22.04.2023)

Kaya, M. (2015). Elektronik Ortamda Kişilik Hakkının Korunması. Ankara: Seçkin.

Kişisel Verileri Koruma Kurumu, Kişisel Veri İhlali Bildirim Formu Kılavuzu, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/369d954a-aaee-44ca-9ca6-105e8b4102f9.pdf adresinden erişilmiştir. (24.04.2023)

Kişisel Verileri Koruma Kurumu, Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin KVKK'nın T.24.01.2019, 2019/10 K. Sayılı Kararına İlişkin Duyuru, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi adresinden erişilmiştir. (20.04.2023)

Kişisel Verileri Koruma Kurumu, 2020/201 Sayılı 03.03.2020 Tarihli Kararı, https://www.lexpera.com.tr/ictihat/kisisel-verileri-koruma-kurumu/karar-no-2020-201-t-3-3-2020 adresinden erişilmiştir. (29.04.2023)

Kişisel Verileri Koruma Kurumu, 2020/934 Sayılı 08.12.2020 Tarihli Kararı, https://www.lexpera.com.tr/ictihat/kisisel-verileri-koruma-kurumu/karar-no-2020-934-t-8-12-2020 adresinden erişilmiştir. (19.04.2023)

Korucu, O. (2021). Veri Güvenliğinin İyileştirilmesi Sürecinde Küresel Standart, Çerçeve ve En İyi Uygulamalarının Hukuki Uyuma Desteği. Ankara: Adalet Yayınevi.

Küzeci, E. (2010). Kişisel Verilerin Korunması. Ankara: Turhan Kitabevi.

Reinke, G. (2020). Blue Paper on Data Protection- A Data Breach Accountability Framework: How to reduce the risk of GDPR sanctions. London: Goldrush Publishing.

Room, S. (2019) European Data Protection Law and Practice. *Security of Personal Data*. New Hampshire: International Association of Privacy Professionals.

Tosoni, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. *Article 4(12). Personal data breach*. New York: Oxford Academic.

Yörük, Onur Doğan. (2019). (AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması. (Yüksek Lisans Tezi, İzmir Ekonomi Üniversitesi). İzmir.