T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLERİN YERİNE GETİRİLMEMESİ KABAHATİ

YÜKSEK LİSANS TEZİ

Mehmet Semih ÖZTEKİN

Tez Danışmanı: Prof. Dr. E. Eylem AKSOY RETORNAZ

HAZİRAN 2023

ÖNSÖZ

Çalışma kapsamında Kişisel Verileri Koruma Kurulu'nun yayımladığı kararlar ışığında kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati incelenmiş ve ulaşılan sonuçlar kapsamında konuya ilişkin öneriler ifade edilmiştir.

Öncelikle benim için zor bir zamanda tez danışmanlığımı üstlenen, büyük bir nezaketle tüm sorularımı cevaplandıran, yardımını ve bilgisini hiç esirgemeyen Prof. Dr. E. Eylem Aksoy Retornaz'a tüm emekleri ve nezaketi için minnet ve teşekkürlerimi sunarım.

Yüksek lisans eğitimim boyunca hayatın her alanında bana kattıklarının yanında tezimin yazımı konusunda da her daim yanımda olan değerli dostlarım Ertuğrul Kaan Yıldırım ve Yasin Uysal'a teşekkür ederim.

Kişisel verilerin korunması hukukunu öğrenmemde büyük emeği olan, bu alanda çalışma yapmam konusunda beni her zaman teşvik eden avukatlık mesleğindeki ilk üstadım Av. Deniz Güngör'e ayrıca teşekkürrü bir borç bilirim.

Elbette en büyük minnettarlığım bu süreç boyunca yanımda olan, beni her zaman sabır ve anlayışla karşılayan, tüm kahrımı çeken can yoldaşım Sıla'ya. Emekleri için tüm kalbimle teşekkür ederim. Bir buçuk yıllık emeğimin karşılığı olan bu çalışmamı kendisine ithaf ediyorum.

İÇİNDEKİLER

KISALTMALAR

ABAD	:	Avrupa Birliği Adalet Divanı
Bkz	:	Bakınız
C	:	Cilt
CMK	:	5271 Sayılı Ceza Muhakemesi Kanunu
DEÜ	:	Doküz Eylül Üniversitesi
Direktif	:	Avrupa Birliği Veri Koruma Direktifi 95/46/EC
DPD	:	Avrupa Birliği Veri Koruma Direktifi 95/46/EC
EDPB	:	Avrupa Veri Koruma Kurulu
ERÜHFD	:	Erciyes Üniversitesi Hukuk Fakültesi Dergisi
EU	:	Avrupa Birliği
E.T.	:	Erişim Tarihi
GDPR	:	2016/679 Sayılı Avrupa Birliği Veri Koruma Tüzüğü
İİBF	:	İktisadi ve İdari Bilimler Fakültesi
KK	:	5326 Sayılı Kabahatler Kanunu
KVKK	:	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kurul	:	Kişisel Verileri Koruma Kurulu
Kurum	:	Kişisel Verileri Koruma Kurumu
M	:	Madde
S	:	Sayı
s	:	Sayfa
ss	:	Sayfalar
TAAD	:	Türkiye Adalet Akademisi Dergisi
TBB	:	Türkiye Barolar Birliği
TBK	:	6098 Sayılı Türk Borçlar Kanunu
TBMM	:	Türkiye Büyük Millet Meclisi
TCK	:	5237 Sayılı Türk Ceza Kanunu
UK	:	Birleşik Krallık
WP	:	Madde 29 Çalışma Grubu

LE RESUME

Le sujet de cette thèse est, une contravention, le non-respect des obligations en matière de sécurité des données personnelles. Cette contravention est régie par l'alinéa (b) du paragraphe 1 de l'article 18 de la Loi sur La Protection des Données Personnelles (“LPDP/KVKK”) intitulé "Contraventions". Dans le cadre de ladite contravention, il est prévu qu'une amende administrative sera infligée aux personnes qui ne remplissent pas leurs obligations en matière de sécurité des données en vertu de l'article 12 de LPDP. Dans les paragraphes 2 et 3 de l'article, il est stipulé que les responsables du traitement des données, qui sont personnes physiques ou des personnes morales de droit privé, sont sujets aux sanctions dans le cadre de la contravention, et que des dispositions disciplinaires sont appliquées aux fonctionnaires ou aux personnes qui travaillent à tel titre dans le cas où ladite contravention se produit au sein des établissements et des institutions publics et des organisations professionnelles ayant le statut d’institution publique. Dans notre étude, nous examinons en détail la contravention de non-respect des obligations en matière de sécurité des données et les obligations prévues à l'article 12 de LPDP dans ce contexte. Dans ce cadre, l'étude se compose de deux parties principales, intitulées Aperçu du droit sur la protection des données personnelles et Contravention de non-respect des obligations relatives à la sécurité des données personnelles.

Les obligations à remplir en matière de sécurité des données personnelles sont énoncées dans quatre paragraphes distincts de l'article 12 de LPDP. En conséquence, prendre des mesures techniques et administratives pour assurer le niveau de sécurité nécessaire contre le traitement illicite des données personnelles, l'accès illégal aux données personnelles et pour la conservation des données personnelles, le respect des obligations d'inspection, l'interdiction de divulgation des données personnelles et l'utilisation des données personnelles pour le finalité autre que la finalité de traitement en violation de LPDP, remplir l'obligation de notification de violation de données sont les obligations réglementées dans le LPDP concernant la sécurité des données. La violation de ces dispositions est réglementée comme une contravention.

Dans le cadre du premier chapitre, nous expliquons diverses réglementations concernant la protection des données personnelles. Ces sujets sont composés d'enjeux que nous considérons importants pour comprendre les obligations liées à ladite contravention et à la sécurité des données. Dans ce cadre, dans la première partie du premier chapitre, nous examinons plusieurs concepts. Les données personnelles, le traitement des données personnelles, le responsable du traitement et le sous-traitant constituent ces concepts de base. Ces concepts constituent divers éléments et composantes de la contravention en question. De plus, on met également en lumière les principes de base du droit sur la protection des données personnelles dans le premier chapitre. Les principes fondamentaux du droit sur la protection des données personnelles sont la licéité et la loyauté, être exactes et tenues à jour si nécessaire, être traitées pour des finalités déterminées, explicites et légitimes, être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, être conservées pendant la période prévue par la législation pertinente ou la période requise aux fins pour lesquelles les données

personnelles sont traitées. Ces principes montrent les principaux objectifs du droit sur la protection des données personnelles et aussi constituent des critères de base que les responsables du traitement doivent respecter dans toutes leurs responsabilités au regard de LPDP.

Le concept de sécurité des données personnelles constitue le concept central de l'étude. Dans sa définition la plus générale, la sécurité des données personnelles signifie la protection des données personnelles contre les risques et les menaces. Les données personnelles sont un type d'informations présentant certaines caractéristiques. Dans ce cadre, ce terme a pris un sens dans le contexte des principes et des objectifs de la sécurité de l'information. La sécurité de l'information vise à assurer la confidentialité, l'intégrité et la disponibilité des informations. Sous cet angle, dans le cadre de la sécurité des données personnelles, les données personnelles doivent être protégées conformément aux principes de confidentialité, d'intégrité et de disponibilité.

La sécurité des données personnelles, qui a une substance conforme à la sécurité de l'information, est l'une des composantes les plus importantes de la législation sur la protection des données personnelles depuis la naissance du droit sur la protection des données personnelles. Dans ce cadre, des obligations liées à la sécurité des données personnelles ont été incorporées dans la législation élaborée sur la protection des données personnelles en Europe depuis les années 1970. La loi Hessen sur la protection des données, qui a été promulguée en 1970 et qui est la première loi sur la protection des données, comporte des obligations concernant la sécurité des données personnelles. De la même manière, la loi allemande sur la protection des données, promulguée en 1970, et la loi française sur la protection des données, promulguée en 1978, ont imposé l'obligation de prendre des mesures techniques et administratives concernant la sécurité des données. Ensuite, la sécurité des données personnelles, qui a été érigée en obligation dans la Convention n°108 et la directive européenne sur la protection des données, est enfin réglementée en détail avec le RGPD.

Dans le droit turque, les obligations concernant la sécurité des données personnelles sont régies sous l'influence de la directive européenne sur la protection des données. Alors que la sécurité des données personnelles dans le projet de loi sur la protection des données personnelles en 2008 qui est tombé en désuétude, avait un contenu formé conformément à la directive, LPDP a amené une différenciation grande à l'égard des dispositions de la directive. Bien que cette situation ait rendu unique l'obligation de sécurité des données existante dans LPDP, elle a également fait en sorte que les obligations de sécurité des données aient un contenu qui dépasse sa propre capacité conceptuelle.

Dans le deuxième chapitre de l'étude, nous nous penchons sur la contravention de non-respect des obligations relatives à la sécurité des données personnelles. Dans ce cadre, l'intérêt juridiquement protégé à l'égard de la contravention, l'élément matériel et moral de la contravention, les faits justificatifs, la culpabilité, les formes particulières d'apparition de l'infraction, la sanction et les activités judiciaires sont discutés.

L'auteur de la contravention de non-respect des obligations en matière de sécurité des données personnelles est le responsable du traitement. Dans ce cadre, cette contravention est une contravention spécifique. Cependant, dans certains cas, comme les

personnes morales étant des responsables, l'organe, le représentant et l'employé peuvent également être les auteurs. Dans ce cas, le responsable du traitement est susceptible de faire l'objet d'une amende administrative en raison de l'action de l'organe, du représentant ou de l'employé.

La victime du délit de non-respect des obligations en matière de sécurité des données est la personne concernée. Les données personnelles sont toutes les informations relatives à une personne physique identifiée ou identifiable. Cette personne, à laquelle des données personnelles peuvent être associées, est la personne concernée et constitue la victime dans le cadre de la contravention. L'objet de la contravention est les données personnelles traitées par des moyens automatiques ou non-automatiques à condition qu'elles fassent partie d'un système de saisie de données conformément à LPDP. L'information relative à la violation de données ne constitue l'objet d'infraction que dans l'action de ne pas informer d'une violation de la sécurité des données.

À l'égard de la contravention de ne pas remplir les obligations concernant la sécurité des données personnelles, quatre actions différentes sont prévues. Les actions consistant à ne pas prendre de mesures techniques et organisationnelles, à ne pas remplir l'obligation d'inspection, à divulguer des données personnelles en violation de LPDP et à utiliser des données personnelles à des fins autres que le traitement et à ne pas remplir l'obligation de notification de violation de données constituent les actions de la contravention. Les actions autres que le non-respect des obligations de notification de violation de données sont des actions alternatives dans le cadre de l'infraction. Comme l'objet de l'acte de non-respect de l'obligation de notification de violation de données est différent des autres actes, cet acte constitue une autre contravention. Les actes de ne pas prendre de mesures techniques et organisationnelles et de ne pas remplir l'obligation d'inspection peuvent être commis par négligence et constituent des infractions continues. L'action de divulguer des données personnelles en violation de LPDP et d'utiliser des données personnelles à des fins autres que le traitement constitue une infraction instantanée et peut être commise avec une action positive. Le non-respect de l'obligation de notification de violation de données n'est pas non plus une infraction continue, et cette action peut être commise par négligence. De plus, toutes les actions de la contravention sont des infractions de conduite et dans ce contexte, aucun résultat n'est prévu dans LPDP.

Le responsable du traitement est exigé de prendre des mesures techniques et organisationnelles pour assurer le niveau de sécurité approprié afin d'empêcher le traitement illicite des données personnelles, d'empêcher l'accès illicite aux données personnelles et d'assurer la conservation des données personnelles. Sinon, l'action se produit. L'action de ne pas prendre de mesures techniques et organisationnelles est aussi une action continue. En outre, le Conseil considère les activités de traitement illégales effectuées au sein du corps du responsable du traitement comme relevant de l'acte de ne pas prendre de mesures techniques et organisationnelles pour assurer le niveau de sécurité approprié afin d'empêcher le traitement illicite de données personnelles. En raison de l'interprétation par le Conseil de l'article pertinent de cette manière, les responsables du traitement sont passibles d'amendes administratives pour ne pas avoir pris de mesures techniques et organisationnelles s'ils traitent illégalement des données personnelles. Cette situation viole les principes de légalité et de sécurité.

L'action de ne pas remplir l'obligation d'inspection et les actes de divulgation de données personnelles à des tiers et de les utiliser à des fins autres que le traitement en violation de LPDP constitue rarement le motif de la décision du Conseil pour l'amende administrative. Cette situation est due au fait que le Conseil considère que l'action concernée relève de la non-prise de mesures techniques et organisationnelles et inflige une amende administrative en considérant les actions comme des mesures techniques et organisationnelles n'ont pas été prises. Le fait de ne pas remplir l'obligation de notification de violation de données constitue le motif de la décision du Conseil et se produit si la violation de données n'est pas notifiée au Conseil dès que possible et la personne concernée n'est pas informée dans un délai raisonnable. L'expression « dès que possible » a été fixée à 72 heures dans une décision du Conseil.

La contravention peut être commise intentionnellement et par négligence. Dans ce contexte, l'élément moral n’est pas déterminé dans LPDP. En revanche, les faits justificatifs peuvent être appliqués en fonction de la contravention. En particulier, l’ordre de la loi, l'application des exceptions de l'article 28 de LPDP et l'exercice d'un droit peuvent constituer des faits justificatifs. En termes de culpabilité, en particulier, l’état de nécessité peut être appliquée dans certains cas.

Il n'est pas possible de tenter de la contravention de ne pas remplir les obligations en matière de sécurité des données personnelles. Tout d'abord, trois actions de l’infraction constituent une contravention de danger abstrait et la tentative de commettre des contraventions de danger abstraits n'est pas reconnue. D'autre part, il n'y a pas de réglementation dans le LPDP concernant la tentative, alors qu'il n'est possible de tenter de commettre une contravention qu'en cas de réglementation spéciale. En revanche, il peut être possible de participer au délit. Cependant, conformément à l'article 18/2 du LPDP, seul le responsable du traitement sera passible d'une amende administrative en cas de participation.

Comme indiqué, dans le cas où le responsable du traitement traite illégalement des données personnelles, le Conseil évalue cette situation comme ne prenant pas de mesures techniques et organisationnelles et soumet l'action positive à une amende administrative dans le cadre de l’infraction qui peut être commis par négligence. Cette situation entraîne le fait que l'agrégation conceptuelle n'est pas appliquée en cas de traitement illicite de données personnelles et de commission d'un délit ou d'un crime en raison de cette omission, l'action et l'action positive ne sont pas considérées dans le cadre de l'agrégation conceptuelle. En particulier, la commission d'un délit avec un acte qui constitue également un crime au regard du droit pénal turc (TCK) entraîne l'assujettissement à deux sanctions pour le même acte. De plus, l'évaluation d'une action en tant qu'action continue et omission qui ne devrait pas être réglementée en tant qu'action continue, a entraîné l'évaluation que plusieurs actions sont considérées comme une seule action continue en cas de commettre l'action plusieurs fois.

Une amende administrative de 89.751 à 5.971.989 lires turques est imposée pour l'année 2023, dans le cas où la contravention de non-respect des obligations en matière de sécurité des données est commis. Bien que la limite supérieure de l'amende administrative ne soit pas dissuasive pour une entreprise internationale, la limite inférieure est un montant très élevé pour de nombreuses personnes. En revanche, l'instance d'objection à l'amende

administrative est le juge pénal de paix, et l'impossibilité de former un recours en annulation dans le cadre de la juridiction administrative dans un domaine qui requiert des connaissances techniques est une situation qu'il convient de critiquer.

Dans le cadre de la compétence territoriale du Conseil, le lieu de la contravention de non-respect des obligations en matière de sécurité des données diffère selon les actes commis. Le fait de ne pas prendre de mesures techniques et organisationnelles, qui est le fait le plus fréquemment commis en pratique, est un fait continu et une infraction qui peut être commis par négligence, le lieu où il est commis constitue les lieux où il faut prendre des mesures technique et administrative. Cependant, le Conseil détermine généralement sa compétence territoriale sur la base du principe de la personnalité, qui ne constitue pas une pratique correcte.

Dans le cadre de l'étude, on essaye d’exposer la contravention de non-respect des obligations en matière de sécurité des données personnelles dans une perspective large. Dans ce contexte, l'étude s'appuie sur les décisions du Conseil et de la magistrature. La contravention en question est présentée dans le cadre d’une systématique de crime/contravention.

ABSTRACT

The subject of this thesis is the misdemeanor of not fulfilling the obligations regarding personal data security. This misdemeanor is regulated in subparagraph (b) of paragraph 1 of Article 18 of the Personal Data Protection Law (“PDPL/KVKK”) titled "Misdemeanors". Within the scope of the misdemeanor, it is regulated that an administrative fine shall be imposed on persons who do not fulfill their obligations regarding data security in Article 12 of the PDPL. In paragraphs 2 and 3 of the article, it is regulated that private law legal entities and natural person data controllers are subject to sanctions within the scope of the misdemeanor, and that disciplinary provisions shall be applied to civil servants or persons working in the case of professional organisations with public institution status and public institutions and organizations. In our study, the misdemeanor of not fulfilling the obligations regarding data security and the obligations regulated in Article 12 of the PDPL in this context are discussed in detail. Within this scope, the study consists of two main parts, titled Overview of Personal Data Protection Law and Misdemeanor of not Fulfilling Obligations Regarding Personal Data Security.

Obligations to be taken regarding personal data security are regulated as 4 separate paragraphs in Article 12 of the PDPL. Accordingly, taking technical and administrative measures to ensure the necessary level of security for unlawful processing of personal data, illegal access to personal data and preservation of personal data, fulfillment of inspection obligations, prohibition of disclosure contrary to personal data and use personal data for the purpose other than processing purpose, fulfilling the data breach notification obligation are the obligations regulated in the PDPL regarding the data security. Violations of these provisions is regulated as misdemeanor.

Within the scope of the first chapter, various regulations regarding the personal data protection are explained. These subjects are composed of issues which we consider as important in order to comprehend the obligations related to misdemeanor and data security. Within this framework, in the first part of the first chapter several concepts are explained. Personal data, processing of personal data, data controller and data processor constitute these basic concepts. These concepts constitute various elements and components of the misdemeanor. Moreover, the basic principles in the personal data protection law are also explained in the first chapter. The basic principles of personal data protection law are lawfulness and fairness, being accurate and kept up to date where necessary, being processed for specified, explicit and legitimate purposes, being relevant, limited and proportionate to the purposes for which they are processed, being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed. These principles show the main objectives of personal data protection law and constitute basic criteria that the controllers must comply with all their responsibilities in terms of the PDPL.

The concept of personal data security constitutes the central concept of the study. In its most general definition, personal data security means the protection of personal data against risk and threats. Personal data is a type of information having certain characteristics. Within this scope, personal data gained a meaning in the direction of

principles and objectives of information security. It is aimed to ensure confidentiality, integrity and availability of information in information security. In this direction, within the scope of personal data security, personal data must be protected in line with the principles of confidentiality, integrity and availability.

Personal data security which has a substance in line with information security, has existed as one of the most important components of personal data protection law since the birth of personal data protection law. Within this scope, obligations related to personal data security have been included in the legislation prepared on the protection of personal data in Europe since the 1970s. The Hessen Data Protection Law which was enacted in 1970, and which is the first data protection law, contains obligations regarding personal data security. In the same way, the German Data Protection Law which was legislated in 1970 and the French Data Protection Law which was legislated in 1978 made it an obligation to take technical and administrative measures regarding data security. Afterwards, Personal data security, which has been made an obligation in the Convention No. 108 and the European Data Protection Directive, is finally regulated in detail with the GDPR.

In Turkish law, obligations regarding the personal data security are regulated with reference to European Data Protection Directive. While personal data security in the draft law on the personal data protection in 2008 which became obsolote, had a content formed in line with the Directive, It occured differentiation in the PDPL from the provisions of the Directive. Although this situation has made the existing data security obligation in the PDPL unique, it has also caused the data security obligations to have a content that exceed its own conceptual capacity.

In the second chapter of the study, the misdemeanor of not fulfilling the obligations regarding the personal data security is explained. Within this framework, legally protected interest of the misdemeanor, material and moral element of the misdemeanor, justification reasons, culpability, special apperance forms of the misdemeanor, sanction and judicial activities are discussed.

The perpetrator of the the misdemeanor of not fulfilling the obligations regarding the personal data security is the controller. Within this scope, this misdemeanor is a spesific misdemeanor. However, in some cases, such as legal entitites being controllers, the organ, representative and employee may also be perpetrators. In this case, the controller is subject to an administrative fine due to the action of the organ, representative or employee.

The victim of the misdemeanor of not fulfilling the obligations regarding data security is the data subject. Personal data amounts to any information relating to an identified or identifiable natural person. This person, to whom personal data can be related, is the data subject and constitutes the victim within the scope of the misdemeanor. The subject of the misdemeanor is the personal data processed by non-automatic means provided that they are part of a filling system system or automatic means in accordance with the PDPL. In the action of not fulfilling the data breach notification, the subject is information about the data breach fact.

In the misdemeanor of not fulfilling the obligations regarding the personal data security, it is regulated four different actions. Actions of not taking technical and organisational measures, not fulfilling the inspection obligation, disclosing personal data in violation of the PDPL and using personal data for the purpose other than processing purpose and not fulfilling the data breach notification obligation constitute the actions of the misdemeanor. The actions apart from not fulfilling data breach notification obligations are alternative actions within the scope of the misdemeanor. Since the subject of the act of not fulfilling the data breach notification obligation is different from other acts, this act constitutes another misdemeanor. The acts of not taking technical and organisational measures and not fulfilling the inspection obligation can be committed negligently and they are continuing misdemeanors. The action of disclosing personal data in violation of the PDPL and using personal data for the purpose other than processing purpose is not continuing misdemeanor and can be committed with positive action. Not fulfilling the data breach notification obligation is not contunuing misdemeanor either, plus this action can be committed negligently. Moreover all actions of the misdemeanor are conduct misdemeanor and within this context, no result is regulated in the PDPL.

The controller is required to take technical and organisational measures to ensure the appropriate level of security in order to prevent the unlawful processing of personal data, to prevent unlawful access to personal data and to ensure the preservation of personal data. Otherwise, the action takes place. The action of not taking technical and organisational measures is also continiuing action. Moreover, the Board considers the unlawful processing activities carried out within the body of the controller within the scope of the act of not taking technical and organisational measures to ensure the appropriate level of security in order to prevent processing personal data unlawfully. As a result of the Board's interpretation of the relevant article in this way, controllers are subject to administrative fines for not taking technical and organisational measures in case they process personal data unlawfully. This situation violates the principles of legality and certainty.

The action of not fulfilling the inspection obligation and the acts of disclosing personal data to others and using it for any purpose other than processing purpose in violation of the PDPL rarely constitute the reason of the decision of the board for the administrative fine. This situation is due to the fact that the Board considers the relevant action to be within the scope of not taking technical and organisational measures and imposes administrative fine by considering the actions as technical and organisational measures have not been taken. The act of not fulfilling the data breach notification obligation constitutes the reason of the decision of the Board, and occurs in case the data breach is not notified to the Board as soon as possible and the relevant person is not notified within a reasonable time. The expression of "as soon as possible" was determined as 72 hours in a decision of the Board.

The misdemeanor can be committed intentionally and negligently. In this context, it is not determined the moral element in the PDPL. On the other hand, justification reasons can be applied in terms of the misdemeanor. In particular, the application of the provision of law, application of the exceptions in Article 28 of the PDPL and the exercise of a right may constitute justification reasons. In terms of culpability, in particular, obligation can be applied in some cases.

It is not possible to attempt the misdemeanor of not fulfilling the obligations regarding personal data security. First of all, three actions of the misdemeanor constitute abstract danger misdemeanor and attempting to commit abstract danger misdemeanors are not accepted. On the other hand, there is no regulation in the PDPL regarding attempting to commit the misdemeanor, while it is only possible to attempt to commit a misdemeanor in case of special regulation. On the other hand, it may be possible to participate in the misdemeanor. However, in accordance with the article 18/2 of the PDPL, only the controller will be subject to an administrative fine in case of the participation.

As stated, in the event that the controller process personal data unlawfully, The Board evaluates this situation as not taking technical and organisational measures and subjects the positive action to an administrative fine within the scope of the misdemeanor which can be committed negligently. This situation causes the fact that conceptual aggregation is not applied in case of processing personal data unlawfully along with committing a misdemeanor or a crime owing to that omission action and positive action are not considered within the scope of conceptual aggregation. In particular, the committing of a misdemeanor with an act that also constitutes a crime under the Turkish Criminal Law (TCK) results in being subject to two sanctions for the same action. Moreover, the evaluation of an action as a continuing and omission action that should not be regulated as continuing action, caused the evaluation that multiple actions are considered as only one continuous action in case of committing the action multiple times.

Administrative fine of 89.751 to 5.971.989 Turkish lira is imposed for the year 2023, in the event that the misdemeanor of not fulfilling the obligations regarding data security is committed. While the upper limit of the administrative fine is not a dissuasive for an international company, the lower limit is a very high amount for many people. On the other hand, the objection authority to the administrative fine is the criminal judgeship of peace, and the inability to file an annulment case within the scope of administrative jurisdiction in an area that requires technical knowledge is a situation that should be criticized.

Within the scope of the territorial jurisdiction of the Board, the place of the misdemeanor of not fulfilling the obligations regarding the data security differs according to the actions committed. Since the act of not taking technical and organisational measures, which is the most frequently committed act in practice is a continuing act and since it is a misdemeanor that can be committed by negligence, the place where it is committed constitutes the places where technical and administrative measures should be taken. However, the Board generally determines its territorial jurisdiction on the basis of the principle of personality, which does not constitute a correct practive.

Within the scope of the study, the misdemeanor of not fulfilling the obligations regarding personal data security is tried to be presented from a broad persective. In this context, the study is supported by the decisions of the Board and judiciary. It is presented within the scope of crime/misdemeanor systematic.

ÖZET

Bu tez çalışmasının konusu kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatidir. Bu kabahat KVKK'nın "Kabahatler başlıklı" 18. maddesinin 1. fıkrasının (b) bendinde düzenlenmiştir. Kabahat kapsamında KVKK'nın 12. maddesinde yer alan veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyen kişiler hakkında idari para cezasına uygulanacağı öngörülmüştür. Maddenin 2. ve 3. fıkrasında ise kabahat kapsamında özel hukuk tüzel kişisi ve gerçek kişi veri sorumlularının yaptırıma tabi oldukları, kamu kurum niteliğindeki meslek kuruluşları ve kamu kurum ve kuruluşları bünyesinde gerçekleşmesi durumunda ise memur yahut görev yapan kişiler hakkında disiplin hükümlerinin uygulanacağı öngörülmüştür. Çalışmamızda veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati ve bu kapsamda KVKK'nın 12. maddesi düzenlenen yükümlülükler detaylı şekilde ele alınmaktadır. Bu kapsamda çalışma, Kişisel Verilerin Korunması Hukukuna Bakış ve Kişisel Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi Kabahati başlıklı iki bölümden oluşmaktadır.

Kişisel veri güvenliğine ilişkin alınması gereken yükümlülükler, KVKK'nın 12. maddesinde 4 ayrı fıkra olarak düzenlenmiştir. Buna göre kişisel verilerin hukuka aykırı şekilde işlenmesi, kişisel verilere hukuka aykırı şekilde erişilmesi ve kişisel verilerin muhafazası için gerekli güvenlik düzeyini temin etmek amacıyla teknik ve idari tedbirlerin alınması, denetim yükümlülüklerinin yerine getirilmesi, KVKK'ya aykırı kişisel verileri açıklama ve amacı dışında kullanma yasağı ve veri ihlal bildirim yükümlülüğünü yerine getirilmesi veri güvenliğine ilişkin KVKK'da öngörülen yükümlülüklerdir. Bu hükümlere aykırı davranış kabahat olarak düzenlenmiştir.

Birinci bölüm kapsamında kişisel verilerin korunması hukukuna ilişkin çeşitli düzenlemeler açıklanmaktadır. Bu konu başlıklarını kabahat ve veri güvenliğine ilişkin yükümlülüklerin anlaşılabilmesi için önem arz ettiğini düşündüğümüz hususlar oluşturmaktadır. Bu kapsamda birinci bölümün ilk kısmında çeşitli kavramlar açıklanmıştır. Kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu ve veri işleyen bu temel kavramları oluşturmaktadır. Bu kavramlar, kabahatin çeşitli öge ve unsurlarını teşkil etmektedir. Ayrıca kişisel verilerin korunması hukukunda yer alan temel ilkeler yine birinci bölüm kapsamında ifade edilmektedir. Kişisel verilerin korunması hukukunun ilkeleri, hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, Belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmedir. Bu ilkeler kişisel verilerin korunması hukukunun temel amaçlarını gösterdiği gibi veri sorumlularının KVKK kapsamında yer alan tüm yükümlülüklerinde uyması gereken temel ölçütleri teşkil etmektedir.

Kişisel veri güvenliği kavramı çalışmanın merkez kavramını oluşturmaktadır. Kişisel veri güvenliği en genel tanımıyla kişisel verilerin risk ve tehditlere karşı korunmasını ifade etmektedir. Kişisel veri, belirli özellikleri bulunduran bir tür bilgidir. Bu kapsamda kişisel veri güvenliği de bilgi güvenliği ilkeleri ve amaçları doğrultusunda bir anlam kazanmıştır. Bilgi güvenliğinde bilginin gizliliğinin, bütünlüğünün ve bilgiye

erişilebilirliğin sağlanması hedeflenmektedir. Bu doğrultuda kişisel veri güvenliği kapsamında da kişisel veriler gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmalıdır.

Bilgi güvenliği doğrultusunda bir içeriğe sahip olan kişisel veri güvenliği kişisel verilerin korunması hukukunun doğduğu günden bu yana kişisel verilerin korunması hukukunun en önemli bileşenlerinden birisi olarak var olagelmiştir. Bu kapsamda Avrupa'da 1970'li yıllardan bu yana kişisel verilerin korunmasına ilişkin hazırlanmış mevzuatlarda kişisel veri güvenliğine ilişkin yükümlülükler yer almıştır. İlk veri koruma yasası olan 1970 yılında çıkarılan Hessen Veri Koruma Yasası'nda kişisel veri güvenliğine ilişkin yükümlülükler mevcuttur. Aynı şekilde 1977 yılında yasalaşan Alman Veri Koruma Yasası ve 1978 yılında yasalaşan Fransız Veri Koruma Yasası da veri güvenliğine ilişkin olarak teknik ve idari tedbirlerin alınmasını bir yükümlülük haline getirmiştir. 108 Sayılı Sözleşme ve Avrupa Veri Koruma Direktifi'nde de bir yükümlülük haline getirilen kişisel veri güvenliği, nihayetinde GDPR ile detaylı bir şekilde düzenlenmiştir.

Türk hukukunda ise kişisel veri güvenliğine ilişkin yükümlülükler Avrupa Veri Koruma Direktifi'nden hareketle düzenlenmiştir. Özellikle 2008 yılında kadük kalan kişisel verilerin korunması kanunu tasarısında kişisel veri güvenliği Direktif doğrultusunda oluşmuş bir içeriğe sahip iken KVKK'da Direktif hükümlerinden büyük ölçüde farklılaşma gerçekleşmiştir. Bu durum KVKK'daki mevcut veri güvenliğine ilişkin yükümlülükleri özgün bir haline getirmiş olmasına rağmen aynı zamanda veri güvenliğine ilişkin yükümlülüklerin kendi kavramsal yapısını aşar şekilde bir içerik kazanmasına neden olmuştur.

Çalışmanın ikinci bölümünde kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati ele alınmaktadır. Bu kapsamda kabahat bakımından korunan hukuki değer, maddi ve manevi unsurlar, hukuka uygunluk sebepleri, kusurluluk, kabahatin özel görünüş biçimleri, yaptırım ve yargılama faaliyetleri açıklanmaktadır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin faili veri sorumlusudur. Bu kapsamda kabahat özgü bir kabahattir. Bununla birlikte tüzel kişilerin veri sorumlusu olması gibi bazı durumlarda ise organ, temsilci ve çalışan da fail olabilecektir. Bu durumda veri sorumlusu organ, temsilci yahut çalışanın hareketi dolayısıyla idari para cezasına tabi tutulmaktadır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin mağdurunu ise ilgili kişi oluşturmaktadır. Kişisel veri, belirli yahut belirlenebilir bir kişi ile ilişkilendirilebilir bir bilgi anlamına gelmektedir. Kişisel verinin ilişkilendirilebilir olduğu bu kişi ilgili kişi olup kabahat kapsamında mağduru teşkil etmektedir. Kabahatin konusu ise KVKK dolayısıyla bir veri kayıt sisteminin parçası haline getirilmek şartıyla otomatik olmayan yahut otomatik yollarla işlenmiş kişisel verilerdir. Yalnızca veri ihlal bildiriminin yerine getirilmemesi hareketinde konu unsurunu veri ihlali olgusuna ilişkin bilgiler teşkil etmektedir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde dört farklı hareket öngörülmüştür. Teknik ve idari tedbirlerin alınmaması, denetim

yükümlülüğünün yerine getirilmemesi, kişisel verilerin KVKK'ya aykırı şekilde açıklanması ve amacı dışında kullanılması, veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi kabahatin hareketlerini teşkil etmektedir. Veri ihlal bildirimi yükümlülüğü haricinde düzenlenen hareketler kabahat kapsamında seçimlik hareketlerdir. Veri ihlal bildirimi yükümlülüğünü yerine getirmeme hareketinin konusu diğer hareketlerden farklı olduğu için bu hareket başkaca bir kabahati teşkil etmektedir. Kabahatin teknik ve idari tedbirlerin alınmaması, denetim yükümlülüğünün yerine getirilmemesi hareketleri ihmali şekilde işlenebilmekte olup mütemadi hareket niteliğindedir. KVKK'ya aykırı kişisel verileri açıklama ve amacı dışında kullanma hareketi ise ani hareketli bir kabahat olup ayrıca hareket icrai hareketle işlenebilmektedir. Veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi ise ani hareketli bir kabahat olup ihmali şekilde işlenebilmektedir. Ayrıca kabahatin tüm hareketleri sırf hareket kabahati teşkil etmekte olup bu kapsamda KVKK'da herhangi bir netice öngörülmemiştir.

Veri sorumlusunun kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişimi önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmek için teknik ve idari tedbirleri alması gerekmektedir. Aksi halde hareket gerçekleşmektedir. Teknik ve idari tedbirlerin alınmaması hareketi aynı zamanda mütemadi nitelikte bir harekettir. Ayrıca Kurul, veri sorumlusu bünyesinde gerçekleşen hukuka aykırı işleme faaliyetlerini kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmek için teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirmektedir. Kurul'un ilgili maddeyi bu şekilde yorumlaması sonucunda veri sorumluları hukuka aykırı kişisel veri işlemeleri halinde teknik ve idari tedbirleri almamaları dolayısıyla idari para cezasına tabi olmaktadır. Bu durum kanunilik ve belirlilik ilkelerine aykırılık teşkil etmektedir.

Denetim yükümlülüğünün yerine getirilmemesi hareketi ve KVKK'ya aykırı şekilde kişisel verileri başkasına açıklama ve amacı dışında kullanma hareketleri ise nadiren Kurul'un idari para cezası kararlarının gerekçesini teşkil etmektedir. Bu durumun nedeni her iki hareket bakımından da hareketin gerçekleşmesi halinde Kurul'un ilgili hareketi teknik ve idari tedbirlerin alınmaması kapsamında değerlendirerek idari para cezası vermesidir. Veri ihlal bildiriminin yerine getirilmemesi hareketi ise Kurul kararlarında sıklıkla yaptırım kararının gerekçesini teşkil etmekte olup veri ihlalinin en kısa sürede Kurul'a makul sürede ise ilgilisine bildirim yapılmaması halinde gerçekleşmektedir. En kısa sürede ifadesi Kurul'un bir kararında 72 saat olarak belirlenmiştir.

Kabahat kasten işlenebileceği gibi taksirle de işlenebilmektedir. Bu noktada KVKK'da manevi unsur belirlemesi yapılmamıştır. Öte yandan hukuka uygunluk sebepleri çeşitli durumlarda kabahat bakımından söz konusu olabilecektir. Özellikle kanun hükmünün uygulanması ve KVKK'nın 28. maddesinde yer alan istisnaların uygulanması ve bir hakkın kullanılması hukuka uygunluk sebebi teşkil edebilecektir. Kusurluluk bakımından ise özellikle zorunluluk hali belli durumlarda kabahat bakımından söz konusu olabilecektir.

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatine teşebbüs mümkün değildir. Öncelikle kabahatin üç hareketi soyut tehlike kabahati teşkil etmekte olup soyut tehlike kabahatlerine teşebbüs kabul edilmemektedir. Bununla birlikte kabahatlere teşebbüs ancak özel düzenleme halinde mümkün olabilmekte olup KVKK'da

teşebbüse ilişkin bir düzenleme bulunmamaktadır. Öte yandan kabahate iştirak söz konusu olabilecektir. Bununla birlikte kabahate iştirak halinde KVKK'nın 18/2. maddesi gereği yalnızca veri sorumlusu idari para cezasına tabi olacaktır.

İfade edildiği üzere Kurul veri sorumlusunun hukuka aykırı şekilde kişisel veri işlemesi halinde bu durumu teknik ve idari tedbirlerin alınmaması altında değerlendirmekte, icrai bir hareketi ihmali bir kabahat kapsamında idari para cezasına tabi tutmaktadır. Bu durum ihmali hareket ve icrai hareketin fikri içtima kapsamında değerlendirilmemesi dolayısıyla hukuka aykırı şekilde kişisel verilerin işlenmesi ile birlikte başka bir suç yahut kabahatin de işlenmesi halinde fikri içtimanın uygulanmaması sonucunu doğurmaktadır. Özellike TCK kapsamında suç teşkil eden bir hareketle birlikte kabahatin uygulanması aynı hareket dolayısıyla iki defa yaptırıma tabi tutulma sonucunu doğurmaktadır. Ayrıca sırf hareketli bir kabahat olarak düzenlenmesi gereken bir hareketin mütemadi ve ihmali şekilde işlenebilen bir kabahat kapsamında değerlendirilmesi hareketin birden çok kez işlenmesi durumunda dahi mütemadi bir hareket olarak tek bir hareket gibi değerlendirilmesine yol açacaktır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin işlenmesi halinde 2023 yılı için 89.571 ila 5.971.989 Türk lirası idari para cezası uygulanmaktadır. İdari para cezasının üst sınırı uluslararası bir şirket için caydırıcılık niteliğine sahip değilken alt sınırı ise birçok kişi bakımından çok yüksek bir tutar arz etmektedir. Öte yandan idari para cezasına itiraz mercii sulh ceza hakimliği olup teknik bilgi gerektiren bir alanda idari yargı kapsamında iptal davası açılamaması eleştirilmesi gereken bir durumdur.

Kurul'un yer bakımından yetkisi kapsamında veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin işlendiği yer harekete göre değişiklik göstermektedir. Uygulamada en sık işlenen hareket olan teknik ve idari tedbirlerin alınmaması hareketi mütemadi hareket olup ihmali hareketle işlenebilen bir kabahat olduğu için işlendiği yeri teknik ve idari tedbirlerin alınması gereken yerler teşkil etmektedir. Bununla birlikte Kurul, genel olarak kişisellik ilkesi üzerinden yetkisini tayin etmekte olup bu durum doğru bir uygulama teşkil etmemektedir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati çalışmamız kapsamında geniş bir perspektiften sunulmaya çalışılmıştır. Bu kapsamda çalışma Kurul ve yargı kararlarıyla desteklenmiştir. Kabahat, okuyucuya suç/kabahat sistematiği kapsamında sunulmuştur.

GİRİŞ

Kişisel veri güvenliği, kişisel verilerin korunması hukukunun en önemli başlıklarından birisini teşkil etmektedir. Kişisel verilerin korunmasının tam olarak sağlanabilmesi için kişisel veri güvenliğinin temin ediliyor olması hayati önem taşımaktadır. Bu kapsamda KVKK'nın Amaç başlıklı 1. maddesinin gerekçesinde KVKK'nın amaçlarından birisi olarak bilgi güvenliğinin korunmasının zikredilmesi konunun önemini göstermektedir[1]. GDPR'da ise kişisel veri güvenliği mevzuatın temel ilkelerinden birisi olarak yer almaktadır (GDPR md. 5/1-f).

Kişisel veri belirli özellikleri bünyesinde taşıyan bir bilgi teşkil etmektedir. Bir bilgi türü olan kişisel verinin güvenliğinin sağlanması bu doğrultuda bilgi güvenliği ile doğrudan ilişkilidir. Bu kapsamda kişisel veri güvenliği, bilgi güvenliği amaçları ve prensipleri doğrultusunda bir anlama sahiptir[2]. Bilgi güvenliği bilginin yetkisiz erişim, yetkisiz kullanım, bozulma, değiştirme, yok olmasına karşı korunmasını ifade etmektedir[3]. Bu kapsamda kişisel veri güvenliği ise kişisel verilerin bozulmasına, yok olmasına, kişisel verilere yetkisiz erişim gerçekleşmesine, kişisel verilerin yetkisiz şekilde kullanımına karşı korunmasını ifade etmektedir. Dolayısıyla kişisel veri güvenliği ancak bilgi güvenliği çerçevesinde gerçekleştirilebilecek bir yükümlülüktür[4].

Kişisel veri güvenliğine ilişkin yükümlülükler KVKK'nın 12. maddesinde düzenlenmiştir. Buna göre veri sorumlularının veri güvenliğini temin etmek adına dört farklı yükümlülüğü yerine getirmesi gerekmektedir. Ayrıca maddede özel hukuk kapsamında müşterek sorumluluğa ilişkin bir hüküm mevcuttur. 12. madde şu şekildedir:

---

[1] Kişisel Verilerin Korunması Kanunu Gerekçesi (https://www.lexpera.com.tr/mevzuat/gerekceler/kisisel-verilerin-korunmasi-kanunu-madde-gerekceleri/1 E.T. 08.06.2023)

[2] European Union Agency for Cybersecurity, Guidelines for SMEs on the Security of Personal Data Processing, 2016, s. 12. (https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing E.T. 04.12.2022)

[3] Committee on National Security System, **National Information Assurance (IA) Glossarry**, CNSSI No. 4009, 2015, s. 64 (https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf E.T. 08.06.2023)

[4] Adnrew Denley, Mark Foulsham ve diğ. **GDPR, How to Achieve and Maintain Compliance,** New York: Routledge, 2019, s

"(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir".

Veri güvenliğine ilişkin sayılan yükümlülüklere uyulmaması ise bir kabahat olarak düzenlenmiştir. Buna göre KVKK'da veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirası ila 1.000.000 Türk lirası arasında idari para cezasına hükmolunacağı düzenlenmiştir (KVKK md. 18/1-b. Kabahatler Kanunu'nun 17. maddesi uyarınca idari para cezalarının yeniden değerlemesi sonucu 2023 yılı için bu tutarlar 89.571 Türk lirası ila 5.971.989 Türk lirası olmuştur[5].

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati, kanaatimizce KVKK'da düzenlenen en önemli yaptırımı teşkil etmektedir. Kanaatimizce bu durumun temel sebepleri, veri ihlallerinin sıklıkla yaşanması, veri güvenliğine ilişkin yükümlülüklerin KVKK'da veri güvenliğinin kapsamını aşar şekilde düzenlenmesi ve

[5] Kişisel Verileri Koruma Kurumu Duyurusu (https://www.kvkk.gov.tr/Icerik/7530/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Idari-Para-Cezasi-Tutarlari E.T. 29.03.2023.)

ayrıca Kurul'un bu düzenlemeyi kişisel verilerin hukuka uygun şekilde işlenmesini de kapsayacak şekilde geniş yorumlamasıdır. Bunun sonucu olarak veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati Kurul'un verdiği kararların büyük bir kısmının gerekçesini oluşturmaktadır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati özellikle uygulayıcılar arasında sıklıkla eleştirilmektedir. Eleştirilerin temel gerekçeleri kişisel verilerin hukuka aykırı şekilde işlenmesinin veri güvenliği kapsamında değerlendirilmesi, idari para cezalarının yüksekliği ve Kurul'un konu hakkında verdiği çeşitli kararlardır. Bununla birlikte veri güvenliği ve veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin ifade ettiğimiz önemine ve uygulamada sıklıkla eleştirilerle karşı karşıya kalmasına rağmen konu Türk hukukunda kapsamında henüz yeteri kadar incelenmemiştir. Konu hakkında kişisel verilerin korunması hukukuna ilişkin kaleme alınmış eserlerde yer alan genel açıklamalar dışında Zeynel Kangal'ın "Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması" adlı eserinde bir bölüm ayrılmış olup kabahat ilk defa bu eserde detaylı şekilde çözümlenmiştir[6]. Ayrıca KVKK'da düzenlenen kabahatlerin içtima bakımından değerlendirilmesine ilişkin Muammer Ketizmen ve Aslıhan Kart tarafından yazılan "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme" adlı eserde de kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati içtima hükümleri bakımından değerlendirilmiştir[7].

İşbu çalışma, veri güvenliği ve veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatini incelemek amacıyla yazılmıştır. Bu kapsamda çalışma, gerek akademik eser sayısının az olduğu konu hakkında Türk hukukuna mütevazı bir katkıda bulunmak gerekse de konu hakkında dile getirilen eleştirilere kulak vermek gayesiyle kaleme alınmıştır.

---

[6] Zeynel Kangal, **Kişisel Verilerin Ceza ve Kabahat Hukukunda Korunması**, İstanbul: On İki Levha Yayıncılık, 2019, **passim**

[7] Aslıhan Kart ve Muammer Ketizmen, "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", **Kişisel Verileri Koruma Dergisi,** Cilt: 1 Sayı: 2**,** 2019, **passim**

Çalışmamızın Kişisel Verilerin Korunması Hukukuna Bakış başlıklı birinci bölümünde çalışma boyunca kullanılacak kavramlar açıklanmış, kişisel verilerin korunması hukukunun özü olan temel ilkeler ifade edilmiş ve veri güvenliğine ilişkin yükümlülükler değerlendirilmiştir. Bu kapsamda veri güvenliği ve veri güvenliğine ilişkin yükümlülükler, Avrupa'da eski ve yeni düzenlemeler ile karşılaştırılarak açıklanmış, kavram ve yükümlülüklerin kapsamı Türk hukuku açısından incelenmiştir.

Çalışmamızın Kişisel Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi Kabahati adlı ikinci bölümünde ise kabahat sistematik bir biçimde incelenmiştir. Korunan hukuki değer, kabahatin maddi ve manevi unsurları, hukuka uygunluk sebepleri, kusurluluk ve kabahatin özel görünüş biçimleri bu bölüm kapsamında ele alınmıştır. Son olarak kabahatin yaptırım ve yargılanması ele alınmış olup bu bölüm kapsamında kabahatin Kurul tarafından ne şekilde yaptırıma tabi tutulduğu, Kurul'un yer bakımından yetkisi ve Kurul tarafından verilen idari yaptırım kararlarına karşı itiraz prosedürü açıklanmıştır.

Çalışmamız kapsamında Kurul'un günümüze dek yayımladığı kararlarından yararlanılmıştır. Kurum tarafından yayımlanan rehber ve iyi uygulama örnekleri de çalışmanın başvuru kaynaklarının önemli bir kısmını oluşturmaktadır. Ayrıca Avrupa'daki Veri Koruma Otoriteleri'nin de yayımladığı rehber, iyi uygulama örnekleri ve kararlardan da yararlanılarak Türk hukukunun yanı sıra Avrupa'da mevcut düzenlemelere de gerekli oldukça yer verilmiştir. Böylece okuyucuya konu farklı bir perspektiften de sunulmaya çalışılmıştır.

BİRİNCİ BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI HUKUKUNA BAKIŞ

I. Kavramlar

Kişisel verilerin korunması hukukunda belirli kavramlar büyük önem arz etmektedir. Bu kavramların sınırlarının çizilmesi ve kapsamlarına nelerin dahil olduğunun tespit edilmesi, hem kişisel verilerin korunması hukukunun kapsamını netleştirmek açısından hem de veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin çeşitli unsurlarını açıklayabilmek açısından elzemdir. Bu kapsamda birinci bölümün ilk kısmında çeşitli kavramlar açıklanacaktır. Çalışmamızda detaylı şekilde açıklayacağımız kavramlar; kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu ve veri işleyen kavramlarıdır.

A. Kişisel Veri

Kişisel veri, kişisel verilerin korunması hukuku bakımından temel kavramı oluşturmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kapsamını temel olarak kişisel veri kavramının belirlediği ifade edilebilir[8]. Bir verinin kişisel veri sayılması tabi olduğu hukuki güvenceleri ciddi bir şekilde değiştirmektedir. Bu noktada bir kavram olarak kişisel veriyi ve kişisel verinin sınırlarını tespit etmek çalışmamız açısından büyük önem arz etmektedir.

Kişisel veri kavramı KVKK kapsamında; "*Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır (KVKK 3/1-d). Avrupa Veri Koruma Direktifi'nde[9] ve Genel Veri Koruma Tüzüğü'nün 4. maddesinde ise kişisel verinin belirli ya da belirlenebilir gerçek kişiye ilişkin herhangi bir bilgiden

[8] Genel Veri Koruma Tüzüğü ("GDPR") bakımından: Irmak Erdoğan, **Yapay Zeka ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri**, Ankara: Seçkin Yayıncılık, 2022, s. 63

[9] Directive 95/46/Ec of the European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

müteşekkil olduğu düzenlenmiştir (DPD md. 2/a, GDPR md. 4/1-a)[10]. Görüldüğü üzere KVKK'da mevcut kişisel veri tanımı Avrupa'daki veri koruma düzenlemeleriyle uyumlu bir tanımlamadır.

Yukarıda yer verilen tanımdan bir bilgiyi kişisel veri olarak addedebilmek için belirli şartları sağlaması gerektiği anlaşılmaktadır. Bu şartlar; türüne bakılmaksızın bir bilginin mevcut olması, gerçek kişiye ilişkin olması, bilginin ilişkili bulunduğu gerçek kişinin "belirli" ya da "belirlenebilir" olmasıdır[11]. Sayılan koşulları taşıyan bir bilgi, kişisel veri teşkil edecektir.

1. Her Türlü Bilgi

KVKK'daki tanımda yer alan ilk unsur her türlü bilgi unsurudur. Kişisel veri belirli şartları taşıyan bir bilgidir. Madde 29 Çalışma Grubu, Direktif kapsamında *"herhangi bir bilgi (information)"* ifadesinin kullanılmasının, kişisel veri kavramının geniş bir şekilde tanımlanması amacına işaret ettiği görüşündedir[12]. Yine KVKK kapsamında da "her türlü bilgi" ibaresinin aynı amacı ifa ettiği söylenmelidir[13]. Bilgi kişinin adı ve soyadı olabileceği gibi beden ölçüsü, internet geçmişi, IP adresi veya tüketim alışkanlıkları vb. olabilecektir. Bilginin nesnel olmasına gerek bulunmamaktadır, öznel bir bilgi de kişisel veri teşkil edebilir[14]. Aynı şekilde bilginin doğru yahut yanlış olması kişisel veri teşkil etmesi bakımından önem arz etmemektedir[15].

---

[10] Regulation (Eu) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[11] Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 01248/07/EN WP 136, 2007, s. 6 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 10.10.2021). Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması**, İstanbul: On İki Levha Yayıncılık, 2017, s. 30

[12] Article 29 Working Party (2007), **loc.cit.**

[13] Nitekim Kişisel Verileri Koruma Kurumu da yayımladığı bir rehberde bu ibarenin genişliğine vurgu yapmıştır. Bkz: Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, Ankara: KVKK Yayınları, 2019, s. 21

[14] Develioğlu, **op.cit.** s. 37

[15] **Ibid**. Erbil Beytar, **İşçinin Kişiliğininin ve Kişisel Verilerinin Korunması**, İstanbul: On İki Levha, 2017, s. 51

Veri (data), bilgi (information) ve bilgi (knowledge) kavramları sıklıkla birbirleri yerine kullanılan kavramlardır[16]. Özellikle veri ve bilgi (information) kavramları arasındaki farkların netleştirilmesi ise kişisel verilerin korunması hukuku bakımından büyük önem arz etmektedir. Bu kapsamda Avrupa öğretisinde, bilgi ve veri kavramlarının nasıl anlaşılması gerektiğine dair bir açıklık getirilmemesi daha ziyade bu kavramların kişi ile ilişkisi üzerinde durulması eleştirilmiştir[17]. Türkçe ve dolayısıyla Türk hukuku bakımından ise bu kavramların muhtevası çok daha problemli bir konudur. Her ne kadar "data" kavramı Türkçe'de "veri" kavramı ile karşılansa dahi "information" ve "knowledge" kavramları yerine Türkçe'de genelde bilgi kavramı kullanılmaktadır ve bu durum ayrıca karışıklığa yol açmaktadır[18].

Bilgi kavramını anlamak için öncelikle bu kavramlarla ilişkili veri kavramının açıklanması gerekmektedir. Veri kavramı genel olarak ham durumda olan işlenmemiş malzemeye benzetilmektedir[19]. **Ackoff,** veriyi bir nesneyi, ortamı veya olayın niteliklerini temsil eden semboller olarak tanımlamıştır[20]. Aslında veri, dış dünyada, işlenmemiş şekilde verili olandır. Nitekim **Zins**, veri için duyusal uyaran (*sensory stimulus*) kavramını kullanmaktadır[21]. Veri kavramı Türkçe'de vermek fiilinden gelmektedir. Fransızca'da da benzeri bir etimolojik temel mevcut olup "données" (veri) kelimesi aslında "vermek" fiilinin (donner) geçmiş zaman çekiminden gelmektedir. Aynı şekilde İngilizce'de de data

---

[16] Nazan (Özenç) Uçak, "Bilgi Üzerine Kuramsal Bir Yaklaşım", **Bilgi Dünyası**, Cilt: 1, Sayı: 1, 2000, s. 146, Raphaël Gellert, "Comparing Definitions of Data and Information in Data Protection Law and Machine Learning: A Useful Way Forward to Meaningfully Regulate Algorithms?", **Regulation & Governance**, Cilt: 16 Sayı: 1, 2020, s. 4. Hakan Çetin, "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi", **Akdeniz İ.İ.B.F. Dergisi**, Cilt: 14 Sayı: 29,2014, s. 88. Bu kavramlar konusunda yaşanan karışıklıklar bakımından ayrıca bkz: Yavuz Erdoğan, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi", **Erciyes Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 8 Sayı: 2, 2013, ss. 573, 574

[17] Bkz: Lee A. Bygrave, **Data Privacy Law: An International Perspective**, Oxford: Oxford University Press, 2014, ss. 126-127

[18] Küzeci bu üç kavramı veri (data), enformasyon (information) ve bilgi (knowledge) kavramları olarak ayırmıştır (Elif Küzeci, **Kişisel Verilerin Korunması,** Ankara: Turhan Kitabevi, 2019, s. 9). Yine Aynı şekilde Erdoğan da "information" kavramının bilgi olarak Türkçe'ye çevrilmesinin hatalı olduğunu bilgi kavramının tam anlamıyla "information" kavramını karşılamadığından bahisle "enformasyon" kavramını tercih etmiştir (Erdoğan, **op.cit**. s. 67). Ancak gerek "knowledge" gerek "information" kavramları yerine Türkçe'de bilgi kavramının kullanılması dolayısıyla çalışmamız kapsamında bu şekilde bir ayrıma gidilmemiştir.

[19] Aysan Şentürk, **Veri Madenciliği**, Bursa: Ekin Basım Yayın, 2006, s. 4

[20] Russell Ackoff,"From Data to Wisdom", **Journal of Applied System Analysis**, Cilt: 16 1989, s. 3

[21] Chaim Zins, "Conceptual Approaches for Defining Data, Information and Knowledge", **Journal of the American Society For Information Science and Technology**, Cilt: 58, Sayı: 4, 2007, s. 487.

(veri), verilmiş ya da bahşedilmiş olan şey anlamına gelen "datum" kelimesinden türemektedir[22].

Bilgi (information) kavramı ise Latince biçimlendirmek anlamına gelen "Informare" fiilinden türemektedir[23]. Bilgi (information), verilerin işlenmiş, şekil verilmiş halini belirtmektedir[24]. **Zins**, bilgi (information) kavramının, verinin ya da diğer bir deyişle duyusal uyaranın anlamı olduğu görüşündedir[25]. **Ackoff** da aynı yönde "information" kavramının, veriden çıkarsanan kim, ne, nerede gibi sorulara cevap veren tasvirler içeren şeyler olduğunu ifade etmiştir[26]. Ancak bilginin yalnızca bahsedilen anlama (bilgi = veri + anlam) sahip olmadığını, iki katmanlı bir anlama sahip olduğunu değerlendiren yazarlar da bulunmaktadır[27]. **Gellert**'e göre bilgi hem çıkarsanan şey (veri + anlam) hem de objektif gerçekliği temsil eden işaretlerdir[28]. Bu noktada bilginin bahsi geçen ikinci anlamı, verinin yukarıda açıklanan anlamına yakındır. **Gellert**, Çalışma Grubu'nun bir resmi yahut ses kaydını bilgi kabul etmesinden dolayı bilginin bahsedilen ikinci anlamda da kabul edildiğini savunmaktadır[29]. Bu kapsamda kişisel verinin tanımı bakımından da veri ve bilgi kavramları arasında keskin bir ayrım bulunmamakta olup tanımda yer alan bilgi unsurunun bilginin her iki anlamını da kapsadığı kabul edilmelidir[30]. Aynı şekilde Türk öğretisinde de veri ve bilgi kavramlarının çoğu defa

---

[22] Oxford University, **The Concise Oxford Dictionary of English Etymology**, Editör: T. F. Hoad, New York: Oxford University Press, 1996 s. 113. Bilgi teorisi ve bilişim dünyasındaki gelişmeler sonrasında veri ikinci bir anlama daha sahip olmuştur (Daniel Rosenberg, "Data Before the Fact", **"Raw Data" is an Oxymoron**, Edited by Lisa Gitelman, London: MIT Press, 2013, s. 34). Bu yöndeki gelişmeler ışığında örneğin Değirmenci veriyi "*bilgisayarda yer alan formatlanmış bilgi*" şeklinde açıklamıştır (Olgun Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **TBB Dergisi**, Sayı: 58, 2005, s. 200) Veri aynı zamanda durumların, olguların gösterimidir (Tunç Demircan, **Bilişim Alanında Suçlar**, İstanbul: Legal Kitabevi, 2016, s. 20). Bu anlamda veri, bilginin numerik biçimdeki halidir (Rosenberg, op.cit. s. 33). Verinin farklı anlamlara geldiğine ayrıca kimi yazarlarca dikkat çekilmiştir. (Bkz: Mehmet Can Karagöz, **Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, İstanbul: On İki Levha Yayıncılık, 2020, s. 28)

[23] Oxford University, **The Oxford Dictionary of English Etymology**, Editör: C.T. Onions, New York: Oxford University Press, 1966, s. 473

[24] Erdoğan, **op.cit**. s. 68, Nevzat Güngör, **İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik**, Ankara: Gazi Kitabevi, 2021, s. 71

[25] Zins, **loc.cit.** Nitekim Bygrave de verinin temsili işlevi olduğunu; bilginin ise semantik ve bilişsel olduğunu söylemektedir. Bkz: Lee A Bygrave "Information Concepts in Law: Generic Dreams and Definitional Daylight", **Oxford Journal of Legal Studies,** Cilt: 35, Sayı: 1, 2015, s. 23

[26] Ackoff, **loc.cit**.

[27] Bkz: Gellert, **op.cit**. s. 6

[28] **Ibid**.

[29] **Ibid**. s. 8

[30] **Ibid**.

birbirinin yerine geçer şekilde kullanıldığı kabul edilmektedir[31]. Bu kapsamda kişisel veri tanımında yer alan bilgi unsurunu, geniş haliyle gerçekliği temsil eden her türlü işaret anlamını da kabul eder bir şekilde değerlendirmek ve veri kavramına yönelik olarak verdiğimiz tanımı da ihtiva eder şekilde anlamak, çok daha isabetli bir yaklaşım olacaktır. Aksi halde kişisel veri tanımını ve tanımın kapsamını çok daha dar bir şekilde yorumlama mecburiyeti doğacaktır[32].

2. Gerçek Kişi

KVKK'nın tasarı metninde kişisel veri hem gerçek hem de tüzel kişilere ilişkin bilgileri kapsayan bir kavram olarak tanımlanmıştır; ancak tasarı kanunlaştığında kişisel veri yalnızca gerçek kişilere ilişkin bilgiler bakımından kabul edilmiştir[33]. Gerçek kişi bakımından ise KVKK'da herhangi bir ayrım yapılmamış olup ekonomik durum, sosyal statü, vatandaşlık bağı gibi hususlara bakılmaksızın herkes korumanın kapsamındadır[34].

Kişisel verinin yalnızca gerçek kişiye ilişkin olarak kabul edilmesi, iki temel sonuç doğurmaktadır. İlk sonuç, tüzel kişilere ilişkin bilgilerin kişisel veri addedilmediği ve dolayısıyla KVKK kapsamında tüzel kişilerin hak öznesi olmadıklarıdır. Tüzel kişilere ilişkin bilgilerin kişisel veri teşkil edebilmesi ise yine bilginin bir şekilde gerçek kişiye ilişkin olması gerekecektir[35]. Örneğin, bir şirketin sicil gazetesinde tescil bilgileri, gerçek

---

[31] Küzeci (2019a), **op.cit**., s. 12. Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,** Ankara: Seçkin Hukuk, 2020, s. 21. Cemal Başar, **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, İstanbul: On iki Levha, 2020, s. 14. Kanun kapsamında bilgi kavramının anlamlandırılmış veri şeklinde anlaşılması gerektiğini savunan bir görüş için ayrıca bkz: Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul: On iki Levha Yayıncılık, 2019, s. 40. Bygrave (2015), **op.cit**. s. 23

[32] Aynı yönde: İlke Gürsel, **İşçinin Kişisel Verilerinin Korunması Hakkı**, İzmir: Doktora Tezi, Dokuz Eylül Üniversitesi, 2016, s. 6

[33] Göçmen Uyarer, **op.cit**. s. 110. B.02.0.KKG.0.10/101-902/1812 sayılı Kanun Tasarısı md. 3/1-c (https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=64271 E.T. 28.11.2022) Göknil Özcan, **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, İstanbul: On İki Levha, 2020, s. 10. Öte yandan Kişisel veri tanımının genel olarak geniş tutulması ve bu noktada bilginin anlamının muğlak bir şekilde ele alınması öğretide ayrıca eleştirilmiştir (Bkz: Nadezhda Purtova, "The Law of Everything, Broad Concept of Personal Data and Future of EU Data Protection Law", **Law, Innovation and Technology**, Cilt: 10, Sayı: 1, 2018, s. 12)

[34] Develioğlu, **op.cit**. s. 32

[35] Onur Baskın, **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması,** Ankara: Seçkin Yayıncılık, 2021, s. 24. Nitekim Kişisel Verileri Koruma Kurulu da tüzel kişilerin verilerinin 2. madde kapsamında değerlendirilemeyeceğine hükmetmiştir. Kişisel Verileri Koruma

kişi pay sahiplerinin adı, soyadı ve kendisini belirli ya da belirlenebilir kılan diğer tüm bilgileri dolayısıyla kişisel veri içerebilecektir[36].

Bir bilginin kişisel veri sayılabilmesi için gerçek kişiye ilişkin olması gerekliliğinin ikinci sonucu ise ancak kişiler hukuku kapsamında "kişiye" ilişkin bilgilerin kişisel veri teşkil edebilecek olmalarıdır. Kişilik ise Türk hukukunda tamamiyle ve sağ doğumla başlamakta ve ölümle sona ermektedir[37]. Nitekim Kurul bir kararında, mirasçının vefat eden yakınının kişisel sağlık verilerini almak için veri sorumlusu sağlık kuruluşuna yaptığı başvuruda Türk Medeni Kanunu'nun 28. maddesine dayanarak ölen bir kimsenin kişi sayılamayacağı dolayısıyla da KVKK Kapsamında yapılacak bir işlem olmadığına hükmetmiştir[38]. Ölmüş kimselerin yanı sıra cenine ait bilgiler de kişisel veri kabul edilemeyecektir[39]. Cenine ilişkin bilgiler ceninin doğumuna kadar annenin kişisel verisi niteliğinde olacağı için annenin sağlık verisi olarak KVKK kapsamında korunacaktır[40].

Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5423/2018-131 E.T. 25.02.2023) Özcan, **loc.cit.**

[36] Ticaret müdürlükleri tarafından işlenen gerçek kişi tacir ve hissedarların verilerinin kişisel veri, üzerinde gerçekleştirilen faaliyetlerin ise kişisel veri işleme faaliyeti olduğuna ilişkin olarak ayrıca bkz: Kişisel Verileri Koruma Kurulu 2020/307 sayılı karar (https://www.kvkk.gov.tr/Icerik/6895/2020-307 E.T. 27.10.2022)

[37] Şaban Kayıhan ve Mustafa Ünlütepe, **Medeni Hukuk Bilgisi**, Ankara: Seçkin Yayıncılık, 2017, 4. baskı, ss. 156-158, Mehmet Ayan, Nurşen Ayan, **Kişiler Hukuku**, Ankara: Seçkin Yayıncılık, 2016, 8. baskı, ss. 43, 171.

[38] Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/273 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6710/2019-273 E.T. 27.10.2022). Yine Kurul'un benzeri bir sağlık verisi talebine ilişkin verdiği kararda da aynı husus ifade edilmiştir. Bu karar kapsamında ifade ettiğimiz ilk karara atıf yapan Kurul yukarıda zikrettiğimiz karara atıf yaparak görüşünü tekrarlamış ve ölmüş kişiye ilişkin bilgilerin Kanun kapsamında korunmayacağı hususunu bu karar kapsamında da tekrar etmiştir. Bkz: Kişisel Verileri Koruma Kurulu'nun 30.06.2020 tarihli ve 2020/507 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6926/2020-507273 E.T. 27.10.2022)

[39] Baskın **op.cit.** s. 26, Aksi görüş: Taştan **op.cit.** s. 36, Develioğlu **op.cit.** s. 31. Öte yandan ölüm karinesi ve gaiplik de bir bilginin kişisel veri sayılması bakımından önem arz etmektedir. Kişinin ölümüne kesin gözle bakılan bir olay içerisinde kaybolması ve cesedinin bulunamamış olması durumunda ölüm kaydının düşülmesi ile kişi olayın gerçekleştiği an itibarıyla ölmüş sayılır (Ayan ve Ayan, **op.cit.** s. 174, 175) Bu durumda olayın gerçekleştiği andan itibaren kişiye ilişkin bilgilerin kişisel veri addetmediği kabul edilmelidir. Aynı şekilde kişi hakkında gaiplik kararı verilmesi halinde, kişinin ölüm tehlikesi içerisinde kaybolduğu yahut kişiden son haber alındığı tarihten itibaren ölüme bağlı haklar kullanılabilmektedir (Şaban Kayıhan, **Kişiler Hukuku,** Ankara: Seçkin Yayıncılık, 2022, s. 28). Dolayısıyla bu tarihten itibaren kişiye ilişkin bilgiler kişisel veri olarak kabul edilmemelidir.

[40] Anne bakımından korunacağını savunan bir diğer görüş için bkz: Taştan, **loc.cit.** Cenine ilişkin bilgilerin anne bakımından korunması uygulamada herhangi bir farklılık yaratmayacağı kanaatinde olduğumuz gibi anne bakımından korunması noktasında cenine ilişkin tüm bilgilerin sağlık verisi olarak özel nitelikli veri kabul edilmesi gerekeceği için uygulamada daha sıkı bir koruma sağlama olanağı da bulunmaktadır.

3. Belirli ya da Belirlenebilir Kişi

Kişisel veri tanımında yer alan diğer şart ise kişinin kimliğinin belirli ya da belirlenebilir olmasıdır. Kurum, belirli ya da belirlenebilir olmayı, "*mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi*" şeklinde ifade etmektedir[41]. Bazı bilgiler kişiyi doğrudan belirli kılabilirken bazı bilgiler kişiyi doğrudan doğruya belirli kılacak vasfa sahip değildir; ancak bu bilginin başka bilgilerle birlikte varlığı, kişinin belirlenebilmesini mümkün kılabilecektir[42].

Belirli ve belirlenebilir ifadelerinin nasıl anlamlandırılabileceğine ilişkin olarak Çalışma Grubu yayımladığı rehberde iki aşamalı bir test sunmuştur: Bu kapsamda bir gruptaki herhangi bir kişi, grubun tüm üyelerinden bir şekilde ayrıştırılabiliyorsa bu kişinin kimliğinin belirli olduğunu; henüz diğerleri arasından ayrıştırılamamakta ancak ayrıştırılması ihtimal dahilinde olduğu halde ise kimliğinin belirlenebilir olduğunu söylemek gerekmektedir[43]. Belirlilik halinde bilgi doğrudan kişiyi ayrıştırmaya yeter niteliktedir[44]. Belirlenebilirlik halinde ise kişiye ilişkin bilgi onu diğerlerinden tam anlamıyla ayırmaya yetmeyecektir; ancak başka bir bilgiyle birlikte kullanılması halinde, kişinin belirlenmesi mümkün hale gelecektir[45]. Örneğin, kişinin sahip olduğu araç plakası başkaca bilgilerle eşleştirilerek kişinin teşhisini mümkün kılabilecektir.

KVKK'nın gerekçesinde ad, soyadı, doğum tarih ve doğum yeri gibi verileri kişinin kesin teşhisini sağlayan örnekler olarak ifade edilmiştir[46]. Ancak gerekçedeki niteleme

---

[41] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**, s. 14 (https://kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022)

[42] Bu bilgiyi "tanımlayıcı" yahut "belirleyici" olarak ifade etmek mümkündür (Develioğlu, **op.cit.** s. 33)

[43] Article 29 Working Party (2007), **Ibid**. s. 12. Ayrıştırma testi olarak ifade edebileceğimiz bu teste GDPR Recital 26 kapsamında atıf yapılmış ve belirlenebilirlik değerlendirilmesine ilişkin örneklerden biri olarak ifade edilmiştir. (Lee A. Bygrave ve Luca Tosoni, "Personal Data", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020, ss. 108,109)

[44] Sevg Erarslan Türkmen, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, İstanbul On İki Levha, 2019, s. 20

[45] Mesut Serdar Çekin, **Kişisel Verilerin Korunması Hukuku**, İstanbul: On İki Levha yayıncılık, 2020, s. 45

[46] Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, Ankara: KVKK Yayınları, 2019, s. 9

hatalı sonuçlar doğurabilecektir. Nitekim kişinin mutlak teşhisini sağlayacağı ifade edilen kişisel verilerin her durumda kendi başına mutlak anlamda kişinin teşhisini sağlaması söz konusu değildir. Örneğin bir bakkalın veresiye defterinde yazan "Ahmet Yılmaz 5 ekmek aldı" ifadesindeki Ahmet Yılmaz ifadesi kişiyi her zaman mutlak anlamda teşhis kudretine sahip değildir[47]. Bu noktada her bir bilgi için somut olay nezdinde objektif bir biçimde değerlendirme yapılması gerekmektedir[48].

Kurul'un belirlenebilme değerlendirmesi yaptığı kararları bulunmaktadır. Örneğin, Kurul bir kararında telefon numarasının kişinin adı, soyadı ve telefon numarası ile eşleştirilerek saklanması halinde kişinin kimliğinin belirlenebilir olduğunu, dolayısıyla telefon numarasının kişisel veri olduğunu ifade etmiştir. İlgili olay kapsamında bir seyahat için rezervasyon yapan kişi sistemde kayıtlı telefon numarası dışında farklı bir numara yazmış ve rezervasyona ilişkin SMS talep etmiştir. Ancak sisteme girilen numara başkaca bir kişiye aittir. Kurul, kararında numarası kaydedilmiş üçüncü kişinin numarasının herhangi bir kayıtla eşleşmediğini ifade etmiştir. Kurul kararında açıkça ifade etmese de bu ifadeden telefon numarasının olay kapsamında başkaca bir kayıt ile eşleşmediği için kişinin belirli ya yahut belirlenebilir olmadığı, dolayısıyla ilgili numaranın kişisel veri teşkil etmediği sonucu çıkarılmaktadır[49].

Kurul başkaca bir kararında ise kan ve doku örneklerinin barkodlanmış tüplerde saklandığı belirterek hastaların kimliklerine ulaşılabilme ihtimalini ifade etmiş ve ilgili verilerin kişisel veri teşkil ettiğini tespit etmiştir[50]. İlgili kan ve doku örneklerinin

---

[47] Aynı yönde: Develioğlu, **op.cit**. s. 33

[48] Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, Ankara: KVKK Yayınları, 2019, s. 18. Nitekim Çalışma Grubu da kişisel veriye ilişkin belirlilik değerlendirmesinin mevcut durumun şartlarına dayandığını belirtmektedir. Bkz: Article 29 Working Party (2007), **op.cit**. s. 13.

[49] Kişisel Verileri Koruma Kurulu'nun 11.08.2021 tarihli 2020/608 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6927/2020-608 E.T. 26.10.2022). Kararın kişisel veriye ilişkin kısmı tam olarak şu şekildedir: "*6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin (1) numaralı fıkrasının (d) bendi gereğince "kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlandığı, bu kapsamda ilgili kişiye ait telefon numarasının, adı- soyadı ve TC kimlik numarası ile eşleştirilerek saklandığından ve kimliği belirlenebilir gerçek bir kişiye ulaşılması sonucu doğurduğundan kişisel veri niteliğinde olduğu, ancak somut olayda ilgili kişiye ait telefon numarasının kendisine ait herhangi bir kayıtla eşleşmediği aksine sehven yazılmış olan numaranın bileti satın alan kişi tarafından veri sorumlusu sistemlerine girildiğinin anlaşıldığı…*".

[50] Kişisel Verileri Koruma Kurulu 30.10.2019 tarihli 2019/316 sayılı karar (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 26.10.2022). Biyolojik örneklerin kişisel veri oluşturup oluşturmadığı ayrıca öğretide tartışılmış bir husustur. Bilgi ve veri kavramlarının anlamları

üzerindeki barkodlarla birlikte kişiyi belirlenebilir kılmakta olduğu için kişisel veri kabul edilmiştir.

B. Kişisel Verilerin İşlenmesi

Bir kişisel veri bakımından KVKK kapsamında değerlendirme yapabilmek için kişisel veri üzerinde gerçekleşecek fiilin "işleme" niteliğinde olması gerekmektedir. İşleme faaliyeti ise KVKK'da: "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi…"* şeklinde tanımlanmıştır (KVKK 3/1-e). Görüldüğü üzere işleme faaliyeti oldukça geniş bir biçimde düzenlenmiştir. İşleme fiilinin geniş düzenlenmesi dolayısıyla veri üzerinde gerçekleşen herhangi bir işlemin işleme faaliyeti dışında kalma olasılığı oldukça düşüktür[51].

Schreiber, kişisel veri işleme faaliyetinin iki temeli olduğunu ifade etmiştir. Bunlar; "veri üzerinde gerçekleşme" ve "işlem" unsurlarıdır[52]. KVKK kapsamında ise üç unsurdan bahsetmek mümkündür. Buna göre, kısmen ya da tamamen otomatik olan yollarla veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla olan, kişisel veri üzerinde gerçekleştirilen herhangi bir işlem, işlemenin unsurlarını teşkil etmektedir[53].

üzerine yoğunlaşan tartışma verinin bir şeyin temsili mi yoksa ayrıca bizatihi kendisinin de mi olabileceği noktasında düğümlenmekte olup Avrupa'da GVKT öncesi dönemde farklı yönde kararlar bulunmaktadır (Lee A Bygrave, "The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law", **Law, Innovation and Technology**, Cilt: 1, Sayı: 2, 2010)

[51] GDPR bakımından: Lee A. Bygrave ve Luca Tosoni, "Processing", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve diğ., New York: Oxford University Press, 2020, s. 119

[52] Arye Schreiber, "Mere Access to Personal Data: Is It Processing?", **International Data Privacy Law**, 2020, Cilt 10, Sayı: 3, s. 4

[53] GDPR kapsamında otomatik olmayan yollarla işlemenin veri kayıt sisteminin parçası olmak kaydıyla işleme sayılması şartı işlemenin tanımında yer almamaktadır, bu şarta 2. madde kapsamında mevzuatın maddi kapsamına ilişkin maddede yer verilmiştir (GPDR md. 2/1), (Bygrave ve Tosoni(2020b), **loc.cit**.) KVKK'da ise bu şart doğrudan işlemeye ilişkin tanım kapsamında düzenlenmiştir (KVKK 3/1-e).

Kişisel verinin otomatik ya da otomatik olmayan yollarla işlenmesi iki farklı değerlendirmeyi ortaya koymaktadır. Bu iki yöntem arasındaki temel fark insan unsurunun süreçte aldığı role bağlıdır[54]. Otomatik işleme süreci, insan unsurunun olmadığı faaliyetin kendiliğinden işlediği süreci ifade etmektedir[55]. İşleme sürecinin hiçbir makine veya araç kullanılmadan insan marifetiyle yürütülmesi halinde artık otomatik olmayan bir veri işleme faaliyetinden bahsetmek gerekir[56]. Otomatik olmayan yolla yapılan eylemin veri işleme kapsamında sayılabilmesi için kişisel verinin ayrıca veri kayıt sisteminin parçası olması gerekmektedir. Veri kayıt sistemi, "*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini*" ifade etmektedir (KVKK md. 3/1-h). Bu kapsamda veri kayıt sistemi her ne kadar dijitalize bir yapıyı çağrıştırsa da fiziki bir yapıda da olabilir[57]. Kurul'un bir önceki bölümde andığımız bir kararında doku ve kan örneklerinin ad ve tüp adedine göre sınıflandırılması dolayısıyla faaliyetin kişisel veri işleme niteliğinde olduğunu kabul etmiştir[58]. Burada yapılan sınıflandırma, kişisel veri işlemeye ilişkin maddede yer verilen örnek işleme hallerinden birini teşkil ederken aynı zamanda "*belirli kriterlere göre"* bir tasnifin yapıldığını gösterir. Öte yandan Kurul, üzerinde kişisel veri içeren dilekçeleri KVKK kapsamında kişisel veri işleme faaliyeti kapsamında değerlendirmemiştir[59].

Veri işleme faaliyetinin otomatik olsun yahut olmasın veri üzerinde gerçekleşmesi gerekmektedir. KVKK bu noktada yapılan işlemin "işleme" addedilebilmesi için kişisel veri üzerinde gerçekleştirilmesini aramıştır. Kişisel verilerin sınıflandırılması, depolanması, elde edilmesi gibi hususların kişisel veri üzerinde gerçekleştirildiğine şüphe bulunmamaktadır; ancak işleme açısından değerlendirilen fiilin kişisel veri üzerinde tam olarak gerçekleşmediği durumlar da mevcut olabilir. Örneğin KVKK'daki kişisel veri

---

[54] Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku,** İstanbul: Hukuk Akademisi, 2020, s. 183,
[55] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,** Ankara: KVKK Yayınları, 2019, No: 1, s. 55
[56] Paul Voigt ve Axel von dem Bussche, **The EU General Data Protection Regulation**, Cham: Springer, 2017, s. 10.
[57] Dülger (2019), **op.cit**. s. 184. Burçak Ünsal ve Kaan Özdemir, "Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Veri Kayıt Sistemi", **İstanbul Barosu Dergisi**, Cilt: 93 Sayı: 3, 2019, s. 254
[58] Kişisel Verileri Koruma Kurulu 30.10.2019 tarihli 2019/316 sayılı karar. (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 26.10.2022)
[59] Kişisel Verileri Koruma Kurulu 2019/47 sayılı karar (https://www.kvkk.gov.tr/Icerik/5462/2019/47 E.T. 26.10.2022)

tanımında da sayılan kişisel verinin kullanılmasının engellenmesinin her zaman kişisel veri üzerinde gerçekleştiği söylenemez. Nitekim kişisel verinin kullanılmasının engellenmesi, doğrudan kişisel verinin üzerinde gerçekleşmesi zorunlu bir durum değildir. Kişisel verilerin üzerinde gerçekleşmeyen erişimi engelleyici herhangi bir önlem alınması da kişisel verinin kullanımı engelleyecektir. Bu noktada "üzerinde" ifadesinin geniş bir şekilde yorumlanması gerekmektedir[60].

Son olarak KVKK'da veri işleme faaliyeti kapsamında değerlendirilebilecek hususların her türlü işlem olabileceği düzenlenmiştir. KVKK'da on iki farklı fiilin işleme niteliğinde olduğunun ifade edilmesi sonrasında "gibi" ifadesi kullanılmıştır. Dolayısıyla işleme niteliğindeki işlemler sınırlı sayıda değildir[61]. Nitekim GDPR kapsamında da "herhangi bir işlem" şeklinde düzenlenmiş olup düzenlemenin bu şekilde olması öğretide mevzuatın herhangi bir şekilde dolanılmasının önlenmesi ve uygulanabilirliğinin sağlanmasının amaçlandığı şeklinde değerlendirilmiştir[62]. Aynı yorum pekâlâ KVKK için de geçerlidir. Nitekim KVKK'nın gerekçesinde kişisel verilerin elde edilmesinden itibaren kişisel veri üzerinde gerçekleştirilen her işlem tipinin bu kapsamda olduğu belirtilerek kapsamının genişliği tesis edilmiştir[63]. Bu kapsamda; bir tıp merkezinin kendi internet sitesinde kişiye ait görüntülerin reklam amaçlı yayınlanan tanıtım videosunda yer alması[64], ticaret sicil müdürlüklerince şirket hissedarları ve gerçek kişi tacirlerin bilgileri üzerinde çeşitli işlemlerin gerçekleştirilmesi[65], bir eğitim kurumu tarafından öğrencilerin değerlendirme yeteneklerini ölçen bir test yapılıp değerlendirme sonuçlarının ortaya çıkarılması[66] Kurul tarafından kişisel veri işleme faaliyeti olarak kabul edilmiş durumlara örnek olarak gösterilebilir.

---

[60] Bu hususu Schreiber GDPR'da yer alan "restriction" kavramı dolayısıyla ifade etmiştir. "Kullanımın engellenmesi" Direktif'de yer alan "blocking" ve GDPR'da mevcut olan "restriction" kavramının KVKK'daki ifadesidir. Schreiber, kısıtlama diye çevirebileceğimiz "restriction" eyleminin her zaman doğrudan doğruya kişisel veri üzerinde gerçekleşmediğini ifade eder, örneğin sistemde yer alan bir kişisel verinin üzerinde doğrudan herhangi bir fiilde bulunmadan kullanıma ilişkin yetkilerin alınması halinde kullanım engellenmiş olacaktır. **Bkz**: Schreiber, **op.cit.** s. 4

[61] Çekin, **op.cit**. s. 49, Erarslan Türkmen, **op.cit.** s. 88

[62] Bygrave ve Tosoni (2020b), **op.cit.,** s. 117

[63] Kişisel Verileri Koruma Kurumu (2019b), **loc.cit.**

[64] Kişisel Verileri Koruma Kurulu 2020/379 sayılı karar (https://www.kvkk.gov.tr/Icerik/6911/2020-379 E.T. 26.10.2022)

[65] Kişisel Verileri Koruma Kurulu 2020/307 sayılı karar (https://www.kvkk.gov.tr/Icerik/6895/2020-307 E.T. 26.10.2022)

[66] Kişisel Verileri Koruma Kurulu 2020/255 sayılı karar(https://www.kvkk.gov.tr/Icerik/6894/2020-255 E.T. 26.10.2022)

C. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu ve veri işleyen kavramları kişisel verilerin korunması hukukunun temel iki öznesini oluşturmaktadır. Bu iki kavramın sınırlarının çizilmesi ve birbirlerinden ayrıştırılması, gerek kişisel verilere ilişkin yükümlülüklerin yerine getirilmesi bakımından temel sorumlunun kim olduğunun tespiti gerekse de KVKK kapsamındaki sorumlulukları dolayısıyla idari para cezasına muhatap olan kişilerin belirlenmesi bakımından büyük önem arz etmektedir[67]. Dolayısıyla veri sorumlusu ve veri işleyen kavramlarının netleştirilmesi ve aralarındaki farkın ortaya konması çalışmamızın devamı bakımından elzemdir.

1. Veri Sorumlusu

Veri sorumlusu KVKK'da: "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* şeklinde tanımlanmıştır (KVKK 3/1-I). Tanımdan anlaşılacağı üzere veri sorumlusu, işleme amaçlarını ve vasıtalarını belirlemesi, veri kayıt sisteminin kurması ile yönetmesi ve son olarak gerçek veya tüzel kişi olması ile üç temel özelliğe sahiptir[68].

Veri sorumlusu öncelikle işleme faaliyeti kapsamındaki amaç ve vasıtaları belirlemektedir. Amaç ve vasıtaların belirlenmesi işlenen kişisel verinin neden ve nasıl işlendiğinin belirlenmesini ifade etmektedir[69]. Dolayısıyla veri sorumlusu kişisel verilerin

---

[67] Kişisel Verilerin Korunması Kanunu 18. maddesinin 2. fıkrası şöyledir: "*Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır*". Kişisel Verilerin Korunması Kanunu'ndan farklı olarak Avrupa Genel Veri Koruma Tüzüğü kapsamında veri işleyen de idari para cezalarına muhatap olabilmektedir. European Data Protection Board, **Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR**, Version 2.1, 2021, s. 25 (https://edpb.europa.eu/system/files/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf E.T. 26.10.2022)

[68] Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul: On iki Levha Yayıncılık, 2018, s. 112, GDPR bakımından yapılan bir tasnif için ayrıca bakınız: Yusuf Manzur Özer, **Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler ve Hukuki Engeller**, İstanbul: On İki Levha Yayıncılık, 2020, s. 46

[69] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s. 2 (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022). Cüneyt Pekmez, "Overview of the Definitions of Data controller and Data Processor within the Scope of the Turkish Code of Personal Data Protection (TCDP)", **Annales de la Faculté de Droit d'Istanbul,** Cilt: 0 Sayı:67, 2018, ss. 61-62.

işlenmesine ilişkin süreçteki temel hususları takdir etmekte ve asıl karar alıcı konumunda bulunmaktadır[70]. Bu noktada işlenen kişisel verilere erişiminin olup olmaması bir önem taşımamaktadır[71]. Çünkü veri sorumlusunun tespitinde merkezi unsur, veri sorumlusunun işlenen kişisel veriye erişimi ya da doğrudan faaliyeti gerçekleştirmesi değil, kişisel verinin neden ve nasıl işleneceğine ilişkin karar sürecindeki belirleyiciliğidir[72].

Kişisel veri işlemeye ilişkin amaç ve vasıtaları belirleyen kişinin yani veri sorumlusunun tespitinde olgusal bir değerlendirme yapılması gerekmektedir[73]. Bu şekilde yapılacak değerlendirmede veri sorumlusu kavramının özerk bir kavram olduğu dikkate alınmalıdır[74]. Bu noktada veri sorumlusunu temel olarak kişisel verinin işleme amacını yani bu kişisel verinin ne şekilde bir sonuç elde etmek için işlenmekte olduğu sorusunun cevabını belirlemektedir[75]. Amacın belirlenmesi daha farklı bir ifadeyle işleme faaliyetinin maksadı ve aynı zamanda gerekçesini ifade etmektedir[76]. Bir şirketin müşterilerine pazarlama maksatlı kısa mesaj göndermesi, bankanın ödenmeyen kredi borcuna ilişkin olarak yasal takip işlemlerinin gerçekleştirilmesi için kredi müşterisinin kişisel verilerini hizmet aldığı avukata aktarması amaç belirlenimine ilişkin olarak örnek verilebilecektir.

Abdulhamid Zor, **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020, s.68

[70] Elif Küzeci, "6698 Sayılı Kişisel Verilerin Korunması. Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", **İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi,** Cilt 16, Sayı 63, 2019, s. 964

[71] European Data Protection Board (2021), **op.cit**. ss. 3, 17.

[72] ABAD, Facebook üzerinde mevcut bir hayran sayfası yöneticisinin hayran sayfasına ilişkin ziyaretçi istatistiklerinin çıkarılması için çerez kullanımı bakımından, sayfa yöneticisinin yalnızca anonim bir şekilde istatistiklerini görebildiği kişilere ilişkin çerezler vasıtasıyla kişisel veri işlenmesinde amaç ve araçların belirlenmesi sürecinde yer aldığı kabulü dolayısıyla işleme faaliyeti bakımından veri sorumlusu olduğuna hükmetmiştir. CJEU - C-210/16 - Wirtschaftsakademie (Facebook Fan page), para 39 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5127976 E.T. 27.10.2022), Özer, **op.cit**. s. 47

[73] Article 29 Data Protection Working Party, **Opinion 1/2010 on the Concepts of "Controller" and "Processor**, 00264/10/EN WP169, 2010, s.9 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

[74] **Ibid**.

[75] Çekin **op.cit**. 54

[76] Lee A. Bygrave ve Luca Tosoni, "Controller", **The Eu General Data Protection Regulation (GDPR), A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020, s. 150

Vasıta kavramının kapsamını neyin oluşturduğu ise KVKK bakımından açık bir husus değildir. Avrupa Çalışma Grubu da aynı şekilde Direktif'te yer alan "araç"[77] kavramının ne şekilde anlaşılacağı sorusunu gündeme getirmiş ve Avrupa Veri Koruma Direktifi'nin tasarı metninde ifade edilen bir işleme faaliyeti bakımından veri sorumlusunun belirleyici olması gereken 4 faktörün (hangi kişisel verinin işlenmesi gerektiği, işlemenin amacı, işleme süreci, işlenen veriler bakımından kimlerin erişim sahibi olacağı) kabul edilen metinde amaç ve araçlar olarak formüle edildiğini, bu durumun kabul edilen metinde doğrudan ifade edilmeyen şartlar bakımından dışlayıcı olmadığını ifade etmiştir[78]. Bu kapsamda araç kavramı işleme faaliyetinin nasıl olacağına ilişkin olup, hangi kişisel verinin işleneceği, kişisel veriye kimin erişebileceği, ne kadar süreyle kişisel verinin saklanacağı gibi çeşitli hususları kapsamaktadır[79]. Aynı durum KVKK bakımından da geçerlidir. Kurul bir kararında teknik ve organizasyonel araçların tespiti, hangi verilerin işleneceği, verilerin saklama süresi, verileri saklama yöntemi, verilere erişim yetkisi olan kişilerin belirlenmesi gibi temel hususların veri sorumlusunca belirleneceğini değerlendirerek işlemeye ilişkin veri sorumlusunca belirlenecek vasıtaları Çalışma Grubu'na benzer şekilde örneklendirmiştir.[80].

KVKK'da yer alan tanımda veri sorumlusunun veri kayıt sisteminin kurulması ve yönetiminden sorumlu kişi olduğu düzenlenmiştir. Veri sorumlusuna ilişkin olarak bu şekilde bir şartın getirilmesi, Direktif ve GDPR'da bulunmayıp KVKK'ya özgü bir durumdur. Bu şartın KVKK kapsamında veri sorumlusu bakımından öngörülmesi çeşitli soru işaretlerini ve problemleri gündeme getirdiği gibi bu unsurun ne şekilde anlaşılması gerektiği de belirsizlikler içermektedir[81]. Öğretide bir görüş bu şartın özellikle kişisel verilerin otomatik olmayan yollarla işlendiği hallerde değerlendirme konusu olacağını

---

[77] Direktif'te vasıta kavramının muadili olarak "means" kavramı ile ifade kullanılmıştır. Kişisel Verileri Koruma Kurulu da bir kararında vasıta yerine ayrıca "araç" kavramını da kullanmıştır. Bkz: Kişisel Verileri Koruma Kurulu'nun 09.02.2021 tarihli ve 2021/111 sayılı kararı (www.kvkk.gov.tr E.T. 26.10.2022)

[78] Article 29 Data Protection Working Party (2010), **op.cit**. s. 14

[79] **Ibid**.

[80] Kişisel Verileri Koruma Kurulu 30.01.2020 tarihli ve 2020/71 sayılı kararı (https://www.kvkk.gov.tr E.T. 26.10.2022)

[81] Nitekim Kurul kararları incelendiğinde Kurul'un veri sorumlusunu tayin ederken bu unsuru dikkate almadığı ve nasıl anlaşılması gerektiği üzerinde durmadığı dikkat çekicidir. Aynı şekilde Kişisel Verileri Koruma Kurumu tarafından yayımlanan veri sorumlusunu açıklayan ilgili rehberde bu şart sadece anılmış olup veri sorumlusuna ilişkin değerlendirme amaç ve vasıtaları belirleme şartı üzerinden yapılmıştır. Bkz: Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen, op.cit.** ss. 1,2

ifade etmiştir[82]. Diğer bir görüş ise veri sorumlusunun tespitine ilişkin bu şartın işleme faaliyetine ilişkin kişisel verilerin nasıl toplandığı ve kaydedildiğine ilişkin vasıtaları ifade eden bir faktör olduğunu, veri sorumlusuna ilişkin ayrıca bir şart getirmeyip amaç ve araçların belirlenmesine ilişkin şartı açıklayıcı nitelikte olduğunu ifade etmiştir[83].

Veri sorumlusunun veri kayıt sisteminin kurulması ve yönetiminden sorumlu olması şartının açıklayıcı bir nitelikte yahut otomatik olmayan yollarla işlemeye ilişkin bir şart olmadığı kanaatindeyiz. Veri kayıt sistemini kuran ve yöneten kişi ile kişisel verinin amaç ve vasıtalarını belirleyen kişi çeşitli durumlarda farklılaşabilecektir. Örneğin veri merkezi hizmeti alan bir şirket bakımından kişisel veriler üzerindeki nihai kontrol, hizmet alan şirkette iken pekala veri kayıt sistemi olarak addedilebilecek veri merkezinin kurulması ve yönetimi hizmet veren kişide olabilecektir. Bu gibi durumlarda veri sorumlusunun kim olduğu sorusu ile karşı karşıya kalınacaktır. Öte yandan kişisel verilere ilişkin kavramlar genel olarak kişisel veri ve veri işleme kavramları üzerine inşa edilmektedir. Veri kayıt sisteminin kurulması ve yönetiminin ayrıca bir şart olarak ele alınması ise veri sorumlusu kavramının genel sistematik dışında farklı bir temel üzerinden inşa edilmesi anlamına gelecektir[84]. Son olarak kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu kavramları mevzuatlarda geniş şekilde tanımlandığı gibi aynı zamanda veri koruma otoriteleri

---

[82] Küzeci (2019b) **op.cit**. s. 966

[83] Pekmez **op.cit.** ss. 62-63

[84] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nde kişisel veri kavramı haricinde ayrıca işleme konusu olan tüm verileri ifade eden bir kavram olarak "otomatik veri dosyası" (automated data file) düzenlenmiş ve dosya yöneticisi (KVKK bakımından veri sorumlusunu ifade etmekte olup İngilizce'de "controller of the file" ifadesinden gelmektedir. Daha sonra Veri Koruma Direktifi'nde yalnızca "controller" olarak ifade edilmiş olup Türkçe'ye bu sefer ise veri sorumlusu olarak aktarılmıştır) kişisel veri ile birlikte otomatik veri dosyası kavramı üzerinden tanımlanmıştır. Veri kayıt sistemi ile otomatik veri dosyası ifadeleri birbirinden farklı olmakla birlikte benzerlik gösterirler. Nitekim Bygrave Direktif bakımından dosya kavramının tamamen terkedilmediğini "veri kayıt sistemi" kavramı dahilinde otomatik olmayan yollarla işlenen kişisel veriler bakımından varlığını sürdürdüğünü ifade ederek bu iki kavram arasında ilişki kurmuştur (Bygrave (2014), **op.cit.** s.141). Aynı şekilde Kişisel Verilerin Korunması Kanunu tasarısında da veri kayıt sistemi yerine kullanılan "veri kütüğü" kavramı ve veri sorumlusu yerine kullanılan ve "veri kütüğü" ifadesinden türeyen "veri kütüğü sahibi" kavramları düşüncemizi destekler niteliktedir Kanun koyucunun bu noktada nihai metinde veri sorumlusunu veri kayıt sistemi üzerinden tanımlamakla Sözleşme'ye paralel bir tanım yapma arzusunda olduğu söylenebilecektir (Bkz: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No.108), Kişisel Verilerin Korunması Kanunu Tasarısı 3/1-h,ı, B.02.0.KKG.*010/101-902/1812, 22.04.2008)
(https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=64271 E.T. 22.11.2022)

tarafından geniş bir şekilde yorumlanmaktadır[85]. Veri kayıt sistemine ilişkin getirilen bu ek şart, dar bir şekilde yoruma sebebiyet vermesi ihtimali dolayısıyla kişisel verilerin korunması hukukunun amaçlarına aykırı sonuçlar doğurabilme riskini bünyesinde barındırmaktadır[86].

Son olarak, veri sorumlusunun bir kişi olması gerekmektedir. Burada kanun koyucu ilgili kişilerden farklı olarak tüzel kişi ve gerçek kişi arasında herhangi bir ayrım yapmamış ve hem tüzel kişinin hem de gerçek kişinin veri sorumlusu olabileceğini kabul etmiştir[87]. Ayrıca kanun koyucu bir belirleme yapmayarak kamu tüzel kişilerini de tanımın kapsamı dahilinde tutmuştur. Öğretide KVKK açısından tüzel kişiliği olmayan ve merkez teşkilatına bağlı olan tüm kurum ve kuruluşlar bakımından yalnızca devlet tüzel kişiliğinin veri sorumlusu olarak değerlendirilmesi söz konusu olacağı ve bu durum kişisel verilerin korunması hukukunun sağladığı şeffaflık gibi unsurlara gölge düşüreceği görüşü öne sürülmüştür[88]. Öte yandan Kurul'un ise kamu tüzel kişiliği olmayan kişiler bakımından da veri sorumlusu değerlendirmesinde bulunduğu kararları mevcuttur. Nitekim Kurul bir kararında bakanlığın veri sorumlusu olduğu değerlendirmesinde bulunmuştur[89]. Aynı şekilde başka bir kararda ise "*veri sorumlusu bir valilik*" ifadelerine yer verilmiştir[90]. Kişiliğin veri sorumlusu olmak bakımından bir şart olmasının kamu tüzel kişilikleri bakımından olumsuz sonuçları olacağına ilişkin görüşe katılmakla birlikte KVKK'daki tanıma aykırı şekilde kamu tüzel kişiliği bulunmayan kurum ve kuruluşların veri

---

[85] Veri Sorumlusu kavramının geniş şekilde düzenlenerek etkili bir korumanın sağlandığı hususu farklı zamanlarda ABAD kararlarında vurgulanmıştır, Bkz: Fashion ID GmbH & Co. KG ECLI:EU:C:2019:629 para. 70, Google Spain SL, Google Inc. ECLI:EU:C:2014:317 para. 34, Nitekim, doktrinde de ABAD kararları bakımından veri sorumlusu kavramının bu şekilde teleolojik bir biçimde yorumlanarak kişisel verilere daha kapsamlı bir koruma getirilmeye çalışıldığı ifade edilmiştir (https://curia.europa.eu/juris/liste.jsf?num=C-40/17 E.T. 26.10.2022). Bkz: Maria Berger ve David Eisendle, "Web 2.0 and the Concept of 'Data Controller': Recent Developments in EU Data Protection Law" **Indian Journal of Technology and Law,** Cilt: 15 Sayı: 1, 2019**,** s. 33

[86] Veri sorumlusunun amaç ve vasıta ölçütleri üzerinden değerlendirilmesinin isabetli olacağına ilişkin doktrinde başka bir görüş için bkz: Çekin **op.cit.** s. 54. Veri kayıt sistemi bakımından karar verici konumda olmasını değerlendiren bir görüş için ayrıca bkz: Aşıkoğlu, **op.cit**. s. 113

[87] Dülger (2019), **op.cit**. s. 188

[88] Çekin **op.cit**. s. 62

[89] Kişisel Verileri Koruma Kurulu'nun 13.02.2020 tarihli ve 2020/120 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6923/2020-120 E.T. 25.02.2023)
. Merkez ve taşra teşkilatının ayrı bir kamu tüzel kişiliği olmayıp devlet tüzel kişiliği içinde kabul edildiğine ilişkin olarak Bkz: Ramazan Çağlayan, "Hukukumuzda Kamu Tüzel Kişiliği Kavramı ve Kıstasları", **Uyuşmazlık Mahkemesi Dergisi**, Cilt: 0 Sayı: 7, 2016, s. 379

[90] Kişisel Verileri Koruma Kurulu'nun 19.03.2020 tarihli ve 2020/226 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6893/2020-226 E.T. 25.02.2023)

sorumlusu olduğuna ilişkin değerlendirmelerin kabul edilmesi mümkün değildir. Bu kapsamda veri sorumlusunun bir kişi olması gerekliliği KVKK'da açıkça düzenlendiği için ancak tüzel kişiliği bulunan kamu kurum ve kuruluşları veri sorumlusu olabilecektir[91].

2. Veri İşleyen

Veri işleyen, veri sorumlusu ile birlikte KVKK kapsamında veri işleme sürecinde yer alan ikinci öznedir. Veri işleyen KVKK'da "*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*" olarak tanımlanmıştır (KVKK 3/1-ğ). Tanımdan da anlaşılacağı üzere veri işleyen kavramı öncelikle bir veri sorumlusunun varlığını gerektirmektedir[92]. Bu kapsamda veri işleyen, ancak veri sorumlusunun tespiti sonrasında saptanabilecektir.

Veri işleyenin temel nitelikleri iki noktada toplanmaktadır: Bunlar; veri sorumlusundan ayrı onun organizasyonel kapsamından bağımsız bir varlığının olması ve veri sorumlusunun adına faaliyet göstermesidir[93]. Veri sorumlusu adına faaliyet göstermesinin bir sonucu olarak veri işleyen, veri sorumlusunun talimatları doğrultusunda hareket etmektedir[94]. Veri işleyenin organizasyonel açıdan veri sorumlusundan bağımsız olmasının sonucu ise veri sorumlusunun çalışanlarının organizasyonun bir parçası olmaları bakımından veri işleyen olarak değerlendirilmeyecek olmalarıdır[95].

Veri sorumlusu işlemeye ilişkin veri işleyene bazı hususları belirleme yetkisi tanıyabilmektedir[96]. Bu yetkinin kapsamını işlemenin amacı değil vasıtaları

---

[91] Karşı yönde: Çağla Tansuğ, **İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması**, İstanbul: On İki Levha Yayıncılık, 2023, ss. 35, 36

[92] Özer, **op.cit**. s. 48

[93] European Data Protection Board (2021), **op.cit**. s. 25

[94] Dülger (2019), **op.cit** s. 208, Mustafa Baysal, **KVKK Kişisel Verilerin Korunması Kanunu El Kitabı**, Ankara: Seçkin Yayıncılık, 2021, s. 52

[95] **Ibid**, European Data Protection Board (2021), **op.cit**. s. 26, Aşıkoğlu **op.cit.** ss. 113,114. Öğretide aksi yönde değerlendirmeler bulunmaktaysa da ne KVKK bakımından ne de GDPR bakımından çalışanlar veri işleyen olarak değerlendirilmemektedir Çalışanın veri işleyen olduğunu ileri süren görüşler için bkz: Tekin Memiş, "Veri Sorumlusu ile Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", **Beykent Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 3 Sayı: 6, Aralık 2017, ss. 15-16, Ahmet Sevimli, "Kişisel Verilerin Korunması Kanunu'ndaki Temel Kavramların İşçi-İşveren İlişkisindeki Karşılıkları", **İnşaat Sanayii Dergisi,** 2018, s. 76

[96] Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen, op.cit.** s. 3

oluşturmaktadır[97]. Buna karşın yetki tanınacak hususlar işlemeye ilişkin temel vasıtalar olmamalıdır. Veri işleyenin karar verebileceği hususlar kişisel verinin hangi müddet boyunca saklanacağı gibi temel sorulardan ziyade kişisel verilerin saklanacağı ortamın güvenliği bakımından alınacak teknik tedbirlerden hangilerinin seçileceği gibi ikincil hususlar olmalıdır[98]. Nihai olarak veri işleyen, veri sorumlusunun talimatları doğrultusunda onun adına hareket etmekte ve ancak sınırlı bir alanda karar verme yetkisine sahip olabilmektedir.

II. İlkeler

KVKK'nın 4. maddesinde kişisel verilerin işlenmesine ilişkin temel ilkeler öngörülmüş ve işleme faaliyetinde bu ilkelere uyulmasının zorunlu olduğu ifade edilmiştir (KVKK 4/2). Bu noktada ilgili ilkelerin kaynağı 108 Sayılı Sözleşme ve Avrupa Veri Koruma Direktifi'dir[99]. Daha sonraki süreçte ise GDPR'da ilgili ilkeler korunmuş, aynı ilkeler yalnızca küçük farklarla benimsenmiştir[100]. KVKK bakımından da aynı durum söz konusu olup 108 Sayılı Sözleşme'de yer alan ilkeler ufak değişiklikler sonucu kabul edilmiştir.

Veri sorumluları kişisel veri işleme faaliyetlerinde KVKK'ya uygun davranmakla birlikte ayrıca ilkelere uygun faaliyette bulunulmasını da gözetmelidir[101]. İlkelere uygun olmayan bir biçimde kişisel veri işlenmesi de bizatihi hukuka aykırılığı gündeme getirmektedir. Diğer bir ifadeyle ilkelerin normatif gücü bulunduğu gibi aynı zamanda ilkeler hukuka uygunluğun tespitinde yorum bakımından dikkate alınacaktır[102]. Bu noktada KVKK'da zikredilen ve veri sorumlularınca işleme faaliyetlerinde uyulması gereken ilkeler; "hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için işlenme", "işlendikleri amaçla

---

[97] Article 29 Data Protection Working Party (2010), **op.cit**. s. 14
[98] **Ibid**.
[99] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler,** s.1. (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022)
[100] Cécile de Teerwangne, "Article 5. Principles Relating to Processing of Personal Data", **GDPR: A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press. 2020, s. 311.
[101] Dülger (2019), **op.cit.** s. 261
[102] Bygrave (2014), **op.cit.** s. 145

bağlantılı, sınırlı ve ölçülü olma" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkeleridir (KVKK 4/2).

A. Hukuka ve Dürüstlük Kurallarına Uygun Olma

Hukuka ve dürüstlük kurallarına uygun olma ilkesi kişisel verilerin işlenmesi bakımından temel ilke olmasının yanı sıra diğer ilkeler bakımından da bir çatı ilke işlevi görmektedir[103]. Öğretide bu ilkenin hukuk devletinin bir sonucu olduğu değerlendirilmiştir[104]. 108 Sayılı Sözleşme'de aynı ilke kişisel verilerin işlenmesine ilişkin olarak "*adil biçimde ve yasal yoldan elde edilir ve işlenir*" şeklinde ifade edilmiştir (108 Sayılı Sözleşme 5/1-a).

Hukuka ve dürüstlük kurallarına uygun işleme ilkesi kişisel verilerin hukuka uygun işlenmesi ve kişisel verilerin dürüstlük kurallarına uygun işlenmesi şeklinde iki öncüle sahiptir. Kişisel verilerin hukuka uygun şekilde işlenmesi öğretide bir görüşe göre KVKK'nın 4., 5. ve 6. maddelerine uygun şekilde veri işlemeyi ifade etmektedir[105]. Katıldığımız görüş ise hukuka uygunluk ifadesini geniş bir biçimde yorumlamaktadır. Buna göre hukuka uygunluk ifadesi yalnızca KVKK'ya ilişkin özel normlarını değil genel bir şekilde hukuk düzenlemelerini işaret etmektedir[106]. Öğretide ayrıca hukuka uygunluk ifadesinin evrensel hukuk kaidelerini de kapsadığı ifade edilmiştir[107]. Nitekim Kişisel Verileri Koruma Kurumu da yalnızca özel normlara değil genel normlara da uygunluk dahil olmak üzere hukuka uygunluğu geniş kapsamlı bir şekilde değerlendirmektedir[108]. Dolayısıyla KVKK dışındaki diğer hukuk normlarına aykırılık halinde de hukuka ve dürüstlük kurallarına uygun olma ilkesinin ihlal edilmesi söz konusu olabilecektir.

---

[103] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit**. s.2
[104] Çekin **op.cit**. s. 69.
[105] Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", **Kişisel Verileri Koruma Dergisi,** Cilt: 1 Sayı: 1, 2019**,** s. 49.
[106] E. Eylem Aksoy Retornaz ve Osman Gazi Güçlütürk, "Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilere İlişkin Temel İlkelerle İlişkisi", **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Editörler: E. Eylem Aksoy Retornaz ve Osman Gazi Güçlütürk, İstanbul: On İki Levha Yayıncılık, 2021, s. 287, Taştan **op.cit**. s. 49
[107] Dülger (2019), **op.cit**. s. 263.
[108] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit.** s.2

Dürüstlük kurallarına uygun işleme ise ilkede mevcut olan ikinci öncüldür. **Çekin** dürüstlük kuralına uygunluğun Türk Medeni Kanunu'nda yer alan dürüstlük kuralı ile tam olarak aynı anlama gelmediğini, ilkenin aynı zamanda ilgili kişilere karşı "*adil olma*" prensibi gereğince veri sorumlusu ile ilgili kişinin menfaatlerinin bir dengede tutulması doğrultusunda ele alınması gerektiğini görüşündedir[109]. Bu görüş adil olma ve menfaat kavramlarını gündeme getirmesiyle Avrupa Veri Koruma Direktifi ile paralel niteliktedir. Nitekim Direktif kapsamında ilgili ilke doğrudan işlemenin adil olmasına vurgu yapmaktadır (DPD md. 6/1-a). Adillik (fairness) ifadesi ilgili kişiye karşı yanıltıcı olmamak, ilgili kişinin meşru beklentilerine saygılı olmak ve diğer hukuki yükümlülükleri yerine getirmek anlamına gelmektedir[110]. Diğer bir ifadeyle adillik, verisi işlenen kimseye karşı adil olmak, zarar verici, beklenmedik ve aldatıcı olmaktan kaçınmaktır[111].

Adil olma, yanıltıcı olmama gerekliliğini taşıması doğrultusunda ilgili kişiye karşı sürece ilişkin doğru bilgilendirmeyi de gerektirmektedir[112]. Dolayısıyla da adil olma zorunlu olarak şeffaf olma prensibini içerisinde barındırmaktadır. Direktif'te şeffaflık ilkesine açıkça yer verilmemiş, şeffaflık ilkesi adillik ilkesi içerisinde değerlendirilmiştir; ancak daha sonra şeffaflık prensibi GDPR'da bir ilke olarak ayrıca zikredilmiştir[113]. KVKK'da da şeffaflık prensibi açıkça zikredilmemiş olsa dahi ilke Kurum tarafından kabul edilmektedir[114]. Kurul da bir kararında ilgili kişiye şeffaf davranmayan veri sorumlusunun dürüstlük kuralına aykırı davrandığına karar vermiştir[115].

Dürüstlük kuralına uygunluk bakımından öğretideki diğer bir değerlendirme ise Türk Medeni Kanunu'nun ikinci maddesi doğrultusunda bir yorum getirmektedir. Bu

---

[109] Çekin **op.cit**. s. 70

[110] Estelle Dehon ve Pater Carey, "Fair, Lawful and Transparent Processing", **Data Protection: A Practical Guide to UK and EU Law**, Editör: Peter Carey, Oxford: Oxford University Press, 2018, s. 42

[111] An Coimisiún um Chosaint Sonraí (Data Protection Comission), **Quick Guide to the Principles of Data Protection,** 2019, s. 2. (https://www.dataprotection.ie/en/dpc-guidance E.T. 20.11.2022)

[112] Council of Europe ve diğ., **Handbook on European Data Protection Law**,, Luxembourg: Publication Office of the European Union, 2018, s. 181

[113] Teerwangne, **op.cit.** s. 314

[114] Bkz: Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, loc.cit.**

[115] "*Öte yandan veri sorumlusunun kimlik görüntüsünün muhafaza edilmesine rağmen kayıt altına alınmadığı yönünde ilgili kişiye cevap vermesinden dolayı şeffaf olmadığı, bu nedenlerle de dürüstlük kuralına aykırı veri işleme faaliyetinde bulunduğu*", (Kişisel Verileri Koruma Kurulu'nun 01.10.2019 tarihli ve 2019/294 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6556/2019-294 E.T. 25.02.2023)). Şeffaflık ilkesinin zikredildiği bir diğer karar için bkz: Kişisel Verileri Koruma Kurulu'nun 03/02/2021 tarihli ve 2021/85 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7112/2021-85 E.T. 25.02.2023)

noktada dürüstlük kuralının ne şekilde anlaşılması gerektiği bakımından önem arz eden husus ise kişiden objektif bir şekilde beklenebilecek davranışlar olacaktır[116]. Nitekim Kurum'un bu yönde de değerlendirmeleri mevcut olup Kurum, dürüstlük kuralını kişinin makul bir kişiden beklenebilecek şekilde davranması doğrultusunda ifade etmiştir[117]. Ayrıca bu ilke kapsamında hakkın kötüye kullanılması yasağı da uygulama alanı bulmaktadır[118]. Kurul bir kararında borçlunun telefon numarasının varlık yönetim şirketi tarafından işlenmesinin hukuka uygun olduğuna ancak farklı tarihlerde ilgili numaraya birden fazla SMS gönderilmesinin hakkın kötüye kullanılması niteliğinde olduğuna ve dolayısıyla hukuka ve dürüstlük kurallarına aykırı olduğuna karar vermiştir[119]. Bu noktada Kurum'un dürüstlük kuralına uygun olma ilkesini hem Türk Medeni Kanunu'nun ikinci maddesi kapsamında hem de "adil olma" ilkesini kapsayacak şekilde yorumladığı kabul edilmelidir.

B. Doğru ve Gerektiğinde Güncel Olma

KVKK'da öngörülen ikinci ilke kişisel verinin doğru ve gerektiğinde güncel olmasıdır. İlgili ilke kişisel verilerin düzeltilmesini ve silinmesini isteme hakkı ile doğrudan irtibatlıdır[120]. Kişisel verilerin doğruluğu bu noktada sağlanarak kişilerin verileri üzerinden yanlış biçimde temsilinin önüne geçilmek istenmektedir[121]. Yine aynı şekilde verinin doğru şekilde işlenmesi veri sorumlusunun veri işlemesindeki amacın gerçekleşmesini de sağlayacaktır[122].

Kişisel verinin doğru ve gerektiğinde güncel olmasının ne anlama geldiğine ilişkin genel olarak öğretide kavramın kendini açıklar nitelikte olduğu ifade edilmiştir[123]. Doğruluk ilkesine ilişkin tartışmalar temelde hangi kişisel veriler bakımından bu ilkenin

---

[116] Dülger (2019), **op.cit**. s. 265
[117] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit**. s.3
[118] **Ibid**.
[119] Kişisel Verileri Koruma Kurulu 31.05.2019 tarihli ve 2019/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5494/2019-159 E.T. 25.02.2023)
[120] Voigt ve von dem Bussche, **op.cit.** s. 92
[121] Dara Hallinan ve Frederik Zuiderveen Borgesius, "Opinions Can be Incorrect (in our opinion)! On Data Protection Law's Accuracy Principle", **International Data Privacy Law,** Cilt: 10 Sayı: 1, 2020, s.1
[122] Aşıkoğlu, **op.cit**. s. 76
[123] Bkz: Carey **op.cit.** s. 37, Dülger (2019), **op.cit**. s. 293

uygulanıp uygulanmayacağı noktasında toplanmaktadır. Bir görüş doğruluk ilkesinin olgular dışında uygulanmayacağı düşüncesindedir[124]. Nitekim Çalışma Grubu da doğruluk ilkesini açıklarken yalnızca olgulara ilişkin doğruluğun bu kapsamda olabileceğini ifade etmiştir[125]. Bu görüşün temelinde olgusal olmayan düşüncelerin yanlışlanabilir olmadığı fikri yatmaktadır. Katıldığımız diğer görüş ise fikirlerin olgu ve yorumsal bir çerçeveden oluştuğunu ve bunlar bakımından da doğruluk ilkesinin uygulanabileceğini söylemektedir[126].

Kişisel verilerin doğru ve gerektiğinde güncel olması kapsamında alınacak önlemlerin ilgili faaliyet kapsamında objektif olarak değerlendirilmesi gerekmektedir[127]. Bu noktada genel olarak ilgili kişiye ilişkin ortaya bir sonuç çıkarılmadıkça (örneğin profilleme faaliyetleri gibi) ilgili ilke veri sorumlularına aktif bir özen yükümlülüğü getirmemektedir[128]. Veri sorumlularının, ilgili kişilerin bilgilerini güncellemeleri için gerekli vasıtaları oluşturmaları, ilkenin karşılanması bakımından genel olarak yeterlidir[129]. Nitekim Kurul bu doğrultuda bir kararında ilgili kişinin başvurularına rağmen kendisine ait olmayan aboneliklere ilişkin fatura bilgilerini ilgili kişinin numarasına ileten veri sorumlusunun bilgilerin düzeltilmesi kapsamında başvuruları değerlendirmemesi ve bu noktada ilgili kişiye çıkardığı güçlükler bakımından veri sorumlusunun doğru ve gerektiğinde güncel olma ilkesine aykırı hareket ettiğine kanaat getirmiştir[130]. Ancak yukarıda ifade edildiği üzere bu değerlendirmeler somut olay özelinde objektif bir biçimde gerçekleştirilmeli ve işleme amacı bilahare dikkate alınmalıdır[131].

---

[124] Bkz: Carey **loc.cit.** Dülger (2019),**op.cit** s. 294

[125] Article 29 Data Protection Working Party, **Guıdelınes On The Implementatıon Of The Court Of Justıce Of The European Unıon Judgment On"Google Spaın And Inc V. Agencıa Española De Proteccıón De Datos (Aepd) And Marıo Costeja González" C-131/12,** 2014, s. 15 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

[126] Hallinan ve Borgesius, **op.cit**. s. 9

[127] Yücedağ, **op.cit**. s. 51

[128] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit.** s.6

[129] **Ibid**.

[130] Kişisel Verileri Koruma Kurulu, 2020/66 sayılı kararı Kişisel Verileri Koruma Kurulu 27.01.2020 tarihli ve 2020/66 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6873/2020-66 E.T. 25.02.2023)

[131] Doğruluk prensibinin somut olay kapsamında değerlendirilmesi gerekliliğine ilişkin olarak bkz.: Hallinan ve Borgesius **op.cit.** s. 10. ABAD bir kişinin sınavda verdiği cevapların işleme amacı kapsamında kişinin bilgisini ölçmek olması dolayısıyla doğru ve gerektiğinde güncel olma ilkesinin

C. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

Belirli, açık ve meşru amaçlar için işleme ilkesi KVKK'da öngörülen üçüncü ilkedir. Çalışma Grubu ilgili ilkenin önemini ilkeyi verilerin korunması bakımından "mihenk taşı" addederek ifade etmiştir[132]. İlke kapsamında kişisel verinin işlenme amacına ilişkin olarak üç farklı alt prensip getirilmiştir: Buna göre, işleme faaliyetinin amacı belirli, açık ve meşru olmalıdır.

Belirli amaçlar için işlenme, işleme faaliyeti kapsamında amacın açıkça ve spesifik bir biçimde belirlenmesini ifade eder[133]. Kurul bir kararında ilke kapsamında "…*işleme faaliyetinin ve gerçekleştirme amacının belirliliğini sağlayacak detayda*…" ortaya konulması gerektiğini ifade etmiştir[134]. Böylece veri sorumlularının herhangi bir amaç olmaksızın ne olur ne olmaz düşüncesiyle veri işlemelerinin önüne geçilmek istenmektedir[135]. Aynı şekilde "*kullanıcı deneyimini geliştirmek*" gibi geniş ve muğlak amaçlarla veri işlenmesi de ilkeye aykırılık oluşturacaktır[136].

Amacın açık olması ise ilgili kişi tarafından işleme faaliyetinin ne için gerçekleştiğinin anlaşılabilir olmasını hedeflemektedir[137]. Bu kapsamda belirlenen amacın ilgili kişinin anlayabileceği şekilde olması ve herhangi bir şüpheye mahal bırakmaması önem arz etmektedir[138]. Bu nedenle amacın açık olması ile şeffaflık ilkesi

---

uygulanamayacağına karar vermiştir. bkz: Peter Nowak v. Data Protection Comissioner, 2017, ECLI:EU:C:2017:994, para 50-53.
(https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0434 E.T. 25.02.2023)

[132] Article 29 Working Party, **Opinion 03/2013 on Purpose Limitation**, Adopted on 2 April 2013, s. 4 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

[133] **Ibid**. s. 15.

[134] Kişisel Verileri Koruma Kurulu 12.03.2020 tarihli ve 2020/212 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/6892/2020-212 E.T. 25.02.2023)

[135] Evelien Brouwer, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", **The Eclipse of the Legality Principle in the European Union**, Edited by: Leonard Besselink, Frans Pennings, Sacha Prechal, Alphen aan den Rijn: Kluver Law International, 2010, s. 277. Efe Yamakoğlu, **Bilişim Teknolojilerinin Kullanılmasının İş Sözleşmesinin Taraflarının Fesih Hakkına Etkisi**, İstanbul: On İki Levha Yayıncılık, 2020, s. 188

[136] Article 29 Working Party (2013), **op.cit.** s. 16.

[137] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit.** s. 8

[138] Article 29 Working Party (2013), **op.cit** s. 17.

doğrudan irtibatlıdır[139]. Bu doğrultuda Kurul, Whatsapp hakkında verdiği bir kararında hangi verilerin hangi amaçla Facebook'a aktarılacağı konusunda net bir biçimde bilgilendirme yapılmaması dolayısıyla ilgili ilkeye aykırılık olduğuna karar vermiştir[140].

Amacın meşru olması ise ilkenin üçüncü alt prensibidir. Kurum amacın meşru olmasını yapılan iş ve hizmetle irtibatlı ve bu faaliyeti gerçekleştirmek için gereken verilerin işlenmesi şeklinde yorumlamaktadır[141]. Ancak amacın meşru olmasının daha farklı bir kapsamı olduğu kanaatindeyiz. Çünkü belirli, açık ve meşru amaçlar için işlenme ilkesi en temelde işlenen kişisel verilerden ziyade kişisel verilerin işlenme amacına ilişkin bir ilkedir. Bu noktada meşru amaç kapsamında yapılacak hukuka uygunluk denetiminin hangi kişisel verinin işlenmesinden ziyade amacın genel olarak hukuka uygun olup olmadığı noktasında toplanması gerektiği kanaatindeyiz[142]. Nitekim Çalışma Grubu da amacın meşruluğunu işleme şartlarından birisinin varlığına uygunluk, veri koruma hükümlerine uygunluk ve diğer uygulanabilir hukuk kurallarına uygunluk şeklinde değerlendirmesi ile birlikte ayrıca duruma ilişkin olguların, örf ve adet gibi hususların da değerlendirme kapsamında dikkate alınabileceği görüşündedir[143]. Örnek olarak; Türk Borçlar Kanunu'na[144] göre işçinin kişisel verileri yalnızca işe yatkınlığı ve hizmet sözleşmenin ifası için zorunlu olması halinde kullanılabilecektir (TBK 419). Dolayısıyla TBK'ya göre sayılan hususlar dışında başka bir amacın olması halinde meşru olmayan bir amaçtan söz etmek gerekmektedir. Diğer bir örnek ise reklam yasağı bulunan meslek grupları bakımından verilebilir. Bir avukatın verdiği hizmetin tanıtımını yapmak için kişisel veri işlemesinde de yine aynı şekilde meşru bir amaç bulunmaması dolayısıyla

---

[139] Asia J. Biega ve Michéle Finck, "Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems", **Technology and Regulation,** 2021, s. 48

[140] Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli ve 2021/891 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7045/whatsapp-uygulamasi-hakkında-yurutulen-resen-incelemeye-ilişkin-kamuoyu-duyurusu E.T. 25.02.2023)

[141] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit**. s. 9,

[142] Kurum, bu hususu izah etmek için giyim mağazasının gerekmeksizin müşterinin anne kızlık soyadını işlemesini örnek göstermiştir (Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesi Bakımından Temel İlkeler, op.cit**. s. 7). Bu örnek öğretide amaçla bağlantılı işleme ilkesi kapsamında değerlendirilmesi gerekliliği dolayısıyla eleştirilmiştir. (Bkz: Aksoy Retornaz ve Güçlütürk, **op.cit.** s. 292). Öğretide ayrıca meşru olma kavramının hukuki olma kavramından daha farklı bir kapsama sahip olduğu "toplumun kendiliğinden kabul ettiği değerleri" ifade ettiği de ayrıca değerlendirilmiştir. Bkz: Bahri Öztürk, Elif Altınok Çalışkan ve diğ., **Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı**, Ankara: Seçkin Yayıncılık, 2021, s. 54.

[143] Article 29 Working Party (2013), **op.cit.** s. 20

[144] 6098 Sayılı Türk Borçlar Kanunu, 4 Şubat 2011 tarihli 27826 sayılı Resmi Gazete'de yayımlanmıştır.

işleme faaliyetinin ilkeye ve dolayısıyla hukuka aykırı olduğunu kabul etmek gerekmektedir.

D. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Günümüzde veri hem bir meta hem de bir sermaye halini almıştır[145]. Bu durum ise nihayetsiz bir veri biriktirme isteği ile sonuçlanmaktadır[146]. Kişisel verilerin belli, açık ve meşru amaçlarla işlenmesi ilkesi bu yönde oluşan temayülü sınırlandırma amacındadır. Yine aynı şekilde amaçla bağlantılı, sınırlı ve ölçülü işleme ilkesi de bu noktada zikrettiğimiz ilkeyi tamamlar nitelikte olup veri sorumlularının veri işleme faaliyetini sınırlandırma amacındaki diğer bir ilkedir.

Amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi kapsamında kişisel verinin işlenmesine dayanak olan amacın gerçekleştirilmesi için gerektiği kadar, asgari sayıda veri işlenmelidir[147]. Mefhumu muhalifinden ifade etmek gerekirse ilke dolayısıyla amaçla irtibatı bulunmayan ya da amacın gerçekleşmesi için gerekmeyen kişisel verilerin işlenmemesi gerekmektedir[148]. Amaçla sınırlı, bağlantılı ve ölçülü işleme ilkesi yalnızca kişisel verinin niceliğini kapsamamaktadır, ilke aynı şekilde işlenecek kişisel verilerin niteliği bakımından da geçerlidir[149]. Ayrıca ilgili ilke yalnızca verinin elde edilmesi bakımından değil veri işleme faaliyetinin tüm süreçleri bakımından dikkate alınmalıdır[150]. Örneğin yalnızca iş kapsamında kişisel verilere erişim ihtiyacı bulunan kişilere erişim izninin verilmesi yerine gerekli olup olmadığına bakılmaksızın tüm çalışanlara erişim yetkisi verilmesi ilkeye aykırılık oluşturacaktır[151]. Benzeri şekilde Kurul verdiği bir ilke

---

[145] Jathan Sadowski, "When Data is Capital: Datafication, Accumulation, and Extraction", **Big Data & Society**, 2019, ss. 3-4
[146] Bkz: **Ibid**. ss. 4, 7
[147] Küzeci (2019a), **op.cit**. s. 208. Nitekim veri minimizasyonu prensibi Türk Hukuku'nda bu ilke kapsamında uygulama alanı bulmuştur (Develioğlu **op.cit**. s. 48, Aksoy Retornaz ve Güçlütürk **op.cit**. s. 296)
[148] Murat Altındere, **Kişisel Verilerin Korunması Hukuku ve Uygulanması**, Ankara: Adalet Yayınevi, 2020, s. 38
[149] Cécile de Teerwangne, **op.cit**. s. 317
[150] Carey, **op.cit**. s. 36
[151] **Ibid**.

kararında araç kiralama şirketlerinin işledikleri verileri sınırsız sayıda araç kiralama şirketiyle paylaşmasını ilkeye aykırı bulmuştur[152].

Amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi, özellikle giriş çıkış kontrollerinde gerçekleştirilen veri işleme faaliyetleri bakımından Kurul kararlarına konu olmuştur. Kurul, çalışanların giriş çıkışlarının takibi için parmak izi sistemi kullanılmasına ilişkin olarak verdiği bir kararında ölçülülüğü; "*…veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması…*" şeklinde ifade ederek mesai kontrolünün özel nitelikli veriler işlenmeden daha farklı şekillerde de yapılabileceğini değerlendirmiştir[153]. Kurul açık rızanın alınması halinde dahi hukuka aykırılığın giderilemeyeceğini kabul etmiş ve ilgili faaliyetin ilkeye aykırı olduğuna karar vermiştir[154]. Yine Kurul, başka bir kararında başka yollarla giriş çıkışları kontrol etmesi mümkün iken özel nitelikli veri olan avuç içi iziyle bu işlemleri gerçekleştiren spor salonu işleticisi veri sorumlusunun faaliyetinin hukuka aykırı olduğuna hükmetmiştir[155].

Bu ilke kapsamındaki son husus ise amaçla bağdaşmayan ikincil işlemedir (further processing). GDPR'a göre veri işlendikten sonra ikincil bir işleme faaliyeti, istisnalar saklı olmak üzere, ancak amaçla bağdaşması ölçücüsünde mümkündür[156]. Çalışma Grubu da farklı yorumlamalar ve gelişen teknolojiler dolayısıyla ikincil işlemeye ilişkin çeşitli uyumluluk kriterleri getirmiştir[157]. KVKK bakımından ise ikincil işlemeye ilişkin herhangi bir özel hüküm öngörülmemiş ve ilke kapsamında herhangi bir değerlendirmede bulunulmamıştır. Nitekim bu durum öğretide KVKK bakımından bir eksiklik olarak değerlendirilmiştir[158]. Öğretide bir görüş, Kurul kararlarından hareketle ikincil işlemeye ilişkin bir hukuki sebebin mevcut olması ve KVKK'da yer alan ilkelere bağdaşır nitelikte

---

[152] Kişisel Verileri Koruma Kurulu 2021/1304 sayılı kararı (20 Ocak 2022 Perşembe tarihli 31725 sayılı Resmi Gazete'de yayımlanmıştır)
[153] Kişisel Verileri Koruma Kurulu'nun 1.12.2020 tairhli ve 2020/915 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6872/2020-915 E.T. 25.02.2023)
[154] Kişisel Verileri Koruma Kurulu'nun 1.12.2020 tairhli ve 2020/915 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6872/2020-915 E.T. 25.02.2023)
[155] Kişisel Verileri Koruma Kurulu 25.03.2019 tarihli ve 2019/81 sayılı ile 31.05.2019 tarihli ve 2019/165 sayılı kararları https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 E.T. 26.02.2023)
[156] Biega ve Finck, **op.cit**. s. 49.
[157] Bkz: Article 29 Working Party (2013), **op.cit**. ss. 23-27
[158] Çekin, **op.cit**. s. 76

bir işleme faaliyetinin olması halinde bu şekilde yapılan işleme faaliyetine izin verildiği görüşündedir[159]. Bununla birlikte bu konuda bir düzenlemenin yapılması, sorunun çözümü için en isabetli yol olacaktır.

E. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

KVKK'da öngörülen son ilke mevzuatta öngörülen süre yahut işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesidir. Kişisel verilerin işlenme amacının gerçekleşmesi halinde artık bir amaçtan söz edilememektedir[160]. Aynı şekilde ilgili amaca ulaşılmasının istenmediği, bu amaçtan vazgeçildiği ya da amacın ortadan kalktığı bir durumda da artık kişisel veri işlemek için gerekli bir amaç olmadığından söz etmek gerekmektedir[161]. Bu noktada bir amacın kalmaması halinde kişisel verinin muhafaza edilmemesi gerekliliği ortaya çıkmaktadır. Bu kapsamda kişisel verinin amaç için gereği kadar muhafaza edilmesi ilkesi belirli, açık ve meşru amaçlar için işleme ilkesi ve amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi ile ilişkilidir[162].

Bazı durumlarda ise işleme amacının ortadan kalkması halinde mevzuatta saklama için öngörülen süreler dolayısıyla kişisel verilerin saklanması gerekmektedir. Örneğin sağlık sektöründe sağlık verilerinin saklanması için mevzuatlarda çeşitli süreler bulunmaktadır[163]. Aynı yönde, ilgili kişinin memur olarak çalıştığı dönemde hakkında başlatılan soruşturma dosyasının silinmesi için yaptığı başvuruda Kurul, henüz ilgili mevzuat gereği saklama süresinin dolmaması dolayısıyla veri sorumlusunu haklı bulmuştur[164]. Dolayısıyla amacın ortadan kalktığı hallerde dahi kişisel verinin saklanmasını gerektiren başkaca bir kural olması halinde ilgili işleme faaliyeti ilkeye

---

[159] Cenk Konukpay ve Uğur Tabak, "Kişisel Verilerin İşlenme Amacının Sonradan Değişmesi: Uyumluluk Kriterlerinin Uygulanması Sorunu", **Kişisel Verileri Koruma Dergisi**, Cilt: 3 Sayı: 2, 2021, s. 28. Aksi yönde: Aksoy Retornaz ve Güçlütürk, **op.cit**. s. 295, Özcan, **op.cit**. s. 98

[160] Dülger (2019), **op.cit**. s. 301

[161] **Ibid**. s. 302

[162] Olga Mironenko Enerstvedt, **Avitation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles,** Cham Switzerland: Springer International Publishing, 2017, s. 195

[163] Bkz: Hamza Bayındır, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, İstanbul: On İki Levha, 2020, s. 47

[164] Kişisel Verileri Koruma Kurulu'nun 28.06.2018 tarihli ve 2018/169 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5366/2018-69 E.T. 26.02.2023)

aykırılık teşkil etmeyecektir. Sonuç olarak ilke kapsamında kişisel verilerin amaç için gerektiği kadar saklanması gerekmekte, amacın ortadan kalkması halinde saklanmasını öngören bir düzenleme bulunmamaktaysa kişisel verilerin silinmesi gerekmektedir. Aksi halde ilke ihlal edilmiş olacaktır.

III. Kişisel Veri Güvenliğine İlişkin Yükümlülükler

Kişisel veri güvenliği KVKK 12. maddesinde düzenlenmekte olup kişisel verilerin korunması kapsamında veri sorumluları bakımından yerine getirilmesi gereken temel yükümlülüklerden birisini oluşturmaktadır. Kişisel veri güvenliği en geniş tanımıyla risk ve tehditlere karşı kişisel verilerin korunmasına ilişkin çeşitli yükümlülükleri ifade etmektedir. Kişisel Verileri Koruma Kurumu ise veri güvenliğini, "*kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemeye ve bunların hukuka uygun olarak muhafazasını sağlamaya yönelik gerekli her türlü teknik ve idari tedbirlerin alınması*" şeklinde tanımlamıştır[165]. 108 Sayılı Sözleşme ve Direktif tanımı kapsamında her ne kadar bu tanım isabetli olsa da KVKK kapsamında kişisel veri güvenliğinin farklı yükümlülükleri de içermesi, bu tanımı KVKK bakımından eksik kılmaktadır. Nitekim ilgili tanım teknik ve idari tedbirlerin alınması yükümlülüğü paralelinde yapılmış bir tanım olup teknik ve idari tedbirlerin alınması, KVKK kapsamında veri güvenliğine ilişkin yükümlülüklerden sadece birini teşkil etmektedir. Mevzubahis eleştirimiz bu bölümün devamı kapsamında açıklık kazanacaktır.

Kişisel veri güvenliği kavramı kişisel verilerin korunması kavramından farklı bir kapsama ve anlama sahiptir[166]. Öğretide kişisel verilerin korunması kavramından farklı olarak kişisel veri güvenliği kavramının daha ziyade kişisel veriyi korumaya yönelik olduğu, ancak kişisel verinin güvenliğini amaçlaması dolayısıyla dolaylı olarak kişiye ilişkin koruma sağladığı kabul edilmektedir[167]. Kişisel verilerin korunması kavramı ise kişisel veri güvenliğinden daha geniş bir kavram olup kişisel veri güvenliğini de içerisinde

---

[165] Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Terimler**, s. 11 (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 27.10.2022)
[166] Küzeci (2019a), **op.cit**. s. 253, Bygrave (2014), **op.cit**. s. 2
[167] **Ibid**. Başar, **op.cit**. s. 128

barındırmaktadır[168]. Bu kapsamda kişisel veri güvenliği, kişisel verilerin korunmasının sağlanması açısından kişisel verilerin korunması kavramının temel enstrümanlarından birisi olarak ifade edilebilmektedir[169].

A. Bilgi Güvenliği ve Kişisel Veri Güvenliği

Kişisel veri ifade edildiği üzere KVKK'da tanımlandığı şekliyle belirli şartları taşıyan bir tür bilgidir (KVKK md. 3/1-d). Dolayısıyla bilgi güvenliği kapsamında ifade edilen bilgi, kişisel verileri de ihtiva etmektedir[170]. Bir bilgi türünün güvenliğine ilişkin bir kavram olarak kişisel veri güvenliği de bu doğrultuda bilgi güvenliğine ilişkin genel esaslar çerçevesinde bir içerik kazanmıştır[171]. Bu doğrultuda kişisel veri güvenliği, bilgi güvenliğine ilişkin önlem ve tedbirlerin gerçekleştirilmesiyle birlikte sağlanabilecek bir yükümlülüktür[172]. Dolayısıyla kişisel veri güvenliğini anlamak için bilgi güvenliğinin temel olarak anlaşılması büyük önem arz etmektedir.

Bilgi güvenliğini bilginin karşılaşacağı her türlü tehdide karşı korunması şeklinde geniş bir şekilde tanımlamak mümkündür[173]. Daha özgül bir tanımla ise bilgi güvenliği; bilginin yetkisiz erişim, kullanım, değişim ve tahribatına karşı bilginin korunmasını amaçlayan yöntem ve araçlar bütünüdür[174]. Bu noktada bilgi güvenliğinin üç temel amacı bulunmaktadır. Genel olarak bilgi güvenliğinin temelini oluşturan bu üç amaç; gizlilik

---

[168] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, İkinci Baskı, Ankara: Seçkin Yayıncılık, 2019, s. 129. Veri koruma kavramının bir şemsiye kavram olmasına ilişkin olarak ayrıca bkz: David Hill, **Data Protection, Governance, Risk Management and Compliance**, Boca Raton: CRC Press Taylor & Francis Group, 2009, s. 113. Bygrave (2014), **loc.cit.**

[169] Thomas H. Lenhard, **Data Security, Technical and Organizational Protection Measures against Data Loss and Computer Crime**, Wiesbaden: Springer, 2021, ss. 3,4, Veri güvenliği ifadesinde yer alan veri ifadesi KVKK kapsamında olduğu şekliyle yalnızca kişisel verilerin ifade etmekle genel veri güvenliği literatüründe veri güvenliği ifadesi kişisel yahut kişisel olmayan verileri ayırmaksızın tüm verilerin güvenliği bakımından kullanılmaktadır (Bkz: **Ibid.**)

[170] Türkay Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara: Yetkin Yayınları, 2015, s. 36

[171] European Union Agency for Cybersecurity, **loc.cit.**

[172] Adnrew Denley, Mark Foulsham ve diğ, **op.cit.** s. 46. Çetin, **op.cit**. s. 87, Melisa Geko ve Simon Tjoa, "An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security", **The Central European Cybersecurity Conference,** No: 19, 2018, s. 2

[173] **Ibid**. s. 89. Benzeri bir tanım için bkz: Radi P. Romansky ve Irina S. Noninska, "Challenges of the Digital Age for Privacy and Personal Data Protection", **Mathematical Biosciences and Engineering**, Cilt: 17 Sayı: 5, 2020, s. 5290.

[174] Izzat Alsmadi, Robert Burdwell ve diğ., **Practical Information Security, A Competency-Based Education Course**, Cham: Springer, 2018, s. 1

(confidentiality), bütünlük (integrity) ve erişilebilirliktir (availability)[175]. Bilgi güvenliğinin objektiflerini oluşturan bu unsurlar, bilgi ve bilgi sistemlerinin karşılaşabileceği üç temel risk faktörüne karşı bilgi güvenliği yönetiminin yerine getirmesi gereken hedefleri işaret etmektedir[176].

Gizlilik, bilgiye yalnızca erişimi gerekli kişilerin erişebileceğini, yetkisiz kimselerin ise ilgili bilgiye erişiminin olmamasını ifade etmektedir[177]. Gizlilik, erişimin sınırlandırılması, kullanım sınırlandırılması ve bilginin üçüncü kişiler bakımından kullanışsız hale getirilmesi gibi vasıtalarla sağlanmaktadır[178]. Bütünlük, bilginin değiştirilmemesini veya bozulmamasının teminini açıklamaktadır[179]. Bu kapsamda hedeflenen husus bilginin "*doğru*", "*bütün*" ve "*sağlam*" olmasıdır[180]. Erişilebilirlik ise bilgiye zamanlı bir şekilde erişilebilmesi ve zamanlı bir biçimde kullanılabilmesi şeklinde tanımlanmaktadır[181]. Bu kapsamda bilginin gerektiği zamanlarda erişilebilir olması ve sistem hatası veya veri kaybı halinde zamanlı bir şekilde geri getirilebilmesi erişilebilirlik bakımından hedeflenen temel hususlardır[182]. Nitekim kişisel verilerin korunmasına yönelik kişisel veri güvenliği hükümleri de bu prensipleri gerçekleştirme doğrultusunda bir içeriğe sahiptir[183].

---

[175] John McCumber, **Assessing and Managing Security Risk in IT Systems: A Structured Methodology**, Boca Raton: Auerbach Publications, 2005, s. 32, Alan Calder ve Steve Watkins, **IT Governance: A Manager's Guide to Data Security and ISO27001 / ISO 27002**, London; Kogan Page, 2008 , s. 6. Bu üç unsur "*CIA Triad*" olarak bilinmekte olup bir kavramsal çerçeve olarak oluşumunun 1975'e kadar dayandığı ifade edilmiştir (Yulia Cherdantseva ve Jeremy Hilton, "A Reference Model of Information Assurance & Security", **Availability, Reliability and Security**, Eighth International Conference, 2013, s. 2). Yıllar içinde çeşitli yazarlar tarafından bu kavramsal çerçevenin yeterliliği tartışılmış ve kimi yazarlarca hesap verilebilirlik (accountability), inkar edememe (non-repudiation) gibi kavramlar ayrıca bu kavramsal çerçeveye eklenmiştir (McCumber **loc.cit**., ayrıca bkz: Cherdantseva ve Hilton, **op.cit**. s. 3)

[176] Bilgi güvenliği bakımından temel üç risk faktörü bilginin ifşası, bilginin değiştirilmesi ve bilgiye erişimin engellenmesidir. DAD üçlüsü (disclosure, alteration ve denial) olarak da bilinen üç temel risk faktörü bakımından; gizlilik ile bilginin ifşasının, bütünlük ile bilginin değiştirilmesinin, erişilebilirlik hedefi ile ise bilgiye erişimin engellenmesinin önlenmesi hedeflenmektedir. (Bkz: Michael G. Solomon ve Mike Chapple, **Information Security Illuminated**, Massachusetts: Jones and Barlett Publishers, 2005, ss 5-6)

[177] Alsmadi, Burdwell ve diğ, **op.cit**. s. 5,

[178] Hill, **op.cit.** s. 124.

[179] Alsmadi, Burdwell ve diğ., **loc.cit.,**

[180] McCumber, **op,cit**., s. 36

[181] Alsmadi, Burdwell ve diğ., **loc.cit.**

[182] McCumber, **op.cit**. s. 39

[183] Bu ilkeler GDPR 32. maddesinde doğrudan anılmıştır. Aynı şekilde Kişisel Verileri Koruma Kurumu'na yapılan veri ihlal bildirimi kapsamında kişisel veri ihlalinin gizlilik, erişilebilirlik ve bütünlük prensiplerinden hangisi yahut hangilerinin ihlal edildiğine dair bilgileri içermesi gerekmektedir. Bkz: Kişisel Verileri Koruma Kurumu, **Veri ihlal bildirim formu** s.7

Bilgi güvenliğinin gerçekleştirilmesi çeşitli tedbirler vasıtasıyla sağlanmaktadır. Her ne kadar bilgi güvenliği eski dönemlerinde salt teknik bir mesele olarak addedilmekteyse de günümüzde daha ziyade idari ve insani boyutları da ele alınmaktadır[184]. Bu kapsamda bilgi güvenliği tedbirleri temelde teknik ve idari/organizasyonel olarak tasnif edilmiştir[185]. Bu tasnifin dışında ayrıca teknik, organizasyonel, beşeri ve yasal tedbirler şeklinde tasnifler de bulunmaktadır[186]. KVKK, GDPR ve Veri Koruma Direktifi'nde de kişisel verilerin güvenliğine ilişkin olarak çeşitli tedbirlerin alınması gerekliliği kabul edilmiş ve bu tedbirler teknik ve idari/organizasyonel olarak tasnif edilmiştir (KVKK md. 12/1, GDPR md. 32, DPD md. 17).

İfade edildiği üzere, kişisel veri güvenliği ile bilgi güvenliği birbiriyle etkileşim içinde olan iki alan olduğu gibi kişisel veri güvenliğine ilişkin yükümlülükler de bilgi güvenliği prensipleri paralelinde bir içeriğe sahiptir[187]. Kişisel veri güvenliği de temelde kişisel verilerin risk ve tehditlere karşı korunmasını bakımından yerine getirilmesi ve bu kapsamında alınması gereken yükümlülükleri ifade etmektedir. Bilgi güvenliği ile irtibatından hareketle kişisel veri güvenliğini daha özgül bir şekilde tanımlamak da mümkündür. Bu kapsamda bilgi güvenliğinin prensiplerinden hareketle kişisel veri güvenliği; kişisel verilere yetkisiz erişimin, kişisel verilerin bozulmasının ya da değiştirilmesinin, kişisel verilerin yok edilmesinin engellenmesi ve kişisel verilerin bu tehditlere karşı korunmasıdır[188].

(https://kvkk.gov.tr/SharedFolderServer/CMSFiles/4e601093-24a4-4507-893f-edfa0081695c.pdf E.T. 21.11.2022)

[184] Alsmadi, Burdwell ve diğ., **op.cit.** s. 11., Ayrıca bkz: Mete Eminağaoğlu ve Yılmaz Gökşen, "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,** Cilt 11, Sayı: 4, Yıl: 2009, s. 8, ayrıca bkz: S.H. von Solms ve R. von Solms, **Information Security Governance**, New York: Springer, 2009, s. 17.

[185] Romansky ve Noninska, **op.cit.** s. 5292..

[186] Bkz: Alsmadi, Burdwell ve diğ, **op.cit**. s. 10, Henkoğlu ise tedbirleri teknik önlemler, idari önlemler ve bilgi hukuku şeklinde üçe ayırmıştır. (Türkay Henkoğlu, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", **Arşiv Dünyası Dergisi**, Sayı: 18-19, 2017, ss: 49-50

[187] Enerstvedt, **op.cit**. s. 197

[188]Bygrave (2014), **op.cit**. s. 164, Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Ankara: Seçkin Yayıncılık, 2019, s. 96. Başar, **loc.cit.**

B. Kişisel Veri Güvenliğinin Düzenlemeler Kapsamında Gelişimi

Çalışmamızın bu kısmında kişisel veri güvenliğinin, kişisel verilerin korunmasına ilişkin 1970'li yıllardan itibaren kabul edilip uygulanan düzenlemeler kapsamındaki serüveni ele alınacaktır. Böylece ilk ortaya çıktığı günden itibaren kişisel veri güvenliğinin nasıl düzenlendiği, nasıl bir serüven geçirdiği gibi konuların izah edilmesi amaçlanmaktadır. Bu kapsamda öncelikle 108 Sayılı Sözleşme öncesi dönem incelenerek kişisel veri güvenliğine ilişkin getirilen yükümlülüklerin kişisel verilerin korunması hukukundaki ilk nüveleri ele alınacaktır. Ardından 108 Sayılı Sözleşme, OECD Rehber İlkeleri ve Direktif kapsamında veri güvenliği hükümlerinin ne şekilde geliştiği değerlendirilecektir. Son olarak ise Avrupa'daki güncel düzenleme olan GDPR incelenecektir. Bölüm kapsamında incelememiz nihayetinde KVKK'da mevcut kişisel veri güvenliği düzenlemesinin nasıl bir seyir izlediğini ve hangi konularda özgünleştiğini ve KVKK'daki düzenlemenin ne gibi problemlere sahip olduğunun değerlendirilmesi ile son bulacaktır.

1. 108 Sayılı Sözleşme Öncesi Dönemde Kişisel Veri Güvenliği

1970'li yıllarda dünya, birçok ülkenin kendi iç hukuklarında kişisel verilerin korunmasına ilişkin yaptığı düzenlemelere şahit olmuştur. Ancak ulusal düzenlemelerin öncesinde kişisel verilerin korunması hukuku bakımından ilk veri koruma yasası[189] bir eyalet düzenlemesi olan ve 1970 yılında kabul edilen Hessen Veri Koruma Yasası'dır (*Hessische Datenschutzgesetz*). Bu düzenleme ile kişisel veri güvenliğine ilişkin yükümlülükler de getirilmiştir. Hessen Veri Koruma Yasası ikinci maddesinde işleme faaliyetinin, yetkisiz kimselerce değiştirilmesi yahut yok edilmesi gibi kişisel veri güvenliğini ihlal eden fiillerin meydana gelmesi mümkün olmayacak şekilde gerçekleştirilmesi gerektiği düzenlenmiştir[190]. Dolayısıyla bu hüküm, yükümlüler bakımından çeşitli tedbirlerin alınmasını gerekli kılmıştır[191]. Daha sonraki süreçte 1973

---

[189] Frits W. Hondius, "A Decade of International Data Protection" , **Netherlands International Law Review**, Cilt: 30 Sayı: 2, 1983, s. 103, Gloria Gonzàlez Fuster, **The Emergence of Personal Data Protection as a Fundemental Right of the EU**, Switzerland: Springer, 2014, s. 69

[190] Brendan Van Alsenoy, **Data Protection Law in Eu: Roles, Resposibilities, and Liability,** Cambridge: Intersentia, 2019, s. 166. Ayrıca bkz.: Fuster, **op.cit**. s. 57.

[191] **Ibid**. ss. 166-167.

yılında kabul edilen ve dünyadaki ilk ulusal veri koruma yasası olma özelliğini elinde bulunduran İsveç Veri Koruma Yasası da aynı şekilde veri güvenliğine ilişkin yükümlülükler getirmiştir. Günümüzde kişisel veri güvenliğinden anlaşıldığı şekliyle olmamakla birlikte daha ziyade gizlilik ve sır saklama yükümlülüğü ile ilişkilendirilebilecek olan düzenlemenin 13. maddesinde, yetkisiz bir biçimde bireyin şahsi durumuna ilişkin öğrenilen şeylerin ifşa edilmesini açıkça yasaklanmıştır[192].

Veri güvenliğine ilişkin hükümler yalnızca yukarıda sayılan düzenlemelerdeki hükümlerden ibaret kalmamış ve takip eden birçok veri koruma yasasında kendisine yer bulmuştur. Örneğin, 1978 yılında kabul edilen Fransız Veri Koruma Yasası'nda da (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) işlenen bilgilerin güvenliğine ilişkin yükümlülükler düzenlenmiştir[193]. Yasa'nın 29. maddesi ile özellikle verilerin zarar görmesinin ya da yetkisiz üçüncü kişilerin eline geçmesini engellemek olmak üzere verilerin korunması için gerekli tedbirlerin alınması yükümlülüğünü getirilmiştir[194]. Yine aynı şekilde 1977 yılında kabul edilen Alman Veri Koruma Yasası'nın (Bundesdatenschutzgesetz) 6. maddesinde yetkisiz erişim, yetkisiz bir şekilde verilerin değiştirilmesi gibi mevzuatta öngörülen hususların gerçekleştirilmesi için teknik ve idari tedbirlerin alınması bir yükümlülük olarak düzenlenmiştir[195].

Görüldüğü üzere 108 Sayılı Sözleşme öncesi dönemde veri güvenliğine ilişkin hükümler veri koruma düzenlemelerinin ana başlıklarından birisi olarak kendisine yer bulmaktadır. Ayrıca 108 Sayılı Sözleşme öncesi dönemde tavsiye niteliğinde uluslararası kararlar da mevcuttur. Teknolojik gelişmeler karşısında bireyin ve kişisel verilerin ne derece korunabildiği sorusuyla karşılaşan Avrupa Konseyi, mevcut düzenlemelerin yetersizliği kanısı üzerine ve bu konuda yapılacak düzenlemelerin birbirleri arasında radikal farklılıklara sahip olmasını önlemek üzere 1973 ve 1974 yıllarında iki farklı

---

[192] "The Swedish Data Bank Statute and Regulation of May 11", 1973, Çeviren: Finn Henriksen, **Library of Congress Law Library**, Cilt: 73 No: 2, 1973, s. 7, sec. 13.
[193] Gonzàlez Fuster, **op.cit**. s. 64.
[194] Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, art. 29 (https://www.ssi.ens.fr/textes/a78-17-text.html E.T. 26.03.2022). Van Alsenoy op.cit. s. 196.
[195] German Federal Data Act, section 6, Annex to Section 6 (1) 1, **Selected Foreign National Data Protection Laws and Bills: Volume 1**, Editor: Charles K. Wilk, Washington: U.S. Department of Commerce, Office of Telecommunications OT Special Publication, Cilt: 78 No: 19, 1978 ss. 13, 41.

tavsiye karar kabul etmiştir[196]. Artan veri işleme faaliyetleri kapsamında üye devletlerin alması tavsiye edilen prensipleri içeren bu kararlarda kişisel veri güvenliği de düzenlenen başlıklardan birisi olmuştur. Özel sektöre ilişkin olan 73 (22) sayılı Karar'ın 8. maddesinde bilgilerin kötüye kullanımı ve suiistimaline karşı gereken tedbirlerin alınması gerekliliği ifade edilmiştir[197]. Kamu sektörüne ilişkin getirilen 74 (29) sayılı Karar'ın 6. prensibinde de aynı riskler tekrar edilmiş ve bu tehditlere karşı tedbirlerin alınması gerekliliği düzenlenmiştir[198].

2. 108 Sayılı Sözleşme, OECD Rehber İlkeleri ve Veri Koruma Direktifi

Avrupa Konseyi'nin bir önceki bölümde yer verilen tavsiye niteliğindeki kararlarını takip eden dönemde yukarıda da ifade edildiği üzere Almanya, Fransa, Avusturya, Danimarka, İsveç gibi birçok ülke kendi veri koruma mevzuatını kabul etmiştir[199]. Ayrıca birçok ulusal yasa ve uluslararası belge kişisel veri güvenliğine ilişkin hükümler içermekte olup veri güvenliği, kişisel verilerin korunması bakımından halihazırda temel başlıklardan birisi olmuştur[200]. Bununla birlikte birden çok bağımsız düzenlemenin mevcudiyeti kişisel verilerin korunması ve kişisel veri güvenliğine ilişkin olarak her bir mevzuat bakımından farklı standartlar meydana getirmiş, nihayetinde bu durum yeterli korumanın bulunduğu ülke değerlendirmesini güçleştirmiş ve kişisel verilerin yurt dışına aktarımı bakımından sorun teşkil eder hale gelmiştir[201]. Nihayetinde ulusal yasaları birbiri ile uyumlu hale getirme ve yurt dışına veri transferi önündeki problemlerin giderilmesi hususu gündeme gelmiş ve uluslararası alanda düzenlemeler yapma ihtiyacı doğmuştur[202].

---

[196] A. C. Evans, "European Data Protection Law", **The American Journal of Comparative Law,** Cilt: 29, Sayı: 4, 1981, ss. 572, 573

[197] Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973), Annex, Principle 8 (https://www.legislationline.org/documents/id/6498#:~:text=1.,recorded%2C%20should%20not%20be%20disseminated. E.T. 27.03.2022)

[198] Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (1974), Principle 6 (https://www.legislationline.org/documents/id/6499#:~:text=29.,to%20carry%20out%20their%20duties. E.T. 27.03.2022)

[199] Amy Fleischmann, "Personal Data Security: Divergent Standarts in the European Union and the United States", **Fordham International Law Journal**, Cilt: 19, Sayı: 1, 1995, s. 150

[200] Michael D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy", **Stanford Journal of International Law,** Sayı: 16, 1980, s. 56

[201] Fleischmann, **op.cit**. ss, 150,151.

[202] Hondius, **op.cit**. s. 104

Bu dönemde Uluslararası alanda yapılan iki temel düzenleme OECD'nin yayımladığı Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler ve 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir[203]. İki metin de yaklaşık olarak aynı yıllarda, aynı ülkelerin katılımıyla hazırlanmıştır ve birçok yönden birbirlerine benzemektedirler[204]. Tavsiye niteliğindeki OECD Rehber İlkeleri 11. maddesinde; yetkisiz erişim, kaybolma, yok olma, değiştirilme, ifşa gibi riskler karşısında kişisel verilerin makul güvenlik önlemleri ile korunması gerektiği ifade edilmiştir[205]. Kişisel Verilerin Korunması Hukuku bakımından ilk bağlayıcı uluslararası metin olan[206] 108 Sayılı Sözleşme'nin ise veri güvenliği başlıklı 7. maddesinde ise veri güvenliği, "*otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına uygun güvenlik önlemleri alınır*" şeklinde düzenlenmiştir (108 Sayılı Sözleşme md. 7).

108 Sayılı Sözleşme sonrasındaki dönemde ise 1995 yılında Avrupa Birliği üyesi ülkelerin kişisel verilerin korunmasına ilişkin düzenlemelerinin uyumlu olmasını sağlamak ve birbirleri ile çatışmasını engelleme amacıyla Avrupa Veri Koruma Direktifi kabul edilmiştir[207]. Avrupa Veri Koruma Direktifi'nde veri güvenliğine ilişkin yükümlülüklere "işlemenin güvenliği" başlıklı 17. maddede yer verilmiştir. Buna göre üye devletler; veri sorumlularının, kazayla ya da hukuka aykırı şekilde verilerin imhasına, kaza sonucu kaybolmasına, değiştirilmesine, yetkisiz bir biçimde açıklanmasına veya erişimine ve diğer tüm hukuka aykırı işleme biçimlerine karşı uygun teknik ve idari tedbirleri temin etmesini düzenlemektedir (DPD md 17/1). Uygun teknik ve idari

---

[203] OECD Mahremiyetin Korunması ve Kiisel Verilerin Sınır Ötesi Akıına İlişkin Rehber İlkeleri 23 Eylül 1980, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Strazburg 28.1.1981.

[204] Hondius, **op.cit**, s. 113

[205] OECD, **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** France: OECD Publication Service, 2001, s. 15.

[206] Paul de Hert ve Vagelis Papakontantinou, "The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on its Global Ambition", **Computer Law & Security Review,** Cilt: 30 Sayı: 6, 2014, s. 634.

[207] Alsenoy, **op.cit.** s. 276,

tedbirlerin belirlenmesinde Direktif'e göre uygulama maliyetleri, günün teknolojisi ve olası riskler dikkate alınmalıdır (DPD md. 17/1). Direktif'in kişisel veri güvenliğine ilişkin getirdiği yükümlülükler bununla sınırlı olmayıp ayrıca veri sorumlusunun, veri işleyenin sayılan tedbirlere uymasını sağlama yükümlülüğü bulunmaktadır (DPD md. 17/2). Veri işleyen ile veri sorumlusu arasında sözleşme bulunması ise Direktif bakımından getirilen bir diğer yükümlülüktür (DPD md. 17/3).

Direktif'in getirdiği yükümlülükler doğrultusunda üye devletler kişisel veri güvenliğine ilişkin benzeri düzenlemelere yer vermişlerdir[208]. Bazı devletlerce iç hukuklarında ek yükümlülükler getirilmiş yahut alınması gereken belirli tedbirler açıkça zikredilmiş olmakla birlikte genel olarak Direktif'in veri güvenliğine ilişkin ilgili hükmü üye devletlerin iç hukuklarında tekrar edilmiştir[209]. Dolayısıyla Direktif'in üye devletlerin kendi aralarında kişisel veri güvenliği bakımından tutarlılık gösteren düzenlemelere vasıta olduğu söylenmelidir.

3. Genel Veri Koruma Tüzüğü

Avrupa Birliği 2016 yılında Genel Veri Koruma Tüzüğü'nü (General Data Protection Regulation, GDPR) kabul etmiştir[210]. Genel Veri Koruma Tüzüğü gerek Avrupa Birliği içerisinde gerekse de uluslararası düzlemde birçok ülke mevzuatını etkileyerek kişisel verilerin korunması hukuku bakımından yeni bir sayfa açmıştır[211]. 2018 yılında yürürlüğe giren bu yeni düzenleme Avrupa Veri Koruma Direktifi'nden farklı olarak üye ülkelerde doğrudan uygulanabilir niteliktedir[212]. Doğrudan uygulanmasının yanı sıra GDPR kapsamında kişisel veri güvenliğine ilişkin daha detaylı düzenlemeler

---

[208] Douwe Korff, **Ec Study on Implementation of Data Protection Directive Comparative Smmary of National Laws,** Cambridge: Human Right Centre, 2002, s. 157. (https://gegevensbeschermingsrecht.nl/onewebmedia/douwe.pdf E.T. 04.12.2022)
[209] **Ibid**. ss. 158, 160,
[210] Regulation (EU) 2016/679 Of The European Parlıament And of the Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation),
[211] Bkz: Paul Breithbarth, "The İmpact of GDPR One Year on", **Network Security,** Sayı 8, 2019, s. 13.
[212] Joao Serrado ve diğ., "Information Security Frameworks for Assisting GDPR Compliance in Banking Industry", **Digital Policy, Regulation and Governance**; Cilt: 22 Sayı: 3, 2020, s. 228

getirilmiş ve kişisel veri güvenliğine ilişkin olarak yükümlülükler daha da somutlaştırılmıştır[213].

GDPR, öncelikle kişisel veri güvenliğini 5. maddede yer alan ilkeler kapsamında uygun güvenlik önlemlerinin alınmasını bir ilke olarak zikretmektedir (GDPR md. 5). Ayrıca GDPR'ın dördüncü bölümünün ikinci kısmı kişisel veri güvenliğini düzenlemektedir. Kişisel veri güvenliği ilgili bölüm kapsamında iki başlığa ayrılmıştır. Bu başlıklar işlemenin güvenliği ve veri ihlal bildirimidir (GPDR md. 32,33,34). İşlemenin güvenliği kapsamında veri sorumlusu ve veri işleyen riske uygun güvenlik seviyesini sağlamak için teknik ve idari tedbirleri almakla yükümlüdür (GDPR 32). Bu noktada Veri Koruma Direktifi'nden farklı olarak kişisel veri güvenliğinden veri işleyen de sorumlu kılınmıştır[214].

Veri sorumlusu ve veri işleyen gerekli tedbirleri alırken ilgili riskleri gözeterek hareket etmekle yükümlüdür. Bu noktada GDPR risk temelli bir yaklaşımı benimsemiştir[215]. Risk temelli yaklaşım alınacak tedbirler ile olası riskler arasındaki ilişkiyi ifade etmektedir[216]. Risk temelli yaklaşım kapsamında; ilgili kişiler bakımından mevcut olabilecek riskler, üçüncü taraf, veri sorumlusu yahut veri işleyenden kaynaklanan ya da bu kişiler bakımından mevcut olan riskler hesaba katılarak uygun tedbirler alınmalıdır[217]. Uygunluk ifadesi ise orantılılık ilkesinin bir görünümü olarak değerlendirilmiştir[218]. Buna göre riske uygun, diğer bir deyişle, riskle orantılı teknik ve idari tedbirler alınmalıdır[219]. GDPR ayrıca bu uygunluk değerlendirmesinin de ne şekilde yapılacağına ilişkin ölçütler getirmiştir. Buna göre riske uygun tedbirlerin belirlenmesi

---

213 Information Commissioner's Office, **Guide to General Data Protection Regulation**, 2019, s. 227 (https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf E.T. 04.12.2022)

214 P. T. J. Wolters, "The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility", **International Data Privacy Law,** Cilt: 7, Sayı: 3, 2017 ss. 4, 10. Cedric Burton, "Security of Processing", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020, s.634.

215 Voigt ve von dem Bussche, **op.cit**. s. 40.

216 Annika Selzer, "The Appropriateness of Technical and Organisational Measures under Article 32 GDPR", **European Data Protection Law Review**, Vol. 7, No. 1,2021, s. 120

217 Voigt ve von dem Bussche, **loc.cit.**

218 Burton **op.cit**. s. 635.

219 Aynı şekilde KVKK'da da "uygun güvenlik düzeyini temin etmeye yönelik" şekilde teknik ve idari tedbirlerin alınması gerektiği düzenlenmiştir (KVKK 12/1).

kapsamında teknolojinin geldiği nokta, uygulama masrafları, işleme faaliyetinin doğası, kapsamı, bağlamı, amacı, riskin olasılığı ve şiddeti hesaba katılmalıdır (GDPR md. 32/1)[220].

GDPR, riske uygun teknik ve idari tedbirlerin alınmasını bir yükümlülük olarak düzenlemekle birlikte KVKK ve diğer birçok mevzuattan farklı olarak bu tedbirlerden bazılarını zikretmiştir. Zikredilen teknik ve idari tedbirler sınırlı sayıda olmayıp örnekleme yoluna gidilmiştir[221]. Bu tedbirler kimliksizleştirme[222] ve şifreleme, işleme hizmet ve sistemlerinin gizliliği, bütünlüğü, erişilebilirliği, dirençliliği[223], fiziki ya da teknik bir vaka durumunda, erişilebilirliğin sağlanabilmesi ve uygulanan tedbirlerin etkililiğinin periyodik olarak değerlendirilmesi şeklinde özetlenebilecektir (GDPR md. 32/1). Öğretide bu tedbirlerin uygun güvenlik seviyesi için asgari olarak uygulanması gereken tedbirler olduğunu değerlendiren yazanlar bulunmakla birlikte kimliksizleştirme ve şifreleme tedbirlerinin uygun güvenlik düzeyini temin etmek için uygun bir tedbir olmadıkça zorunlu olmadığı değerlendirmesinde bulunan görüşler de mevcuttur[224].

GDPR kapsamında veri sorumlusu ve veri işleyen kendi idareleri altında görev alan ve kişisel verilere erişim sağlayan kimselerin veri sorumlusu talimatları dışında da kişisel veri işlemelerinin engellenmesini sağlamak için gerekli önlemleri almakla yükümlü kılınmıştır (GDPR md. 32/4). Bu nedenle çalışanların eğitimi, kişisel verilere ilişkin olarak bilinçlendirilmesi ve güvenilir çalışanlarla faaliyet göstermek kişisel veri güvenliği bakımından ayrıca önem arz etmektedir[225].

---

[220] Burton, **Ibid**. Carey, **op.cit**. s. 92.
[221] Paul Lambert, **Understanding the New European Data Protection Rules**, Boca Raton: CRC Press„ 2017, s. 281.
[222] "Pseudonymisation" kavramı KVKK kapsamında tanımlanmamıştır ancak Kişisel Sağlık Verileri Hakkında Yönetmelik kapsamında Türk Hukuku'nda "kimliksizleştirme olarak düzenlenmiştir (21 Haziran 2019 Cuma, 30808 Sayılı Resmi Gazete). Bu nedenle kavramı kimliksizleştirme olarak nakletmeyi tercih ettik.
[223] GDPR kapsamında bilgi güvenliğinin prensiplerine doğrudan işaret edilmiş ve bu prensiplerin sağlanması gerektiği düzenlenmiştir. Bu husus bilgi güvenliği ve kişisel veri güvenliğinin yoğun bir biçimde irtibatlı olduğunu göstermektedir. Yine benzeri şekilde Kişisel Verileri Koruma Kurumu'na yapılan veri ihlali bildiriminde veri ihlalinin etkisine ilişkin olarak verinin gizliliği, bütünlüğü yahut erişilebilirliğinden hangisini ihlal ettiğine yönelik de bildirimde bulunulması gerekmektedir (Kişisel Verileri Koruma Kurumu, Veri İhlal Bildirimi Formu s. 2. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8217d07e-5af7-43f0-ad02-a48cb1e23cd7.pdf E.T. 05.05.2022)
[224] Voigt ve von dem Bussche, **op.cit**. s. 39. Information Comissioner's Office, **op.cit.** ss. 233, 239.
[225] Information Commissioner's Office, **op.cit**. s. 237.

GDPR kapsamında kişisel veri güvenliğinin ikinci alt başlığı ise veri ihlal bildirimidir. Veri Koruma Direktifi'nde bulunmayan veri ihlali bildirimi Gizlilik ve Elektronik Haberleşme Direktifi'nde yapılan bir değişiklik ile önce belli sektörlere getirilmiş bir yükümlülük iken GDPR'da sektöre bakılmaksızın tüm veri sorumlularınca yerine getirilmesi gereken bir yükümlülük olarak öngörülmüştür[226]. GDPR'a göre kişisel veri güvenliğine dair herhangi bir ihlal meydana geldiği halde veri sorumlusu ihlalin farkında olmasından itibaren 72 saat içinde ihlali veri otoritesine bildirmekle yükümlüdür (GDPR md. 33/1). Yine aynı şekilde ilgili kişiler de gecikmeksizin veri ihlalinden haberdar edilmelidir (GDPR md. 34/1).

C. Kişisel Verilerin Korunması Kanunu'nda Kişisel Veri Güvenliğine İlişkin Yerine Gerilmesi Gereken Yükümlülükler

KVKK'nın Veri Güvenliğine İlişkin Yükümlülükler başlıklı 12. Maddesinde dört farklı yükümlülük ve bir sorumluluk hükmü öngörülmüştür. Aşağıda detaylıca inceleyeceğimiz yükümlülükleri kısaca özetleyecek olursak bunlar; veri sorumlusunun gerekli teknik ve idari tedbirleri alması (KVKK md. 12/1), veri sorumlusunun kanun hükümlerinin uygulanmasına ilişkin kendi kurum ve kuruluşlarında gerekli denetimleri yapması veya yaptırması (KVKK md. 12/3), kişisel verilerin amacı dışında kullanılmaması veya hukuka aykırı başkalarına açıklanmaması (KVKK md. 12/4) ve veri ihlal bildiriminin yapılmasıdır (KVKK md. 12/5). Sorumluluk maddesi ise özel hukuka ilişkin olup veri sorumlusu ve veri işleyenin işleme faaliyetinde birlikte bulunmaları halinde teknik ve idari tedbirleri alması bakımından müşterek olarak sorumlu olduklarını düzenlemektedir (KVKK md. 12/2)[227]. Görüldüğü üzere KVKK'da öngörülen haliyle kişisel veri güvenliğine ilişkin yükümlülüklerin kapsamı teknik ve idari tedbirlerin alınması ile sınırlı tutulmamış, yukarıda bahsedilen diğer düzenlemelere göre daha geniş ve daha farklı şekilde düzenlenmiştir.

---

[226] Rebecca Wong, **Data Security Breaches and Privacy in Europe**, London: Springer London, 2013 s. 10

[227] Nitekim KVKK'nın 18/2 maddesinde idari para cezalarının özel hukuk tüzel kişisi veya gerçek kişi veri sorumluları hakkında uygulanacağı düzenlenmiştir.

KVKK, Avrupa Veri Koruma Direktifi'nden hareketle hazırlanmıştır[228]. Bu noktada KVKK'daki birçok hükmün Direktif hükümleriyle paralellik arz etmesi dikkate değerdir[229]. Ancak bu durum, veri güvenliğine ilişkin yükümlülükler bakımından farklılık göstermektedir. Veri güvenliğine ilişkin yükümlülükler kapsamında Direktif hükümlerinden kopuş kişisel verilerin korunması bakımından Türkiye'de TBMM'ye sunulmuş üç farklı kanun tasarısının karşılaştırmalı incelemesi ile açık hale gelmektedir. Öncelikle 2008 yılında kadük olan Kişisel Verilerin Korunması Kanunu Tasarısı, veri güvenliğine ilişkin Direktif doğrultusunda hükümler benimsemişken daha sonraki tasarılar ve nihayetinde KVKK'da ilgili hüküm, farklı şekilde düzenlenmiştir. 2008 yılındaki tasarının 15. maddesine göre "*kişisel verilerin, tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını değiştirilmesini, yetkisiz olarak açıklanmasını veya aktarılmasını ve başka şekillerdeki tüm hukuka aykırı işlenmelerini önlemek için"* veri kütüğü sahibinin (veri sorumlusu) uygun teknik ve idari tedbirleri alma yükümlülüğü bulunmaktadır[230]. Tasarı'da ayrıca uygun teknik ve idari tedbirlerin seçiminde kişisel verinin niteliği, günün teknolojisi ve maliyetlerin göz önünde bulundurulması hüküm altına alınmıştır[231]. 2008 Tasarısı kişisel veri güvenliğine ilişkin tedbirleri bunlarla sınırlı tutmamış ve ayrıca veri işleyenin mevcudiyeti halinde veri kütüğü sahibinin yazılı sözleşme yapmasını zorunlu tutmuştur[232]. Son olarak veri kütüğü sahibinin, kendisi adına kişisel verilere erişimi bulunan kişilerin veri kütüğü sahibi talimatları doğrultusunda hareket etmesini sağlama yükümlülüğü bulunmaktadır[233]. Görüldüğü üzere, 2008 yılında kadük olan bu Tasarı'daki kişisel veri güvenliğine ilişkin yükümlülükler Avrupa Veri Koruma Direktifi hükümleri ile tamamen paralellik arz etmektedir[234].

---

[228] Altındere, **op.cit**. s. 22
[229] Onur Baskın **op.cit**. s. 37
[230] Kişisel Verilerin Korunması Kanunu Tasarısı, B.02.0.KKG.*010/101-902/1812, 22.04.2008. (https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=64271 E.T. 22.11.2022). **Kişisel Verilerin Korunmasına Dair Eski Kanun Tasarıları ve Gerekçeleri Üzerine Karşılaştırma** (2008-2014) Editör: Tuğba Karaer ve Burcu Sarı, Yayın No: 18, Yayım Tarihi 06.02.2015 s. 12, (www.kanunum.com E.T. 24.06.2022)
[231] **Ibid**.
[232] **Ibid**. ss. 12-13.
[233] **Ibid**. s. 13.
[234] Aynı yönde: Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**,, Cilt: 61 Sayı: 3, 2012, s. 1154

2008'deki yasa tasarısının yanı sıra 2014 yılında Türkiye Büyük Millet Meclisi'ne ikinci bir kişisel verilerin korunması kanunu tasarısı sunulmuştur. Yine kadük hale gelen bu tasarıda ise 2008'deki tasarıdan çok farklı bir kişisel veri güvenliği hükmü bulunmakta olup bu hüküm 2016 yılında yasalaşan mevcut KVKK'nın tasarısındaki ilgili hükümle aynıdır. 2014 yılında sunulan tasarıda kişisel veri güvenliğini sağlamak için uygun teknik ve idari tedbirlerin alınması, veri ihlali halinin bildirimi, gerekli denetimlerin yapılması ile kişisel verilerin amacı dışında kullanılmaması ve açıklanmamasına ilişkin yükümlülükler yer almıştır[235]. Bu kapsamda teknik ve idari tedbirlerin alınması dışındaki tüm yükümlülükler 2014 tasarısı ile eklenmiştir. Teknik ve idari tedbirlerin alınması yükümlülüğü ise Direktif ve 2008 tasarısından çok daha farklı bir biçimde kaleme alınmıştır.

Yukarıda ifade ettiğimiz üzere 2016'da yasalaşan KVKK'da kişisel veri güvenliğine ilişkin hüküm son halini 2014'te sunulan tasarı ile almıştır. Nihayetinde 6698 sayılı Kanun'daki haliyle kişisel veri güvenliğine ilişkin yükümlülükler gerek ek yükümlülükler öngörülmesi gerek teknik ve idari tedbirlerin lafzi olarak farklı şekilde düzenlenmesi, gerekse de Kurul'un maddeyi yorumlama biçimi dolayısıyla hareket noktası olan Avrupa Veri Koruma Direktifi'nden daha farklı ve daha geniş bir düzenleme hüviyetine bürünmüştür. Böylece ilk olarak 2014 yılındaki tasarıda daha sonra ise KVKK'da bulunan mevcut veri güvenliğine ilişkin düzenleme, yalnızca verinin güvenliğine ilişkin bir yükümlülük olma niteliğinden uzaklaşmış ve veri güvenliği kavramının sınırlarını aşarak adeta KVKK'da getirilen tüm hükümlerin koruyucusu haline gelmiştir. Bu bölümün devamında mevcut düzenlemedeki veri güvenliğine ilişkin yükümlülükler izah edilmeye çalışılacaktır.

1. Veri Sorumlusunun Teknik ve İdari Tedbirleri Alma Yükümlülüğü

KVKK'nın 12. maddesinde veri sorumlusunun teknik ve idari tedbirleri alma yükümlülüğü şu şekilde düzenlenmiştir: "*Veri sorumlusu; a) kişisel verilerin hukuka*

---

[235] Kişisel Verilerin Korunması Kanunu Tasarısı, 31853584-101-580-5204, 26.12.2014, (https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=173481 E.T. 22.11.2022). Kişisel Verilerin Korunmasına Dair Eski Kanun Tasarıları ve Gerekçeleri Üzerine Karşılaştırma (2008-2014), **loc.cit**. s. 13

aykırı olarak işlenmesini önlemek, b) kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır" (KVKK md. 12/1). 2008 tasarısındaki düzenlemeye göre ise veri sorumluları: "*Kişisel verilerin, tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını, değiştirilmesini, yetkisiz olarak açıklanmasını veya aktarılmasını ve başka şekillerdeki tüm hukuka aykırı işlenmelerini* korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre uygun teknik ve idarî tedbirleri almak zorundadır*"*[236]. Görüldüğü üzere 2008 tasarısının ilgili hükmü ile KVKK'nın teknik ve idari tedbirlerin alınmasına ilişkin hükmü arasında lafzi olarak önemli farklar bulunmaktadır.

2008 tasarısındaki hüküm, ifade edildiği üzere, Direktif doğrultusunda hazırlanmış olup bilgi güvenliği ile yoğun şekilde irtibatlı bir düzenlemedir. Kişisel verilerin yetkisiz şekilde açıklanması ve aktarılmasının önlenmesi gizlilik ilkesini, kişisel verilerin değiştirilmesi ve yok edilmesinin önlenmesi bütünlük ilkesini, kişisel verilerin kaybolmasının önlenmesi ise erişilebilirlik ilkesini amaçlamaktadır. Maddenin sonunda yer alan başka şekillerdeki tüm hukuka aykırı işlenmelerin önlenmesi ise sayılan durumlar dışında herhangi bir risk yahut tehdidin kalmamasını temin etmek ve sayılan risk ve tehditlerin sınırlı sayıda olmadığını vurgulamak amacıyla maddede bulunmaktadır.

KVKK'da yer alan düzenlemede ise veri sorumlusunun; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak için gerekli güvenlik düzeyini temin etmesi gerekmektedir[237]. Görüldüğü üzere KVKK'daki ilgili hüküm bilgi güvenliği

---

[236] Kişisel Verilerin Korunması Kanunu Tasarısı, B.02.0.KKG.*010/101-902/1812, 22.04.2008. (https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=64271 E.T. 12.10.2022)

[237] 12. maddenin birinci fıkrasına göre teknik ve idari tedbirlerin sağlaması gereken üç yükümlülük yukarıda ifade edilmiştir. Bu yükümlülükler; olumsuz yükümlülükler (kişisel verilerin hukuka aykırı işlenmesinin önlenmesi ve kişisel verilere hukuka aykırı erişimin önlenmesi) ve olumlu yükümlülük (kişisel verilerin muhafazası) şeklinde tasnif edilebilecektir (Metin Turan, **Kişisel Verilerin Korunması,** Ankara: Seçkin Yayıncılık, 2021, 4. Baskı, s. 90). Öte yandan öğretide, teknik ve idari tedbirler bakımından kişisel verilerin hukuka aykırı işlenmesi durumu var olduğu için diğer iki yükümlülüğün KVKK'da bulunmasına gerek olmadığını savunan bir görüş bulunmaktadır (Sezen Kama Işık, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış,** İstanbul: On İki Levha Yayıncılık, 2020, s. 277). Ancak bu görüşe, her erişim niteliğindeki fiilin işleme niteliğinde olmaması ve kişisel verilerin güvenliğinin işleme yahut erişme dışı hallerle de risk altında olması dolayısıyla iştirak etmek mümkün gözükmemektedir.

terminolojisinden farklı bir terminolojiye sahiptir. İlk olarak muhafaza kavramının ne anlama geldiği KVKK bakımından belirsiz olup bilgi güvenliği ile nasıl ilişkilenebileceği soru işaretleri barındırmaktadır. Diğer yandan her ne kadar hukuka aykırı işlenmenin önlenmesi ifadesi, Direktif ve 2008 tasarısı bakımından veri güvenliğini riske eden herhangi bir durumun maddenin koruması dışında kalmaması amacıyla düzenlenmiş iken KVKK'da teknik ve idari tedbirlerin sağlaması gereken üç temel amaçtan ilki olarak sayılmıştır. 2008 tasarısı ve Direktif'te veri güvenliği kapsamında sayılmayan risk ve tehditlerin sınırlı sayıda olmadığını vurgulamak için kullanılmış bu ibarenin, KVKK'da düzenlendiği yer itibarıyla ne şekilde yorumlanacağı muğlaklaşmış ve Kurul'un içtihatları ile çok daha farklı bir hüviyete bürünmüştür. Bu husus bir sonraki bölüm kapsamında ele alınacaktır.

a. Kişisel verilerin hukuka aykırı işlenmesini önlemek

Birinci fıkranın (a) bendinde teknik ve idari tedbirler vasıtasıyla sağlanacak ilk amaç hukuka aykırı işlenmenin önlenmesi şeklinde öngörülmüştür. İşleme, otomatik ya da veri kayıt sisteminin parçası kılınması kaydıyla otomatik olmayan yollarla kişisel veri üzerinde gerçekleştirilen her türlü işlemdir. İşleme faaliyeti hukuka uygun olabileceği gibi KVKK'daki şartları sağlamaması halinde hukuka aykırı da olabilecektir. Bu kapsamda veri sorumluları hukuka aykırı işleme faaliyetlerine karşı tedbir alma yükümlülüğüne sahiptir.

Kurul, alınacak tedbirlerle önlenmesi gerekli olan hukuka aykırı işleme faaliyetlerini veri sorumlusunun gerçekleştirdiği işleme faaliyetleri olarak değerlendirmektedir. Örnek olarak Kurul, 2021/1243 sayılı kararında herhangi bir işleme şartına dayanmaksızın ilgili kişinin e-posta adresine tanıtım amaçlı e-posta gönderen veri sorumlusunun 12. Maddenin birinci fıkrasına aykırı hareket ettiğine karar vermiştir[238]. Yine başka bir kararda ise Kurul, veri sorumlusunun video olarak kaydedilen halı saha maçlarını internet sitesinde yayımlamasının hiçbir hukuki işleme şartını taşımadığına, bu nedenle de veri sorumlusunun kişisel verilerin hukuka aykırı işlenmesini önlemeye

[238] Kişisel Verileri Koruma Kurulu'nun 09.12.2021 tarihli 2021/1243 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7274/2021-1243 E.T. 02.03.2023)

yönelik teknik ve idari tedbirleri almadığına hükmetmiştir[239]. Son olarak ise veri sorumlusu avukat tarafından dava dosyası kapsamında tanık olarak dinlenen kişinin ceza mahkumiyetine ilişkin bilgilerin dosyaya sunulmasına ilişkin olarak Kurul, veri sorumlusu avukatın hiçbir işleme şartına dayanmadığı ve bu kapsamda hukuka aykırı veri işlediğinden bahisle gerekli teknik ve idari tedbirleri yerine getirmediğine hükmetmiştir[240].

Kararlarda görüldüğü üzere hukuka aykırı işleme ifadesi veri sorumlusu gerçekleştirdiği işleme faaliyetleri kapsamında yorumlanmaktadır. Kanaatimizce ilgili fıkrada yer alan hukuka aykırı işleme ibaresinden kasıt, veri sorumlusunun işlemiş olduğu verilere karşı üçüncü kişiler tarafından gerçekleştirilebilecek hukuka aykırı şekilde işleme niteliğindeki risk ve tehditlerdir[241]. Nitekim 12. maddenin birinci fıkrası, veri sorumlularına olası risk ve tehditlere karşı bir önlem alma yükümlülüğü getirmektedir. Alınan önlemlere karşın yine de risk ve tehditler gerçekleşebilecektir[242]. Dolayısıyla teknik ve idari tedbirler, veri sorumlusunun tamamen kontrol edemediği risk ve tehditleri bertaraf etme amacıyla alınmaktadır. Bu nedenle de teknik ve idari tedbirlerin alınacağı hususlarda veri sorumlusunun bir sonuç garanti edebilmesi mümkün değildir. Ancak veri sorumlusunun kendi faaliyetleri kapsamında hukuka uygun bir şekilde kişisel veri işlemesi, aydınlatma yükümlülüğünün yerine getirilmesi gibi kontrolü altında olan ve belirli bir sonucu gerçekleştirebileceği bir yükümlülüktür. Dolayısıyla Kurul'un veri sorumlularınca gerçekleştirilen hukuka aykırı işleme faaliyetlerini madde kapsamında değerlendirmesi makul bir yorum teşkil etmemektedir. Veri sorumlusunun hukuka uygun veri işlemesi veri güvenliğini düzenleyen 12. maddenin değil, işleme faaliyetinin

---

239 Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli 2021/889 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7139/2021-889 E.T. 02.03.2023)

240 Kişisel Verileri Koruma Kurulu'nun 02.11.2021 tarihli 2021/1111 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7266/2021-1111 E.T. 02.03.2023)

241 Aksi görüş: Çekin, **op.cit**. s. 195. Çekin'e göre ilgili veri sorumluları bakımından işleme şartlarına uygunluk denetimi yükümlülüğü getirmektedir.

242 "*Önem arz eden bir diğer husus ise, söz konusu yükümlülüklerin mutlak bir neticeyi gerekli kılmamasıdır. Şöyle ki veri sorumlusu, her türlü saldırıyı önlemekle yükümlü değildir. Kanun'da öngörülen düzenleme, neticeye bağlı bir sorumluluk hali değildir. Bilakis Kanun, veri sorumlusunun "gerekli" önlemleri almasını zorunlu kılmakla, veri sorumlusunun kendi üzerine düşen önlemleri alması halinde artık sorumluluktan kurtulabileceğine işaret etmektedir. Aksi takdirde, yani veri sorumlusunun neticeden dolayı sorumlu kılınması halinde, "gerekli" önlemlerin alınması şartının hiçbir anlamı kalmazdı. Dolayısıyla bu çerçevede bir özen sorumluluğu halinden bahsetmek daha isabetli gözükmektedir". (*Çekin, **op.cit**. ss. 186,187), Kama Işık, **op.cit**. s. 276

hukukiliğini düzenleyen 5 ila 9. maddelerin konusudur. Sayılan nedenler ve maddenin lafzından hareketle hukuka aykırı işleme faaliyetinden üçüncü kişilerce bir risk olarak ortaya konan hukuka aykırı olarak kişisel veri üzerinde gerçekleşen her türlü işlem şeklinde yorumlanması daha isabetli olacaktır. Ayrıca hukuka aykırı işleme faaliyetinin üçüncü kişiler tarafından gerçekleştirilen faaliyetleri ifade eder şekilde yorumlanması, ilgili bendin bilgi güvenliği ilkelerinden gizlilik prensibi paralelinde bir anlama kavuşması imkanını sağlayacaktır.

Öte yandan kararlarda dikkat çeken diğer bir husus ise Kurul'un veri sorumlusu bünyesinde hukuka aykırı bir işleme faaliyetinin meydana gelmesi halinde doğrudan teknik ve idari tedbirlerin alınmadığı yönünde değerlendirmede bulunmasıdır. Kurul kararlarında, herhangi bir şekilde veri sorumlusu bünyesinde olan hukuka aykırı işleme faaliyetinin, hangi teknik ve idari tedbirin alınmaması dolayısıyla oluştuğunu değerlendirilmemektedir. Bunun sebebi işleme faaliyetinin hukukiliğinin teknik ve idari tedbirler vasıtasıyla sağlanabilecek bir yükümlülük olmamasıdır. Örneğin, ilgili kişinin açık rızası alınmaksızın sınav sonucunun bir haber sitesinde paylaşılması konusunda Kurul, işleme faaliyetinin hukuka aykırı olduğuna ve bu nedenle teknik ve idari tedbirlerin alınması yükümlülüğüne aykırı hareket edildiğine karar vermiştir[243]. Kararda hangi tedbirin alınmadığına dair herhangi bir değerlendirme bulunmamaktadır. Hukuka aykırı işleme faaliyetinin gerçekleştirilmiş olması teknik ve idari tedbirlerin alınmamasının doğrudan gerekçesini teşkil etmektedir. Hukuka aykırı işlemeyi önlemek amacıyla gerekli teknik ve idari tedbirleri almadığı değerlendirilen veri sorumlusunun ihlal ettiği asıl yükümlülük, hukuka uygun kişisel veri işleme yükümlülüğüdür. Görüldüğü üzere Kurul, gerekli teknik ve idari tedbirlerin alınıp alınmamasından ziyade madde kapsamında hukuka aykırı veri işleme faaliyetinin gerçekleşip gerçekleşmediğini değerlendirme konusu yapmaktadır. Kurul'un bu şekilde inceleme yapması, veri güvenliğine ilişkin yükümlülükler üzerinden işlemenin hukukiliğine ilişkin olarak değerlendirme yapıldığını göstermektedir.

[243] Kişisel Verileri Koruma Kurulu'nun 06.01.2022 tarihli ve 2022/13 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7179/2022-13 E.T. 28.02.2023)

Kurul'un hukuka aykırı işleme ibaresini bu şekilde yorumlaması kişisel veri güvenliğinin kapsamını genişletmekte ve bunun sonucu olarak veri sorumlusunun organizasyonu kapsamında gerçekleştirilen her türlü kişisel veri işleme niteliğindeki faaliyeti veri güvenliğinin konusu haline getirmektedir. Böylece kişisel verilerin işlenme şartlarının veri güvenliği içerisinde değerlendirilmesi mecburiyeti bulunmaktadır. Bu noktada öncelikle veri sorumlusunun KVKK'nın beşinci ve altıncı maddesine uygun olarak kişisel veri işleme faaliyetinde bulunması gerekmektedir. Ayrıca işleme faaliyeti, kişisel verilerin işlenmesine ilişkin ilkelere de uygun olmak olmalıdır[244]. Bu kapsamda özel nitelikli olmayan kişisel verilerin hukuka uygun şekilde işlenmesi için; ilgili kişinin açık rızasının olması, kanunlarda açıkça öngörülmesi, veri işlemenin rızasını açıklayamayacak kişinin hayatını ve beden bütünlüğünün korunması için zorunlu olması, sözleşmenin taraflarına ait verilerin ifa yahut sözleşmenin kurulması için işlenmesinin zorunlu olması, hukuki yükümlülüğün yerine getirilmesi için veri işlemenin zorunlu olması, kişisel verinin alenileştirilmiş olması, bir hakkın tesis edilmesi, hakkın kullanılması yahut korunması için kişisel veri işlemenin gerekli olması veya kişisel veri işlenmesinde veri sorumlusunun meşru bir menfaatinin olması gerekmektedir (KVKK md. 5). Özel nitelikli kişisel verilerin işlenmesi bakımından ise kişinin açık rızasının bulunması yahut işleme durumunun kanunlarda öngörülmesi durumlarında işleme faaliyeti hukuka uygun olacaktır. Sağlık ve cinsel hayat verileri bakımından ise yalnızca sır saklama yükümlülüğü altında bulunan kişiler ve yetkili kurum ve kuruluşlar KVKK'da yer alan amaçlarla kişinin açık rızasını almaksızın özel nitelikli kişisel verileri işleyebilecektir (KVKK md 6).

Kurul'un yukarıda ifade edilen görüşü, kişisel verilerin silinmesi imha edilmesi veya anonim hale getirilmesine ilişkin 7. maddeyi de[245] aynı şekilde veri güvenliği

---

[244] Çekin, **loc.cit.** Umniyahasghar Yosif, "Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler", **Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,** Cilt: 4 Sayı: 1, s. 10

[245] Kişisel verilerin silinmemesi, imha edilmemesi veya anonim hale getirilmemesi de ayrıca kişisel verilerin hukuka aykırı işlenmesi niteliğindedir. Örneğin iş başvurusu sonrası işe alınmayan ilgili kişinin kişisel verilerinin silinmesi talebini reddeden veri sorumlusu hakkında Kurul hiçbir işleme şartına dayanmaksızın kişisel veri işlenmeye devam edilmesi nedeniyle "hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı…" dolayısıyla idari para cezasına hükmetmiştir (Kişisel Verileri Koruma Kurulu'nun 06.07.2021 tarihli 2021/670 sayılı kararı https://www.kvkk.gov.tr/Icerik/7136/2021-670 E.T. 02.03.2023)

kapsamında değerlendirmeyi gerektirmektedir. Buna göre kişisel verinin işlenmesi sebebini teşkil eden herhangi bir hususun kalmaması halinde kişisel verinin silinmesi, imha edilmesi yahut anonim hale getirilmesi gerekmektedir. Aksi durumda kişisel veri hukuka aykırı şekilde işlenmiş olacaktır. Yine aynı şekilde kişisel veri aktarımı da bir kişisel veri işleme faaliyetidir[246]. Buna göre kişisel verilerin aktarılması da özel nitelikli kişisel veriler bakımından 6. maddeye uygun (özel nitelikli kişisel veri işleme şartları), diğer kişisel veriler bakımından ise 5. maddeye uygun şekilde icra edilmelidir (kişisel veri işleme şartları). Yurt dışına yapılan aktarımlar bakımından ise açık rıza alınmaksızın kişisel veriler yurt dışına aktarılamayacaktır (KVKK md. 9/1). Eğer ki aktarım yapılacak ülke yeterli korumanın bulunduğu bir ülke ise yahut bu konuda veri sorumlusu tarafından yeterli koruma taahhüt edilmiş olup Kurul tarafından izin verilmiş ise bu iki durumda da normal işleme şartları kapsamında yurt dışına aktarım yapılabilecektir (KVKK md 9/2).

b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek

Kişisel verilere hukuka aykırı erişimi önlemek ise tedbirler vasıtasıyla gerçekleştirilmesi gereken ikinci yükümlülüktür. Hukuka aykırı şekilde erişim; veri sorumlusunca işlenmiş olan kişisel verilere erişim yetkisi bulunmayan bir kimsenin hukuka aykırı şekilde erişimi yahut erişim yetkisi bulunan bir kimsenin amacı veya yetkisi dışında kişisel verilere erişim sağlaması halidir[247]. Hukuka aykırı erişim fiziki ortamda mümkün olabileceği gibi fiziki ortamda bulunmayan kişisel verilere erişim şeklinde de gerçekleşebilir[248]. Bu noktada bir siber saldırı da gündeme geleceği gibi fiziki bir şekilde kişisel verilere hırsızlık ya da başka bir yolla ulaşılması da söz konusu olabilecektir. Uygulamada ise hukuka aykırı erişim durumu sıklıkla siber saldırı şeklinde gündeme gelmektedir. Bu kapsamda hukuka aykırı erişimin önlenmesi bilgi güvenliği kapsamında gizlilik ilkesine paralel bir görünüm arz etmektedir.

---

[246] Kişisel verilerin aktarılması da kişisel verinin üzerinde gerçekleştirilen bir işlem olması bakımından işleme faaliyetidir. Bkz: Sevgi Ünsal Özden, İdil Uz ve Mert Karamustafaoğlu, "Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği", **Kişisel Verileri Koruma Dergisi,** Cilt: 3, Sayı: 1, 2021, s.22

[247] Amaç ve yetki dışında kişisel verilere erişimin hukuka aykırı erişim ve hukuka aykırı işleme niteliğinde olabileceği hususuna ilişkin olarak ayrıca bkz.: Kişisel Verileri Koruma Kurulu 13.02.2020 tarihli 2020/124 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6886/2020-124 E.T. 02.03.2023)
Kişisel Verileri Koruma Kurulu'nun 03.03.2020 tarihli ve 2020/191,192,193,194 sayılı kararları (https://www.kvkk.gov.tr/Icerik/6762/2020-191-192-193-194 E.T. 02.03.2023)

[248] Çekin **op.cit**. ss. 195-196.

Veri sorumlularının, hukuka aykırı erişimin önlenmesine yönelik gerekli teknik ve idari tedbirleri almamaları dolayısıyla KVKK'yı ihlal ettikleri çok sayıda Kurul kararı mevcuttur. Örneğin bir kararda, bilişim hizmeti veren veri sorumlusunun yetkilendirme çalışması sırasında yazılım kodunda meydana gelen bir hata sonucu hizmet verilen bir müşteri şirkete, yapılan diğer yardım bildirimleri de erişilebilir hale gelmiştir. Kurul, incelemesi neticesinde, ihlalin yetki düzenlemelerinin hatalı yapılmasından ve yazılım geliştirme çalışmalarının test ortamında yapılmamasından dolayı veri sorumlusunun hukuka aykırı erişimin önlenmesi amacıyla gerekli teknik ve idari tedbirlerin alınması yükümlülüğüne aykırı davrandığına karar vermiştir[249]. Diğer bir olayda ise bir sigorta şirketinin test sunucusu siber saldırıya uğramış, saldırgan 7 kez denemesi üzerine sisteme erişebilmiştir. Saldırgan test sunucusu veri tabanını silerek sisteme fidye taleplerini ileten bir mesaj yüklemiştir. Kurul, incelemesi neticesinde, test sunucularının yıllık sızma testleri kapsamına alınmaması, gerekli kontrollerin yapılmaması, güçlü parolaların kullanılmaması, güvenli iletişim yöntemlerinin kullanılmaması değerlendirmelerinde bulunarak veri güvenliğine ilişkin yükümlülüklerin yerine getirilmediğine karar vermiştir[250].

c. Kişisel verilerin muhafazasını sağlamak

Kişisel verilerin muhafazasını sağlamak fıkra kapsamındaki üçüncü yükümlülüktür. Muhafaza kavramının ne anlama geldiği muğlak olup geniş bir şekilde yorumlanabilme olanağına sahip bir kavramdır[251]. **Çekin** bu noktada kişisel verilerin muhafazasının kasıt bulunmadan kişisel verilerin kaybolmasına yahut yok olması gibi durumlara ilişkin olarak teknik ve idari tedbirlerin alınmasını gerekli kıldığını değerlendirmektedir[252]. Bu doğrultuda kişisel verilerin muhafazası açısından risk arz eden hususlar doğal afetler,

---

[249] Kişisel Verileri Koruma Kurulu 27.04.2021 tarihli 2021/426 sayılı kararı (https://kvkk.gov.tr/Icerik/6981/2021-426 E.T. 02.03.2023)

[250] Kişisel Verileri Koruma Kurulu 24.11.2020 tarihli 2020/905 sayılı kararı (https://kvkk.gov.tr/Icerik/6862/2020-905 E.T. 02.03.2023)

[251] Muhafaza kavramı için ayrıca bkz: Mesut Serdar Çekin, Ahmet Esad Berktaş ve diğ., **Veri Hukuku,** İstanbul: On İki Levha Yayıncılık, 2023, s. 294

[252] Çekin, **op.cit.** s. 196

yangın gibi durumlar olabilecektir[253]. Muhafaza kavramının bu kapsamda değerlendirilmesi, kavrama bilgi güvenliği doğrultusunda bir anlam kazandıracağı gibi KVKK bakımından kavramın hem bütünlük hem de erişilebilirlik ilkelerine paralel bir görev ifa etmesini sağlayacaktır.

Yukarıda sayılan hallerin dışında Kurul, hukuka aykırı işleme yahut hukuka aykırı erişim gibi bir durum söz konusu olmaksızın kişisel verilerin erişilebilir hale geldiği durumları kişisel verilerin muhafazası kapsamında değerlendirmektedir. Bu noktada kişisel verilerin muhafazası diğer yükümlülükler bakımından tamamlayıcı bir rol üstlenmektedir. Veri sorumlusu bir banka tarafından ilgili kişiye gönderilen kartın başka bir kimseye teslim edilmesi Kurul tarafından kişisel verilerin muhafazasına yönelik olarak gerekli teknik ve idari tedbirlerin alınmadığı şeklinde değerlendirilmiştir[254]. Diğer bir kararında ise Kurul, müşterilere verilen takip numaralarının son hanelerinin değiştirilmesi ile başkaca müşterilerin kişisel verilerine erişilebilmesi dolayısıyla veri sorumlusunun kişisel verilerin muhafazasını sağlamak için yeterli teknik ve idari tedbirleri sağlamadığına kanaat getirmiştir[255]. Her iki kararda da herhangi bir hukuka aykırı erişim yahut işleme durumu olmaksızın kişisel verilerin erişimi yetkili olmayan kişilerce erişime açık hale gelmesi söz konusudur. Görüldüğü üzere, Kurul bu durumlarda kişisel verilerin muhafazası bakımından teknik ve idari tedbirlerin alınıp alınmaması yönünden inceleme yapmaktadır.

d. Teknik ve idari tedbirler

Veri sorumlusu kişisel verilerin hukuka aykırı işlenmesini, kişisel verilere hukuka aykırı erişilmesini önlemeyi ve kişisel verilerin muhafazasını sağlamayı alacağı teknik ve idari tedbirler vasıtası ile yerine getirmek ile yükümlüdür. KVKK'da bu tedbirler somut olarak sayılmadığı gibi GDPR'dan farklı olarak örneklendirilmemiştir. Bu durumun bir nedeni teknolojide meydana gelen sürekli değişimlerdir[256]. Diğer bir nedeni ise hangi

---

[253] **Ibid**. s. 197

[254] Kişisel Verileri Koruma Kurulu'nun 16.01.2020 tarihli 2020/32 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6700/2020-32 E.T. 02.03.2023)

[255] Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli 2019/23 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5464/2019/52 E.T. 02.03.2023)

[256] Turan **op.cit**. s. 110

tedbirin alınması gerektiğinin ancak somut olayın özellikleri kapsamında cevaplanabilecek olmasıdır[257]. Sektör, kişisel veri türü, veri sorumlusunun kimliği gibi birçok değişken dolayısıyla kişisel veriler farklı risklerle karşılaşabilecektir. Bu noktada tedbirlerin bir liste halinde belirlenmesinden ziyade somut olayın getirdiği risk ve tehditler çerçevesinde değerlendirilmesi elzemdir.

Teknik ve idari tedbirler KVKK'da zikredilmemekle birlikte bu tedbirlerin neler olacağı Kişisel Verileri Koruma Kurumu'nun yayımladığı rehberlerde, Kurul kararlarında ve ikincil mevzuatlarda yer bulmaktadır. Özellikle Kurum tarafından yayımlanan Kişisel Veri Güvenliği Rehberi bu noktada veri sorumluları bakımından yol göstericidir. Kurum, rehber kapsamında tedbirleri iki başlık altında incelemiştir. İdari tedbirler bakımından öncelikle mevcut risk ve tehditlerin belirlenmesi gerektiği ifade edilmiştir[258]. Uygun güvenlik düzeyinin temini için risk düzeyinin anlaşılması büyük önem taşımaktadır. Ayrıca çalışanların bilinçlendirilmesi ve bilgilendirilmesi önem arz etmektedir[259]. Kurum'un açıkladığı diğer idari tedbirler ise politika ve prosedürlerin belirlenmesi, kişisel verilerin asgariye indirilmesi ve veri işleyenden hizmet alınması halinde yazılı bir sözleşme yapılması ve veri sorumlusunun talimatları doğrultusunda hareket edilmesidir[260].

Kurum ayrıca Rehber kapsamında teknik tedbirlere yer vermiştir. Bu kapsamda siber güvenlik önlemleri alınması, veri ihlallerinin tespiti ve zamanlı şekilde müdahale edebilmek için log kayıtlarının tutulması gibi takiplerin yapılması, kişisel verilerin bulunduğu fiziki yahut fiziki olmayan ortamlarda güvenlik önlemlerinin alınması, kişisel verilerin yedeklenmesi gibi hususlar Kurum tarafından sayılan teknik tedbirlerden bazılarıdır[261]. Yukarıda ifade edildiği gibi kişisel veri güvenliğine ilişkin tedbirlerin somut olay nezdinde değerlendirilmesi gerekmektedir. Nitekim Kurum da Rehber'de ifade ettiği tedbirleri "*alınabilecek teknik ve idari tedbirler*" şeklinde ifade etmiştir[262]. Dolayısıyla

---

[257] Küzeci (2019), **op.cit**. 256.
[258] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, Ankara: KVKK Yayınları, 2018, s. 8
[259] **Ibid**. s. 9
[260] **Ibid**. ss.11-13
[261] **Ibid**. ss. 16-24.
[262] **Ibid**. s. 3

Rehber'de sayılan tedbirler de asgari alınması gereken tedbirleri teşkil etmeyip bu tedbirler iyi uygulama niteliğindeki örneklerdir.

Kurul'un kararları alınacak tedbirler bakımından ayrıca yol gösterici niteliktedir. Öncelikle Kurul'un veri güvenliğine ilişkin yükümlülükler konusunda düzenleyici işlem yapma ve özel nitelikli kişisel veriler kapsamında yeterli önlemleri belirleme yetkisi bulunmaktadır (KVKK md. 22/1-ç,f). Bu kapsamda Kurul 2018/10 sayılı kararı ile özel nitelikli kişisel veriler işlenirken alınması gereken teknik ve idari tedbirleri belirlemiştir[263]. Ayrıca Kurul'un teknik ve idari tedbirler konusunda aldığı ilke kararları bulunmaktadır[264]. Ayrıca birçok ikincil mevzuatta bilgi güvenliği ve kişisel veri güvenliğine ilişkin tedbirler öngörülmüştür ve dolayısıyla tedbirlerin kaynağı bu düzenlemeler de olabilir[265]. Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ kapsamında bilgi güvenliğine ilişkin yükümlülükler bu kapsamda örnek teşkil etmektedir[266].

Görüldüğü üzere teknik ve idari tedbirlerin çeşitli kaynakları bulunmaktadır. Ancak nihayetinde alınması gerekli teknik ve idari tedbirler somut olay kapsamında belirlenmelidir. Somut olay için teknik ve idari tedbirler belirlenirken ise ölçüt "*uygun güvenlik düzeyini temin*" etmek olacaktır (KVKK 12/1). Hükümde ifade edilen uygun ifadesi GDPR'da düzenlendiği gibi kişisel verinin karşılaşacağı risk karşısında alınması gereken tedbirlerin ölçülülüğünü ifade etmektedir. Bu uygunluk derecesinin sağlanması ile veri sorumluları yükümlülüklerini yerine getirmiş olacaklardır. Ayrıca şu hususu da ifade etmek gerekmektedir: 2008 tasarısında teknik ve idari tedbirlerin belirlenmesi için günün teknolojisi ve uygulama maliyetleri uygunluk değerlendirmesinin ölçütleri olarak düzenlenmiştir. KVKK'da ise böyle bir düzenleme öngörülmemiştir. Bu kapsamda teknik

---

263 Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarihli 2018/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/4110/2018-10 E.T. 02.03.2023)

264 Bkz: Kişisel Verileri Koruma Kurulu'nun 21.12.2017 tarihli ve 2017/61 sayılı ilke kararı, 30312 sayılı 25 Ocak 2018 tarihli Resmi Gazete'de yayımlanmıştır.

265 Altındere, **op.cit.** s. 79

266 Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ, 1 Aralık 2021 Çarşamba, 31676 sayılı Resmi Gazete.

ve idari tedbirlerin alınması konusunda tek uygunluk ölçüsü mevzuatın gerektirdiği yükümlülüklerin yerine getirilebilmesi amacıyla uygun güvenlik düzeyinin temin edilmesi olup bu durum veri sorumluları bakımından ağır külfetler doğurabilecek niteliktedir. Zira veri sorumlularının uygulama maliyetlerini hesaba katması bir ölçüt olarak değerlendirilmemiştir. Bu kapsamda ifade edilen uygunluk ölçütlerinin de 12. maddeye eklenmesi isabetli bir çözüm yöntemi olacaktır.

2. Veri Sorumlusunun Denetim Yükümlülüğü

12. madde kapsamında veri sorumlusunun diğer bir yükümlülüğü denetime ilişkindir. Buna göre veri sorumlusu, KVKK hükümlerinin uygulanmasını temin etmek için denetim yaptırmak yahut yapmakla yükümlüdür (KVKK 12/3). Yükümlülüğün veri sorumlusunca şahsen yerine getirilmesi zorunlu olmayıp veri sorumlusu denetime ilişkin olarak dış hizmeti alımı yaparak da bu yükümlülüğünü yerine getirebilecektir[267]. Denetim yükümlülüğünün yerine getirilmesi açısından denetimin konusu ve kapsamının ne olduğunu belirlemek önem arz etmektedir. KVKK'nın lafzından anlaşıldığı üzere yalnızca veri güvenliğine ilişkin hususlar değil, KVKK hükümlerinin uygulanmasına ilişkin tüm hususlar denetimin konusunu oluşturacaktır. Örneğin aydınlatma metinlerinin KVKK'ya uygunluğu da denetimin kapsamı dahilinde olacaktır[268]. Kurul aydınlatma metinleri mevzuata uygun olmayan ve ilgili kişiye 30 gün içinde cevap vermeyen veri sorumlusunun gerekli denetimleri yapmak bakımından da ihlale sebep olduğuna ve disiplin hükümleri doğrultusunda yükümlü kişiler hakkında işlem yapılmasına karar vermiştir[269]. Görüldüğü üzere ilgili denetimin kapsamı yalnızca veri güvenliği çerçevesi ile sınırlı değildir; KVKK'nın tüm hükümleri kapsamında yapılacak denetim, veri güvenliğinin konusu olarak düzenlenmiştir.

---

[267] Aynı yönde, Serdar Çelikel, **Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri**, Ankara: Seçkin Yayıncılık, 2022, s. 111, Kişisel Verileri Koruma Kurumu, **Kanun Kapsamında Hak ve Yükümlülükler,** s.5 (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 26.10.2022)

[268] Aynı yönde, Yasemin Avcı**, Kişisel Verilerin Korunması**, Konya: Selçuk Üniversitesi, yayımlanmamış yüksek lisans tezi, 2019, s. 90.

[269] Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli 2019/122 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5461/2019/122 E.T. 02.03.2023)

Kurum içi periyodik yahut rastgele denetimler Kurum tarafından aynı zamanda bir idari tedbir olarak sayılmıştır[270]. Teknik ve idari tedbir olan denetim ile ayrıca bir yükümlülük olan KVKK'ya uygunluğu sağlama amaçlı denetim arasındaki fark kanaatimizce denetimin konusu ve kapsamıdır[271]. Bir idari tedbir olan denetimin periyodik yahut rastgele olabileceği belirtilmişken KVKK'ya uygunluk amaçlı denetim bakımından ise herhangi bir zaman dilimi öngörülmemiştir. Yalnızca KVKK'da bir ölçüt olarak "*gerekli*" ibaresi kullanılmıştır (KVKK 12/3). Denetimin ne aralıkla yapılacağı bu noktada veri sorumlusunca takdir edilecektir.

3. Kanuna Aykırı Başkasına Açıklama ve İşleme Amacı Dışında Kullanma Yasağı

Kişisel veri güvenliğine ilişkin bir diğer yükümlülük ise veri sorumlusu ve veri işleyen kişilerin kişisel verileri amacı dışında kullanmaması ve KVKK'nın hükümlerine aykırı bir şekilde başkasına açıklamamasıdır. İlgili fıkra şu şekildedir: "*Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder*" (KVKK 12/4). Maddenin gerekçesinde bu hükmün bir sır saklama yükümlülüğü olduğu ifade edilmiştir[272]. Nitekim kimi yazarlarca da yükümlülük bu şekilde adlandırılmıştır[273]. Ancak amaç dışı kullanımın yasaklanmasının da yükümlülük kapsamında olması hükmün sır saklama yükümlülüğünden daha geniş kapsamlı olduğunu göstermektedir. Nitekim kişisel verinin üçüncü bir kişiye açıklanmaksızın da amaç dışı kullanımı mümkündür.

Amaç dışı kullanımın yasaklanması kişisel verilerin işlenmesine ilişkin ilkelerle bağlantılıdır. Nitekim kişisel veriler belirli, meşru ve açık amaçlar dahilinde işlenmelidir.

---

[270] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, **op.cit**. s. 29

[271] Öte yandan Kurum yayımladığı bir rehberde idari tedbir olarak addettiği denetim ile ayrı bir yükümlülük olarak öngörülen denetimi aynı doğrultuda yorumlamıştır. Bkz: Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi,** Ankara: KVKK Yayınları: No 41, 2022, s. 125

[272] Kişisel Verileri Koruma Kurumu(2019b), **op.cit**. s. 31

[273] Bkz: Çelikel, **op.cit**. s. 103, Oğulcan Özkan, **Kişisel Verilerin Korunması**, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2020, s. 177, Canan İmançlı, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu,** İstanbul: On İki Levha Yayıncılık, 2020, s. 195

Bu kapsamda amaçla bağdaşmayan şekilde bir ikinci işleme faaliyetinin de yapılması yasaklanmıştır[274]. KVKK'da herhangi bir istisna öngörülmemesine rağmen öğretide bir görüş Kurul'un muhtelif kararlarından yola çıkarak KVKK kapsamında Kurul'un belirli bir uygunluk testi uyguladığı ve ikincil işlemeyi tamamen hukuka aykırı olarak değerlendirmediği ifade etmektedir[275]. Ancak amaç dışı kullanımdaki bu durumun veri işleyenler[276] bakımından geçerliliği söz konusu olmayacaktır. Veri işleyenin bir kişisel veriyi amacı dışında kullanması halinde artık veri işleyenin veri sorumlusu olduğundan bahsetmek gerekmektedir. Zira veri sorumlusu kişisel verilerin işlenme amacı ve vasıtasını belirleyen kimsedir. Dolayısıyla işleme amacı dışında kişisel veriyi kullanan kimse veri işleyen değil amacı belirleyen bir kişi olarak veri sorumlusu olacaktır[277] ve bu kapsamda idari yaptırıma tabi olacaktır.

Kişisel verilerin açıklanması ve amacı dışında kullanılması kişisel verilerin işlenmesi niteliğindedir[278]. Bu kapsamda kişisel veri güvenliğinin kapsamına bir kez daha işlemenin şartlarına ve hukuka uygun kişisel veri işlemeye ilişkin olarak bir yasak getirilmiş ve kişisel veri güvenliği bir kez daha işlemenin hukukiliğini kapsayacak şekilde genişletilmiştir. Sonuç olarak KVKK'da veri sorumluları ve veri işleyenlerin öğrendikleri kişisel verileri kişisel verinin işleme amacı dışında kullanması ve KVKK hükümlerine aykırı olarak açıklaması kişisel veri güvenliği kapsamında yasaklanmıştır.

---

[274] **Supra**. s. 30

[275] Konukpay ve Tabak, **op.cit**. s. 28,

[276] 12. maddede dördüncü fıkra kapsamında ilk defa veri sorumlusu dışında "veri işleyen kişiler" de hükmün muhatabı olmuştur. Bu ibarenin veri işleyen kişiler şeklinde yazılması soru işaretleri barındırmaktadır. Veri işleyen Kanun'da tanımlanmış olmasına rağmen veri işleyen kişiler şeklinde yazılması bu ibareyi veri sorumlusunun veri işlemekle görevli çalışanları şeklinde de anlaşılmaya müsait hale getirmektedir. Nitekim yükümlülüğün görevden ayrılma ile de devam edeceğinin düzenlenmesi de hükmü yine bu yönde yorumlamayı mümkün kılar çünkü Kişisel Verilerin Korunması Hukuku'nun kavramları otonom kavramlar olarak görev ilişkisi kapsamında değil kişisel veri ile kurulan ilişki nezdinde anlam kazanır. Tüm bu açıklamalarla birlikte madde gerekçesinde hiçbir duraksamaya yer vermeksizin kastedilen kişinin veri işleyen olduğu ifade edilmiştir Bkz: Kişisel Verileri Koruma Kurumu (2019b), **loc.cit.**

[277] Amacı belirleyen kimsenin veri sorumlusu olarak kabul edilmesine ilişkin olarak bkz: Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarih ve 2020/172 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6890/2020-172 E.T. 21.11.2022)

[278] İlgili fıkranın kaynağının Direktif ve 2008 tasarısı olduğu kanaatindeyiz. 2008 tasarısında yer alan "*yetkisiz olarak açıklanmasını veya aktarılmasını"* önlemeye ilişkin getirilen yükümlülük KVKK'da ayrı bir hüküm olarak bu şekilde yer almıştır. Ancak tasarı ve KVKK'da düzenlenişi itibarıyla bu iki yükümlülüğün önemli bir farklı bulunmaktadır. 2008 tasarısında yer alan yükümlülük kişisel veriler bakımından risk teşkil eden yetkisiz açıklama ve aktarılma fiillerinin veri güvenliği ile korunmasını amaçlarken KVKK'da yer alan yükümlülük işlemenin hukukiliği bakımından veri sorumlusu ve veri işleyene bir yasak getirmektedir.

4. Veri İhlal Bildirimi

KVKK'da kişisel veri güvenliği kapsamında öngörülen son yükümlülük veri ihlali durumunun bildirilmesidir. Veri ihlal bildirimi ifadesi KVKK'da geçmemekle birlikte Kurul 2019/10 sayılı kararında veri ihlal bildirimi adlandırmasını kullanmıştır[279].

Veri ihlal bildirimi kapsamında öngörülen yükümlülük veri ihlali halinde bu durumun en kısa süre içerisinde Kurul'a ve ilgilisine bildirilmesidir. Bildirimin amacı veri ihlalinin ortaya çıkarabileceği sonuçları azaltmak ve tekrarlanmasını engellemektir[280]. Ayrıca veri sorumlusunun veri ihlali bakımından kusuru, ihmali gibi bir durumun söz konusu olmasına gerek yoktur[281]. Veri ihlal bildirimi, veri ihlalinin gerçekleşmesi halinde yerine getirilmesi gereken bağımsız bir yükümlülüktür.

12. maddenin beşinci fıkrasında veri ihlali: "*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi…*" şeklinde ifade edilmiştir (KVKK md. 12/5). Dolayısıyla veri ihlalini kişisel verilerin başkaları tarafından elde edilmesi ve bu elde edilmenin kanuni olmayan yollarla gerçekleşmesi tesis etmektedir. KVKK kapsamında veri ihlalinin içeriği bu noktada GDPR'dan farklılaşmaktadır. Nitekim GDPR kapsamında kişisel verilerin kaza yahut hukuka aykırı şekilde kaybolması, yok olması, değiştirilmesi, yetkisi şekilde açıklanması, kişisel verilere yetkisiz şekilde erişilmesi gibi durumlar veri ihlali teşkil etmektedir. Ancak KVKK kapsamında yalnızca KVKK'ya aykırı biçimde elde edilme hali veri ihlali olarak değerlendirilerek bildirime tabi kılınmıştır[282]. Bir görüş bu farklılık dolayısıyla veri ihlalinin GDPR'da sahip olduğu anlam kapsamında geniş yorumlanması gerektiğini ifade etmiştir[283]. Ancak KVKK'nın bu konuda şüpheye yer vermeksizin açık olduğu ve bildirimi yapmamanın idari para cezasına tabi olduğu düşünüldüğünde veri ihlalinin kapsamının yorum yoluyla genişletilmesinin ciddi bir belirsizliğe yol açacağı kanaatindeyiz.

---

[279] Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 02.03.2023)
[280] Çekin **op.cit**. s. 206
[281] **Ibid**.
[282] Aynı yönde: Çelikel **op.cit**. s. 104.
[283] Avcı, **op.cit**. s. 91

Veri ihlali bildiriminin hangi süre içerisinde yapıldığı yükümlülüğün yerine getirilebilmesi için önem arz eden diğer bir husustur. Bu noktada KVKK yalnızca "*en kısa süre*" ibaresini kullanarak net süreyi tespit etmemiştir (KVKK md. 12/5). Ancak Kurul 2019/10 sayılı kararında en kısa süre ibaresinin azami olarak 72 saat olarak tayin etmiştir[284]. İlgilisine bildirim süresi ise bu kararda net bir biçimde belirlenmemiş olup makul olan en kısa sürede bu bildirimin yapılması gerektiğine karar verilmiştir[285]. Dolayısıyla ilgiliye yapılacak bildirimin somut olay nezdinde ayrıca değerlendirilmesi gerekmektedir.

Özetlemek gerekirse veri ihlal bildirimi GDPR'dan farklı olarak Türk hukukunda yalnızca kanuni olmayan yollarla kişisel verilerin elde edilmesi durumu bakımından düzenlenmiştir. Veri ihlal bildiriminin süresi ise Kurul'un konu hakkındaki kararı ile netlik kazanmış olup Kurum'a yapılacak bildirimin süresi veri ihlalinin öğrenilmesinden itibaren 72 saat iken ilgilisine yapılacak bildirimin süresi makul olan en kısa süredir. Hem Kurum'a hem de ilgilisine bildirim yapılması şart olup aksi durumda yükümlülük yerine getirilmemiş olacaktır.

[284] Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/10 sayılı kararı, (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 02.03.2023)
[285] **Ibid**.

İKİNCİ BÖLÜM: KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLERİN YERİNE GETİRİLMEMESİ KABAHATİ

Çalışmamızın ikinci bölümünde kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati ele alınacaktır. Kişisel verilerin korunmasına ilişkin mevcut olan hukuki çarelerden birisi ve hatta belki de en önemlisi KVKK'da düzenlenen kabahatlerdir. KVKK'da toplamda dört farklı kabahat düzenlenmiş olup bunlar; aydınlatma yükümlüğünün yerine getirilmemesi kabahati, kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati, kurul tarafından verilen kararların yerine getirilmemesi kabahati ve veri siciline kayıt ve bildirim yükümlülüğüne aykırı hareket etme kabahatidir (KVKK 18/1).

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bu kabahatler içinde özel bir yere sahiptir. Bu durumun başlıca iki sebebi, kanaatimizce kişisel veri güvenliği kapsamında öngörülen yükümlülüklerin veri güvenliğinin kavramsal yapısını aşar şekilde geniş bir şekilde düzenlenmesi ve bunun dolaylı bir sonucu olarak kişisel verilerin işlenmesinin hukukiliği dahil olmak üzere birçok yükümlülüğün veri güvenliği kapsamında yorumlanması ve değerlendirilmesidir. Böylece KVKK'ya aykırılık teşkil edecek birçok işlem ve eylem bu kabahatin kapsamında incelenmektedir. İkinci sebep ise ilk sebeple ilişkili olup uygulamada KVKK'nın en çok ihlal edildiği durumların hukuka aykırı şekilde kişisel veri işlenmesi ve veri güvenliğine ilişkin risk ve tehditleri bertaraf edecek şekilde yeterli tedbirlerin alınmamasıdır. Sayılan nedenler dolayısıyla Kurul'un verdiği yaptırım kararlarının çoğunluğunu kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati teşkil etmektedir.

KVKK'nın 18. maddesinde *"12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar"* idari para cezası verileceği düzenlenmiştir (KVKK 18/1-b). 12. maddede ise 18. maddede yer alan kabahat hükmünün işaret ettiği dört yükümlülük bulunmaktadır. Buna göre gerekli teknik ve idari tedbirlerin alınmaması, denetim yükümlülüğünün yerine getirilmemesi, kişisel verilerin amacı dışında kullanılması ve Kanuna aykırı başkasına

açıklanması ile son olarak veri ihlal bildiriminin yapılmaması kabahat kapsamında haksızlık teşkil eden hareketlerdir (KVKK 12).

Kabahatler Kanunu'nda kabahatin idari yaptırıma tabi tutulan bir haksızlık olduğu düzenlenmiştir (KK md. 2)[286]. Bu noktada kabahatler de suçlarla aynı şekilde haksızlık teşkil eden hareketlerdir[287]. Haksızlık ise tipiklik ve hukuka aykırılıktan oluşmaktadır[288]. Ayrıca bir kabahatten söz edilebilmesi için haksızlığın unsurları olan tipiklik ve hukuka aykırılığın yanı sıra suçlarda olduğu gibi ayrıca kusurun da mevcut olması gerekmektedir[289]. Bu kapsamda suç ve kabahat arasındaki farklılık niteliksel değildir; kabahatler ve suçlar yaptırımlara göre birbirlerinden ayrılmaktadır[290]. Suç ve kabahatlerin niteliksel olarak farklı olmaması ve sistematik olarak aynı unsurları içermesi dolayısıyla kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati de bir kabahat olarak tipiklik, hukuka aykırılık, kusur başta olmak üzere genel suç/kabahat sistematiğinde incelenecektir.

I. Korunan Hukuki Değer

Korunan hukuki değer, tipik harekete karşı hukuk düzenince korunması hedeflenmekte olan ideal değerleri işaret etmektedir[291]. Tipikliğin unsurlarından birisi olan maddi konu ve korunan hukuki değer aynı şeyler olmayıp korunan hukuki değer, diğer bir deyişle hukuki konu, maddi unsurlara ilişkin bir öge değildir[292]. Korunan hukuki değer ifade edildiği üzere kabahat ile korunmak istenen değere işaret etmektedir.

---

[286] 5326 Sayılı Kabahatler Kanunu, 31.03.2005 tarihli 25772 (mükerrer) sayılı Resmi Gazete

[287] Berrin Akbulut, **Türk Ceza Kanunu ile Kabahatler Kanunu Genel Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi**, Ankara: Adalet Yayınevi, 2014, s. 217.

[288] Zeynel T. Kangal, **Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2022, s. 151, İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler,** Ankara: Seçkin Yayıncılık, 2022, s. 174. Akbulut (2014), **op.cit**. ss. 225, 227

[289] Altan Rençber, **Kabahat Genel Teorisi Açısından Vergi Kabahatleri**, İstanbul: On İki Levha Yayıncılık, 2017, s. 331

[290] Yahya Berkol Güleç, "Teoride ve Pozitif Hukukta Suç – Kabahat Ayrımı", **Kabahat Hukuku Yazıları**, Editrör: Zeynel T. Kangal, İstanbul: On İki Levha Yayıncılık, 2017, s. 64. Nur Centel, Hamide Zafer ve diğ, **Türk Ceza Hukukuna Giriş**, İstanbul: Beta Yayıncılık, 2016, s. 222

[291] Vesile Sona Evik, **Görevi Kötüye Kullanma Suçları,** İstanbul: On İki Levha Yayıncılık, 2019, s. 95. Ece Taşçı Aydemir, **Kişisel Verilerin Kaydedilmesi Suçu,** Ankara: Seçkin Hukuk, 2022, s. 45

[292] Bahri Öztürk ve Mustafa Ruhan Erdem, **Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku,** Ankara: Seçkin Yayıncılık, 2021, s. 201.

Öğretide bir görüş, kişisel verilerin güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından korunan hukuki değerin, özel hayatın gizliliği çerçevesinde kişisel verilerin korunması hakkı olduğunu kabul etmektedir[293]. Öğretide benzeri şekilde KVKK'da düzenlenen diğer bir kabahat olan aydınlatma yükümlülüğünün yerine getirilmemesi kabahati bakımından da kişisel verilerin korunması hakkı, korunan hukuki değer olarak değerlendirilmektedir[294]. Kişisel verilere ilişkin kabahatler ile aynı değerleri korumakta olan kişisel verilere ilişkin suçlar bakımından ise bir görüş korunan hukuki değerin özel hayatın gizliliği olduğunu savunmaktadır[295]. Diğer bir görüş ise özel hayatın gizliliği ve kişisel verilerin korunması hakkını birlikte kabul etmektedir[296]. Ayrıca doğrudan kişisel verilerin korunması hakkını da korunan hukuki değer olarak kabul eden bir görüş mevcuttur[297].

Kişisel verilere ilişkin kabahat ve suçlar bakımından korunan hukuki değere ilişkin farklı kabullerin bulunması, kişisel verilerin korunması hakkının Türk hukuku kapsamındaki yeri ve niteliğinden kaynaklanmaktadır[298]. Her iki hakkın niteliksel olarak

---

[293] Zeynel Kangal, **Kişisel Verilerin Ceza ve Kabahat Hukukunda Korunması**, İstanbul: On İki Levha Yayıncılık, 2019, s. 198

[294] Sümeyra Karınçu, **Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019, s. 70. Ramazan Dede, **Kişisel Verilerin Korunması Kanunu Bakımından Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, Yüksek Lisans Tezi, 2022, Altınbaş Üniversitesi, s. 118

[295] Bkz: Veli Özer Özbek, Koray Doğan ve diğ.(2022a), **Türk Ceza Hukuku Özel Hükümler**, Ankara: Seçkin Yayıncılık, 2022, s. 593, Melike Köse Aysun, **Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135),** Ankara: Seçkin Yayıncılık, 2021, 117

[296] Mahmut Koca ve İlhan Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", **D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan**, C.21, Özel Sayı, 2019, s. 75, Göçmen Uyarer, **op.cit**. s. 191, Ceren Yakışır, **Türk Ceza Kanunu'nda Kişisel Verilerin Basın Yoluyla Açıklanması Suçu**, İstanbul: On iki Levha Yayıncılık, 2019, s. 64. *"TCK'nun 136. maddesinde korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir."* Yargıtay Kararı - CGK., E. 2017/829 K. 2017/363 T. 4.7.2017 (https://www.lexpera.com.tr/ictihat/yargitay/ceza-genel-kurulu-e-2017-829-k-2017-363-t-4-7-2017 E.T. 11.03.2023).

[297] Korkmaz, **op.cit**. ss. 446, 494,

[298] Çeşitli yazarlara göre kişisel verilerin korunması hakkı özel hayatın gizliliği kapsamında bir haktır: Bkz: Faruk Bilir, "Önsöz", Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması**, Ankara: KVKK Yayınları No: 03, 2019, s. 9. Ayhan Döner, "Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 26, Sayı: 1, 2022, s. 45, Bayram Doğan, **Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı**, Ankara: Adalet Yayınevi, 2022, s. 216. Diğer görüş ise özel hayatın gizliliği ve kişisel verilerin korunması hakkı arasındaki ilişkiyi yadsımamakla birlikte kişisel verilerin korunması hakkının kendine özgü unsurlar barındırması dolayısıyla bu hakkı ayrı bir hak olarak değerlendirmektedir. Bkz: Selen Uncular, **İş İlişkisinde İşçinin Kişisel Verilerin Korunması**, Ankara: Seçkin Yayıncılık, 2018, s. 43. Küzeci (2019a), **op.cit**. s. 72

belirli farkları bulunmakla birlikte KVKK'nın amaç başlıklı birinci maddesinde kişisel verilerin korunması hakkına değinilmeksizin özel hayatın gizliliği hakkına bizatihi vurgu yapılmıştır (KVKK md. 1). Aynı şekilde kişisel verilerin korunması hakkı Anayasa'da özel hayatın gizliliği hakkı kapsamında düzenlenmiştir (Anayasa md. 20). Bu noktalardan hareketle kişisel verilerin korunması hakkının özel hayatın gizliliği hakkı kapsamında bir hak olduğu sonucuna varılmalıdır. Bu kapsamda öğretideki kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatine ilişkin olarak ifade edilen görüşe iştirak ederek kabahat bakımından korunan hukuki değerin özel hayatın gizliliği hakkı çerçevesinde kişisel verilerin korunması hakkı olduğunu kabul etmek gerekmektedir.

II. Kabahatin Maddi Unsurları

A. Fail

Fail, tipiklikte yer alan unsurları gerçekleştiren kişidir[299]. İcrai hareketle işlenen kabahatlerle aynı doğrultuda ihmali hareketle işlenen kabahatler bakımından da fail, tipikliği gerçekleştirme biçimi doğrultusunda ihmali hareketle yükümlülüğü ihlal ederek yahut neticeyi engellemeyerek tipik hareketi gerçekleştiren kişidir[300]. Ceza hukuku ile aynı şekilde kabahatler hukuku kapsamında da tüzel kişilerin hareket yeteneği kabul edilmediği için yalnızca gerçek kişiler kabahatin faili olabileceklerdir[301]. Çünkü tüzel kişilerin hareket yeteneği olmadığı için haksızlığı gerçekleştirdiğinden, iradesi olmadığı için ise kusurundan söz edilemeyecektir[302]. İhmali şekilde işlenen kabahatler bakımından da herhangi bir farklılık söz konusu değildir[303]. Dolayısıyla tüzel kişiler ihmali ve icrai

[299] Kangal (2022) **op.cit**. 163, Mahmut Koca ve İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2021, s. 114
[300] Mustafa Özen, **İdari Ceza Hukuku**, Ankara: Adalet Yayınevi, 2013, s. 82.
[301] Akbulut (2014), **op.cit**. s. 351, Ali Pehlivan, **Kabahatler Hukukunun Genel Esasları**, İstanbul: Beta Basım Yayın, 2020, s.264, Berrin Akbulut, **Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2022, s. 288, Aksi yönde: Devrim Aydın, "Tüzel Kişilerin Ceza Sorumluluğu Tartışmaları", **Uyuşmazlık Mahkemesi Dergisi**, Yıl: 5 Sayı: 10, 2017, s. 107
[302] Akbulut (2022), **op.cit**. s. 290, Ferhat Uslu ve Oğuzcan Kutkan, Kabahatler Hukukunda Tüzel Kişilerin Sorumluluğu, **D.E.Ü. Hukuk Fakültesi Dergisi**, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, s. 2812.
[303] Akbulut (2014), **loc.cit**.

hareketle işlenebilen kabahatlerde fail olamayacaklar; ancak idari yaptırımın muhatabı olabileceklerdir[304].

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati 18. maddede "*12'nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar…"* şeklinde düzenlenmiştir (KVKK md. 18/1-b). Veri güvenliğine ilişkin yükümlülükler 12. madde kapsamında ise veri sorumlusu bakımından yükümlülük olarak öngörülmüştür. Bu durumda fail, veri güvenliğine ilişkin yükümlülükleri yerine getirmeyen veri sorumlusu olacaktır.

Kabahatler herkes tarafından işlenebilmeleri ve ancak belirli kişiler tarafından işlenebilmeleri bakımından ikiye ayrılmaktadır[305]. Belirli kişiler tarafından işlenebilen kabahatler özgü kabahatlerdir. Veri güvenliğine ilişkin yükümlülükler veri sorumlusu tarafından yerine getirilmesi gereken yükümlülüklerdir. Dolayısıyla yükümlülükleri yerine getirmeyerek kabahati gerçekleştirebilecek kişinin veri sorumlusu olması dolayısıyla bu kabahatin herkes tarafından işlenememekte ve özgü bir kabahat teşkil etmektedir[306].

Veri sorumlusunun tüzel kişi olması uygulamada çok sık karşılaşılan bir durumdur. Bu durumda tipik hareketi gerçekleştiren kişi, diğer bir deyişle fail, tüzel kişi değildir[307]. Dolayısıyla tüzel kişinin hareket yeteneğinin olmaması tüzel kişinin, diğer kabahatlerde olduğu gibi veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde de faili olamaması ile sonuçlanmaktadır.

Tüzel kişilerin hareket yeteneğinin olmaması dolayısıyla tüzel kişilerin fail olarak idari yaptırıma tabi olmaması kanun koyucuyu tüzel kişi adına eylem ve işlemde bulunan

---

[304] Şerif Ahmet Öztürk, "Bankacılık Kanunu'nda Düzenlenen Kabahatler", **Kabahat Hukuku Yazıları -II**, Editör: Zeynel Kangal, İstanbul: On İki Levha Yayıncılık, 2018, s. 187
[305] Özgenç, **op.cit.,** ss. 211,212.
[306] Kangal (2019), **op.cit**. s. 202
[307] Uslu ve Kutkan, **op.cit.** s. 2815.

gerçek kişilerin fiillerine yöneltmiş[308] ve bu hususta Kabahatler Kanunu'nda özel bir hüküm öngörülmüştür. Kabahatler Kanunu 8. maddesinin 1. fıkrasına göre tüzel kişinin organı, temsilcisi ve tüzel kişinin faaliyetlerinde çerçevesinde görev alan ve bu kapsamda kabahat işleyen kişilerin işlemiş olduğu kabahatlerden dolayı tüzel kişiye de yaptırım uygulanabilmektedir (KK md. 8/1). Aynı durum gerçek kişiler bakımından da söz konusudur: Temsilcinin temsilcilik sıfatı kapsamında işlediği kabahatten temsil olunan gerçek kişi ve iş faaliyeti kapsamında çalışanın işi çerçevesinde işlediği kabahatten işveren gerçek kişi de idari yaptırıma muhatap olabilecektir (KK md. 8/2,3).

Kabahatler Kanunu'nun 8. maddesinde düzenlenen gerçek kişinin hareketi dolayısıyla tüzel kişinin veya temsil olunan yahut işveren gerçek kişinin idari yaptırıma tabi tutulması noktasında idarenin takdir yetkisi bulunmakta olup hüküm emredici değildir[309]. Ancak birçok özel düzenlemede Kabahatler Kanunu'nun aksi öngörülmüş ve hareketi gerçekleştiren gerçek kişinin değil yalnızca tüzel kişi, temsil olunan veya işveren gerçek kişinin idari yaptırıma tabi olduğu düzenlenmiştir[310]. Nitekim KVKK'da "*bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır*" denilerek yalnızca veri sorumlusun yaptırıma tabi olacağı düzenlenmiştir (KVKK md. 18/2). Bu kapsamda KVKK'da özel hüküm öngörülmüş olup fail ve veri sorumlusunun farklı kişiler olduğu durumlarda yalnızca gerçek ve özel tüzel kişi veri sorumluları yaptırıma tabi olacaktır.

Görüldüğü üzere veri sorumlusunun tüzel kişi olduğu hallerde veri sorumlusu bünyesindeki belirli bir kişi yahut kişiler bu kabahatin faili olabilecektir[311]. **Kangal** bu yetkili kişinin, işleme amaç ve vasıtalarını belirleyen ve veri kayıt sisteminden sorumlu kişi olduğunu ifade etmiştir[312]. Ancak amaç ve vasıtaları belirleme ve veri kayıt sisteminden sorumluluk, veri sorumlusunun tespiti açısından bit ölçüt olarak KVKK'da yer alıyor olmakla birlikte bu nitelikleri taşıyan kişi kabahatin tipik hareketlerini gerçekleştiren kişilerden farklı bir kişi de olabilecektir. Örneğin veri sorumlusunun

---

[308] Koray Doğan, "Tüzel Kişilerin İdari Para Cezası Sorumluluğunda İsnadiyet Sorunu", **D.E.Ü. Hukuk Fakültesi Dergisi**, Cilt: 17 Sayı: 1, 2015, s. 19
[309] Pehlivan, **loc.cit.**, Öztürk, **loc.cit**.
[310] **Ibid**.
[311] Kangal (2019), **op.cit.** s. 201
[312] **Ibid**., Akbulut (2014), **op.cit**. s. 351

çalışanı KVKK'ya aykırı olarak görevi kapsamında kişisel verileri üçüncü bir kişiye açıklamış ise bu çalışanın amaç ve vasıtaları belirleme ve veri kayıt sisteminden sorumlu olup olmadığına bakılmaksızın fail olduğunu kabul etmek gerekmektedir. Bu noktada fail olabilecek yetkili kişiyi veri sorumlusu bünyesinde ilgili veri güvenliği yükümlülüğünü yerine getirmesi gerekli olan kişi oluşturmalıdır.

Veri sorumlusu bünyesinde veri güvenliğine ilişkin yükümlülüğü alması gerekli kişi her bir hareket bakımından ayrı ayrı değerlendirilmelidir. Örneğin veri sorumlusu yönetimince teknik ve idari tedbirleri almakla görevlendirilmiş bir ya da birkaç kişinin veri sorumlusu organizasyonunda mevcut olması ile birlikte teknik ve idari tedbirler uygun güvenlik düzeyini temin edecek şekilde alınmamışsa konu hakkında görevlendirilmiş bu kişilerin fail olduğunu kabul etmek gerekmektedir. Denetim yükümlülüğünün yerine getirilmemesi ve veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi konusunda da veri sorumlusu bünyesinde yetkilendirilmiş kişi veya kişiler bulunmakta ise yine bu kişilerin fail olduğu söylenmelidir. Veri sorumlusunun organizasyonu kapsamında herhangi bir görevlendirilme yapılmaması halinde ise veri sorumlusu bünyesinde yönetim görevini sürdüren kişilerin veri güvenliğine ilişkin yükümlülükleri yerine getirme yükümlülüğü bulunması dolayısıyla bu kişilerin fail olduğu kabul edilmelidir.

Kişisel verilerin KVKK'ya aykırı şekilde açıklanması ve amacı dışında kullanılması hareketi bakımından ise kişisel verileri üçüncü kişilere aktarabilecek yahut amacı dışında kullanabilecek veri sorumlusu bünyesindeki herhangi bir kişi tipik hareketi gerçekleştirebilmektedir. Örneğin bir şirketin insan kaynakları departmanında çalışan bir kişinin işe giriş için başvuran çalışan adayına ait özgeçmişi amacı dışında kullanması halinde insan kaynaklarında çalışan bu kişi kabahat bakımından faili teşkil edecektir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin özgü bir kabahat iken veri sorumlusunun tipikliği gerçekleştirebilecek organı, temsilcisi yahut veri sorumlusu bünyesinde görev alan kişiler veri sorumlusunun işlediği kişisel veriler

bakımından veri sorumlusu niteliğini haiz değildir[313]. Aynı durum gerçek kişi işveren ve temsil edilen gerçek kişi bakımından da söz konusudur. Bu husus veri sorumlusu olmayan kişilerin özgü nitelikteki bir kabahatin hareket unsurunu gerçekleştirip gerçekleştiremeyecekleri sorusunu gündeme getirmektedir. Kabahatler Kanunu'nda bu duruma ilişkin olarak özel bir hüküm bulunmaktadır. İlgili düzenlemeye göre; organ, temsilci veya temsil edilen kişide özel bir nitelik aranması durumunda da organ veya temsilcinin davranışından dolayı sorumluluk hükümlerinin uygulanacağını düzenlenmektedir. (KK md 8/3). Öğretide bir görüş bu hükmün tüzel kişiler bakımından uygulanamayacağını ve özel niteliklerin tüzel kişiler bakımından söz konusu olamayacağını savunmaktadır[314]. Bizim de katıldığımız diğer görüş ise tüzel kişiler bakımından da özel niteliklerin olabileceği şeklindedir[315]. Bu doğrultuda veri sorumlusu olmak özel bir nitelik olarak kabul edilmeli ve Kabahatler Kanunu 8/3. maddesi tüzel kişi veri sorumlusu adına hareket eden kişiler bakımından uygulanmalıdır. Bu hükmün uygulanması neticesinde özgü faillik durumuna sahip olmayan gerçek kişinin hareketi dolayısıyla özel niteliğe sahip olan veri sorumlusuna yaptırım uygulanabilecektir.

Son olarak şu hususu belirtmek gerekmektedir: İfade edildiği üzere veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde hareket unsurunu oluşturan yükümlülüklerin tümü veri sorumluları bakımından öngörülmüştür. Yalnızca kişisel verilerin amacı dışında kullanılması ve Kanun hükümlerine aykırı olarak başkasına açıklanması bakımından veri işleyenler de yükümlüdür (KVKK md. 12/4). Bu noktada veri işleyenlerin gerçek kişi olmak kaydıyla 4. fıkra bakımından fail olarak tipikliği gerçekleştirebileceklerini kabul etmek gerekir. Ancak KVKK'nın 18. maddesinde kabahat kapsamında gerçek ve özel hukuk tüzel kişi veri sorumlularının idari para cezasına tabi olduğu düzenlenmiştir (KVKK md. 18/2). Bu nedenle kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi dolayısıyla veri işleyenler hakkında idari para cezasına hükmedilemeyecektir. Bu noktada Kabahatler Kanunu'nun 8. Maddesi uyarınca veri işleyenin tipik hareketi gerçekleştirmesi dolayısıyla veri sorumlusunun idari para cezasına tabi olup olmayacağı sorusu gündeme gelebilecektir. Veri işleyen, veri

[313] Şirket birimlerinin veri sorumlusu olmadığına ilişkin olarak bkz: Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, **op.cit**. s. 2.
[314] Bkz: Akbulut (2022), **op.cit**. s. 300
[315] Bkz: Kangal (2022), **op.cit**. s. 179

sorumlusunun organı, temsilcisi yahut çalışanı değildir. Bu nedenle veri işleyenin tipik hareketi dolayısıyla veri sorumlusunun 8. madde kapsamında bir sorumluluğu söz konusu olmamaktadır. Bununla birlikte veri sorumlusunun veri işleyenden hizmet alması durumunda da kişisel verilere ilişkin olarak teknik ve idari tedbirleri alma yükümlülüğü sona ermemektedir ve bu sebeple veri işleyenin KVKK'ya aykırı şekilde kişisel verileri açıklaması yahut amacı dışında kişisel verileri kullanması veri sorumlusunun yeterli güvenlik düzeyine ilişkin teknik ve idari tedbirleri alıp almadığı kapsamında incelenmelidir. Sonuç olarak veri işleyenin tipik hareketi işlemesi durumunda veri sorumlusunun kabahatten dolayı sorumluluğu, veri işleyenin organ veya temsilci olarak hareket etmesi dolayısıyla oluşacak bir sorumluluk kapsamında değil, bizatihi veri sorumlusunun teknik ve idari tedbirleri almaması ile sebep olduğu ihmali hareketinden dolayı gündeme gelebilecektir[316].

B. Mağdur

Mağdur, tipik hareketin gerçekleştirilmesiyle ihlal edilen menfaat yahut varlığın hamili olan kişidir[317]. Dolayısıyla korunan hukuki değer üzerinden mağdur değerlendirilmesi yapılmalıdır[318]. Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati kapsamında korunan hukuki değer özel hayatın gizliliği kapsamında kişisel verilerin korunması hakkıdır. Bu kapsamda hakkı yahut menfaati ihlal

---

[316] Bkz: **Infra**, s. 85

[317] Baş, **op.cit**. s. 669, Veli Özer Özbek, Koray Doğan ve diğ. (2022a), **Türk Ceza Hukuku Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2022, on ikinci baskı,s. 213, Hamide Zafer, **Ceza Hukuku Genel** Hükümler, İstanbul: Beta Yayıncılık, 2010, s. 114, Zeki Hafızoğulları ve Muharrem Özen, **Türk Ceza Hukuku Genel Hükümler**, Ankara: US-A Yayıncılık, s. 233, Tuğrul Katoğlu, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** 2012, 61(2), s. 661

[318] Baş, **loc.cit**. Zafer, **loc.cit.,** Katoğlu, **loc.cit**., Diğer bir görüşe göre ise mağdur kavramı maddi konunun ait olduğu kimseyi ifade etmektedir. (Bkz: M. Emin Artuk, Ahmet Gökcen ve A. Caner Yenidünya, **Ceza Hukuku Genel Hükümler,** Ankara: Adalet Yayınevi, 2015, 9. Baskı, s. 288, Özgenç, **op.cit.** s. 223, Akbulut (2020), **op.cit**. s. 159) Ancak maddi konu üzerinden mağdur kavramını açıklamak her zaman kolay olmamaktadır. Örneğin Aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinin maddi konusu aydınlatma kapsamında verilecek bilgilerdir (Kangal (2019), **op.cit**. s. 185. Katılmadığımız diğer görüşe göre ise bu kabahatin konusu kişisel veridir. Bkz: Karınçu, **op.cit.** s. 71). Kabahatin konusunun verilmesi gereken bilgi olduğunun kabulü halinde maddi konunun sahibi olan kimse tanımı üzerinden mağdurun tespiti imkansız hale gelmektedir. Ancak hukuki konu üzerinden değerlendirme yapılması halinde aydınlatma yükümlülüğü kendisine karşı yerine getirilmeyen ve bu şekilde kişisel verilerin korunması hakkı ihlal edilen ilgili kişinin mağdur olacağı rahatlıkla söylenebilecektir.

edilen kişi ise kişisel verisi işlenen kimsedir. Dolayısıyla bu kabahatin mağduru kişisel verisi işlenen kişi[319] olup bu kişi ilgili kişi olarak adlandırılmaktadır[320].

C. Konu

Konu unsuru öğretide çeşitli şekillerde tanımlanmıştır. "*Fiilden etkilenen kişi veya şey*[321]*"*, "*hareketin yöneldiği kişi veya şey*[322]", *"tehlikeye atılan veya kendisine zarar verilen şey"*[323]*, "hareketin üzerinde gerçekleştiği şey*[324]*"* konu unsuruna ilişkin olarak öğretide yer alan tanımlara örnek gösterilebilir. İhmali hareketle işlenebilen kabahat ve suçlarda da konu unsuru bakımından bir farklılık olmayıp ihmali hareketin üzerinde meydana geldiği kişi yahut şey konu unsurunu oluşturmaktadır[325]. Diğer taraftan kabahat ve suçların konusu genel olarak maddi bir varlığa sahip olsa da bazı suç ve kabahatlerde maddi varlığa sahip olmayan şey yahut bir olgu da yine konu unsurunu teşkil edebilmektedir[326].

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin konusunu işlenmiş olan kişisel verilerin oluşturduğu söylenebilecektir[327]. Bu kapsamda konu unsurunun gerçekleşebilmesi bakımından öncelikle bir kişisel verinin mevcut olması ve bu kişisel verinin işlenmiş olması gerekmektedir. İlk bölümde ifade edildiği üzere, kişisel veri "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi*" ifade etmektedir (KVKK md. 3/1-d). Buna göre konu unsurunun mevcudiyeti için öncelikle bir gerçek *kişiye* ilişkin olan, o kişiyi belirli yahut belirlenebilir kılan bir bilginin söz konusu olması gerekmektedir. Örnek olarak bir tüzel kişinin bilgilerinin talep edilmesi üzerine yapılan başvuruda Kurul, tüzel kişilere ilişkin bilgilerin kişisel veri olmaması dolayısıyla

---

[319] Kangal (2019), **op.cit**. s. 203
[320] Altındere, **op.cit**. s. 34
[321] Mahmut Koca ve İlhan Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, Ankara: Adalet Yayınevi, 2016, s. 432
[322] Hakan Hakeri, **Ceza Hukuku Genel Hükümler/Temel Bilgiler**, Ankara: Astana Yayınları, 2020, s. 120
[323] Özen (2013), **op.cit**., s. 84
[324] Özbek, Doğan ve diğ (2022a), **op.cit**. s. 214
[325] Fatih Yurtlu, **İhmali Suçlar,** Ankara: Seçkin Yayıncılık, 2022, ss. 167, 190.
[326] Berrin Akbulut, **Türk Ceza Hukuku Temel Bilgiler**, Ankara: Seçkin Yayıncılık, 2020, s. 161, ayrıca bkz: Çetin Arslan ve İhsan Baştürk, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler", **ERÜHFD**, Cilt: 8, Sayı: 2, 2013, ss. 198-199.
[327] Kangal (2019), **op.cit**. s. 203

başvuruda yapılacak herhangi bir işlem olmadığına karar vermiştir[328]. Dolayısıyla kişisel veri tanımı kapsamına girmeyen bir bilgi, konu unsuru sağlamadığı için kabahatin maddi unsurları oluşmamaktadır.

İşlenmemiş kişisel veriler kabahatin konusunu oluşturmamaktadır; çünkü KVKK'nın kapsamı işlenen kişisel veriler ile sınırlandırılmıştır (KVKK md. 2). Dolayısıyla kabahatin konu unsuru bakımından gerçekleşmesi gereken ikinci şart söz konusu kişisel verinin işlenmesi gerekliliğidir. İlk bölümde ifade edildiği üzere kişisel verilerin işlenmesi, otomatik yollarla yahut veri kayıt sisteminin parçası haline getirmek kaydıyla otomatik olmayan yollarla kişisel veri üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir (KVKK md. 3/1-e). Bu kapsamda konu unsuru bakımından kişisel verilerin işlenmesi tanımını dikkate almak gerekmektedir.

Kurul, 2019/316 sayılı kararında kan ve doku örneklerinin kişisel veri teşkil ettiğini, kan ve doku örneklerinin sınıflandırılarak muhafaza edilmesinin ise kişisel verilerin işlenmesi niteliğinde olduğu tespitinde bulunmuştur[329]. Nitekim belirli kriterlere göre sınıflandırılmış bir kayıt mekanizması veri kayıt sistemi teşkil edecektir[330]. Kişisel verileri sınıflandırarak muhafaza etmek kişisel verileri işleme niteliğinde bir işlem arz etmektedir. Kurul, bu yönde bir değerlendirmede bulunarak ilgili kararda konu unsurunun kişisel veri ve işleme faaliyeti bakımından gerçekleştiğini saptamıştır.

Kabahatin konu unsuruna ilişkin bu iki şart, teknik ve idari tedbirlerin alınmaması, denetim yükümlülüğünün yerine getirilmemesi ve KVKK'ya aykırı başkasına açıklama ve işleme amacı dışında kişisel verilerin kullanılması tipik hareketleri bakımından geçerlidir. Veri ihlalini bildirmeme hareketinde ise konu unsurunun diğer tipik hareketlerden farklı olduğu kanaatindeyiz. Veri ihlalini bildirmeme hareketinde, işlenen kişisel verilerin kanuna aykırı bir şekilde elde edilmesi üzerine bu durumun Kurul'a ve ilgilisine en kısa sürede bildirilmemesi kabahati teşkil etmektedir. Bu kapsamda tipik

---

[328] Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5423/2018-131 E.T. 04.03.2023)

[329] Kişisel Verileri Koruma Kurulu'nun 30.10.2019 tarihli ve 2019/136 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 04.03.2023)

[330] Ayrıca bkz: Uncular, **op.cit**. ss. 107,108.

hareketin gerçekleştilmemesi için belirli bilgilerin Kurul'a ve ilgilisine bildirilmesi gerekmektedir. Yukarıda ifade edildiği üzere ihmali davranışlarda hareketin konusu hareketin üzerinde meydana geldiği kişi yahut şeydir[331]. Bu kapsamda veri ihlal bildiriminin yapılmaması hareketi, ihmali olarak veri ihlal bildirimi yapılmasına konu bilgiler üzerinde meydana gelmektedir. Dolayısıyla veri ihlal bildirimi yükümlülüğünü yerine getirmeme hareketinin konusunu veri ihlal bildirimine konu bilgiler teşkil etmektedir.

D. Hareket ve Netice

Kabahatlerin oluşabilmesi için dış dünyada meydana gelmiş bir hareketin bulunması gerekmektedir[332]. Dolayısıyla hareket unsuru kabahatin temelini oluşturmaktadır[333]. Haksızlığın unsurlarının kabahatler ve suçlarda aynı olması dolayısıyla hareket, ceza hukuku ve kabahatler hukuku bakımından aynı anlama gelmektedir[334]. Bu noktada ceza hukukunda harekete ilişkin yapılan tasnif ve açıklamalar kabahatler hukuku bakımından da aynı şekilde geçerlidir.

KVKK'nın on ikinci maddesinde dört farklı hareket düzenlenmiştir. Bir kabahat düzenlemesinde birden çok hareketin belirtildiği ve herhangi birinin gerçekleşmesiyle kabahatin gerçekleştiği hallerde seçimlik hareketli kabahatten bahsetmek gerekmektedir[335]. Bu noktada seçimlik hareketlerden bir ya da birden fazlasının gerçekleşmesi önem arz etmemekte olup kabahatin bir defa gerçekleştiği kabul edilmektedir[336]. Ancak seçimlik olarak gösterilen hareketlerin aynı konu unsuruna sahip olması önem arz etmektedir. Farklı konu unsuruna sahip hareket artık seçimlik hareket teşkil etmeyecektir[337]. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından çeşitli hareketlerin öngörülmesi kabahatin seçimlik hareketli

---

331 **Supra** s. 70
332 Kangal (2021), **op.cit**. ss. 172,173 Pehlivan, **op.cit**. s. 157, Akbulut (2014), **op.cit**. s. 246
333 **Ibid** s. 248.
334 **Ibid**. s. 246.
335 Özen (2013), **op.cit**. s. 77
336 Özgenç, **op.cit**. s. 186
337 **Ibid**., Akbulut (2020), **op.cit**. s. 123 , Murat Aksan, "Başkası Yerine Ceza İnfaz Kurumuna veya Tutukevine Girme Suçu (TCK m. 291)", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 9, Sayı: 2, 2019, s. 359.

kabahat niteliğinde olduğu anlamına gelmektedir. Ancak veri ihlali bildirim yükümlülüğünü yerine getirmeme hareketinin konusu ise diğer tipik hareketlerin konusundan farklı olup bu nedenle farklı bir kabahat teşkil edecektir[338]. Nitekim Kurul'un veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi ve teknik ve idari tedbirlerin alınmaması hareketleri bakımından ayrı ayrı idari para cezasına karar vermesi de görüşümüzü destekler niteliktedir[339]. Bu kapsamda veri ihlal bildirimi yükümlülüğünün ayrı bir kabahat olarak KVKK'da düzenlenmesinin daha isabetli olacağı kanaatindeyiz.

Kabahatlerin hareket unsuru kapsamında ilgili kabahatin hangi hareketle işlenebileceği kanunlarda öngörülebileceği gibi bu konuda bir sınırlama yapılmaması da mümkündür. Kabahatin hangi hareketlerle işlenebileceğinin düzenlenmesi halinde bağlı hareketli kabahatlerden[340]; bu konuda bir belirleme yapılmaması halinde ise serbest hareketli kabahatten söz edilmelidir[341]. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından KVKK'nın 12. maddesinde hangi hareketlerle kabahatin işlenebileceği düzenlenmiştir. Bu kapsamda kabahat bağlı hareketli bir kabahattir[342].

Kabahatler, ihmal hareketle ya da icrai hareketle işlenebilmektedir. Nitekim Kabahatler Kanunu'nda kabahatlerin icrai ve ihmali hareketle işlenebileceği ancak ihmali hareketle işlenebilmesi için bu yönde bir hukuki yükümlülüğün gerekliliği açıkça düzenlenmiştir (KK. md. 7). İcrai hareket, yapılması yasak olan bir davranışın gerçekleştirilmesi ile söz konusu olmaktadır[343]. Bu kapsamda icrai hareketler aktif hareketle meydana gelmektedir[344]. İhmali hareket ise belirli bir icrai hareketi gerçekleştirmekle yükümlü iken kişinin bu davranışı gerçekleştirmemesi halinde

---

[338] Çeşitli kabahatlerde tipik hareketlerin farklı konulara sahip olması dolayısıyla seçimlik hareket olarak değerlendirilemeyeceğine ilişkin ayrıca bkz: Pehlivan, **op.cit**. s. 172

[339] Bkz: Kişisel Verileri Koruma Kurulu'nun 16.04.2020 tarihli ve 2020/286 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6763/2020-286 E.T. 05.03.2023)
Kişisel Verileri Koruma Kurulu'nun 27.04.2021 tarihli ve 2021/427 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/6981/2021-427 E.T. 05.03.2023)

[340] İsmail Yalçın, **Tüm Yönleriyle Kabahatler Hukuku**, Ankara: Seçkin Yayıncılık, 2007, birinci baskı, s. 169. Kangal (2022), **op.cit**. s. 159

[341] Yalçın, **loc.cit**., Kangal (2022), **op.cit**. s. 158, , suçlar bakımından: Özbek, Doğan ve diğ. (2022a), **op.cit**., s. 230, Rençber, **op.cit**. s. 340

[342] Kangal (2019), **op.cit**., s. 199

[343] Yalçın **op.cit**. s. 164.

[344] Akbulut (2014), **op.cit.** s. 274

gündeme gelmektedir[345]. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından ise KVKK'da dört farklı tipik hareket düzenlenmiş olup bu hareketlerden birisi icrai hareketle işlenebilmekteyken diğer üçü ihmali hareketle işlenebilmektedir. Bu konuya her bir hareket bakımından ayrıca değinilecektir.

Tipik hareketlerin değerlendirilmesi bakımından bir diğer ölçüt ise hareketin mütemadi yahut ani hareketli olup olmamasıdır. Ani hareketli kabahatler tipik hareketin icrası yahut ihmali ile tamamlanmaktadır[346]. Mütemadi hareketin mevcudiyeti halinde ise tipik hareket tamamlandıktan sonra belirli bir süre daha devam etmektedir[347]. Dolayısıyla mütemadi hareketle işlenebilen kabahatlerde kabahatin tamamlanması ile sona ermesi farklı zamanlarda gerçekleşmektedir[348]. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından ise KVKK'da yer alan tipik hareketlerden ikisi mütemadi hareket niteliğinde olup diğer ikisi ise ani hareketli kabahat niteliğindedir. Bu hususa her bir hareket açısından ayrıca değinilecektir.

Kabahatler ve suçlar tipik hareketin konu üzerinde meydana getirdiği etki durumuna göre tehlike kabahatleri/suçları ve zarar kabahatleri/suçları olmak üzere ikiye ayrılmaktadır[349]. Tipik hareketin konu unsurunu teşkil eden varlık üzerinde bir zarar meydana getirmesi beklenmekte ise bu halde zarar kabahati söz konusudur[350]. Ancak bir zararın meydana gelmesi gerekmeksizin tehlikenin varlığı yeterli kabul edilmiş ise bu halde tehlike kabahati söz konusudur. Tehlike kabahatleri ise soyut tehlike ve somut tehlike kabahatleri olarak ikiye ayrılmaktadır[351]. Somut tehlike kabahatlerinde hareketin belli somut bir tehlikeye neden olması gerekmekte iken[352] soyut tehlike kabahatlerinde ise

---

[345] Özbek, Doğan ve Bacaksız(2022a)**, op.cit**. s. 228, Özgenç, **op.cit**. s. 391
[346] Kangal (2022), **op.cit**. s. 160
[347] Kangal **loc.cit**. Akbulut (2020), **op.cit**. s. 123. "*Kesintisiz suç, hukuka aykırı durumun birden sona ermeyip zaman içinde devam etmesi ve bu devamlılığın failin iradî bir davranışına bağlı olması hâlinde söz konusu olmaktadır*." (Danıştay Kararı - 13. D., E. 2019/2694 K. 2021/1471 T. 20.4.2021 Lexpera.com.tr E.T. 20.02.2023)
[348] Akbulut (2014), **op.cit**. s. 272
[349]Özgenç, **op.cit**. s. 220, Erdem ve Öztürk **op.cit**. s. 214. Ayrıca öğretide bu konuya ilişkin olarak ikili tasnifin dışında farklı tasnifler de değerlendirilmektedir (Bkz: Mehmet Maden, "Bir Tehlike Suçu Olarak "Gürültüye Neden Olma" (TCK, m. 83) ve Tehlike Suçlarına İlişkin Genel Tespitler", **Ankara Hacı Bayram Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 18, Sayı: 1, 2021, ss. 448-453
[350] Akbulut (2014), **op.cit**. s. 398. Suçlar bakımından: Özgenç, **op.cit**. s. 221
[351] Akbulut (2014), **loc.cit**, Özen (2013), **op.cit**. s. 85
[352] Özen (2013), **loc.cit.**

düzenlenişi itibarıyla bizatihi hareketin gerçekleşmesi tehlikeli addedilmekte, kabahatin gerçekleşmesi bakımından yeterli sayılmaktadır[353]. Bu nedenle ayrıca somut bir tehlikenin gerçekleşmesi gerekmemektedir. Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde tipik hareketlerin gerçekleşmesi sonucu bir zararın meydana gelmesi gerekmediği gibi kanun koyucu ayrıca konu üzerinde somut bir tehlikenin gerçekleşmesini aramamış, hareketin meydana gelmesini başlı başına konu bakımından tehlikeli addetmiştir. Dolayısıyla kabahat tüm fıkraları bakımından bir soyut tehlike kabahatidir[354].

Netice dış dünyada tipik hareketin yarattığı değişikliktir[355]. Kabahatler bakımından kanun koyucu ayrıca bir neticenin oluşmasını arayabileceği gibi yalnızca hareketin oluşmasını da kabahatin gerçekleşmesi bakımından yeterli sayabilmektedir[356]. Kanun koyucu tarafından hareketin yanında ayrıca bir neticenin arandığı durumlarda neticeli kabahat söz konusudur[357]. Bu kapsamda netice, bir zarar yahut somut bir tehlike olabilecektir[358]. Bir neticenin ayrıca aranmadığı yalnızca hareketin gerçekleştirilmesinin kabahat bakımından yeterli sayıldığı durumlarda ise sırf hareket kabahati söz konusu olacaktır[359]. Kabahatlerin birçoğu sırf hareket kabahati şeklinde düzenlenmiştir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi kabahatini meydana getiren tipik hareketlerin hiçbirinde netice öngörülmemiştir. Bu kapsamda veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin dört tipik hareketi bakımından da netice öngörülmediği için kabahat sırf hareket kabahatidir[360].

İfade edildiği üzere veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin soyut tehlike kabahati teşkil etmekte olup ayrıca kabahatin gerçekleşmesi için

---

[353] Özen (2013), **loc.cit**. Özgenç., **loc.cit**. Akbulut (2014), **loc.cit.**

[354] Kangal (2019), **op.cit**. s. 199. Zarar suçu/kabahati ve tehlike suçu/kabahati tasnifinin konu unsuru mu yoksa korunan hukuki değer mi ölçüt alınarak yapılacağı öğretide tartışmalıdır (Uğur Ersoy, "Ceza Hukukunun Gri Alanı: Tehlike Suçları", **TAAD,** Yıl: 11 Sayı: 41, 2020, s. 33)

[355] Artuk, Gökcen ve Yenidünya, **op.cit.** s. 250, Öztürk ve Erdem, **op.cit.** s. 211

[356] Pehlivan, **op.cit**. s. 175

[357] İbrahim Tan, "Sporda Şiddete Neden Olabilecek Açıklamalarda Bulunma Kabahati", **Kabahat Hukuku Yazıları – II,** Editör: Zeynel Kangal, İstanbul: On İki Levha Yayıncılık, 2018, s, 262

[358] Akbulut (2020), **op.cit**. s. 136

[359] Tan, **loc.cit**. suçlar bakımından: Öztürk ve Erdem, **op.cit**. s. 212, Akbulut (2020), **op.cit**. s. 135

[360] Kangal (2019), **op.cit**. s. 200

herhangi netice de öngörülmemiştir. Bu kapsamda örneğin veri sorumlularının teknik ve idari tedbirleri almaması halinde doğrudan kabahat gerçekleşmektedir. Örneğin veri sorumlularının düzenli olarak kişisel veri güvenliği takibini yapmaları, bu kapsamda da veri sorumlularının düzenli olarak sızma testleri yapmaları, log kayıtlarını tutmaları, bilişim sistemlerinin düzgün şekilde çalışıp çalışmadığını kontrol edilmeleri gerekmektedir[361]. Bu yükümlülüklerin yerine getirilmemesi halinde doğrudan teknik ve idari tedbirlerin alınmaması hareketi gerçekleşmektedir. Bununla birlikte Kurul bu yükümlülüklerin yerine getirilip getirilmediği konusunda yerinde denetimler yapmamakta, idari para cezasına ancak bir veri ihlali yahut şikayet sonucu kişisel verilerin ihlale uğradığı durumlarda hükmedilmektedir.

Daha önceden ifade edildiği üzere veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde toplamda dört farklı tipik hareket söz konusudur. KVKK'nın 12. maddesinde düzenlenen bu dört tipik hareketin her birisi sırasıyla incelenecektir.

1. Uygun Güvenlik Düzeyini Temin Etmeye Yönelik Her Türlü Teknik ve İdari Tedbirin Alınmaması

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin ilk seçimlik hareketi uygun güvenlik düzeyini temin etmek için gerekli teknik ve idari tedbirlerin alınmamasıdır. Veri sorumluları kişisel veri güvenliğini sağlamaya yönelik olarak teknik ve idari tedbirleri almakla yükümlü kılınmıştır. Bu noktada kişisel verilerin güvenliğini sağlamaya yönelik olarak alınacak teknik ve idari tedbirlerin; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişimi önlemek ve kişisel verilerin muhafazasını sağlamak için yeterli güvenlik düzeyini temin etmesi gerekmektedir. Sayılan üç amaçtan herhangi birine yönelik teknik ve idari tedbirlerin alınmamış olması halinde hareket unsuru gerçekleşmiş olacaktır. Dolayısıyla teknik ve idari tedbirlerin alınmaması ihmali hareket niteliğindedir[362]. İhmali hareket gerçek ihmali hareket ve gerçek olmayan ihmali hareket şeklinde ikiye ayrılmaktadır: Gerçek ihmali hareket, hukuk normunun bir hareketin gerçekleştirilmesini düzenlediği halde ilgili

[361] Kişisel Verileri Koruma Kurumu (2018), **op.cit.** s.18
[362] Kangal (2019), **op.cit**. s. 200

hareketin gerçekleştirilmemesi ile mümkün olmaktadır[363]. Gerçek olmayan ihmali hareket ise normal halde icrai şekilde işlenebilen bir hareketin ihmali hareketle işlenebilmesini ifade etmektedir[364]. Bu kapsamda teknik ve idari tedbirlerin alınmaması hali doğrudan bir emredici normun yerine getirilmemesi şeklinde işlendiği için gerçek ihmali bir hareket teşkil etmektedir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde teknik ve idari tedbirleri alma yükümlülüğü yerine getirilmediği anda hareket gerçekleşmektedir. Ancak kabahatin sona ermesi yeterli teknik ve idari tedbirlerin alınması anına dek devam etmektedir. Dolayısıyla teknik ve idari tedbirlerin alınmaması hareketi mütemadi hareket niteliğindedir[365].

a. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik olarak teknik ve idari tedbirleri almamak

Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik olarak gerekli teknik ve idari tedbirlerin alınmaması düzenlemedeki ilk tipik harekettir. Tipik hareket kapsamında yaptırıma tabi tutulan hareket hukuka aykırı şekilde kişisel verilerin işlenmesi değil; hukuka aykırı işleme faaliyetine karşı uygun güvenlik düzeyini sağlamak için gerekli teknik ve idari tedbirlerin alınmamasıdır. Bu kapsamda kabahat, kişisel verilerin hukuka aykırı şekilde işlenmesi halinde değil, kişisel verilerin hukuka aykırı olarak işlenmesine ilişkin olarak uygun güvenlik düzeyini temin etmek için gerekli teknik ve idari tedbirlerin alınmaması halinde gerçekleşmiş olacaktır.

Bir önceki bölümde Kurul'un hukuka aykırı işlenme kavramını veri sorumlusunun organizasyonu kapsamında gerçekleşen hukuka aykırı işleme faaliyetleri açısından değerlendirdiği ifade edilmiştir[366]. Dolayısıyla Kurul'a göre teknik ve idari tedbirlerin konusunu veri sorumlusunun organizasyonu kapsamında meydana gelen hukuka aykırı

---

[363] Özbek, Doğan ve Bacaksız (2022a), **op.cit**. s. 513. Gerçek ihmali hareketlere öğretide ayrıca "saf ihmali hareket" de denmektedir. Ayrıca bkz: Ali Rıza Töngür ve Ekrem Çetintürk, **Ceza Hukuku Genel Hükümler**, Ankara: Adalet Yayınevi, 2020, birinci baskı, s. 138

[364] Özbek, Doğan ve Bacaksız (2022a), **op.cit**. s. 514 Ayrıca gerçek olmayan ihmali hareketlere ihmal suretiyle icra suçları/kabahatleri de denmektedir.

[365] Kangal (2019), **op.cit.** s. 201

[366] Bkz: **Supra**, s. 47

kişisel veri işleme faaliyetleri oluşturmaktadır. Örneğin Kurul bir kararında, özel bir sağlık kuruluşunun hasta kayıtta ilgili kişiden elde ettiği e-posta adresine ticari nitelikte bir elektronik ileti göndermesi konusunda ilgili iletişim adresine ticari elektronik ileti göndermenin herhangi bir işleme şartına dayanmamasını hukuka aykırı bir işleme faaliyeti olarak değerlendirmiş ve uygun güvenlik düzeyini temin etmek için gerekli teknik ve idari tedbirlerin alınmadığına hükmederek kuruluş hakkında idari para cezasına karar vermiştir[367].

Kişisel verilerin veri sorumlusu tarafından hukuka aykırı işlenmemesi, teknik ve idari tedbirler vasıtasıyla sağlanabilecek bir yükümlülük değildir. Nitekim teknik ve idari tedbirler, risk ve tehditlere karşı kişisel verinin gizliliği, bütünlüğü ve erişilebilirliğini sağlamak adına alınmaktadır. Kurum da teknik ve idari tedbirleri, mevcut risk ve tehditlerin belirlenmesi, siber güvenliğin temini, kişisel veriler için yedekleme yapılması gibi risk ve tehditlerin belirlenerek bu risk ve tehditlerin bertaraf edilmesi yönelik alınacak önlemlerle izah etmiştir[368]. Bu kapsamda veri sorumlusu tarafından kişisel verilerin hukuka aykırı işlenmemesi yükümlülüğü ancak veri sorumlusunun kişisel verileri hukuka uygun bir biçimde işlemesi ile gerçekleştirilebilir. Nitekim Kurul, hukuka aykırı işlemeye ilişkin yeterli teknik ve idari tedbirlerin alınması konusunda yaptığı incelemelerde gerekli teknik ve idari tedbirlerin alınıp alınmaması bakımından bir değerlendirme yapmamaktadır. Kurul, kişisel veriler hukuka aykırı bir biçimde işlenmiş ise, doğrudan teknik ve idari tedbirlerin alınmadığına ve dolayısıyla tipik hareketin oluştuğuna karar vermektedir[369]. Diğer bir ifadeyle tipik hareket adeta "*veri sorumlularının hukuka aykırı*

---

[367] "…bu kapsamda veri sorumlusu tarafından bir veri işleme şartı olmaksızın ilgili kişinin e-posta adresine reklam ve pazarlama amacıyla bildirim gönderilmesi suretiyle kişisel verisinin işlenmesi sebebiyle 6698 sayılı Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında 6698 sayılı Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına…" Kişisel Verileri Koruma Kurulu'nun 18.01.2022 tarihli 2022/31 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7292/2022-31 E.T. 05.03.2023)

[368] Kişisel Verileri Koruma Kurumu (2018), **passim.**

[369] Kurul'un çeşitli kararlarında bu durum görülmektedir. Örneğin: "…*ilgili kişilere ait kişisel verilerin veri sorumlusunca herhangi bir işleme şartına dayanmadan işlendiği, bu hususun ise veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 6698 sayılı Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan "Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne aykırılık teşkil ettiği*…". Kişisel Verileri Koruma Kurulu'nun 02.12.2021 tarihli 2021/1217 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7271/2021-1217 E.T. 05.03.2023)

şekilde kişisel veri işlemesi yasaktır" şeklinde yorumlanmaktadır. Dolayısıyla Kurul'un tipik hareket hakkındaki değerlendirmesine katılmak mümkün değildir. Hukuka aykırı kişisel verilerin işlenmesini önlemek için uygun güvenlik düzeyini sağlamak için teknik ve idari tedbirleri almama hareketi, üçüncü kişiler tarafından kişisel verilerin hukuka aykırı şekilde işlenmesi riskine karşı gerekli teknik ve idari tedbirlerin alınmaması şeklinde anlaşılmalıdır.

Kurul, fıkra bakımından getirdiği yorum dolayısıyla kişisel verilerin hukuka uygun şekilde işlenip işlenmediğini madde kapsamında değerlendirmekte ve eğer ki veri sorumlusu kişisel verileri hukuka aykırı şekilde işlemişse gerekli teknik ve idari tedbirlerin alınmaması hareketinin oluştuğuna karar vermektedir. Dolayısıyla icrai bir şekilde gerçekleştirilen bir hareket (hukuka aykırı şekilde kişisel veri işlemek) ihmali bir hareketle işlenebilen bir hareket (teknik ve idari tedbirleri almamak) kapsamında değerlendirilmektedir. Kanaatimizce Kurul'un bu şekilde bir değerlendirmede bulunması normu belirlilik ilkesi açısından tartışmalı hale getirmektedir. Kabahat teşkil eden hareketin tarafsız bir kişi tarafından açıkça anlaşılabilir olması gerekirken Kurul'un yerleşik içtihadı, ilgili normu muhatapları bakımından anlaşılabilir olmaktan çıkarmakta, normun öngörülebilirliğini kısıtlamaktadır[370].

Kurul'un tipik hareketi bu şekilde değerlendirmesi, kabahatin ilk seçimlik hareketi bakımından işleme şartlarını dikkate almayı zorunlu kılmaktadır; çünkü veri sorumlusu hukuka aykırı şekilde kişisel veri işlerse Kurul'a göre gerekli teknik ve idari tedbirleri almamış ve bu kapsamda tipik hareketi gerçekleştirmiş olacaktır. Öncelikle 5. ve 6. maddelerde yer alan kişisel verilerin işlenme şartlarına aykırılık kabahatin gerçekleşmesi ile sonuçlanmaktadır. Örneğin bir kararda, özel bir eğitim kurumunda bilişsel yetenekleri ölçen bir test için öğrencilerin özel nitelikli kişisel verileri işlenmiştir. Kurul, somut olay kapsamında özel nitelikli sağlık verilerinin açık rıza alınarak işlenmesi gerektiğini

[370] Kabahatler bakımından da her ne kadar suçlara göre daha esnek bir anlayış benimsenmiş olsa da kanunilik ilkesi geçerlidir. Bu noktada kanunilik ilkesinin bir sonucu olarak kabahat normu yaptırım ve hareket bakımından anlaşılabilir olmalıdır (Akbulut (2022) **op.cit**. s. 128).

değerlendirmiş, açık rıza almayan ve dolayısıyla işleme şartlarına uygun veri işlemeyen eğitim kurumunun gerekli teknik ve idari tedbirlerin almadığına karar vermiştir[371].

Kişisel verilerin aktarımı da işleme faaliyeti niteliğindedir. Dolayısıyla Kurul, hukuka aykırı aktarım durumlarını da teknik ve idari tedbirlerin alınmaması açısından değerlendirmektedir. Örneğin bir otomotiv şirketi pazarlama amaçlı tanıtım iletileri göndermek üzere ilgili kişilerden açık rıza almış ancak pazarlama faaliyeti için kullanılacak kişisel verileri açık rıza almaksızın yurt dışında bir bulut sunucuya aktarmıştır. Kurul ilgili aktarım faaliyetinin işleme şartlarını yerine getirmemesi ve ayrıca herhangi bir taahhüt izni olmaması dolayısıyla ilgili aktarımın hukuka aykırı bir kişisel veri işleme faaliyeti olduğunu kabul etmiştir. Bu kapsamda Kurul "*gerekli şartlar sağlanmadan kişisel verilerin yurt dışına aktarılması suretiyle hukuka aykırı bir kişisel veri işleme faaliyeti gerçekleştirildiği, bu sebeple Kanunun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen "Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek" yükümlülüğünün yerine getirilmediği kanaatine varıldığı…*" dolayısıyla idari para cezasına karar vermiştir[372]. Kararda dikkat çekici bir diğer nokta ise Kurul'un yükümlülüğü kişisel verilerin hukuka aykırı işlenmesine yönelik teknik ve idari tedbirlerin alınması şeklinde değil "*kişisel verilerin hukuka aykırı işlenmesini önlemek*" şeklinde değerlendirmesidir. Bu ifade adeta teknik ve idari tedbirlerin alınıp alınmadığının değerlendirilmediğini kişisel verilerin hukuka aykırı şekilde işlenmesini kabahat kapsamında dikkate aldığını gösterir niteliktedir.

Kişisel verilerin belli süreler sonunda silinmemesi, imha edilmemesi yahut anonim hale getirilmemesi de hukuka aykırı bir kişisel veri işleme faaliyeti teşkil etmektedir. Kurul bir kararında iş akdi sona eren kişiye ilişkin görsel ve işitsel verilerin veri

---

371 *"Veri sorumlusu eğitim kurumu tarafından ilgili kişilerin özel nitelikli kişisel veri kapsamında olan sağlık verisine ilişkin olarak; ilgili kişinin/velinin açık rızasının alınmadığı, açık rızanın aranmadığı diğer durumların da bulunmadığı gerekçesiyle Kanunun 12 inci maddesi uyarınca; kişisel verilerin hukuka aykırı olarak işlenmesinin engellenmesini teminen gerekli idari ve teknik tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendinde gereğince 50.000 TL idari para cezası uygulanmasına"* Kişisel Verileri Koruma Kurulu'nun 02.04.2020 tarihli ve 2020/255 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6894/2020-255 E.T. 05.03.2023)

372 Kişisel Verileri Koruma Kurulu'nun 22.07.2022 tarih 2020/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6790/2020-559 E.T. 12.12.2022)

sorumlusuna ait internet sitesinde iş akdinin sona ermesinden sonraki dönemde de bulunması dolayısıyla herhangi bir veri işleme şartı bulunmaksızın veri işleme faaliyetinin sürdürüldüğü değerlendirilmesinde bulunmuş ve gerekli tedbirlerin alınmadığı dolayısıyla veri sorumlusu hakkında idari para cezasına karar vermiştir[373].

Veri sorumlusu faaliyetleri kapsamında hukuka aykırı işlemenin gerçekleşip gerçekleşmediği değerlendirmesinde kişisel verilerin işlenmesine ilişkin ilkelerin özel bir yeri bulunmaktadır. Bu ilkelere uygun işleme faaliyetinde bulunulması ayrıca kişisel verilerin hukuka uygun işlenmesi bakımından gereklidir. Kurul, 2019/159 sayılı kararında spor salonu hizmeti sunan veri sorumlularının üyelerin giriş ve çıkışlarını biyometrik veri işleyerek kontrol etmesini incelemiştir. Kurul, spor salonuna giriş ve çıkışların alternatif yollarla sağlanması mümkün olmasına rağmen kontrollerin biyometrik veri işlenerek gerçekleştirilmesinin ölçülülük ilkesine aykırı bir kişisel veri işleme faaliyeti olduğunu, faaliyetin hukuka aykırı kişisel veri işleme niteliğinden olmasından ötürü veri sorumlusunun teknik ve idari tedbirleri almadığına hükmetmiş ve hakkında idari para cezasına karar vermiştir[374]. Diğer bir kararda ise bir varlık yönetim şirketinin farklı zamanlarda borçluya borca ilişkin mesaj gönderilmesinin hakkın kötüye kullanılması anlamına geldiği ve hukuka ve dürüstlük kurallarına uygun olma ilkesini ihlal ettiği değerlendirilmiştir. Bu noktadan hareketle ilkeye aykırılığın işleme faaliyetini hukuka aykırı hale getirmesi dolayısıyla Kurul, veri sorumlusunun hakkında hukuka aykırı işlemeye yönelik teknik ve idari tedbirleri almadığından bahisle idari para cezasına karar vermiştir[375].

Görüldüğü üzere işleme niteliğindeki her türlü fiilin hukuka aykırı şekilde gerçekleşmesi teknik ve idari tedbirlerin alınmaması tipik hareketi çerçevesinde değerlendirilmektedir. Veri sorumlusu tarafından yapılan hukuka aykırı işleme faaliyetlerinin 12. maddenin 1. fıkrasının (a) bendi kapsamında bu şekilde değerlendirilmesi birçok probleme yol açmaktadır. Öncelikle yukarıda bahsedildiği gibi

---

[373] Kişisel Verileri Koruma Kurulu'nun 14.05.2020 tarihli ve 2020/379 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6911/2020-379 E.T. 11.03.2023)

[374] Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/167 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6738/2020-167 E.T. 11.03.2023)

[375] Kişisel Verileri Koruma Kurulu'nun 31.05.2019 tarihli ve 2019/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5494/2019-159 E.T. 11.03.2023)

icrai bir hareket ihmali hareketle işlenebilen bir kabahat kapsamında ele alınmaktadır. Aynı zamanda hukuka aykırı işleme fiilinin, mütemadi hareket olan teknik ve idari tedbirlerin alınmaması hareketi kapsamında incelenmesi, farklı zamanlarda hukuka aykırı şekilde veri işlenmesinin tek bir hareket olarak değerlendirilmesine neden olacaktır; çünkü ihmali ve mütemadi bir hareket olan teknik ve idari tedbirlerin alınmaması hareketi idari para cezası uygulanana kadar tek bir hareket sayılmaktadır. Uygulamada bu durum ciddi olumsuz sonuçlara yol açabilecektir.

Sonuç olarak veri sorumlusunca gerçekleştirilen hukuka aykırı işleme faaliyeti kabahat olarak düzenlenmek istenmekteysebu konuda ayrıca bir kabahatin düzenlenmesi en doğru çözüm yöntemi olacaktır. Nitekim GDPR'da da kişisel veri güvenliğine ilişkin yükümlülükler ve kişisel veri işleme faaliyetinin hukuki bir şekilde gerçekleştirilmesi ayrı ayrı değerlendirilmiş ve kişisel veri işleme faaliyetinin hukuka uygunluğu kişisel veri güvenliği üzerinden yaptırıma tabi tutulmayıp ayrı bir bent olarak düzenlenmiştir. (GDPR md. 83/5-a, 83/4-a). Aynı şekilde KVKK kapsamında da hukuka aykırı şekilde kişisel veri işlenmesi faaliyetinin 18. maddeye bir kabahat olarak eklenmesi en uygun çözüm olacaktır. Bu kapsamda önerimiz "*5 ila 9 ncu maddelerinde öngörülen veri işleme şartlarına aykırı davrananlar hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar"* ibaresinin KVKK'nın 18. maddesinin 1. fıkrasına bir bent olarak eklenmesidir.

b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemeye yönelik olarak teknik ve idari tedbirleri almamak

Hukuka aykırı erişimi önlemeye yönelik gerekli teknik ve idari tedbirlerin alınmaması ise fıkra kapsamında ikinci hareketi teşkil etmektedir. Hukuka aykırı erişime yönelik tedbirlerin alınması halinde Kurul gerekli teknik ve idari tedbirlerin alınıp alınmadığını somut olayda incelemekte ve bu doğrultuda maddi unsurun gerçekleşip gerçekleşmediğine karar vermektedir. Bu kapsamda hukuka aykırı erişimi önlemeye yönelik uygun güvenlik düzeyini sağlamak için teknik ve idari tedbirlerin alınmaması hareketi, Kurul kararlarında ihmali ve mütemadi bir hareket olmasının ruhuna uygun bir şekilde değerlendirilmektedir.

Hukuka aykırı erişim yönünden gerekli tedbirlerin alınmaması durumu genellikle siber saldırılar ve diğer veri ihlali hallerinde söz konusu olmaktadır. Örneğin, 2021 yılında Yemek Sepeti'nin sunucularına yetkisiz erişim gerçekleşmiştir. Yetkisiz erişim ancak sekiz gün sonra fark edilebilmiştir. Yaklaşık olarak yirmi bir milyon kişinin kullanıcı adı, şifresi, iletişim ve adres bilgileri gibi kişisel veri niteliğindeki bilgileri ihlalden etkilenmiştir. Kurul, ihlalin sunucudaki açıktan dolayı meydana geldiğini, ihlalin neredeyse bir hafta sonra tespit edilmesinin veri sorumlusunun kusurunu gösterdiği, 28 GB boyutunda verinin dışarı aktarıldığının tespit edilememesinin kişisel veri güvenliğine ilişkin gerekli takibin yapılmadığına işaret ettiği ve böyle bir ihlalin yaşanmasının ve tespit edilememesinin olası riskleri değerlendirme noktasındaki zafiyete işaret ettiğinden bahisle gerekli teknik ve idari tedbirleri almadığına karar vermiştir[376]. Bir diğer kararda ise; e-posta üzerinden göndereceği kişisel verileri üçüncü kişilerin erişimini önlemek için şifreleyen veri sorumlusunun şikayet edilmesi üzerine Kurul, kişisel verilere hukuka aykırı erişilmesine yönelik gerekli tedbirlerin alındığını ve dolayısıyla veri sorumlusu hakkında yapılacak bir işlem olmadığına karar vermiştir[377].

Hukuka aykırı erişimin gerçekleşmiş olması teknik ve idari tedbirlerin alınmadığı anlamına gelmemektedir, değerlendirme konusu bizatihi teknik ve idari tedbirlerin alınıp alınmadığıdır. Bir ilaç şirketi güvenlik önlemlerini artırmak amacıyla farklı bir sunucuya geçiş yaparken sunucu parametrelerinin optimize edilmemesi dolayısıyla 337 çalışana ilişkin maaş bordro bilgileri sistem hatası nedeniyle yetki sahibi olmayan çalışanlara iletilmiştir. İlgili ihlal, 13 dakika geçtikten sonra saptanmış ve kısa süre içerisinde sonlandırılmıştır. İhlalin sonrasında derhal ihlalin etkisini giderecek önlemler alınmış ve Kurul'a veri ihlal bildiriminde bulunulmuştur. Kurul yaptığı inceleme sonucunda veri sorumlusunun yeterli teknik ve idari tedbirleri aldığını değerlendirerek kabahatin oluşmadığına karar vermiştir[378]. Başka bir olayda ise veri sorumlusunun platformundan eğitim alan kullanıcıların şifre bilgilerinin sehven erişimi bulunmayan kişilere açık halde bulunduğu fark edilmiştir. İhlalden yalnızca iki kişi etkilenmiş olup azami olarak sekiz

[376] Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli ve 2021/1324 sayılı Kararı (https://kvkk.gov.tr/Icerik/7168/2021-1324 E.T. 11.03.2023)
[377] Kişisel Verileri Koruma Kurulu'nun 06.05.2021 tarihli ve 2021/470 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6982/2021-470 E.T. 11.03.2023)
[378] Kişisel Verileri Koruma Kurulu'nun 15.12.2020 tarihli ve 2020/957 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7020/2020-957 E.T. 11.03.2023)

kişinin bilgilere ulaşabilmiş olabileceği kaydedilmiştir. Veri sorumlusu erişimi olabilecek kişilerden gizlilik konusunda taahhüt almış ve şifrelere maskeleme uygulamıştır. İlgili erişime açık dosya derhal erişimden kaldırılmıştır. İlgili kararda kabahat hareket unsuru bakımından oluşmadığı için idari para cezası verilmemiştir[379].

Cathay Pasific'in sunucularında gerçekleşen veri ihlali ise diğer bir karar olarak örnek gösterilebilecektir. Veri sorumlusunun bilgi sistemlerinde meydana gelen hukuka aykırı erişim hali ancak yapılan incelemeler sonucu neredeyse iki ay sonra fark edilebilmiştir. Kurul, veri ihlalinin iki ay sonra tespit edilebilmesini gerekli kontrol ve denetimlerin yapılmadığına ve siber saldırıyı yapan kişilerin şirket sunucularında yatay bir şekilde hareket ederek birçok sisteme etki etmesinin sistemin doğru yapılandırılmadığına işaret ettiğini değerlendirmiş ve bu gerekçelerden hareketle gerekli teknik ve idari tedbirlerin alınmadığına karar vermiştir[380]. Görüldüğü üzere hukuka aykırı erişimin gerçekleşmesi hareket unsurunu teşkil etmemekte olup aynı doğrultuda kabahatin gerçekleşebilmesi için hukuka aykırı erişimin söz konusu olmasına da gerek bulunmamaktadır. Kurul, teknik ve idari tedbirlerin alınıp alınmadığı noktasında değerlendirme yapmakta, alınmadığı durumda ise idari para cezasına karar vermektedir.

Teknik ve idari tedbirleri somut olayın özelliklerine göre çeşitlilik gösterebilmektedir. Öncelikle veri sorumluları teknik ve idari tedbirleri alabilmek adına mevcut risk ve tehditleri belirlemelidir. Kurul tarafından yayınlanan bir kararda, internet sitesine yoğun erişim yapılan veri sorumlusu, sitenin kopyasınının alınması sonrasında kullanıcı girişi yapan müşterilerin, diğer kullanıcıların profillerinin kopyalarına erişebildiğini fark etmiştir. Veri sorumlusu olay sonrasında maskeleme ve şifreleme tedbirlerine başvurmaya karar vermiştir. Kurul halihazırda kişisel verileri maskeleyerek yahut şifreleyerek saklaması gereken veri sorumlusunun mevcut risk ve tehditleri belirlemediği ve risk odaklı bir yaklaşım doğrultusunda hareket etmediğini değerlendirerek hakkında idari para cezasına hükmetmiştir[381].

---

[379] Kişisel Verileri Koruma Kurulu'nun 05.05.2020 tarihli ve 2020/345 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7027/2020-345 E.T. 11.03.2023)

[380] Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/144 sayılı Kararı (https://kvkk.gov.tr/Icerik/5480/2019-144 E.T. 11.03.2023)

[381] Kişisel Verileri Koruma Kurulu'nun 25.03.2021 tarihli ve 2021/311 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7001/2021-311 E.T. 12.06.2023)

Kişisel veri güvenliğinin takibinin yapılması da bir teknik ve idari tedbir olarak büyük önem arz etmektedir. Sızma testleri kişisel verilerin takibi için alınabilecek tedbirlere iyi bir örnek teşkil etmektedir. Örneğin Kurul test sunucularında veri ihlali gerçekleşen bir sigorta şirketinin yıllık olarak yaptığı sızma testlerine test sunucularını dahil etmemesini gerekli kontrollerin yapılmadığı yönünde değerlendirmiş ve veri sorumlusu nezdinde gerekli teknik ve idari tedbirlerin alınmadığına karar vermiştir[382].

Kişisel veri güvenliğine ilişkin politika ve prosedürlerin belirlenmesi ve uygulanması da önemli bir idari tedbir arz etmektedir. Veri ihlali şüphesi olmasına rağmen iki haftayı aşkın bir süre boyunca veri ihlalinin tespit edilememesi dolayısıyla Kurul, veri sorumlusunun politika ve prosedürleri iyi ve etkin şekilde hazırlamadığına ve uygulamadığına karar vermiştir. Olay kapsamında başka teknik ve idari tedbirlerin alınmadığını da tespit eden Kurul kabahatin gerçekleştiğini tespit ederek veri sorumlusu hakkında idari para cezasına karar vermiştir[383].

Veri sorumlusunun çalışanlara kişisel verilerin korunması konusunda eğitimler vermesi ve kişisel verilerin korunmasına ilişkin farkındalık kazandırması da bir idari tedbir teşkil etmektedir. Kurul, bir kararında veri sorumlusunun tüm çalışanlarına henüz kişisel verilerin korunması eğitimi vermediğini ve veri ihlalini gerçekleştiren çalışana eğitim görevi hazırlanmış olmasına rağmen çalışanca eğitimin tamamlanmadığını tespit etmiştir. Bu kapsamda Kurul veri sorumlusu hakkında, veri sorumlusunun gerekli idari tedbirleri almadığı gerekçesiyle idari para cezasına karar vermiştir[384].

Veri işleyenlerden hizmet almaları halinde veri sorumluları, veri işleyenlerin veri güvenliğine ilişkin yükümlülükleri yerine getirmelerini temin etmelidir. Bu kapsamda veri sorumluları asgari olarak kendileri tarafından alınan tedbirlerin veri işleyenler tarafından da alınmasını sağlamalıdır. Bir sigorta şirketinin acentesinde meydana gelen veri ihlali

---

[382] Kişisel Verileri Koruma Kurulu'nun 24.11.2020 tarihli ve 2020/905 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6862/2020-905 E.T. 12.06.2023)

[383] Kişisel Verileri Koruma Kurulu'nun 20.04.2021 tarihli ve 2021/407 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6993/2021-407 E.T. 12.06.2023)

[384] Kişisel Verileri Koruma Kurulu'nun 07.05.2020 tarihli ve 2020/357 sayılı Kararı (https://kvkk.gov.tr/Icerik/7014/2020-357 E.T. 12.06.2023)

sonrasında sigorta şirketinin veri işleyen acenteyi hiçbir şekilde denetlemediğini tespit eden Kurul, teknik ve idari tedbirlerin gerekli şekilde alınmadığına karar vererek kabahatin gerçekleştiğini tespit etmiştir[385].

Veri sorumlularının bir tedbir olarak ayrıca kişisel verileri ağ dışında yedeklemeleri gerekmektedir. Kurul bir kararında veri sorumlusunun zararlı yazılımlar sonucu yedek dosyalarının muhafaza edildiği sunucularının silinmesi üzerine, sunucular üzerinde gerekli kontrollerin yapılmadığı ve ağ dışında kişisel verilerin yedeklemesinin yapılmadığı gerekçeleriyle kabahatin gerçekleştiğine karar vermiştir[386].

c. Kişisel verilerin muhafazasına yönelik olarak teknik ve idari tedbirleri almamak

Kişisel verilerin muhafazası sağlamak için teknik ve idari tedbirleri almamak ise fıkra kapsamında diğer bir hareketi teşkil etmektedir. Kişisel verilerin muhafazasına ilişkin değerlendirme genel olarak veri sorumlusunun kişisel verileri üçüncü kişilerin erişimine karşı güvenliksiz şekilde bıraktığı ancak herhangi bir hukuka aykırı erişim durumun bulunmadığı durumlarda yeterli teknik ve idari tedbirlerin alınmaması bakımından gündeme gelmektedir. Kurul bir kararında, bir üniversitenin personelinin bilgi almaya yönelik olarak verdiği dilekçe karşı cevap yazısının çalıştığı birime herkese açık şekilde resmi yazı olarak iletilmesinin, kişisel verilerin muhafazasına yönelik olarak gerekli teknik ve idari tedbirlerin alınmadığını gösterdiği gerekçesiyle kabahatin gerçekleştiğine karar vermiştir[387]. Diğer bir kararda ise Kurul, veri sorumlusu banka tarafından ilgili kişiye gönderilen kredi kartının ilgili kişinin sistemdeki adresinin güncel olmaması nedeniyle yanlış bir kişiye teslim edilmesi sonucunda veri sorumlusu bankanın kişisel verilerin muhafazasına yönelik gerekli teknik ve idari tedbirleri almadığına karar vermiştir[388]. Son olarak, teknik servis olarak faaliyet gösteren veri sorumlusunun müşterilerine verdiği takip numaralarının ardışık olması dolayısıyla numaranın son hanesi

---

[385] Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/466 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6995/2020-466 E.T. 12.06.2023)

[386] Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/463 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7030/2020-463 E.T. 12.06.2023)

[387] Kişisel Verileri Koruma Kurulu'nun 05.05.2020 tarihli ve 2020/336 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6910/2020-336 E.T. 11.03.2023)

[388] Kişisel Verileri Koruma Kurulu'nun 16.01.2020 tarihli ve 2020/32 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6700/2020-32 E.T. 11.03.2023)

değiştirilerek teknik servisin diğer müşterilerinin kişisel verilerine ulaşılabilmesi konusunda Kurul, ilgili durumun gerekli teknik ve idari tedbirlerin alınmadığını gösterdiğine karar vermiş ve veri sorumlusu hakkında idari para cezası uygulamıştır[389].

2. Gerekli Denetimleri Yapmamak veya Yaptırmamak

Veri Güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin ikinci seçimlik hareketi ise KVKK'nın uygulanmasını sağlamak amacıyla veri sorumlusunun kendi kurum ve kuruluşlarında gerekli denetimlerin yapmaması yahut yaptırmamasıdır. İlgili hareket KVKK'da; "*Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır*" şeklinde düzenlenmiştir (KVKK md. 12/3) Fıkranın lafzından anlaşılacağı üzere bu seçimlik hareket de yine ihmali olarak düzenlenmiş olup[390] bu ihmali hareket gerçek ihmali hareket niteliğindedir.

İlgili yükümlülük kapsamında KVKK'da yahut diğer ikincil düzenlemelerde denetimlerin süresi yahut hangi periyotlarla yapılması gerektiği düzenlenmemiştir. Dolayısıyla denetimin gerektiği ancak yaptırılmadığı anda hareket gerçekleşmiş olmakta ve denetim yaptırılıncaya kadar ilgili hareket devam etmektedir. Bu bakımından denetim yükümlülüğünü yerine getirmeme hali mütemadi hareket niteliğindedir.

Denetim yükümlülüğünü yerine getirmenin kapsamını yalnızca veri güvenliğine ilişkin yükümlülükler oluşturmamaktadır. Nitekim ilgili hareket "*Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır*" şeklinde düzenlenmiştir (KVKK md. 12/3). Kurul daha önce andığımız bir kararında, aydınlatma metinleri mevzuata uygun olmayan ve bu konuda ilgili kişi taleplerine herhangi bir cevap vermeyen Ziraat Bankası'nın teknik ve idari tedbirleri alma ve denetimleri yapma yükümlüğü bulunan sorumlu çalışanları hakkında disiplin hükümlerine göre işlem yapılmasına karar

[389] Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli ve 2019/23 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5464/2019/52 E.T. 11.03.2023)
[390] Kangal (2019), **op.cit**. s. 208.

vermiştir[391]. Dolayısıyla yalnızca veri güvenliğine ilişkin değil, tüm KVKK hükümleri bakımından denetimlerin yaptırılmaması durumunda da hareket unsuru gerçekleşecektir.

Kurul denetim yükümlülüğünün yerine getirilmediği bazı durumlarda teknik ve idari tedbirlerin yerine getirilmediğine ilişkin değerlendirmelerde bulunmaktadır[392]. Nitekim denetim yapmak veya yaptırmak pekala aynı zamanda bir teknik ve idari tedbir olarak değerlendirilebilecektir. Kurul belirli kararlarda ise hem teknik ve idari tedbirleri alma yükümlülüğünün hem de denetim yükümlülüğünün ihlal edildiğine karar vermektedir[393]. Bununla birlikte hem denetim yükümlülüğünün ihlalinin hem de teknik ve idari tedbirlerin alınmamasının aynı kabahatin seçimlik hareketleri olmaları dolayısıyla iki hareketin birlikte mevcudiyeti ayrıca işlenmiş bir kabahat olarak değerlendirilmeyecek olup yalnızca idari para cezasının tayininde önem arz edebilecektir[394].

3. Kişisel Verileri Kanuna Aykırı Açıklamak ve Amacı Dışında Kullanmak

KVKK'nın 12. maddesinde yer alan diğer bir seçimlik hareket ise kişisel verilerin KVKK'ya aykırı açıklanması ve amacı dışında kullanılmasıdır. İlgili hareket KVKK'da "*Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder*" şeklinde düzenlenmiştir (KVKK md. 12/4). Veri güvenliğine ilişkin diğer tüm tipik hareketlerden farklı olarak bu hareket icrai şekilde gerçekleştirilebilecektir[395]. Diğer yandan, hareketin gerçekleşmesi ile birlikte hareket tamamlanmaktadır. Dolayısıyla işleme amacı dışı kullanım ve KVKK'ya aykırı başkasına açıklama hareketi, ani hareketli bir kabahattir[396].

---

[391] Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli ve 2019/122 sayılı Kararı, (https://www.kvkk.gov.tr/Icerik/5461/2019/122 E.T. 11.03.2023)

[392] Bkz: Kişisel Verileri Koruma Kurulu'nun 27.09.2019 tarihli ve 2019/254 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5535/2019-254 E.T. 11.03.2023). Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/269 sayılı Kararı (https://kvkk.gov.tr/Icerik/5534/2019-269 E.T. 11.03.2023)

[393] Bkz: Kişisel Verileri Koruma Kurulu'nun 27.08.2019 tarihli ve 2019/255 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5537/2019-255 E.T. 11.03.2023)

[394] Kangal (2022), **op.cit**. s. 160, suçlar bakımından: Akbulut (2020), **op.cit.** s. 123

[395] Kangal (2019), **op.cit**. s. 208

[396] **Ibid** s. 200

Tipik hareketin gerçekleşebilmesi ilgili fıkrada iki öncülden bahsedilmiştir. Buna göre kişisel verinin KVKK'ya aykırı şekilde başkasına açıklanması ve işleme amacı dışında kullanılması gerekmektedir. Öğretide "ve" bağlacının kullanılması tipik hareketin oluşması bağlamında iki unsurun birlikte gerçekleştirilmesi gerekip gerekmeyeceği açısından tartışılmıştır. **Kangal'**a göre "ve" bağlacının "veya" şeklinde anlaşılması gerekmektedir[397]. Nitekim hareketin çok hareketli olduğu değerlendirilmesinde bulunulması halinde aralarında doğrudan yakın bir bağlantı bulunmayan iki hareketin birlikte gerçekleştirilmesi gerekecek olup hükmün uygulanmasını ciddi şekilde kısıtlayacaktır[398].

Kurul'un bir kararı ilgili seçimlik harekete iyi bir örnek teşkil etmektedir. İlgili olayda doktor kontrolünde ilaç kullanan bir kişinin kullandığı ilaçlara ilişkin bilgi eczane tarafından bir üçüncü kişiye hiçbir işleme şartına dayanmadan açıklanmıştır. Kurul, KVKK hükümlerine aykırı olarak bir başkasına açıklama şeklinde değerlendirmiş olup veri sorumlusu hakkında idari para cezasına karar vermiştir[399].

Kurul tarafından verilen kararların incelenmesi neticesinde ise ilgili fıkranın denetim yükümlülüğünün ihlali hareketinde olduğu gibi çok dar bir uygulaması olduğu sonucuna ulaşılmaktadır. Nitekim ilgili fıkrada yer alan iki hareket de aynı zamanda hukuka aykırı işleme niteliğindedir ve Kurul hukuka aykırı işlemenin gerçekleştiği durumları 12. maddenin 1. fıkrası kapsamında hukuka aykırı işlemeyi önlemeye yönelik gerekli teknik ve idari tedbirlerin alınmaması kapsamında değerlendirmektedir. Örneğin veri sorumlusu avukat tarafından ilgili kişinin borç bilgilerinin SMS şeklinde ilgili kişinin abisine ve iş arkadaşlarına iletilmesi her ne kadar KVKK'ya aykırı bir şekilde başkasına açıklama hareketini teşkil etse dahi Kurul, ilgili hareketi hukuka aykırı işlemeyi önlemeye yönelik gerekli teknik ve idari tedbirlerin alınmaması kapsamında değerlendirmiştir[400].

---

[397] **Ibid** s. 208.
[398] **Ibid**.
[399] Kişisel Verileri Koruma Kurulu'nun 05.12.2018 tarihli ve 2018/143 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5364/2018-143 E.T. 11.03.2023)
[400] Kişisel Verileri Koruma Kurulu'nun 28.05.2020 tarihli ve 2020/429 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6778/2020-429 E.T. 11.03.2023)

4. Veri İhlalini En Kısa Sürede İlgili Kişiye ve Kişisel Verileri Koruma Kurulu'na Bildirmemek

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatini teşkil eden son hareket ise veri ihlali bildiriminin en kısa sürede yapılmamasıdır. Veri ihlal bildirimi yükümlülüğünü bildirmek KVKK'da "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir" şeklinde düzenlenmiştir (KVKK md. 12/5). Veri ihlalini bildirmeme hareketi de yine aynı şekilde ihmali şekilde gerçekleştirilebilecek olup gerçek ihmali hareket niteliğindedir. Veri ihlalinin en kısa sürede yapılması gerekmektedir. En kısa sürede yapılmaması halinde kabahat gerçekleşmekte ve tamamlanmaktadır. Bu kapsamda veri ihlalini bildirmemek ani hareketli bir kabahattir[401].

Kurul'a yapılacak bildirimin süresi veri ihlali halinin öğrenilmesinden itibaren en geç 72 saat olarak kararlaştırılmıştır[402]. Belirmek gerekir ki en kısa süre ibaresinin 72 saat olarak anlaşılması gerekliliği Kurul'un bir kararında belirtilmiştir. Kanaatimizce 72 saat ibaresinin doğrudan KVKK'da düzenlenmesi belirlilik ilkesi açısından daha isabetli bir yaklaşım olacaktır. Kurul bir kararda, veri ihlali dolayısıyla Kurul'a bildirimde bulunan veri sorumlusu hakkında veri sorumlusunun veri ihlalini 6 Ocak 2020 tarihinde tespit ettiği, 8 Ocak 2020 tarihinde Kurul'a bildirdiği ve ilgililere e-posta ile durumu aktardığı için veri ihlal bildirimi yükümlülüğüne aykırı davranmadığını tespit etmiş bu nedenle idari para cezasına karar vermemiştir[403]. Diğer bir kararda ise veri ihlal bildirimini Kurul'a 55 gün sonra ileten veri sorumlusunun bildirimi en kısa sürede yapmaması dolayısıyla hakkında idari para cezasına karar verilmiştir[404].

Veri ihlal bildirimi hem Kurul'a hem de ilgisine yapılmalıdır. Kurul'a bildirim yükümlülüğünün süresi 72 saat olarak kararlaştırılmıştır, ancak ilgili kişilere bildirim

---

401 Kangal (2019), **op.cit**. s. 200

402 Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.03.2023)

403 Kişisel Verileri Koruma Kurulu'nun 09.07.2020 tarihli ve 2020/532 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7032/2020-532 E.T. 11.03.2023)

404 Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/465 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7031/2020-465 E.T. 11.03.2023)

bakımından kesin bir süre kararlaştırılmamış olup "*makul olan en kısa sürede"* bildirimin yapılması gerekliliği değerlendirilmiştir[405]. Kurul, kendisine yapılacak veri ihlal bildirimini 2 aydan fazla süre geciktiren ve yine aynı şekilde ilgililere de bildirim yapmaya 2 ayı aşkın bir süre sonra başlayan veri sorumlusu hakkında en kısa sürede bildirimin yapılmaması nedeniyle kabahatin gerçekleşmesi bakımından idari para cezasına karar vermiştir[406].

III. Kabahatin Manevi Unsuru

Kabahatler Kanunu'nun dokuzuncu maddesine göre açıkça hüküm bulunmadıkça kabahatler hem kasten hem de taksirle işlenebilecektir (KK. md. 9). Dolayısıyla failin asgari olarak taksirle hareket etmesi kabahatin oluşabilmesi açısından bir zorunluluktur[407]. Ceza Kanunu'ndan farklı olarak kabahatler bakımından taksirle işlenebilme istisna olarak kabul edilmemiş ve kural olarak kabahatlerin taksirle de işlenebileceği kabul edilmiştir[408]. Bununla birlikte öğretide birçok kabahat bakımından kabahatin taksirle işlenebileceği düzenlenmedikçe ancak kasten işlenebileceğini savunan bir görüş de bulunmaktadır[409]. Öte yandan bazı kabahatler yapısı gereği ancak kasten işlenebilecektir[410]. Yalnızca bu halde kabahatlerin açıkça belirtilmese dahi taksirle işlenemeyeceği kanaatindeyiz.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati hem kasten hem de taksirle işlenebilecek bir kabahattir; çünkü kabahatimiz bakımından kanun koyucu herhangi bir manevi unsur belirlemesi yapmamıştır.

Fail, ilgili tipikliğin maddi unsurlarında hataya düşebilmektedir. Maddi unsurlarda hataya düşme, failin kabahatin maddi unsurlarına ilişkin bilgisi olmaması, maddi

---

405 Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.03.2023)
406 Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/143 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5479/2019-143 E.T. 11.03.2023)
407 Kangal (2022), **op.cit**. s. 185
408 Akbulut (2014), **op.cit**. s. 404, Erdener Yurtcan, **Yargıtay Kararları Işığında Kabahatler Kanunu ve Uygulaması**, İstanbul: Aristo Yayınevi, 2020, 4. baskı, s. 5
409 Yalçın, **op.cit**. s. 72
410 Kangal (2022), **op.cit**. s. 184

unsurlarını yanlış veya eksik bilmesi şeklinde gerçekleşebilecektir[411]. Bu kapsamda maddi unsurlarda hata kişinin tasavvuru ile maddi gerçeklik arasındaki uyumsuzluktur[412]. Tipikliğin maddi unsurlarına ilişkin yanılgı halinde bu hata kastı kaldırmakta ancak taksirle işlenmesi mümkün ise sorumluluk devam etmektedir.[413]. Kabahatler Kanunu 10. maddesinde hata kapsamında Türk Ceza Kanunu hükümlerinin uygulanacağı ve kasten işlenebilen kabahatler bakımından uygulanabileceği hüküm altına alınmıştır (KK md. 10). Dolayısıyla kabahatler bakımından kastı kaldıran hata düzenlemesi suçlarla aynı şekildedir[414].

Tipik hareketin unsurları deskriptif olabileceği gibi normatif de olabilmektedir[415]. Deskriptif unsurlar tipikliğin algılanabilir unsurlarını ifade etmekteyken (örneğin insan bedeni), normatif unsurlar ise norm vasıtasıyla idrak edilebilecek unsurlara işaret etmektedir[416]. Kastın gerçekleşebilmesi için failin deskriptif ve normatif unsurlara ilişkin bilgisinin bulunmasının yanı sıra failin ayrıca normatif unsurların sosyal anlamlarına ilişkin de tasavvur sahibi olması şarttır[417]. Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından örneğin kişisel veri normatif bir unsurdur. Bu noktada failin kasten tipikliği gerçekleştirebilmesi bakımından kişisel verinin bir kişiye ilişkin fonksiyonel bir bilgi olduğuna dair bilgisi olması gerekir[418].

Fail veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin maddi unsurlarında hataya düşebilecektir. Örneğin; öldüğü düşünülen ancak yaşayan bir kişiye ilişkin bilgilerin işleme amacı dışında kullanılması yahut bir kişinin kendisine ait olduğunu zannettiği bir sağlık raporunu başkaca bir kişiye aktarması hallerinde maddi unsurlara ilişkin hata söz konusudur. Ancak şunu da belirtmek gerekir ki veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati hem kast hem de taksirle işlenebilen bir kabahat olduğu için failin maddi unsurlarda hataya düşmesi halinde gerekli

---

411 Erdem ve Öztürk, **op.cit.** ss. 464,465.
412 Rençber, **op.cit**. s. 377
413 Pehlivan, **op.cit**. s. 202, Özbek, Doğan ve diğ. (2022a), **op.cit**. s. 443, Kangal (2021), **op.cit.** s. 191
414 Akbulut (2014), **op.cit**. s. 427
415 Koca ve Üzülmez (2021), **op.cit.**, s. 256, Erdem ve Öztürk, **loc.cit**.
416 Koca ve Üzülmez (2021), **loc.cit**.
417 **Ibid**.
418 Koca ve Üzülmez (2019), **op.cit**. s. 81

dikkat ve özeni göstermediği hallerde taksirli sorumluluğu devam edecektir. Ancak bu durum idari para cezasının takdiri bakımından önem arz edecektir.

IV. Hukuka Aykırılık Unsuru

Hukuka aykırılık, tipik hareketin tüm hukuk düzeniyle çelişmesi anlamına gelmektedir[419]. Kabahat teşkil eden bir tipik hareketin tüm unsurlarıyla gerçekleştirilmiş olması tipik hareketin doğrudan hukuka aykırı olduğu anlamına gelmemektedir[420]. Bu noktada bir kabahatten söz edebilmek için tipik hareketin hukuka uygunluğunu gündeme getiren herhangi bir hukuka uygunluk sebebi olmaması gerekmektedir. Dolayısıyla hukuka uygunluk sebebinin bulunması halinde artık tipik hareketin haksızlığından bahsedilemeyecektir[421].

Kabahatler Kanunu'nun 12. maddesinde, aksine hüküm bulunmadıkça Türk Ceza Kanunu'nda yer verilen hukuka uygunluk nedenlerinin kabahatler bakımından da uygulanacağı düzenlenmiştir (KK md. 12). Bu noktada kabahatler bakımından hukuka uygunluk sebepleri suçlar ile aynıdır.

Kanun hükmünün uygulanması kabahatimiz bakımından bir hukuka uygunluk sebebi teşkil edebilecektir. Öncelikle "kanun" ibaresinin yalnızca kanunla sınırlı değil yazılı hukuk kurallarını kapsayacak şekilde anlaşılması gerekmektedir[422]. Bu kapsamda bir düzenlemenin ilgili tipik hareketlerden birisini gerçekleştirmeyi gerekli kıldığı durumlarda hukuka uygunluk sebebi söz konusu olmaktadır[423]. Örneğin bir düzenleme ile bazı teknik ve idari tedbirlerin alınmaması yükümlülük haline getirilmiş ise ilgili düzenleme dolayısıyla hukuka uygunluk sebebi oluşacaktır[424]. Yahut kişisel verileri

---

[419] Pehlivan, **op.cit**. s. 220, Akbulut (2014), **op.cit.** s. 468, Özen (2013), **op.cit**. s. 95
[420] **Ibid**.
[421] Kangal (2022), **op.cit.** s. 193
[422] Akbulut (2014), **op.cit**. s. 276
[423] Kangal (2019), **op.cit**. s. 211
[424] Kişisel Verileri Koruma Kurulu'nun hukuka aykırı işleme durumunu teknik ve idari tedbirlerin alınmaması şeklinde değerlendirdiğini ifade edilmiştir. Bu noktada hukuka uygunluk sebeplerinin ne şekilde uygulanacağı ilgili düzenleme bakımından belirsizlik yaratmaktadır. Örneğin teknik ve idari tedbirlerin alınmamasına yönelik herhangi bir hukuka uygunluk sebebi yok iken kişisel verilerin hukuka aykırı işlenmesi bakımından bir hukuka uygunluk sebebinin bulunması halinde ne şekilde ilerleneceği hususu soru

kanunda açıkça öngörülmesi veya hukuki yükümlülüklerin yerine getirilmesi amacı olmaksızın işlemiş olan veri sorumlusunun bir kamu kuruluşuna bilgi vermesi gerekliliği doğmuş olabilecektir. Örneğin, bankanın bir müşterisine ilişkin olarak işlediği kişisel verileri, hesaplardaki şüpheli işlemler dolayısıyla işleme amacına aykırı olarak Mali Suçları Araştırma Komisyonu'na bildirmesi gerekebilecektir. Bu kapsamda her ne kadar işleme amacı dışında kullanma hareketi bakımından tipiklik gerçekleşmiş olsa da hukuka uygunluk sebebi bulunmaktadır.

Konuya ilişkin bir diğer örnek de sağlık verileri bakımından verilebilir. Her ne kadar sağlık bilgilerinin işlenmesi belirli istisnalar haricinde açık rızasız mümkün olamamakta ise de yaralı halde bulunan bir kişinin hayatını kurtarmak için kişinin sağlık durumuna ilişkin bilgilerin işlenilmesi ve sonrasında sağlık kuruluşuna aktarılması kapsamında hukuka uygunluk sebebi mevcuttur. Kişinin açık rızası alınmaksızın sağlık verilerinin aktarımı hukuka aykırı bir veri işleme faaliyeti teşkil etmekte ve KVKK hükümlerine aykırı şekilde açıklama hareketini meydana getirmektedir; ancak aksi durumda yardım veya bildirim yükümlülüğünün yerine getirilmemesi suçu oluşacağı ilgili aktarımın yapılması hareketi kanun hükmünün uygulanması dolayısıyla hukuka uygun olacaktır (TCK md. 98).

Hakkın kullanılması da kabahat kapsamında aynı şekilde hukuka uygunluk sebebi teşkil edebilecektir. Gerçek kişi bir tacire ilişkin kişisel verileri fatura kesmek için işleyen veri sorumlusunun, işleme amacı olarak bir hakkın tesisi, kullanılması veya korunması şartına dayanmaması durumunda, ödenmeyen faturayı yasal takip işlemleri için avukatına aktarması hareketi her ne kadar işleme amacı dışında kullanma hareketini teşkil etse de bir hakkın kullanılması kapsamında korunmalıdır. Hakkın kullanılması özellikle amaç değişikliği durumunda söz konusu olabilecektir. Bu noktada önem arz eden husus kullanılacak hakkın subjektif ve doğrudan kullanılabilen bir hak olması ve hakkın sınırları içerisinde kullanılmasıdır[425].

işaretleri taşımaktadır. Kurul'un değerlendirmesi ve Kanun'daki düzenlemeye yaptığımız eleştiriler hukuka uygunluk sebepleri bakımından da geçerlidir.

[425] Töngür ve Çetintürk, **op.cit**. ss. 202,203.

KVKK 28. maddesinde düzenlenen istisnalar da hukuka uygunluk sebepleri kapsamında uygulama alanı bulabilecektir[426]. Örnek olarak KVKK'da *"sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında"* kişisel verilerin ifade özgürlüğü kapsamında işlenmesi bir istisna olarak değerlendirilmiş olup bu hüküm özel bir hukuka uygunluk sebebi düzenlemesidir (KVKK md. 28/1-c)[427]. Bu kapsamda işlenen bir kişisel veri bakımından kabahatin maddi unsurları gerçekleşmiş olsa dahi ifade özgürlüğü kapsamında kişisel veri işlenmiş ise hukuka uygunluk sebebi bulunmaktadır. Habercilik faaliyetleri dolayısıyla işlenen kişisel veriler bu kapsamda değerlendirmeye tabi tutulmaktadır. Örnek bir kararda Kurul, cezası infaz edilmiş ilgili kişinin bir haber sitesinde işlediği suça ilişkin hakkında haber yapılması dolayısıyla yaptığı başvuruda, yapılan haberin 28. maddesi kapsamında ifade özgürlüğüne girip girmemesi bakımından değerlendirme yapmıştır. İfade özgürlüğü kapsamında kamu yararının varlığı, haberin doğruluğu ve güncelliği ve haberin öz ve biçimi arasındaki denge ölçütlerini kullanan Kurul, ilgili haber kapsamında kişisel verilerin işlenmesinin hala kamu yararı bulundurması dolayısıyla ifade özgürlüğü dolayısıyla ifade özgürlüğü kapsamında bir işleme faaliyeti gerçekleştiğine karar vermiştir[428].

İlgilinin rızasının kabahat bakımından uygulanması olası bir hukuka uygunluk sebebi teşkil etmediği kanaatindeyiz. **Kangal** ise yalnızca KVKK'ya aykırı şekilde açıklama ve amacı dışında kullanma hareketi bakımından ilgilinin rızasının bir hukuka uygunluk sebebi teşkil edebileceğini savunmaktadır[429].Kabahatin gerçek ihmali şekilde işlenebilen hareketleri bakımından iştirak ettiğimiz bu görüşe göre teknik ve idari tedbirlerin alınmaması, denetim yükümlülüğünün yerine getirilmemesi ve veri ihlal bildiriminin yapılmaması "*kurumsal tehlike tedbirleri*" olarak değerlendirilmelidir ve bu nedenle ilgilinin mutlak olarak tasarruf edebileceği bir hak ihtiva etmemektedir[430].

---

[426] Korkmaz, **op.cit.** s. 473, Göçmen Uyarer, **op.cit.** s. 273 Bu maddede sayılan hallerin doğrudan hukuka uygunluk sebebi kabul edilemeyeceğine ilişkin olarak ayrıca bkz: Börekçi, **op.cit.** s. 126

[427] **Ibid**. s. 126, 127. Börekçi ayrıca bu hükmün yerine ifade özgürlüğü ve kişisel verilerin korunması hakkının çatıştığı durumlarda iki hakkın sınırlarını çizecek bir düzenlemenin getirilmesini savunmaktadır. Yakışır, **op.cit.** s. 129

[428] Kişisel Verileri Koruma Kurulu'nun 22.05.2020 tarihli ve 2020/414 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6915/2020-414 E.T. 04.03.2023). Ayrıca bkz: Kişisel Verileri Koruma Kurulu'nun 30.09.2021 tarihli ve 2021/989 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7143/2021-989 E.T. 04.03.2023)

[429] Kangal (2019), **op.cit.** ss. 212, 213.

[430] **Ibid**. s. 213

Dolayısıyla ilgilinin rızasının bir hukuka uygunluk sebebi olması bu üç tipik hareket bakımından mümkün değildir[431]. Bununla birlikte icrai şekilde işlenen kişisel verilerin KVKK hükümlerine aykırı şekilde bir başkasına açıklanması bakımından ise ilgilinin rızası, kişisel veri işleme şartı olan açık rıza ile örtüşebilecektir[432]. Bu durumda kişinin rızasının alınması aynı zamanda bir işleme şartı olan açık rıza olarak görünüm kazanacağı için KVKK'ya aykırı şekilde işleme hareketi gerçekleşmeyecek ve kişinin rızasının alınması halinde kabahat tipiklik gereği oluşmayacaktır. Aynı durum kabahatin kişisel verilerin amacı dışında kullanılması halinde de söz konusu olacaktır. Bu nedenle KVKK'ya aykırı açıklama ve amacı dışında kullanma hareketi bakımından ilgilinin rızasının hukuka uygunluk sebebi oluşturmasının olası bir durum teşkil etmediği kanaatindeyiz.

V. Kusurluluk

Kusurluluk, haksızlığı gerçekleştiren failin kınanıp kınanamayacağı ile ilgili olup failin işlediği haksızlığa ilişkin yargıyı konu edinmektedir[433]. Bu noktada tipik ve hukuka aykırı hareketin idari para cezasına tabi tutulabilmesi için failin kusurlu olması gerekmektedir. Failin kusurunun olduğunu kabul edebilmek için ise failin algılama ve irade yeteneğine sahip olması, haksızlık bilincine sahip olması ve kusurluluğu ortadan kaldıran herhangi bir neden olmaması şarttır[434].

Kabahatler Kanunu'nun 12. maddesine göre Türk Ceza Kanunu'nda yer alan kusurluluğu ortadan kaldıran haller aksi hüküm bulunmadıkça kabahatler bakımından da uygulanacaktır (KK md. 12). Bu noktada maddede yalnızca kusurluluğu ortadan kaldıran hallere atıf yapılmış ve kusurluluğu azaltan hallere değinilmemiştir. Bu nedenle TCK'da düzenlenen kusurluluğu azaltan haller kabahatler bakımından uygulanmayacaktır[435]. Yaş küçüklüğü ve akıl hastalığı bakımından ise Kabahatler Kanunu'nda özel hüküm

---

[431] **Ibid**. s. 212

[432] Açık rızanın, ilgilinin rızasına göre özel norm teşkil ettiğine ve açık rıza ile ilgilinin rızası arasındaki farklara ilişkin olarak Bkz: Börekçi, **op.cit.** ss. 97-104.

[433] Koca ve Üzülmez (2021), **op.cit.** s. 310, Akbulut (2014), **op.cit**. s. 503

[434] Koca ve Üzülmez (2021), **op.cit**. s. 314

[435] Cengiz Otacı ve İbrahim Keskin, **Türk Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2010, s.30

öngörüldüğü için bu hususlarda aksi hüküm bulunmaktadır. Dolayısıyla yaş küçüklüğü ve akıl hastalığı durumlarında Kabahatler Kanunu'nun ilgili hükümleri uygulanacaktır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatini işleyen kişinin 15 yaşını henüz doldurmamış olması durumunda idari para cezasına hükmedilmeyecektir. Kabahatler Kanunu'nun on birinci maddesine göre 15 yaşını doldurmamış bir kişi kabahatten dolayı idari para cezasına tabi tutulmamaktadır. Ancak Kabahatler Kanunu'nda 15 ila 18 yaş arasında bir kişinin kabahati işlemesi halinde ne olacağına ilişkin herhangi bir düzenleme mevcut değildir. Bu durumun gerçekleşmesi halinde kabahatimiz bakımından idari para cezasının alt ve üst sınırı arasında tayininde dikkate alınması gerekecektir[436].

Aynı şekilde akıl hastalığı bakımından da Kabahatler Kanunu'nda özel düzenleme bulunmaktadır. Buna göre kişinin kusur yeteneğini ortadan kaldıran bir akıl hastalığı olması halinde yine idari para cezası uygulanmayacaktır (KK md. 11). Kusur yeteneğini azaltan bir akıl hastalığının olması söz konusu ise bu husus kabahatimiz bakımından idari para cezasının alt ve üst sınırı arası tayininde dikkate alınacaktır[437].

Zorunluluk hali veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati kapsamında gündeme gelebilecektir. Öncelikle zorunluluk halinin hukuki niteliğinin tartışmalı olduğu ifade edilmelidir. Buna göre zorunluluk halinin hukuki niteliğine ilişkin üç görüş bulunmaktadır. Bu görüşlerden ilki zorunluluk halinin bir hukuka uygunluk sebebi olduğunu savunmaktadır[438]. Diğer bir görüş ise zorunluluk halini bir kusurluluğu ortadan kaldıran bir neden olarak kabul etmektedir[439]. Son görüş ise zorunluluk halinin hem bir hukuka uygunluk sebebi hem de bir mazeret nedeni olduğunu değerlendirmektedir[440]. Kanaatimizce zorunluluk halini kusurluluğu ortadan kaldıran neden olarak kabul etmek gerekmektedir. Türk Ceza Kanunu 25. maddesinin gerekçesinde

---

[436] Akbulut (2022), **op.cit.**, s. 393
[437] **Ibid**. ss. 394-395
[438] İçel, **op.cit.** s. 361, Hafızoğulları ve Özen, **op.cit.** s. 247
[439] Koca ve Üzülmez (2021), **op.cit.** s. 347, Artuk, Gökçen ve diğ. **op.cit.** s. 486, Özgenç, **op.cit.** s. 492
[440] Timur Demirbaş, **Ceza Hukuku Genel Hükümler,** Ankara: Seçkin Yayıncılık, 2022, s. 323. Zeynel Kangal, **Ceza Hukukunda Zorunluluk Durumu,** Ankara: Seçkin Yayıncılık, 2010, s. 48 Zafer, **op.cit.** s. 227, Centel, Zafer ve diğ. **op.cit. s.** 318

zorunluluk halinin kusuru kaldıran bir neden olduğu açıkça ifade edilmiştir[441]. Kabahatler Kanunu'nun gerekçesinde de hukuka uygunluk nedenleri sayılmış ancak zorunluluk haline sayılanlar arasında yer verilmemiştir[442]. Öte yandan CMK'da zorunluluk halinin söz konusu olması halinde kusur olmadığı için ceza verilmesine yer olmadığına karar verilmesi gerektiği düzenlenmiştir (CMK md. 223/3-b)[443]. Bu sebeplerle zorunluluk halinin kusurluluğu kaldıran bir neden olarak değerlendirilmesi gerekir.

Zorunluluk hali, kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin KVKK'ya aykırı başkasına açıklama ve amacı dışında kullanma hareketi bakımından uygulanabilecektir. Örneğin bir doktorun HIV Pozitif olduğunu öğrendiği hastasının ailesine, kendilerine bulaşmasını önlemek adına dikkatli davranmaları için konu hakkında bilgi vermesi zorunluluk hali kapsamında değerlendirilebilecektir[444].

Kişisel veri güvenliğine ilişkin yükümlülükleri yerine getirmeme kabahati bakımından kusurluluğu kaldıran diğer haller de Kabahatler Kanunu'nun 12. maddesi gereğince uygulanması mümkündür. Bununla birlikte kabahatimiz kapsamında diğer kusurluluğu kaldıran hallerin uygulanması sık rastlanılabilecek bir durum teşkil etmemektedir.

Fail, kabahatin tüm unsurlarını bilmesine rağmen gerçekleştirdiği unsurların hukuk düzenini ihlal ettiği konusunda yanılgıya düşebilmektedir. Failin bu şekilde bir hataya düşmesi haksızlık yanılgısıdır[445]. Bu şekilde düşülen hata kaçınılmaz ise kusurluluğu

---

441 *"Maddenin ikinci fıkrasında, kusurluluğu ortadan kaldıran bir neden olarak zorunluluk (zaruret, ıztırar) hâli düzenlenmiştir"* (Türk Ceza Kanunu 25. maddesi gerekçesi (https://www.lexpera.com.tr/mevzuat/gerekceler/turk-ceza-kanunu-madde-gerekceleri/1 E.T. 05.06.2023) Öte yandan gerekçenin madde metnine dahil olmadığı dolayısıyla birçok yazar zorunluluk halinin bu sebeple kusuru kaldıran bir neden olarak kabul edilmesine karşı çıkmıştır. Bkz: Kangal (2010), **op.cit.** s. 47, Özbek, Doğan ve diğ. (2022a) **op.cit. s.** 409. Öztürk ve Erdem, **op.cit.** s. 280.

442 "*Türk Ceza Kanununun hukuka uygunluk nedenlerine ilişkin hükümleri, hakkın kullanılması, görevin yerine getirilmesi, meşru savunma ve ilgilinin rızası olmak üzere dört ana grupta toplanabilir". (*Kabahatler Kanunu 12. maddesi gerekçesi https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss840m.htm E.T. 05.06.2023)

443 Ayrıca bkz: Özbek Doğan ve diğ. **loc.cit.** CMK ve TCK gerekçesinin zorunluluk halinin hukuki niteliğini tespit etme konusunda yeterli olmayacağına ilişkin olarak bkz: Zafer, **loc.cit.**

444 Kangal (2019) **op.cit. s.** 124, 125. Kangal (2010) **op.cit.** s. 314,315

445 Akbulut (2022), **op.cit**. s. 411

ortadan kaldırmaktadır. Bir görüşe göre Kabahatler Kanunu'nun onuncu maddesi dolayısıyla kasten işlenen kabahatlerde Türk Ceza Kanunu'nun haksızlık yanılgısına ilişkin hükmü uygulama alanı bulacaktır (KK md. 10)[446]. Bizim de katıldığımız diğer görüş ise Kabahatler Kanunu 10. maddesinin kastı kaldıran hata bakımından düzenlendiğini kusurluluk bakımından ise 11. ve 12. maddelerin uygulanacağı ve dolayısıyla kabahatlerde haksızlık yanılgısı bakımından herhangi bir kast veya taksir sınırlaması olmadığı şeklindedir[447].

Öğretide katıldığımız görüşe göre kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından haksızlık yanılgısının uygulanması mümkündür ancak haksızlık yanılgısının kabahat kapsamında uygulamasının çok kısıtlı olacağı değerlendirilmektedir[448]; çünkü kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin faili genel olarak belli bir sektörde faaliyet gösteren kişiler olup bu kişilerin tabi oldukları kuralları inceleme yükümlülüğü bulunmaktadır[449]. Bu nedenle haksızlık yanılgısının kabahatimiz bakımından uygulanma ihtimali oldukça azdır.

VI. Kabahatin Özel Görünüş Biçimleri

A. Teşebbüs

Kabahatler Kanunu'nda kural olarak teşebbüsün cezalandırılmayacağı düzenlenmiştir (KK md. 13/1). Ancak özel kanunlarda kabahate teşebbüsün idari yaptırıma tabi tutulacağı düzenlenebilecek ve bu durumda kabahate teşebbüs halinde de kabahat idari yaptırıma tabi olabilecektir (KK md. 13/1).

---

[446] Kabahatler Kanunu 10. maddesinde yer alan "ancak kasten işlenen kabahatler bakımından uygulanır" ibaresi öğretide farklı şekillerde yorumlanmıştır. Örneğin bir görüş kabahatler bakımından hata hükümlerinin uygulanması için kabahatin tipik hareketinin yalnızca kasten gerçekleştirilebilmesini aramıştır (Artuk, Gökcen ve Yenidünya, **op.cit.** s. 564). Diğer görüş ise taksirle de işlenebilmesi mümkün olan kabahatin kasten işlenmesi halinde hata hükümlerinin uygulanacağını kabul etmektedir (Kangal (2019), **op.cit**. s. 213). Madde gerekçesinde de hata hükümlerinin kabahatin kasten işlendiği halde uygulanacağı ifade edilmiştir (Bkz: Atilla İnan ve İbrahim Demir, **Açıklamalı Gerekçeli Kabahatler Kanunu**, Ankara:, Türkiye Belediyeler Birliği, 2014 s. 94

[447] Akbulut (2014), **op.cit**. ss. 427, 537, Akbulut (2022), **op.cit**. s. 416

[448] Kangal (2019), **op.cit.** s. 213

[449] **Ibid**.

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinde düzenlenen üç hareket gerçek ihmali hareket şeklinde düzenlenmiştir. Gerçek ihmali şekilde işlenebilen kabahatlere teşebbüs mümkün değildir[450]. Dolayısıyla teşebbüse ilişkin özel düzenleme olup olmadığına bakılmaksızın öncelikle kabahatin gerçek ihmali şekilde işlenebilen hareketlerine teşebbüsün mümkün olmadığı söylenmelidir.

KVKK hükümlerine aykırı şekilde bir başkasına açıklama ve amacı dışında kişisel verileri kullanma hareketi ise icrai şekilde işlenebilmekte olan bir sırf hareket kabahatidir. Sırf hareket kabahatlerinde ve suçlarında da kural olarak teşebbüs kabul edilmemektedir[451]. Öte yandan hareketin bölünebilir olması halinde ise öğretide sırf hareket şeklinde işlenebilen kabahat ve suçların teşebbüse elverişli olduğu kabul edilmektedir[452]. Bu kapsamda KVKK hükümlerine aykırı şekilde başkasına açıklama ve amacı dışında kullanma hareketlerinde icra hareketinin parçalara bölünebilmesi mümkündür. Örneğin kişisel verilerin KVKK'ya aykırı şekilde posta yoluyla başkasına açıklanması sırasında postanın teslim edilememiş olması halinde sırf hareketli bir kabahate teşebbüsten söz etmek gerekmektedir. Her ne kadar kabahatin icrai şekilde işlenebilen hareketinin kısıtlı da olsa teşebbüse elverişli bir hareket olduğu söylenebilirse de yukarıda ifade edildiği üzere Kabahatler Kanunu'nda kabahatlere aksi kararlaştırılmadıkça teşebbüsün cezalandırılmayacağı düzenlenmiştir. KVKK'da ise teşebbüsün cezalandırılacağına ilişkin bir düzenleme bulunmamaktadır. Bu nedenle bu hareketin istisnai olarak teşebbüs aşamasında kalması halinde dahi yine de idari para cezasına hükmedilemeyecektir.

---

[450] Gürkan Özocak, **Türk Ceza Hukukunda Suça Teşebbüs**, Ankara: Seçkin Yayıncılık, 2018, s. 216. Pervin Aksoy İpekçioğlu, **Türk Ceza Hukukunda Suça Teşebbüs**, Ankara: Seçkin Yayıncılık, 2009, s. 191. İhmali hareketin parçalara bölünebilmesi halinde gerçek ihmali hareketin teşebbüs aşamasında kalabileceğini kabul eden bir görüş için ayrıca bkz: Yurtlu, **op.cit.**, s. 319, 320

[451] Kayıhan İçel, **Ceza Hukuku Genel** Hükümler, İstanbul: Beta Yayıncılık, 2018, s. 528. Sertaç Işıka, **Gönüllü Vazgeçme**, İstanbul: On İki Levha Yayıncılık, 2021, s. 68. Yargıtay bazı sırf hareket suçlarının teşebbüse elverişli olduğu kanaatindedir: "*6222 sayılı Kanun'un 13/2. maddesindeki suç açısından maddi unsur, esasen bulundurulması suç oluşturmamakla beraber anılan Kanun'un 12. maddesinin birinci fıkrasının (b) bendi kapsamına giren alet veya maddelerin spor alanlarına sokulmasıdır. Bu suç, sırf hareket suçu olduğundan, suçun konusunu oluşturan maddelerin spor alanlarına sokulmasıyla tamamlanmış olur. Uygulama ve öğretide kabul edildiği üzere, bu suç teşebbüse elverişli bir suçtur".* (Yargıtay Kararı - 19. CD., E. 2015/13639 K. 2016/16037 T. 20.4.2016 E.T. 03.06.2023)

[452] Zafer, **op.cit.,** s. 303, İçel, **op.cit.** 529

B. İştirak

Kabahatlere iştirak mümkün olup kabahatler bakımından iştirak eden kişiler için faillik, şeriklik gibi herhangi bir tasnif öngörülmemiştir[453]. Bu bakımdan kabahatlerde tek tip faillik sistemi benimsenmiştir[454]. Tek tip faillik sistemi kapsamında Kabahatler Kanunu'nun 14. maddesine göre kabahate iştirak eden kişiler fail gibi idari para cezasına tabi tutulmaktadırlar (KK md. 14/1). Bunun yanında kabahate iştirak için özgü fail niteliğinin bir önemi bulunmamakta olup özgü niteliğe sahip olmayan ancak kabahate iştirak eden kişiler de idari para cezasına muhatap olacaktır (KK md. 14/2). Dolayısıyla iştirak için kasten gerçekleşmiş ve hukuka aykırı bir hareketin varlığı yeterli olacaktır (KK md. 14/3).

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatine iştirak mümkündür. Örneğin veri sorumlusu bünyesinde birden çok yetkili kişinin teknik ve idari tedbirleri almama yahut diğer seçimlik hareketleri gerçekleştirme konusunda bir iştirak iradesi çerçevesinde kabahati işlemeleri halinde iştirak söz konusu olacaktır[455]. Öte yandan bir kişinin kişisel verilerin işlenme amacı dışında bir başkasına açıklanması konusunda veri sorumlusu yahut bünyesindeki yetkili kişiye yardım etmesi halinde de iştirakten söz etmek gerekir. Ancak KVKK'da idari para cezalarına ilişkin olarak özel hüküm bulunmaktadır. KVKK'nın on sekizinci maddesinin ikinci fıkrasına göre veri sorumlusu olan tüzel kişi ve gerçek kişiler idari para cezasının muhatabıdır (KVKK 18/2). Bu nedenle her ne kadar kabahate iştirak edilmiş olsa dahi bu durum veri sorumlusu olmayan kişilerin idari para cezasına tabi olması ile sonuçlanmayacaktır. Bir veri sorumlusu bünyesinde ortak bir kararla fail olarak kabahati işleyenler bakımından ise nihai olarak ilgili veri sorumlusu yaptırımın muhatabı olacaktır.

---

[453] Akbulut (2022), **op.cit**. s. 434., Kangal (2021), **op.cit.** s. 237

[454] Berrin Akbulut, "Bağlılık Kuralı", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, Sayı: 1, 2010, s. 170, dipnot 8. Rençber, **op.cit**. s. 446. Maddenin gerekçesi şu şekildedir: *"Maddenin birinci fıkrasında, kabahatlere iştirak haliyle ilgili olarak tek tip fail sistemi kabul edilmiştir. Kabahatin işlenişine iştirak eden kişiler arasında fail ve şerik (azmettiren veya yardım eden) ayırımı gözetilmemiştir"* (İnan ve Demir, **op.cit**. s. 105).

[455] Kangal (2019), **op.cit**. s. 214

İştirak bakımından önem arz edecek diğer bir husus ise ortak veri sorumlusu durumudur. Ortak veri sorumlusu kişisel verilerin işlenmesi noktasında amaç ve vasıtaların belirlenmesi konusunda birden çok veri sorumlusunun sürece ortak katılımını ifade etmektedir[456]. Ortak veri sorumlusu kavramı Kurul'un 2021/1304 sayılı ilke kararı ile Türk hukukuna dahil olmuştur[457]. Ortak veri sorumlusunu gündeme getiren olayda bazı yazılım şirketleri araç kiralama şirketlerine yazılım hizmeti ile kara liste uygulaması sunmaktadır. Araç kiralama şirketleri bu bilgileri kullanarak müşterilere araç kiralanmasına ilişkin karar sürecini gerçekleştirdikleri gibi aynı zamanda kendileri de araç kiraladıkları kişilere ilişkin bilgileri sisteme kaydetmekte ve bu bilgiler de başka araç kiralama şirketleri tarafından aynı karar alma sürecinde kullanılmaktadır[458]. Bu aktarım ve erişim sistemi ortaklaşa bir hukuka aykırı veri işleme ve aktarım ağı yaratmakta ve bu durum birden fazla kişinin ortak iradesi ile gerçekleşmektedir. Karardaki veri sorumlularının yetkilileri iştirak halinde hareket ettmektedir. Bu durumda ifadesiyle organ, temsilci yahut çalışanları iştirak halinde olan bu veri sorumlularının her biri bakımından idari para cezası uygulanması gerekmektedir[459].

C. İçtima

İçtima Kabahatler Kanunu'nun 15. maddesinde düzenlenmiş olup bu konuda KVKK'da özel bir hüküm bulunmamaktadır. Hükmün ilk fıkrası, bir hareketle birden fazla kabahatin işlenmesi halinde öngörülen en ağır idari para cezasının verilmesini; ancak başkaca yaptırımların öngörülmesi halinde ise her bir yaptırımın uygulanmasını öngörmektedir (KK md. 15/1)[460]. Bu hüküm farklı neviden fikri içtima düzenlemesidir[461]. Bu kapsamda hükmün uygulanabilmesi için fiil tekliği ve birden fazla farklı kabahatin

[456] European Data Protection Board (2021), **op.cit**. s. 19
[457] Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli 2021/1304 sayılı ilke kararı, 20 Ocak 2022 tarihli 31725 Sayılı Resmi Gazete.
[458] **Ibid**.
[459] Kangal (2019), **op.cit**. s. 215
[460] Bu kapsamda Kabahatler Hukuku bakımından da Non Bis In Dem ilkesi benimsenmiştir (Ahmet Emrah Geçer, "Vergi Ceza Hukukunda Non Bis İn İdem İlkesi", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 65 Sayı:2, 2016 s. 329)
[461] Kabahatler Kanunu kapsamında aynı neviden fikri içtima bakımından özel hüküm bulunmadıkça gerçek içtima uygulanmaktadır. (Akbulut (2022), **op.cit**. s. 485, Kangal (2019), **op.cit**. s. 256)

gerçekleştirilmesi şartları gerçekleşmelidir[462]. Örneğin, kişisel verilere hukuka aykırı erişimi önlemek için teknik ve idari tedbirlerin alınmaması suretiyle hem veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati hem de 6493 sayılı Kanun'un 27. maddesinde yer alan kabahati işlemek mümkündür. Bu şekilde bir aykırılık gündeme geldiğinde iki kabahatin tipik hareketlerinde ayniyet söz konusu olup farklı neviden fikri içtima dolayısıyla en ağır idari para cezasının uygulanması gerekmektedir.

Daha önce ifade edildiği üzere kişisel verilerin hukuka aykırı şekilde işlenmesi halinde Kurul, ihmali şekilde işlenebilen teknik ve idari tedbirlerin alınmaması tipik hareketinin gerçekleştiğini kabul etmektedir. Veri sorumlusu ise hukuka aykırı şekilde kişisel veri işlemesi sırasında aynı zamanda icrai hareketle işlenebilen bir kabahati daha gerçekleştirebilecektir. Bu durumda birisi teknik ve idari tedbirlerin alınmaması hareketi olmak üzere, bir hareketle hem icrai hareketle işlenebilen hem de ihmali hareketle gerçekleştirilebilen iki farklı kabahat gerçekleşebilecek olup farklı neviden fikri içtima ilişkisi doğup doğmayacağı sorusu gündeme gelmektedir. Öğretide ağırlıklı olarak icrai ve ihmali hareketin fiil tekliği içinde olamayacağını kabul edilmektedir[463]. Bu nedenle işlenen iki kabahat bakımından farklı neviden fikri içtima uygulama alanı bulamayacaktır. Bu durum, hukuka aykırı işleme niteliğindeki icrai hareketlerin ihmali hareketle işlenebilen bir kabahat olan teknik ve idari tedbirlerin alınmaması şeklinde değerlendirilmesinin uygulamada yol açtığı sorunlardan bir diğeri olup bir hareket gerçekleştirilmesine rağmen birden çok yaptırımın uygulanmasına yol açabilecektir.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati farklı hareketlerle işlenebilmektedir. Bu hareketlerden üçü seçimlik hareket olup birlikte işlenmeleri halinde hareketin tek bir hareket olarak kabul edilmesi gerekmektedir[464]. Yalnızca veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi hareketi, hareketin konusunun farklı olması dolayısıyla başkaca bir kabahat teşkil etmektedir. Uygulamada teknik ve idari tedbirleri almadığı için herhangi bir şekilde işlediği kişisel verilere hukuka

---

[462] Akbulut (2022), **op.cit**.. ss. 486,489. Kabahatler Kanunu'nda farklı kabahatin olmaması gerekliliği bir açıklık bulunmadığına ilişkin diğer bir görüş için bkz: Mustafa Özen,"5403 Sayılı Toprak Koruma ve Arazi Kullanımı Kanunu'nda Düzenlenen Kabahatler", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 5 Sayı: 1, 2015, s. 221

[463] Akbulut (2022), **op.cit.** s. 473

[464] Koca ve Üzülmez (2021), **op.cit**. s. 513

aykırı erişilen veri sorumluları aynı zamanda veri ihlal bildirimini de yapmamaktadır. Bu durumda hem teknik ve idari tedbirlerin alınmaması hem de veri ihlal bildiriminin yerine getirilmemesi hareketleri gerçekleşmektedir. Bu noktada biri mütemadi biri ani hareketli olmak üzere iki farklı tipik ihmali hareketin gerçekleşmesi söz konusu olmaktadır. Teknik ve idari tedbirlerin alınmaması mütemadi bir hareket teşkil ettiği için yaptırım kararına kadar tek hareket sayılması dolayısıyla kabahatlerin gerçekleşme anları bakımından eş zamanlılık söz konusu olacaktır. Bununla birlikte birbirinden bağımsız şekilde yerine getirilebilen bu iki yükümlülüğün ihlalinde birden fazla hareket ve iki farklı kabahatin varlığını kabul etmek gerekmektedir[465]. Bu nedenle gerçek içtima sonucu her bir hareket bakımından ayrı ayrı idari para cezasına hükmedilmesi gerekliliği söz konusudur. Nitekim Kurul uygulaması da bu yöndedir. Örneğin Kurul, bir kararında veri sorumlusu oyun şirketi bakımından gerekli teknik ve idari tedbirleri alınmaması ve veri ihlal bildirimini zamanında yapılmaması dolayısıyla iki ayrı idari para cezasına karar vermiştir[466].

Yukarıda da anıldığı üzere, mütemadi hareketle işlenebilen kabahatlerde hareket idari para cezasına hükmedilinceye kadar tek bir hareket olarak varsayılmaktadır (KK md. 15/2)[467]. Bu nedenle veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin teknik ve idari tedbirlerin alınmaması ve denetim yükümlülüğünün yerine getirilmemesi suretiyle işlenmesi durumunda idari para cezası verilene kadar hareket tek bir hareket olarak değerlendirilmektedir. Yemek Sepeti 18.03.2021 tarihinde siber saldırıya uğramış ve bunun sonucu olarak yirmi bir milyon kişinin kişisel verilerine hukuka aykırı şekilde erişim gerçekleşmiştir. Kurul söz konusu veri ihlalinden hareketle Yemek Sepeti'nin uygun güvenlik düzeyini sağlamaya yönelik olarak teknik ve idari

---

[465] *"Gerçek ihmali kabahatlerde, fail kendisinden istenen birçok hareket yükümlülüğünü birbirinden bağımsız, gerektiğinde arka arkaya yerine getirebildiğinde ihmali hareket çokluğu bulunmaktadır"(*Akbulut (2022), **op.cit**. s. 470*)*. Benzeri örnekler bakımından ayrıca bkz: Neslihan Coşkun, **Fikri İçtima**, Ankara: 2009, Yayımlanmamış Doktora Tezi, Gazi Üniversitesi, s. 204, Tuba Kelep Pekmez, **Ceza Muhakemesinde Fiil**, İstanbul: On İki Levha Yayıncılık, Eylül 2019, s. 202

[466] Kişisel Verileri Koruma Kurulu'nun 16.04.2020 tarihli ve 2020/286 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6763/2020-286 E.T. 12.11.2022)

[467] "*Somut olayda, aynı devir sözleşmesinden kaynaklanan fiil hakkında farklı tarihlerde yapılan tespitler üzerine mükerrer olarak idarî para cezası verildiği görülmekte olup, kesintisiz fiille işlenen kabahatlerin idarî yaptırım kararı verilinceye kadar tek fiil sayılacağı ve kesintisiz fiil ile işlenen kabahatler hakkında iki ayrı ceza verilemeyeceği sonucuna ulaşıldığından dava konusu işlemde hukuka uygunluk bulunmamaktadır. Bu itibarla, davanın reddi yolundaki İdare Mahkemesi kararında hukukî isabet bulunmamaktadır."* Danıştay Kararı - 13. D., E. 2014/1921 K. 2019/3591 T. 13.11.2019 (lexpera.com.tr E.T. 20.11.2022)

tedbirleri almadığı değerlendirmesinde bulunarak idari para cezasına hükmetmiştir[468]. Kurul'un idari para cezasına karar verdiği tarih olan 23.12.2021 tarihinden önce bir kez daha veri sorumlusu şirketin siber saldırıya uğraması gündeme gelmiştir[469]. Ancak idari para cezası verilene kadar teknik ve idari tedbirleri almamak mütemadi hareket olarak tek bir hareket sayılacağı için ancak 23.12.2021 tarihinden sonra teknik ve idari tedbirlerin veri sorumlusu şirket tarafından alınmadığı saptanmadıkça ikinci bir idari para cezasına hükmedilemeyecektir.

Hukuka aykırı işleme durumunda Kurul bu hususu teknik ve idari tedbirlerin alınmaması şeklinde değerlendirmekte ve buradan hareketle idari para cezasına tabi tutmaktadır. Teknik ve idari tedbirlerin alınmaması hareketi mütemadi niteliktedir ve dolayısıyla idari yaptırım kararına kadar tek bir hareket addedilmektedir. Bu durum uygulamada önemli sorunlara yol açabilecektir. Veri sorumlusu birden çok defa hukuka aykırı şekilde aynı kişi ya da farklı kişilerin kişisel verilerini hukuka aykırı şekilde işlese dahi Kurul bu durumu teknik ve idari tedbirlerin yerine getirilmemesi olarak değerlendirdiği için tek bir hareket sayılacak ve birden çok hareket hukuki anlamda tek bir hareketmiş gibi değerlendirilerek tek bir idari para cezasına hükmedilecektir. Bu durum uygulamada kimi veri sorumlularınca kötüye kullanılabilecektir. Hukuka aykırı işlemenin icrai ve ani hareketli bir kabahat olarak düzenlenmesi gerekmekteyken ihmali ve mütemadi bir tipik hareketin içinde değerlendirilmesinin başkaca bir olumsuz sonucu da bu noktada ortaya çıkmaktadır[470].

Veri güvenliğine ilişin yükümlülüklerin yerine getirilmemesi kabahatinin ihmali hareketlerden birisi şeklinde işlenmesi durumunda salt bir yükümlülüğün icra edilmemesi

---

[468] Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli ve 2021/1324 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7168/2021-1324 E.T. 07.11.2022)

[469] Elçin Top, "Yemek Sepeti'nden siber saldırı iddialarına ilişkin açıklama: Veri sızıntısı yok", Euronews, 16.11.2021. (https://tr.euronews.com/2021/11/16/yemek-sepeti-nden-siber-sald-r-iddialar-na-iliskin-ac-klama-veri-s-z-nt-s-yok# E.T. 07.11.2022)

[470] KVKK'da mevcut diğer bir kabahat olan aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinde her bir yükümlülüğün yerine getirilmemesi ani hareket olması bakımından başkaca bir hareket teşkil etmektedir. Hukuka aykırı işleme hareketinin de teknik ve idari tedbirlerin içerisinde değerlendirilmesi yerine aydınlatma yükümlülüğünün yerine getirilmemesi kabahati gibi düzenlenmesi gerekmektedir. Aydınlatma yükümlülüğünün yerine getirilmemesi kabahati bakımından ayrıca bkz: Bkz: Kangal (2019), **op.cit**. s. 183, karşı yönde: Karınçu **op.cit**. s. 95, Ramazan Dede, **Kişisel Verilerin Korunması Kanunu Bakımından Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Altınbaş Üniversitesi, 2022, s. 143.

şeklinde işlenmesi söz konusu olacağı için birden çok mağdur olması önem taşımayacak ve hareket tek sayılacaktır[471]. Ancak kabahatin kişisel verileri işleme amacı dışında kullanma yahut KVKK hükümlerine aykırı açıklama hareketi ile işlenmesi durumunda mağdur sayısınca hareketin olduğu kabul edilmeli ve her bir mağdur bakımından idari para cezasına hükmedilmesi gerekmektedir[472].

İçtima bakımından diğer bir durum ise tek bir hareketle hem bir suçun hem de bir kabahatin işlenmesi halidir. Bu durumda Kabahatler Kanunu gereği suçtan dolayı cezalandırılma yapılması gerekmekte olup ancak suçtan dolayı yaptırım uygulanamıyorsa failin kabahat bakımından yaptırıma tabi tutulması gerekmektedir (KK md. 15/3). Bu durum veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından söz konusu olabilecektir. Özellikle kabahatin kişisel verilerin Kanuna aykırı şekilde üçüncü bir kişiye açıklanması şeklinde işlenmesi halinde kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu söz konusu olabilecektir (TCK md. 136). Aynı şekilde ilgili hareketin bilişim sistemi üzerinden gerçekleştirilmesi durumunda "*varolan verileri başka bir yere gönderme*" tipik hareketi dolayısıyla sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu da içtima bakımından gündeme gelebilecektir (TCK md. 244/2). Bu durumda Kabahatler Kanunu gereği kişinin suçtan dolayı cezalandırılması gerekmektedir. Veri sorumlusunun tüzel kişi olduğu durumlarda gerçek kişinin suçtan dolayı cezalandırılması söz konusu olduğu zaman ise veri sorumlusu tüzel kişi bakımından idari para cezasının tayin edilip edilemeyeceği sorunu gündeme gelmektedir. Öğretide katıldığımız görüşe göre Kabahatler Kanunu'nun 15/3. maddesinin suç ve kabahat bakımından aynı kişinin yaptırıma tabi tutulacağı hallerde uygulanacağı kabul edilmelidir[473]. Çünkü normun temel olarak muhatapları farklıdır ve bu nedenle kabahat ve suçun tam olarak unsurları örtüşmemektedir[474]. Her ne kadar muhatapları farklı olsa da faillerinin aynı kişi olması halinde tipikliğin örtüştüğü gerekçesiyle bu görüş eleştirilebilirse dahi bu görüş 15. maddenin amacıyla uyum göstermektedir. Nitekim

---

[471] Kangal (2019), **op.cit**. s. 216
[472] **Ibid**.
[473] Öztürk, **op.cit.** s. 195
[474] Kangal (2022), **op.cit**. s. 268, Aynı yönde; Asuman Aytekin İnceoğlu, **Bankacılık Kanunu'nda Yer Alan Suçlar**, Yayımlanmamış Doktora Tezi, 2006, Marmara Üniversitesi, s. 190. Bankacılık suç ve kabahatleri bakımından ayrıca bkz: Fulya Eroğlu, "5411 Sayılı Bankacılık Kanununa Göre İdari Para Cezaları Sistemi" **Suç ve Ceza Dergisi**, Sayı: 4, 2009, ss. 15-18.

hüküm aynı kişinin birden fazla yaptırıma tabi tutulmasını engelleme amacındadır[475]. Dolayısıyla veri sorumlusunun tüzel kişi olduğu durumda veri sorumlusunun kabahat bakımından, gerçek kişinin ise suç bakımından yaptırıma tabi tutulabileceği kanaatindeyiz[476]. Bununla birlikte kabahat ve suçun muhatabının gerçek kişi olması halinde ise Kabahatler Kanunu 15/3 maddesi uygulama alanı bulmakta ve yalnızca suçtan dolayı yaptırım uygulanabilmektedir[477].

Kişisel verilerin hukuka aykırı işlenmesi durumunun Kurul tarafından teknik ve idari tedbirlerin alınmaması şeklinde değerlendirilerek idari para cezası yaptırıma tabi tutulduğunu, kişisel verilerin hukuka aykırı işlenmesinin teknik ve idari tedbirlerin alınmaması şeklinde ihmali hareketle işlenebilen bir kabahat kapsamında yaptırıma tabi tutulmasının uygulamada ciddi problemlere yol açtığını, bu durumun ayrı bir kabahat düzenlemesi ile korunması gerektiğini ifade edilmiştir. Kişisel verilerin hukuka aykırı şekilde işlenmesi haline ilişkin çeşitli hareketler aynı zamanda Türk Ceza Kanunu kapsamında da suç olarak düzenlenmiştir (TCK md. 135-138). Bu noktada ihmali hareketle işlenebilen bir kabahat olan teknik ve idari tedbirlerin alınmaması ve genel olarak icrai hareket olarak düzenlenmiş olan suçların tipiklik unsurları hareket bakımından örtüşmemektedir. Yukarıda ifade edildiği üzere ihmali şekilde işlenebilen hareket ve icrai şekilde işlenebilen hareketin fikri içtima ilişkisi içerisinde bulunabileceği kabul

---

[475] Nitekim gerekçede de Non Bis In Idem ilkesine atıf yapılmıştır. Bkz: İnan ve Demir, **op.cit.** s. 107.

[476] Aynı yönde: Kangal (2019), **op.cit**. s. 217

[477] Öte yandan Kurul bazı kararlarında ise içtima bakımından bu tartışmaya girmemekte doğrudan usul dolayısıyla idari para cezasının uygulanmaması yönünde karar vermektedir. Bu değerlendirmenin temelini KVKK md 15/2 oluşturmaktadır. İlgili maddeye göre şikayet ve ihbarların Dilekçe Hakkının Kullanılmasına Dair Kanun'un 6. maddesine uygun olması gerekmektedir. İlgili 6. maddeye göre yargı makamlarının görevi kapsamındaki konulara ilişkin dilekçeler dikkate alınmayacaktır. Ancak bu maddenin KVKK kapsamında şikayet ve ihbarlar bakımından bir usuli şart olması kanaatimizce uygun değildir. Çünkü Kişisel Verileri Koruma Kurulu'na yapılacak şikayet ve ihbarların ekseriyeti halihazırda yargı makamlarının gerek özel hukuk gerek ceza hukuku gerekse de idare hukuku kapsamında yargı makamlarının görevi kapsamında kalacaktır. Kişisel Verileri Koruma Kurulu örneğin bir kişinin bina içine güvenlik kamerası takması kapsamında komşusunun şikayeti bakımından şu değerlendirmede bulunmuştur: *"İlgili kişinin, komşusu hakkındaki hukuka aykırı olarak kamera taktırılması ve görüntü kaydı alınmasına ilişkin şikâyetlerinin Türk Ceza Kanunu hükümleri çerçevesinde suç unsuru barındırabileceği ve bu çerçevede 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesi dikkate alınarak söz konusu şikâyetin Kanun kapsamında değerlendirilemeyeceğine karar verilmiştir".* (Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/187 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6891/2020-187 E.T. 19.11.2022)). Ancak Kişisel Verileri Koruma Kurulu bu noktada birbiriyle çelişkili kararlar da vermektedir. Örneğin bir kararda ilgili kişiye ilaç kullanım bilgisi eczane tarafından üçüncü kişilerle paylaşılmıştır. Ancak Kurul bu noktada KVKK 15/2. maddesine göre de bir değerlendirmede bulunulmaksızın 12/4 kapsamında idari para cezasına karar verilmiştir (Kişisel Verileri Koruma Kurulu'nun 05.12.2018 tarihli ve 2018/143 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5364/2018-143 E.T. 19.11.2022)).

edilmemektedir[478]. Bu kapsamda yalnızca TCK'da düzenlenen tipik hareketlerin dördüncü fıkra kapsamında kişisel verileri KVKK hükümlerine aykırı başkasına açıklama yahut amacı dışında kullanma hareketi ile örtüşmesi mümkün olabilmektedir. Kabahatler Kanunu 15/3 maddesinin bu düzenleme kapsamında uygulanıp uygulanamayacağı bu noktada soru işaretleri barındırmaktadır. Nitekim kabahat teknik ve idari tedbirlerin alınmamasını; suçlar ise hukuka aykırı kaydetme, ele geçirme hareketlerini düzenlemektedir[479]. Bu durum gerçek kişiler bakımından gerçekleştirdiği hareket dolayısıyla iki defa yaptırıma tabi tutulma sonucunu doğurabilecektir. Nitekim Kurul TCK kapsamında suç niteliği taşıyan çeşitli durumlarda gerçek kişileri idari para cezasına tabi tutmuştur[480]. Dolayısıyla hukuka aykırı işleme durumunun teknik ve idari tedbirlerin alınmaması şeklinde değerlendirilmesi ve hareketin bu doğrultuda yaptırıma tabi tutulması uygulamada ciddi hak ihlallerine de yol açabilecektir[481].

VII. Yaptırım ve Yargılama

A. İdari Yaptırımlarda Yetkili Merci: Kişisel Verileri Koruma Kurulu

Kabahatler Kanunu'nda idari yaptırım bakımından karar verme yetkisinin, düzenleme bulunması halinde, düzenlemede öngörülen mercide olduğu; bir düzenlemenin bulunmaması halinde ise ilgili kamu kurum ve kuruluşunun en üst amirinin idari yaptırım kararı verme bakımından yetkili olduğu düzenlenmiştir (KK md. 22/1,2). Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin incelenmesi ve idari para cezasına karar verilmesi bakımından ise KVKK'da özel bir düzenleme bulunmakta olup bu konuda Kişisel Verileri Koruma Kurulu görevlidir. Nitekim KVKK'nın 22.

---

[478] Bkz: Supra, s. 103

[479] Öğretide bu durumda da Kabahatler Kanunu 15/3 maddesinin uygulanabileceğini savunan bir görüş için bkz: Aslıhan Kart ve Muammer Ketizmen, "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", **Kişisel Verileri Koruma Dergisi,** Cilt: 1 Sayı: 2**,** 2019, s. 27.

[480] Örneğin Kurul, bir kişinin ceza mahkumiyetine ilişkin bilgilerini dava dosyasına sunan gerçek kişi avukat hakkında idari para cezasına hükmetmiştir. Kişisel Verileri Koruma Kurulu'nun 02.11.2021 tarihli 2021/1111 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7266/2021-1111 E.T. 13.11.2022)

[481] Avrupa İnsan Hakları Mahkemesi alkol etkisinde araç kullanarak bir kişiye çarpan aynı fiile dayanılarak fail hakkında hem idari yaptırım hem de cezai yaptırım uygulanması dolayısıyla aynı suçtan iki kez yargılanmama ve cezalandırılmama hakkının ihlal edildiğine karar vermiştir. Bkz: Case of Franz Fischer v. Austria (Application no. 37950/97) (https://hudoc.echr.coe.int/fre-press?i=001-59475 E.T: 12.06.2023)

maddesinde şikayetleri karara bağlama ve idari yaptırımlara karar verme konusunda Kurul yetkilendirilmiştir. (KVKK md. 22/1-b,ğ).

Kurul'un idari yaptırıma karar verme yetkisi bulunmakla birlikte Kabahatler Kanunu dolayısıyla Kurul dışında başka mercilerin de idari yaptırım kararı verdiği durumlar söz konusu olabilecektir. İlk olasılık cumhuriyet savcısının idari yaptırıma karar vermesi durumudur (KK md. 23). Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından cumhuriyet savcısının idari yaptırıma karar vermesi ancak iki durumda mümkün olabilir: Öncelikle cumhuriyet savcısı tarafından yürütülen soruşturma kapsamında kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin işlendiği tespit edilebilecektir. Bu durumda cumhuriyet savcısı ilgili durumu Kurul'a bildirebileceği gibi doğrudan idari yaptırıma da karar verebilir. Dolayısıyla bu durumda cumhuriyet savcısının seçimlik yetkisi bulunmaktadır[482]. Diğer durum ise soruşturulan hareketin kabahat teşkil ettiğinin tespitidir. Bu durumda cumhuriyet savcısının seçimlik yetkisi bulunmamakta olup idari yaptırıma kendisi karar vermelidir. Bununla birlikte idari yaptırım karar verebilmesi için Kurul'ca idari yaptırım kararı verilmemiş olması gerekmektedir[483].

Kabahat bakımından mahkemenin idari yaptırıma karar verdiği durumlar da söz konusu olabilecektir. Kovuşturması yürütülen hareketin kabahat teşkil ettiğinin tespit edildiği durumlarda mahkeme Kabahatler Kanunu gereği idari yaptırıma hükmetmektedir. Kabahatler Kanunu'nda "*kovuşturma konusu*" denmesi dolayısıyla madde kapsamında kastedilen ceza mahkemeleridir[484]. Ceza mahkemesinin yaptırım uygulayabilmesi için hareketin suç teşkil etmemesi yahut suç teşkil etmesine rağmen cezai yaptırımın uygulanamaması gerekmektedir[485]. Bu durumda görevsizlik kararı verilememekte olup ceza mahkemesinin idari yaptırıma hükmetmesi gerekmektedir[486]. Mahkemenin idari yaptırıma hükmetmesi kabahatimiz bakımından özellikle KVKK hükümlerine aykırı

---

[482] Fatma Ebru Gündüz ve Hakan Gündüz, "Kabahatler Kanunu'na Göre Cumhuriyet Savcısı ve Mahkemenin İdari Yaptırım Karar Verme Yetkisi", **Adalet Dergisi,** Sayı: 68, 2022, s. 116
[483] **Ibid**. s. 117
[484] **Ibid**., Yalçın, **op.cit**. s. 116
[485] Gündüz ve Gündüz, **loc.cit.**
[486] Hüsamettin Uğur, "Kabahatler Kanunu ve 5252 Sayılı Kanun'a Göre İdari Para Cezası ve Yargıtay Uygulaması, **TBB Dergisi**, Sayı: 85, 2009, s. 216

olarak başkasına açıklamak ve işleme amacı dışında kullanmak hareketinin işlenmesi halinde olası bir durum teşkil etmektedir.

1. Yer Bakımından Uygulama ve Kişisel Verileri Koruma Kurulu'nun Yetki Alanı

Bir önceki bölümde kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından idari yaptırıma karar verme yetkisinin Kişisel Verileri Koruma Kurulu'nda olduğu ifade edilmiştir. Kurul'un bu yetkisi kabahatin yer bakımından uygulaması ile sınırlıdır. Dolayısıyla kabahatin işlendiği yerin ve kabahatin yer bakımından uygulanma alanının tespiti büyük önem arz etmektedir. Bu şekilde Kurul'un yetkisi de saptanmış olacaktır.

Kabahatler Kanunu'nun uygulanmasına ilişkin olarak, Kabahatler Kanunu'nda kanunlarda hüküm bulunmadığı durumlarda kabahatler bakımından Türk Ceza Kanunu'nun yer bakımından uygulanmasına ilişkin olarak 8. maddesinin uygulanacağı düzenlenmiştir (KK md. 6). KVKK'da ise her ne kadar kişi, zaman ve konu bakımından uygulama alanı düzenlenmiş ise de yer bakımından uygulamaya ilişkin olarak herhangi bir hüküm öngörülmemiştir. Bu husus KVKK bakımından bir eksiklik arz etmektedir[487]. KVKK'da ayrıca bir hüküm bulunmaması ve Kabahatler Kanunu'nun 8. maddesi nedeniyle kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati açısından Türk Ceza Kanunu'nun yer bakımından uygulanmasına ilişkin hüküm uygulama alanı bulacaktır.

Türk Ceza Kanunu'na göre suç bakımından Türk kanunlarının uygulanabilmesi için suçun Türkiye'de işlenmesi gerekmektedir (TCK md. 8). Bir suçun Türkiye'de işlendiğinin kabulü için ise suçun kısmen yahut tamamen Türkiye'de işlenmesi gereklidir, ayrıca neticesi Türkiye'de gerçekleşen suçlar da Türkiye'de işlenmiş sayılmaktadır (TCK md. 8).

[487] Aynı yönde: Kama Işık, **op.cit**. s. 238

Suçun işlendiği yer bakımından maddi unsurun gerçekleştiği yer önem arz etmektedir[488]. Bu kapsamda kabahatimiz bakımından dört tipik hareketin özellikleri kapsamında maddi unsurların nerede gerçekleştiğinin tespiti gerekmektedir. Soyut tehlike suçları/kabahatleri bakımından suçun/kabahatin gerçekleşme yeri, hareketin herhangi bir neticesi de olmaması dolayısıyla, hareketin gerçekleştiği yerdir[489]. İhmali hareketin gerçekleşme yerinin ise icrai harekette bulunulması gereken yer olduğu kabul edilmektedir[490]. Diğer yandan mütemadi suç ve kabahatlerde temadi hareketlerinin bir kısmı Türkiye'de gerçekleşmiş ise suç ve kabahat Türkiye'de gerçekleşmiş kabul edilmektedir[491]. Ayrıca seçimlik hareketli suç ve kabahatlerde seçimlik hareketlerden birisinin Türkiye'de gerçekleşmesi durumunda suçun/kabahatin Türkiye'de de işlendiğini kabul etmek gerekmektedir[492].

İnternet üzerinde gerçekleşen haksız hareketlerde kabahatlerin işlendiği yer hareketin niteliğine göre tespit edilecektir. İnternet üzerinde gerçekleşen suçlar dahil olmak üzere kabahatin sırf hareket kabahati olması halinde hareketin gerçekleşme yeri kabahatin gerçekleştiği yerdir[493]. Hareketin gerçekleştiği yer bakımından ise öğretide veri girişinin Türkiye'den yapılması yahut hedef sunucunun Türkiye'de bulunması halinde kabahat Türkiye'de işlenmiş kabul edilmektedir[494].

---

[488] Demirbaş, **op.cit.,** s. 159

[489] Zafer, **op.cit**. s. 452, Akbulut (2020), **op.cit.** s. 65. Centel, Zafer ve diğ, **op.cit.**, s. 152. Neticenin de değerlendirildiği bir Yargıtay kararı için ayrıca bkz: (https://www.lexpera.com.tr/ictihat/yargitay/19-ceza-dairesi-e-2018-2119-k-2018-5852-t-9-5-2018 E.T. 08.02.2023) Konu hakkındaki tartışmalar için ayrıca bkz: Murat Ceyhan, **Ceza Hukukunda Netice**, İstanbul: On İki Levha Yayıncılık, 2022, s. 269, Erdem ve Öztürk, **op.cit**. s. 83, 2

[490] Zafer, **loc.cit**. Zafer ayrıca ihmali suçlar bakımından neticesi tipiklikte mevcut suçlar bakımından ayrıca suçun işlendiği yerin farklılık gösterebileceğini değerlendirmiştir. Burada kastedilen neticenin gerçekleştiği yerde de suçun işlenmiş sayılacağıdır. Mehmet Tan, **Türk Ceza Kanunu Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2011, s. 255, Özbek, Doğan ve diğ, (2022a), **op.cit**. s. 144. Centel, Zafer ve diğ, **op.cit.** s. 153 İhmali hareket bakımından ihmalin ve sonucun gerçekleştiği yer görüşü için ayrıca bkz: Hasan Gerçeker, **Yorumlu & Uygulamalı Türk Ceza Kanunu**, Ankara: Seçkin Yayıncılık, 2020, s. 188. Mustafa Serhat Kaşıkara, "Kabahatler Kanunu'nun Yer ve Zaman Bakımından Uygulanması", **Kabahatler Hukuku Yazıları – I,** Editör: Zeynel T. Kangal, İstanbul, On İki Levha Yayıncılık, 2017, s. 119.

[491] Zafer, **loc.cit.**, Akbulut(2020), **loc.cit.**, Gerçeker, **loc.cit.** Artuk, Gökçen ve diğ, **op.cit.** s. 1060, Mütemadi hareketin nerede gerçekleştiğine ilişkin tartışmalar için ayrıca bkz: Centel, Zafer ve diğ, **loc.cit.** Ayrıca neticeyi de değerlendiren görüş için bkz: İzzet Erdem Külçür, **Ceza Hukukunda Yer Bakımından Uygulama**, İstanbul: On İki Levha Yayıncılık, 2017, s. 193. Kaşıkara, **op.cit.** s. 118.

[492] Özgenç, **op.cit.** s. 1084, Yalnızca seçimlik hareketlerden ilkinin gerçekleştirildiği ülkeyi yetkili kabul eden görüş için bkz: Kayıhan İçel, **Ceza Hukuku Genel Hükümler**, İstanbul: Beta Yayıncılık, 2018, s. 165

[493] Akbulut(2020), **op.cit.** 67. Kaşıkara, **op.cit.** s. 117

[494] Özbek, Doğan ve diğ, (2022a), **op.cit.** s. 144,145. Aynı yönde: Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, Ankara: Seçkin Yayıncılık, 2018, ss. 214,215. Failin fiziki olarak bulunduğu yeri de değerlendiren görüşler için ayrıca bkz: Akbulut(2020), **loc.cit.** Kaşıkara, **op.cit**. s. 120

Kabahatin ilk seçimlik hareketi teknik ve idari tedbirlerin alınmamasıdır. İlgili hareket ihmali hareketle işlenebilen, mütemadi nitelikte bir soyut tehlike kabahatidir. Bu kapsamda teknik ve idari tedbirlerin alınmadığı müddetçe alınması gereken yerler ilgili hareketin işlendiği yerleri teşkil edecektir. Ancak teknik ve idari tedbirlerin çok çeşitli olması, çok çeşitli yer ve ülkelerde kabahatin işlendiğini kabul etmek gerekliliğini doğuracaktır. Örneğin siber saldırılara karşı güvenlik duvarının oluşturulması, VPN, sFTP gibi yöntemlerle veri aktarımı yapılması gibi farklı yerlerde gerçekleşecek tedbirler aynı somut olayda birlikte bulunabilecektir. Diğer yandan ise çalışanlara eğitim verilmesi, çalışanlarla gizlilik sözleşmelerinin imzalanması gibi tedbirler ise gerçekleştirilmesi gereken herhangi bir somut yere sahip olmayan tedbirlerdir. Burada her ne kadar yer bakımından uygulama açısından veri sorumlusunun merkez adresi gibi alternatif çözümler getirilmesi düşünülebilirse de en isabetli çözüm KVKK'nın yer bakımından uygulamasına ilişkin olarak özel bir hüküm öngörülmesidir.

Kişisel Verileri Koruma Kurul'u kararlarında KVKK'nın yer bakımından uygulanmasına ilişkin örnekler söz konusudur. Kurul Facebook hakkında verdiği bir kararda ihlalden etkilenen kullanıcılardan Facebook'u Türkçe olarak kullanan kişilere vurgu yapmıştır[495]. Facebook hakkında verilen diğer bir kararda ise Türkiye'de yaşayan 300.000 kullanıcının veri ihlalinden etkilenme olasılığının bulunduğu ifade edilmiştir[496]. Cathay Pasific[497] ve Marriott Hotel[498] hakkında verilen kararlarda da Kurul aynı şekilde ihlalden etkilenen Türkiye'deki yerleşik kişilere dikkat çekmiştir. Görüldüğü üzere Kurul, birçok kararında yer bakımından uygulama açısından ülkesellik ilkesine başvurmayarak mağdura göre kişisellik ilkesine göre hareket etmektedir. Yukarıda verilen kararlardaki ihlaller, siber alandaki güvenlik zafiyetleri sonucu meydana geldiği için internet ortamında gerçekleşen kabahatler bakımından öğretide kabul edilen veri girişinin

---

[495] Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/269 sayılı kararı (https://kvkk.gov.tr/Icerik/5534/2019-269 E.T. 12.02.2023)

[496] Kişisel Verileri Koruma Kurulu'nun 11.04.2019 tarihli ve 2019/104 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5450/2019-104 E.T.12.02.2023)

[497] Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/144 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5487/Cathay-Pasific-Airway-Limited-Hakkinda-Kisisel-Verileri-Koruma-Kurulunun-16-05-2019-Tarih-ve-2019-144-Sayili-Karar-Ozeti E.T. 12.02.2023)

[498] Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/143 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5479/2019-143 E.T. 12.02.2023)

yapıldığı ve hedef sunucunun bulunduğu yerlerin hareketin gerçekleştiği yerler olarak kabul edilmesi imkanı da bulunmamaktadır. Çünkü teknik ve idari tedbirlerin alınmaması hareketi, bilişim sistemine girme hareketi gibi tipik hareketin her iki sunucuda da gerçekleştiği bir hareket değildir. Teknik ve idari tedbirlerin alınmaması hareketi ancak teknik ve idari tedbirin alınmadığı sunucuda gerçekleşebilmektedir.

Gerekli denetimlerin yapılmaması veya yaptırılmaması hareketi bakımından da durum teknik ve idari tedbirlerin alınmaması hareketi ile benzer şekildedir. Denetimlerin yurt içi ve yurt dışı çeşitli yerlerde yapılmasının söz konusu olması mümkündür. Denetimin kapsamını veri sorumlusunun sunucuları oluşturabileceği gibi aynı şekilde fiziki olarak dosyalarını bulundurduğu bir yer de olabilir, dolayısıyla net bir işlenme yeri tayin etmek bu seçimlik hareket bakımından da oldukça güçtür.

Kabahatin diğer bir seçimlik hareketi olan kanuna aykırı açıklama ve amacı dışında kişisel verileri kullanma hareketi ise sırf hareket niteliğinde icrai bir hareketli soyut tehlike kabahatidir. Bu kapsamda kişisel verilerin amacı dışında kullanıldığı yer veya kanuna aykırı başkasına açıklandığı yer kabahatin işlendiği yeri teşkil edecektir. Özellikle kanuna aykırı başkasına açıklama hareketinin ağ ve internet ortamında gerçekleşmesi söz konusu olabilecektir. Bu kapsamda hareketin açıklayanın bulunduğu sunucu ve hedef sunucu arasında bölünebilmesi söz konusu olabileceği için hedef sunucunun bulunduğu yer de kabahatin işlendiği yeri teşkil edecektir.

Veri ihlal bildiriminin yapılmaması ise ihmali nitelikte, ani hareketli bir soyut tehlike kabahatidir. Kurul veri ihlalinin usul ve esaslarına ilişin 2019/10 sayılı kararında kimlerin veri ihlali bildirimi yapması gerektiğini düzenlemiştir. Buna göre; yurtdışında yerleşik veri sorumluları nezdinde gerçekleşen ihlalin sonuçlarının Türkiye'de yerleşik kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de yararlanması halinde ilgili veri sorumlularının veri ihlali bildirimi yükümlüsü olduğuna karar vermiştir[499]. Ancak ilgili karar, kabahatin yer bakımından uygulanma alanını belirlememektedir. Ayrıca Kabahatler Kanunu'nda yer bakımından uygulama konusunda

[499] Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.02.2023)

kanunlardaki özel hükümler istisna tutulmuştur (KK md. 6). Bu noktada Kurul'un düzenleyici işlemiyle Kabahatler Kanunu'nun aksinin öngörülmesi mümkün değildir ve yer bakımından uygulama düzenlemesinin Kanun'la yapılması gerekmektedir. Sayılan nedenlerle kabahatin bu hareketinin de yer bakımından uygulaması TCK 8. maddesi kapsamında değerlendirilmelidir. Bu kapsamda veri ihlal bildiriminin yapılması gereken yer belirli değildir. Bu noktada veri sorumlusunun bulunduğu yer bildirimi de yapacağı yer ve dolayısıyla veri sorumlusunun bulunduğu yerin hareketin işlendiği yer olarak kabul edilmesi bir çözüm teşkil edebilecektir. Ancak bu durumda da Kurul 2019/10 sayılı kararında kapsam dahilinde olması amaçlanan birçok veri sorumlusu kabahatin muhatabı olmayacaktır. Ayrıca veri ihlali dolayısıyla teknik ve idari tedbirlerin alınmaması hareketinin Türkiye'de işlenip veri ihlali bildiriminin yapılmaması hareketinin ise Türkiye'de gerçekleşmemiş sayıldığı sonuçlar doğabilecektir.

Görüldüğü üzere Kurul'un kabahatler bakımından idari para cezası tayin etme konusunda yer bakımından yetkisinin TCK 8. maddesince belirlenmesi, kabahatin yer bakımından uygulanması konusunda belirsizliklere ve problemlere neden olabilecek niteliktedir. Ayrıca yer bakımından uygulamanın bu şekilde olması ancak somut olayın esasının incelenmesi ile Kurul'un yetkisini tespit edebilme problemini gündeme getirecektir. Bu nedenle KVKK'da da yer bakımından uygulamaya ilişkin özel bir hükmün düzenlenmesi isabetli olacaktır. Nitekim GDPR'da da yer bakımından uygulamaya ilişkin özel bir hüküm düzenlenmiştir (GDPR md. 3). Bu kapsamda düzenleme kapsamında yer bakımından uygulama iki temel kritere dayanmaktadır: Bunlardan ilki kuruluş kriteridir[500]. Buna göre, işleme faaliyetinin nerede gerçekleştiğine bakılmaksızın Birlik içerisinde yer alan veri sorumlusu yahut veri işleyenin kuruluşunun işleme faaliyetleri kapsamında GDPR uygulanacaktır (GDPR md. 3/1). Kuruluş kriterinin sağlanmadığı durumlarda ise hedef yer kriteri söz konusu olabilecektir[501]. Hedef yer kriteri işleme faaliyetinden etkilenen kişileri esas almaktadır[502]. Veri sorumlusu ve veri

[500] Ayrıca bkz: European Data Protection Board, **Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)**, Version 2.0, 2019, s. 5 (https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_publication_type%3A64&page=4 E.T. 13.02.2023)

[501] **Ibid**. s. 13

[502] Ufuk Dal, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti" **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı: 1, 2019, s. 25

işleyenin Birlik içerisinde olmaması ancak ilgili kişinin Birlik içerisinde olması halinde iki olasılık söz konusu olacaktır. Mal veya hizmet ücretli olsun yahut olmasın kişisel verilerin işlenmesi faaliyeti ilgili kişiye sunulan mal ve hizmet ile ilgiliyse veya işleme faaliyeti ilgili kişinin Birlik içerisinde gerçekleşen davranışlarını izlenmesi ile ilgili ise bu durumlarda da GDPR'ın uygulanacağı düzenlenmiştir (GDPR md. 3/2). Bu kapsamda benzeri bir düzenlemenin KVKK'da da yer alması soru işaretlerinin giderilmesi bakımından en isabetli çözüm olacaktır.

B. Şikayet ve İncelemenin Usul ve Esasları

Kurul'un kişisel veri güvenliğine ilişkin yükümlülükleri yerine getirmeme kabahati bakımından inceleme yapma ve idari para cezasına karar verme konusunda yetkili merci olduğu daha önce ifade edilmiştir. Bu kapsamda Kurul, şikayet ve ihbar üzerine harekete geçebileceği gibi bir başvuru olmaksızın ayrıca görev alanına giren konularda da resen inceleme başlatabilmektedir[503].

Kurul'a şikayette bulunulabilmesi için öncelikle veri sorumlusuna başvuru usulünün tüketilmesi gerekmektedir (KVKK md. 14/2). Buna göre ilgili kişi öncelikle KVKK 13. maddesi gereğince veri sorumlusuna başvurmak mecburiyetindedir. Bu başvurular, başvuru usulüne ilişkin Kişisel Verileri Koruma Kurum'u tarafından yayımlanan Tebliğ'e uygun olarak yapılmalıdır[504]. Veri sorumlusunun başvuruda yer alan talepleri 30 gün içerisinde sonuçlandırması gerekmektedir (KVKK md 13/2). Kurul, başvuruların 30 gün içerisinde sonuçlandırılmaması halinde somut olayı incelerken ayrıca ilgili veri sorumlusunu yükümlülüğü konusunda talimatlandırmakta ve bu kararına aykırı hareket eden veri sorumlularına kurul kararlarının yerine getirilmemesi kabahati dolayısıyla idari para cezası vermektedir[505]. Kabahatimiz bakımından ise ilgili kişinin başvurusu üzerine veri sorumlusunun başvuruyu reddetmesi, başvuruya süresinde cevap verilmemesi yahut verilen cevabın ilgili kişi tarafından yetersiz bulunması hallerinde ilgili kişi, veri

---

[503] Başar, **op.cit.** s. 301

[504] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, 10 Mart 2018 tarihli 30356 sayılı Resmi Gazete'de yayımlanmıştır.

[505] Bkz: Kişisel Verileri Koruma Kurulu'nun 06.02.2020 tarihli 2020/86 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6732/2020-86 E.T. 14.02.2023)

sorumlusunun cevabından itibaren otuz gün ve her halde yapılan başvurudan itibaren en geç altmış gün içinde şikayette bulunma hakkına sahiptir[506].

Kurul'a yapılacak başvurulara ilişkin olarak KVKK'da mevcut iki hüküm dışında ayrıca bir düzenleme bulunmamaktadır. İlk hüküm; Kurul'a yapılan şikayetlerin 3071 sayılı Kanun'un 6. maddesine uygun olması gerekmektedir[507]. Buna göre; ad, soyadı, imza ve adres taşımayan, belli bir konusu olmayan yahut yargının görev alanında bulunan dilekçeler ilgili hükme göre incelenmeyecektir (3071 Sayılı Kanun md. 6). Özellikle uygulamada yargı mercilerinin görevi kapsamında kalan konularda yapılan şikayetlere sık rastlanmaktadır. Bu durumun temel sebebi gerçek kişi veri sorumlularının fiilleri dolayısıyla yapılan şikayetlerin çoğu durumda kişisel verilere ilişkin suçları da teşkil etmesidir. Kurul bu nitelikteki başvuruları reddetmektedir[508]. Diğer düzenleme ise şikayet üzerine incelemenin devam edebilmesi için Kurul'un ilgililere 60 gün içerisinde cevap vermesi gerekliliğidir; Kurul'un cevap vermediği durumda başvuru reddedilmiş sayılmaktadır (KVKK md. 15/4)

Kurul bu kapsamda, resen yahut şikayet üzerine görev alanındaki konularda inceleme yapma yetkisine sahiptir. Kurul'un yerinde inceleme yetkisi bulunmaktadır (KVKK md. 15/3). Kurul'un yerinde inceleme yetkisi dışında veri sorumlusu, 15 gün içinde ilgili bilgi ve belgeleri temin etmekle yükümlüdür (KVKK md. 15/3). Öte yandan Kurul'un; ihlalin varlığı durumunda veri sorumlusunca ihlalin giderimine karar verme, ihlalin yaygın olması durumunda ilke kararı alma, telafisi güç yahut imkansız olan durumlarda ise veri işlenmesini veya yurt dışına aktarımı durdurma konusunda karar alma yetkileri bulunmaktadır (KVKK md. 15/4-6). Elbette Kurul sayılan yetkileri dışında ayrıca idari yaptırıma karar verebilecektir (KVKK md. 22/1-ğ).

---

[506] Ayrıca Bkz: Bkz: Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/9 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu E.T. 15.02.2023)

[507] Dilekçe Hakkının Kullanılmasına Dair Kanun, 10 Kasım 1984 tarihli 18571 sayılı Resmi Gazete'de yayımlanmıştır.

[508] Kişisel Verileri Koruma Kurulu'nun 24.12.2018 tarihli ve 2018/156 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5425/2018-156 E.T. 14.02.2023)

C. Yaptırım

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin yaptırımı 18. maddede düzenlenmiştir. Buna göre yükümlülüklerini yerine getirmeyen kişiler bakımından 15.000'den 1.000.000 Türk lirasına kadar idari para cezası uygulanacaktır (KVKK md. 18/1-b). Kabahatler Kanunu 17/7 maddesi gereği 2023 yılı itibarıyla idari para cezası tutarlarının alt ve üst sınırı 89.571 Türk lirası ve 5.971.989 Türk lirasıdır[509].

Kişisel Verilerin Korunması Kanunu'nda düzenlenen idari para cezası alt ve üst sınırının yeniden düzenlenmesi isabetli olacaktır; çünkü KVKK kapsamında yükümlü olan kişiler oldukça çeşitlilik göstermektedir. Bu doğrultuda küresel çapta gelir elde eden bir şirket KVKK kapsamında yükümlü olduğu gibi bir aile ferdi yahut küçük bir işletme sahibi de bu düzenlemelere uyum sağlama mecburiyetindedir. Gelinen noktada idari para cezalarının alt sınırı kimi kişiler bakımından çok ağır bir yaptırım teşkil edebilecekken büyük şirketler bakımından ise üst sınırdan verilen para cezaları dahi hiçbir caydırıcılık kabiliyetine sahip olamayabilecektir.

Bu noktada GDPR'daki idari yaptırım rejimi güzel bir örnek teşkil etmektedir. GDPR'da idari para cezalarına ilişkin olarak kademeli bir anlayış benimsenmiştir[510]. 83. maddeye göre kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi halinde veri sorumlularına 10.000.000 Euro'ya kadar idari para cezası GDPR kapsamında uygulanabilecektir (GDPR 83/4). İhlali gerçekleştirenin teşebbüs olması halinde önceki mali yıla ait küresel çapta elde edilen toplam cironun %2'si daha yüksek ise idari para cezasının üst sınırı bu oran olacaktır (GDPR 83/4). Böylece GDPR bakımından hem yüksek gelir sahibi veri sorumluları için cezaların daha caydırıcı olması sağlanmış hem de idari para cezası alt sınırı tayin edilmeyip düşük gelirli veri sorumluları bakımından çok daha düşük tutarlarda idari para cezalarının uygulanması mümkün kılınmıştır. Benzeri bir düzenlemenin KVKK kapsamında da yapılması uygulama açısından isabetli olacaktır.

---

[509] Kişisel Verileri Koruma Kurumu Duyurusu (https://www.kvkk.gov.tr/Icerik/7530/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Idari-Para-Cezasi-Tutarlari E.T. 20.11.2022)

[510] İbrahim Barış Sayar, "The Administrative Fines Regime of the General Data Protection Regulation and Its Impact", **Kişisel Verileri Koruma Dergisi,** Cilt: 3 Sayı: 1, 2021 s. 5.

KVKK'nın 18. maddesinin 2. fıkrasında yalnızca veri sorumlusu olan gerçek ve özel hukuk tüzel kişileri bakımından idari para cezasının uygulanacağı düzenlenmiştir (KVKK md. 18/2). Dolayısıyla veri işleyen yahut çalışan gibi veri sorumlusu sıfatına sahip olmayan herhangi bir kimse idari para cezasının muhatabı değildir. Kabahatler Kanunu'na göre organ, temsilci ve tüzel kişi faaliyetinde göre alan kişinin hareketi dolayısıyla hem ilgili fail hem de tüzel kişi yaptırıma tabi kılınabilmektedir (KK md. 8/1). Yine gerçek kişinin çalışanının hareketi dolayısıyla ayrıca gerçek kişi idari para cezasına muhatap olabilmektedir (KK md. 8/2). Ancak bu konularda özel kanunlarda düzenleme yapılarak sadece tüzel kişinin, temsil edilenin yahut iş sahibinin idari yaptırıma tabi olması düzenlenebilmektedir[511]. KVKK'nın 18. maddesinin 2. fıkrası Kabahatler Kanunu'nun 8. maddesine göre özel hüküm teşkil etmektedir. Dolayısıyla bu özel hüküm gereği yalnızca veri sorumlusu bakımından idari para cezasına hükmedilecektir. Son olarak veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin kamu kurumu, kamu kuruluşu ve kamu kurumu niteliğindeki meslek kuruluşu organizasyonu bünyesinde işlenmesi durumunda, bu kuruluşlarda görev alan kişiler hakkında disiplin hükümleri uyarınca işlem yapılmakta olup ilgili kuruluşa idari para cezası verilmemektedir (KVKK md.18/3)[512].

D. Kişisel Verileri Koruma Kurulu'nun Yaptırım Kararlarına Karşı Kanun Yolları

Kabahatler Kanunu'nun 3. maddesinde özel kanunlarda açıkça düzenlenmedikçe kanun yolları bakımından Kabahatler Kanunu'nun uygulanacağı hüküm altına alınmıştır (KK md. 3/1-a). Kişisel Verilerin Korunması Kanunu'nda kanun yollarına ilişkin özel bir hüküm bulunmamaktadır. Bu sebeple veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati dolayısıyla hükmedilen idari yaptırım bakımından Kabahatler Kanunu'nun kanun yollarına ilişkin hükümleri uygulanacaktır. Bu durum özellikle uygulamada eleştirilen hususlardan birisidir. Nitekim Kurul'un verdiği yaptırım kararları

---

[511] Akbulut (2022), **op.cit.** s. 296

[512] "*Kanunun 15 inci maddesinin (3) numaralı fıkrasına aykırılık oluşturduğu dikkate alınarak, kamu kuruluşu olarak değerlendirilen Mimar Sinan Güzel Sanatlar Üniversitesinde görev yapan sorumlular hakkında Kanunun 18 inci maddesinin (3) numaralı fıkrası çerçevesinde disiplin hükümlerine göre işlem yapılmasına"* (Kişisel Verileri Koruma Kurulu'nun 01.07.2019 tarihli ve 2019/188 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5506/2019-188 E.T. 19.03.2023))

teknik bilgi gerektiren bir alana ilişkin olduğu için uzmanlaşmayı ve daha detaylı bir incelemeyi gerektirmektedir. Ayrıca verilen idari para cezalarının tutarları dolayısıyla daha kapsamlı bir hukuki çare, hak kayıplarının yaşanmaması için gereklidir. Nitekim bu durum 2021 yılında Adalet Bakanlığı tarafından yayımlanmış olan İnsan Hakları Eylem Planı'na da yansımıştır. Bu kapsamda KVKK'da yapılması öngörülen değişikliklerden birisi de kanun yolu olarak idari yargının görevlendirilmesidir[513]. Ancak henüz böyle bir değişiklik gerçekleşmediği için kanun yolları konusunda Kabahatler Kanunu uygulanacaktır.

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından bir idari yaptırım söz konusu olması halinde başvuru ve itiraz kanun yolu olmak üzere iki olağan kanun yolu söz konusudur. İdari yaptırıma karar verilmesine yer olmadığına ilişkin kararlar bakımından ise ne KVKK'da ne de Kabahatler Kanunu'nda bir kanun yolu hükmü bulunmaktadır. Bu nedenle ilgili kararlara karşı herhangi bir kanun yoluna başvuru imkanı mevcut değildir[514]. Bu bölümün devamında başvuru kanun yolu ve itiraz kanun yolu incelenecektir.

1. Başvuru Kanun Yolu

Kabahatler Kanunu'na göre idari yaptırım kararının tefhimi yahut tebliğinden itibaren 15 gün içinde sulh ceza hakimliğine başvuruda bulunmak mümkündür (KK md. 27/1). Bu hakkın kullanılmaması halinde yaptırım kararı kesinleşmektedir (KK md. 27/1). İtirazın hangi sulh ceza hakimliğine yapılacağı ise öğretide tartışmalı bir konudur. Bir görüş Ceza Muhakemesi Kanunu 12/1. maddesi gereği kabahatin işlendiği yer sulh ceza hakimliğinin yetkili olduğunu savunmaktadır[515]. Diğer görüş ise kararı veren mercinin bağlı olduğu kurum yahut kuruluşun bulunduğu yer sulh ceza hakimliğini yetkili kabul etmektedir[516]. Katıldığımız bu görüşe göre Kurul'un bağlı olduğu kurum olan Kişisel

---

[513] Türkiye Cumhuriyeti Adalet Bakanlığı, İnsan Hakları Eylem Planı, 2021, s. 92 (https://insanhaklarieylemplani.adalet.gov.tr/ E.T. 17.02.2023)
[514] Akbulut (2022), **op.cit.**, s. 642
[515] Yalçın, **op.cit. s**. 139
[516] Kangal (2022), **op.cit**. s. 476, Akbulut (2022), **op.cit,** s. 655

Verileri Koruma Kurumu'nun bulunduğu yer Çankaya/Ankara olduğu için başvuru kanun yolunda Ankara Adliyesi Sulh Ceza Hakimlikleri yetkilidir.

Sulh ceza hakimliği, veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından son karar olarak başvurunun reddine yahut idari yaptırım kararının kaldırılmasına karar verebilecektir (KK md. 28/8). Ayrıca kabahatimizin alt ve üst sınırı KVKK'da gösterilmiş olduğu için, sulh ceza hakimi para cezasının tutarında değişiklik yaparak da başvurunun kabulüne karar verebilecektir (KK md. 28/9). Sulh ceza hakiminin verdiği karar kapsamında kesinleşme sınırı 3000 Türk lirasıdır (KK md. 28/10). Kabahatimizin KVKK'da gösterilen ceza alt sınırı 2023 yılı itibarıyla 89.571 Türk lirası olduğu için sulh ceza hakiminin vermiş olduğu kararlara karşı itiraz yolu da söz konusu olacaktır.

2. İtiraz Kanun Yolu

Kabahatler Kanunu'nun 29. maddesi uyarınca, sulh ceza hakiminin verdiği kararlara karşı itiraz etmek mümkündür. Buna göre yapılacak itirazın Ceza Muhakemesi Kanunu'na göre yapılması gerekmektedir (KK md. 29). Sulh ceza hakiminin kararına karşı itiraz süresi, kararın tebliğinden itibaren 7 gündür (KK md. 29/1). Ankara Adliyesi'nde birden fazla sulh ceza hakimliği bulunduğu için yetkili ve görevli itiraz mercii bir üst numaralı sulh ceza hakimliği olacaktır (CMK md. 268/3-a). İtirazın yapılacağı merci ise kararı veren sulh ceza hakimliğidir (KK md. 268/1). İtiraz kanun yoluna başvurulması halinde bir üst numaralı sulh ceza hakimliği, itirazı kabul edebileceği gibi itirazı reddede de bilir (KK md. 29/3). İtiraz merci son olağan kanun yolu olup itiraz mercinin verdiği kararlar kesindir.

SONUÇ

Kişisel veri güvenliği, KVKK'nın kabul edildiği günden bu yana KVKK kapsamında yer alan en önemli yükümlülüklerden birisini teşkil etmektedir. Kurul tarafından verilen kararların gerekçesini sıklıkla kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati oluşturmaktadır. Uygulamada da oldukça tartışılan bu konuda akademik olarak yapılan çalışma sayısı ise oldukça azdır. Bunun sonucunda kişisel veri güvenliğine ilişkin yükümlülüklerin uygulamada yarattığı problemler akademik bir tartışma sahası bulamamıştır. Çalışmamız kapsamında bu eksikliğin giderilmesi hedeflenerek kişisel veri güvenliğine ilişkin yükümlülükler ve kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati incelenmiştir. Yapılan inceleme sonucunda konuya öneriler getirilmeye çalışılmıştır.

Çalışmamızda öncelikle kişisel verilerin korunması hukukuna ilişkin kavramlar ve ilkelere yer verilerek kabahat incelemesine bir zemin hazırlanmaya çalışılmıştır. Kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu gibi kabahatin maddi unsurları bakımından merkezi rolleri olan bu kavramların sınırları netleştirilerek kabahatin maddi unsurlarının daha anlaşılabilir hale getirilmesi hedeflenmiştir. Bunun yanında kişisel verilerin korunmasına ilişkin ilkeler açıklanarak kişisel verilerin korunması hukukunun hedeflediği değerler ifade edilmiştir.

Çalışmamızda ayrıca kişisel veri güvenliği kavramı ve yükümlülüğü açıklanmıştır. Buna göre kişisel veri güvenliği bilgi güvenliği doğrultusunda anlam kazanmış bir kavram olup bilgi güvenliği ışığında kişisel verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin teminini hedeflemektedir. Nitekim gerek GDPR gerekse de Direktif'te bu doğrultuda kişisel veri güvenliğine ilişkin düzenlemeler yapılmıştır. Bununla birlikte KVKK'daki düzenleme veri güvenliğine ilişkin yükümlülükler bakımından farklılaşmaktadır. KVKK'daki düzenlemede GDPR ve Direktif'ten farklı olarak kişisel verinin yetkisiz yetkisiz erişim, yetkisiz kullanım, bozulma, değiştirme, yok olmasına karşı teknik ve idari tedbirlerin alınması değil, kişisel verilerin hukuka aykırı işleme

faaliyetine, kişisel verilere hukuka aykırı şekilde erişilmesine karşı ve kişisel verilerin muhafazası amacıyla yeterli güvenlik düzeyini uygun teknik ve idari tedbirlerin alınmasını hüküm altına alınmıştır. Kurul ise "hukuka aykırı işleme" ibaresini veri sorumlusu bünyesinde gerçekleşen işleme faaliyetleri açısından yorumlamaktadır. Bu durumun bir sonucu olarak KVKK'da düzenlenen teknik ve idari tedbirlerin alınması yükümlülüğü bilgi güvenliği paralelinde bir yükümlülük olma niteliğini kısmi olarak yitirmiş, ayrıca işleme faaliyetinin hukuka uygunluğu da kişisel veri güvenliğinin konusu haline gelmiştir.

Veri ihlal bildirimi yükümlülüğü ise teknik ve idari tedbirlerin alınması yükümlülüğünün farklı düzenlenmesi dolayısıyla farklı bir kapsama sahip olmuştur. Veri ihlali GDPR kapsamında doğrudan teknik ve idari tedbirler vasıtasıyla önlenmeye çalışılan yetkisiz erişim, yetkisiz kullanım, bozulma, değiştirme, yok olma durumlarının tümünü ifade etmektedir. KVKK'da ise yalnızca hukuka aykırı şekilde kişisel verilerin elde edilmesi hali veri ihlali olarak değerlendirilmiştir. Bilgi güvenliği terminoljisinden koparak teknik ve idari tedbirlerin alınma amaçlarında farklılaşmaya gidilmesi, veri ihlali kavramının ve dolayısıyla veri ihlal bildirim yükümlülüğünün kapsamının daralmasına etki etmiştir.

Kişisel verilerin KVKK'ya aykırı şekilde açıklanması ve amacı dışında kullanılması yasağı ise veri güvenliği kapsamında diğer bir yükümlülüktür. Bu yükümlülük de kişisel verilerin hukuka uygun şekilde işlenmesine ilişkin bir yükümlülük teşkil etmektedir. Öte yandan veri sorumlularının veri güvenliğine diğer bir yükümlülüğü ise KVKK hükümlerinin uygulanması amacıyla denetim yapma veya yaptırma yükümlülüğüdür. Denetim yükümlülüğünün kapsamını ise KVKK'nın tüm hükümlerinin uygulanmasının temini amacı oluşturmaktadır. Bu kapsamda ifade edilen her iki yükümlülük de yine veri güvenliğine ilişkin yükümlülüklerin kapsamını aşmakta ve kişisel verilerin korunması hukukuna ilişkin farklı yükümlülükleri içermektedir.

Çalışmamızın ikinci bölümünde ise çalışmanın asıl konusunu oluşturan kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati incelenmiştir. KVKK'da kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi bir kabahat olarak düzenlenmiş olup böylece kişisel verilerin korunması hukukunun en

önemli yükümlülüklerinden birisi olan veri güvenliğine ilişkin yükümlülüklerin veri sorumlularınca yerine getirilmesi amaçlanmıştır. Bu kapsamda daha genel bir ifadeyle kişisel verilerin korunmasını sağlama amacıyla getirilen bu kabahatin korunan hukuki değerini özel hayatın gizliliği hakkı kapsamında kişisel verilerin korunması hakkı teşkil etmektedir.

Kabahatin faili veri sorumlusudur. Bu noktada kabahat özgü bir kabahat teşkil etmektedir. Veri sorumlusunun tüzel kişi olduğu hallerde ise kabahatin faili ilgili veri güvenliğine ilişkin yükümlülüğü yerine getirmekle yükümlü olan veri sorumlusunun organı, temsilcisi yahut çalışanıdır. Kabahatin mağduru ise kişisel verilerin korunması hakkı ihlal edilen kişi, diğer bir deyişle ilgili kişidir.

Kabahatin konusu tamamen veya kısmen otomatik yollarla yahut veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerdir. Kişisel veri teşkil etmeyen yahut işlenmemiş herhangi bir kişisel veri kabahatin konusunu oluşturmamaktadır. Veri ihlal bildirimi yükümlülüğünün konusunu ise veri ihlali olgusuna ilişkin bildirim konusu bilgiler oluşturmaktadır. Dolayısıyla veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi hareketi farklı bir kabahat teşkil etmektedir.

Kabahat kapsamında dört farklı hareket öngörülmüştür. Teknik ve idari tedbirlerin alınmaması, denetim yükümlülüğünün yerine getirilmemesi, kişisel verilerin KVKK'ya aykırı şekilde açıklanması ve amacı dışında kullanılması hareketleri seçimlik hareket teşkil etmektedir. Veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi hareketi ise konusu dolayısıyla farklı bir kabahati oluşturmaktadır.

Teknik ve idari tedbirlerin alınmaması ve denetim yükümlülüğünün yerine getirilmemesi hareketi mütemadi ve ihmali şekilde işlenen kabahatlerdir. KVKK'ya aykırı şekilde kişisel verileri açıklama ve amacı dışında kullanma hareketi ani kabahat olup kabahatin icrai şekilde işlenen tek hareketini oluşturmaktadır. Veri ihlali bildirimi yükümlülüğünün yerine getirilmemesi hareketi ise ihmali şekilde işlenen bir ani kabahat teşkil etmektedir. Kabahat düzenlenen tüm hareketleri bakımından sırf hareket kabahati niteliğindedir. Ayrıca konu üzerinde etkisine göre kabahat soyut tehlike kabahatidir.

Kurul, veri sorumlularının hukuka aykırı şekilde veri işlemeleri halinde ilgili hareketi hukuka aykırı şekilde kişisel verilerin işlenmesini önlemek için uygun güvenlik düzeyini temin etmek amacıyla teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirmektedir. Bununla birlikte hukuka aykırı şekilde kişisel verilerin işlenmesi teknik ve idari tedbirler aracılığıyla sağlanabilecek bir yükümlülük değildir. Hukuka aykırı şekilde işleme hareketi icrai bir hareket iken teknik ve idari tedbirlerin alınması ihmali şekilde işlenebilecek bir kabahattir. Kurul'un icra şekilde gerçekleştirilebilecek bir hareketi teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirmesi kanunilik ve belirlilik ilkelerine aykırılık teşkil etmektedir.

Denetim yükümlülüğünün yerine getirilmemesi ve kişisel verileri KVKK'ya aykırı şekilde açıklama hareketleri ise Kurul kararlarında istisnai olarak kabahatin gerekçesini oluşturmaktadır. Nitekim denetim yükümlülüğü kapsamında değerlendirilecek durumlar aynı zamanda teknik ve idari bir tedbir teşkil etmektedir. Bu nedenle ilgili fıkranın ayrıca bir kabahat olarak düzenlenmesine gerek bulunmamaktadır. Öte yandan kişisel verileri KVKK'ya aykırı şekilde açıklama ve amacı dışında kullanma hareketi de hukuka aykırı şekilde kişisel veri işleme niteliğinde bir hareket olup bu şekilde meydana gelen ihlaller Kurul kararlarında teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirilmektedir.

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati kasten veya taksirle işlenebilmektedir. Kabahat kapsamında ayrıca hukuka uygunluk sebepleri de uygulanabilecektir. Bu kapsamda kanun hükmünün uygulanması, hakkın kullanılması ve KVKK'nın 28. maddesinde düzenlenen istisnalar hukuka uygunluk sebebi teşkil edebilecektir. Kusurluluk bakımından ise zorunluluk halinin kabahat kapsamında uygulanabilmesi söz konusudur.

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati teşebbüse elverişli değildir. Öncelikle kabahatin üç hareketi gerçek ihmali harekettir. Gerçek ihmali hareketle işlenebilen kabahatler teşebbüse elverişli değildir. Ayrıca kabahatlere teşebbüsün yaptırıma tabi tutulabilmesi için özel düzenleme bulunması

gerekmektedir. Bununla birlikte KVKK'da böyle bir özel düzenleme öngörülmemiştir. Öte yandan kabahate iştirak mümkündür. Özellikle birlikte veri sorumlusu durumunda iştirak söz konusu olmaktadır. Bununla beraber iştirak durumunda kendisi yahut organı, temsilcisi veya çalışan hareketi gerçekleştirilen veri sorumluları idari yaptırıma muhatap olacaklardır.

Kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahatinin gerçekleşmesi sırasında aynı hareketle başkaca bir kabahat yahut suç meydana gelebilecektir. Bu noktada Kabahatler Kanunu'nun fikri içtima hükümleri dikkate alınmalıdır. Yukarıda ifade edildiği üzere hukuka aykırı şekilde kişisel veri işlenmesi teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirilmektedir. Bu kapsamda hukuka aykırı şekilde kişisel veri işlenirken icrai hareketle işlenen başkaca bir kabahatin gerçekleşmesi halinde bu iki hareket fikri içtima kapsamında değerlendirilemeyecektir; çünkü öğretide ihmali hareket ve icrai hareketin fikri içtima kapsamında değerlendirilemeyeceği kabul edilmektedir. Öte yandan TCK'da düzenlenen kişisel verilere ilişkin suçlar bakımından da aynı durum söz konusudur. Hukuka aykırı şekilde veri işleyen veri sorumlusunun aynı zamanda TCK kapsamında kişisel verilere ilişkin bir suçu da hareket kapsamında işlemesi halinde Kurul bu iki hareketi fikri içtima ilişkisi içerisinde değerlendirmemektedir. Bu kapsamda bir hareket dolayısıyla veri sorumlularının iki defa cezalandırılması söz konusu olabilecek ve bu durum hak ihlallerine yol açabilecektir.

2023 yılı itibarıyla kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati kapsamında verilen idari para cezalarının alt ve üst sınırları 89.571 Türk lirası ila 5.971.989 Türk lirasıdır. Kabahat karşılığı öngörülen yaptırımların alt sınırı birçok kişi için çok yüksek bir para cezası teşkil etmekteyken üst sınırı ise artık uluslararası şirketler için caydırıcılığını yitirmiştir. Bu kapsamda kabahat karşılığı öngörülen idari para cezasının alt sınırının düşürülmesi ve üst sınır bakımından nispi idari para cezasına geçilmesi en isabetli çözüm olacaktır.

Kabahat kapsamında ifade edilmesi gereken diğer bir durum ise Kurul'un yer bakımından yetkisidir. Kurul yer bakımından yetkisini tespit ederken kişisellik prensibini

uygulamaktadır. Bununla birlikte yer bakımından uygulamaya ilişkin özel bir düzenleme bulunmadığı için Kurul'un uygulaması isabetli değildir. Bu doğrultuda KVKK'da kapsam maddesinin değiştirilmesi ile Kurul'un yetki alanının da belirlenmesi isabetli bir çözüm yöntemi olacaktır.

İfade edilen hususlar neticesinde veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati bakımından önerilerimiz şu şekilde sıralanabilir: Hukuka aykırı şekilde kişisel veri işlenmesi durumunun teknik ve idari tedbirlerin alınmaması hareketi kapsamında değerlendirilmesi hak ihlallerine yol açabilecek nitelikte olup hukuka aykırı şekilde kişisel veri işleme faaliyetinin ayrı bir kabahat olarak öngörülmelidir. Teknik ve idari tedbirlerin alınması yükümlülüğü bilgi güvenliği prensipleri doğrultusunda yeniden düzenlenmeli ve bu şekilde kabahatin hareket unsuru bu kapsamda değiştirilmelidir. Konu unsuru diğer kabahatin diğer hareketlerinden farklı olan veri ihlal bildirimi yükümlülüğünün yerine getirilmemesi hareketine ayrı bir kabahat olarak KVKK'da yer verilmelidir. Denetim yükümlülüğününün yerine getirilmemesi hareketi ve kişisel verileri KVKK'ya aykırı şekilde açıklama ve amacı dışında kullanma hareketleri diğer hareketlerin kapsamında olmaları dolayısıyla kabahat kapsamından çıkarılmalıdır. İdari para cezası tutarları yeniden düzenlenmeli ve kabahatin yaptırımı nisbi idari para cezası olarak düzenlenmelidir. Ayrıca sulh ceza hakimlikleri yerine idari yargı, yargı yolu olarak düzenlenmeli böylece teknik bilgi ve daha detaylı inceleme gerektiren kabahatin yanlış uygulanması halinde hak kayıplarının yaşanması engellenmelidir. Ayrıca Kurul'un yer bakımından yetkisi KVKK'nın Kapsam başlıklı 2. maddesinde düzenlenmeli ve Kurul'un yer bakımından yetki alanına ilişkin olarak özel hüküm getirilmelidir.

KVKK'nın "Kabahatler" başlıklı 18. maddesinin 1. fıkrasının (b), (d) ve (e) bendi ve 4. fıkrası bakımından önerilerimiz aşağıdaki gibidir:

"*Kabahatler*

MADDE 18- *(1) Bu Kanunun;*

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinin 1 inci fıkrasında öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, veri sorumlusunun ticari işletme olması halinde bir önceki mali yıla ait yıllık gayri safi gelirlerinin yüzde birinden yüzde beşine kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar,

d) 5 ila 9 ncu maddelerinde öngörülen veri işleme şartlarına aykırı davrananlar hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, veri sorumlusunun ticari işletme olması halinde bir önceki mali yıla ait yıllık gayri safi gelirlerinin yüzde birinden yüzde beşine kadar,

e) 12 nci maddesinin 5 inci fıkrasında öngörülen veri ihlal bildirim yükümlülüğüne aykırı davrananlar hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, veri sorumlusunun ticari işletme olması halinde bir önceki mali yıla ait yıllık gayri safi gelirlerinin yüzde birinden yüzde beşine kadar,

idari para cezası verilir.

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

(4) Kişisel Verileri Koruma Kurulu tarafından verilen idari yaptırım kararlarına karşı 60 gün içerisinde idare mahkemesinde dava açılabilir. Kişisel Verileri Koruma Kurulu tarafından verilen karara karşı başvuru yapılmış olması idari yaptırımın icra ve tahsilini durdurmaz".

KVKK'nın "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12. maddesi bakımından önerilerimiz aşağıdaki şekildedir:

“*Veri güvenliğine ilişkin yükümlülükler*

MADDE 12- *(1) Veri sorumlusu kişisel verilere yetkisiz erişimi, kişisel verilerin yetkisiz şekilde kullanılmasını, yetkisiz şekilde açıklanmasını veya aktarılmasını, bozulmasını, değiştirilmesini, yok olmasını, kaybolmasını veya hukuka aykırı şekilde işlenmesini önlemek amacıyla günün teknolojisini ve uygulama maliyetlerini dikkate alarak uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.*

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri ihlali halinde veri sorumlusu bu durumu 72 saat içinde Kurula ve en geç 30 gün içinde ilgilisine bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir”.

KAYNAKÇA

ACKOFF Russell, "From Data to Wisdom", **Journal of Applied System Analysis**, Cilt: 16, 1989, ss. 3-9

AKBULUT Berrin, "Bağlılık Kuralı", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, , Sayı: 1, 2010, ss. 167 - 214

AKBULUT Berrin, **Türk Ceza Kanunu ile Kabahatler Kanunu Genel Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi**, Ankara: Adalet Yayınevi, 2014

AKBULUT Berrin, **Türk Ceza Hukuku Temel Bilgiler**, Ankara: Seçkin Yayıncılık, 2020

AKBULUT Berrin, **Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2022

AKSAN Murat, "Başkası Yerine Ceza İnfaz Kurumuna veya Tutukevine Girme Suçu (TCK m. 291)", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 9, Sayı: 2, 2019, 335-404

AKSOY RETORNAZ E. Eylem /GÜÇLÜTÜRK Osman Gazi, "Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilere İlişkin Temel İlkelerle İlişkisi", **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Editörler: E. Eylem Aksoy Retornaz ve Osman Gazi Güçlütürk, İstanbul: On İki Levha Yayıncılık, 2021, ss. 275-302

AKSOY İPEKÇİOĞLU Pervin, **Türk Ceza Hukukunda Suça Teşebbüs**, Ankara: Seçkin Yayıncılık, 2009

ALSMADİ Izzat/BURDWELL Robert/ALEROUD Ahmed/WAHBEH Abdallah/AL-QUDAH Mahmoud/AL-OMARİ Ahmad., **Practical Information Security, A Competency-Based Education Course**, Cham: Springer, 2018

An Coimisiún um Chosaint Sonraí (Data Protection Comission), **Quick Guide to the Principles of Data Protection,** 2019 (https://www.dataprotection.ie/en/dpc-guidance Erişim tarihi: 20.11.2022)

Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 01248/07/EN WP 136, 2007 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 10.10.2021)

Article 29 Data Protection Working Party, **Opinion 1/2010 on the Concepts of "Controller" and "Processor**, 00264/10/EN WP169, 2010 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

Article 29 Data Protection Working Party, **Guıdelınes On The Implementatıon Of The Court Of Justıce Of The European Unıon Judgment On"Google Spaın And Inc V. Agencıa Española De Protección De Datos (Aepd) And Marıo Costeja González" C-131/12,** 2014,
(https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

Article 29 Working Party, **Opinion 03/2013 on Purpose Limitation**, 00569/13/EN WP 203, 2013
(https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm E.T. 04.12.2022)

ARSLAN Çetin/BAŞTÜRK İhsan, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler", **ERÜHFD**, Cilt: 8, Sayı: 2, 2013, ss. 195-219

ARTUK M. Emin/ GÖKCEN Ahmet/ YENİDÜNYA A. Caner, **Ceza Hukuku Genel Hükümler,** Ankara: Adalet Yayınevi, 2015, 9. Baskı

AŞIKOĞLU Şehriban İpek, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul: On iki Levha Yayıncılık, 2018

ALTINDERE Murat, **Kişisel Verilerin Korunması Hukuku ve Uygulanması**, Ankara: Adalet Yayınevi, 2020

AVCI Yasemin**, Kişisel Verilerin Korunması**, Konya: Selçuk Üniversitesi, yayımlanmamış yüksek lisans tezi, 2019

AYAN Mehmet/ AYAN Nurşen, **Kişiler Hukuku**, Ankara: Seçkin Yayıncılık, 2016, 8. baskı

AYDEMİR Ece Taşçı, **Kişisel Verilerin Kaydedilmesi Suçu,** Ankara: Seçkin Hukuk, 2022

AYDIN Devrim, "Tüzel Kişilerin Ceza Sorumluluğu Tartışmaları", **Uyuşmazlık Mahkemesi Dergisi**, Yıl: 5 Sayı: 10, 2017, ss. 97-110

BASKIN Onur, **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması,** Ankara: Seçkin Yayıncılık, 2021

BAŞAR Cemal, **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, İstanbul: On iki Levha, 2020

BAYSAL Mustafa, **KVKK Kişisel Verilerin Korunması Kanunu El Kitabı**, Ankara: Seçkin Yayıncılık, 2021

BAYINDIR Hamza, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, İstanbul: On İki Levha, 2020

BERGER Maria/EISENDLE David, "Web 2.0 and the Concept of 'Data Controller': Recent Developments in EU Data Protection Law" **Indian Journal of Technology and Law,** Cilt: 15 Sayı: 1, 2019, ss. 20-39

BEYTAR Erbil, **İşçinin Kişiliğininin ve Kişisel Verilerinin Korunması**, İstanbul: On İki Levha, 2017

BIEGA Asia J./FINCK Michéle, "Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems", **Technology and Regulation,** 2021, ss. 44-61

BİLİR Faruk, "Önsöz", Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması**, Ankara: KVKK Yayınları No: 03, 2019, s. 6

BREİTHBARTH Paul, "The İmpact of GDPR One Year on", **Network Security,** Sayı 8, 2019, ss. 11-13

BROUWER Evelien, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", **The Eclipse of the Legality Principle in the European Union**, Edited by: Leonard Besselink, Frans Pennings, Sacha Prechal, Alphen aan den Rijn: Kluver Law International, 2010, ss. 273-294

BURTON Cedric, "Security of Processing", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020, ss. 630-640

BÜK Alaattin, **Bilişim Alanında Kişisel Verilerin Korunması**, Ankara: Seçkin Yayıncılık, 2018

BYGRAVE Lee A., **Data Privacy Law: An International Perspective**, Oxford: Oxford University Press, 2014

BYGRAVE Lee A., "Information Concepts in Law: Generic Dreams and Definitional Daylight", **Oxford Journal of Legal Studies,** Cilt: 35, Sayı: 1, 2015, ss. 91-120

BYGRAVE Lee A., "The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law", **Law, Innovation and Technology**, Cilt: 1, Sayı: 2, 2010, ss. 1-25

BYGRAVE Lee A./TOSONI Luca (2020a), "Personal Data", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020,ss. 103-115

BYGRAVE Lee A./TOSONI Luca (2020b), "Processing", **The EU General Data Protection Regulation (GDPR) A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey., New York: Oxford University Press, 2020, ss. 116-122

BYGRAVE Lee A./TOSONI Luca(2020c), "Controller", **The Eu General Data Protection Regulation (GDPR), A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press, 2020, ss. 145-156

CALDER Alan/ WATKINS Steve, **IT Governance: A Manager's Guide to Data Security and ISO27001 / ISO 27002**, London; Kogan Page, 2008

CENTELNur/ZAFER Hamide/ÇAKMUT Özlem, **Türk Ceza Hukukuna Giriş**, İstanbul: Beta Yayıncılık, 2016

CEYHAN Murat, **Ceza Hukukunda Netice**, İstanbul: On İki Levha Yayıncılık, 2022

CHERDANTSEVA Yulia/ HILTON Jeremy, "A Reference Model of Information Assurance & Security", **Availability, Reliability and Security**, Eighth International Conference, 2013, ss 546-555

COŞKUN Neslihan, **Fikri İçtima**, Ankara: Gazi Üniversitesi Yayımlanmamış Doktora Tezi, 2009

Council of Europe/European Unıon Agency For Fundamental Rıghts/European Data Protectıon Supervısor/Europen Court of Human Rights, **Handbook on European Data Protection Law**,, Luxembourg: Publication Office of the European Union, 2018

ÇAĞLAYAN Ramazan, "Hukukumuzda Kamu Tüzel Kişiliği Kavramı ve Kıstasları", **Uyuşmazlık Mahkemesi Dergisi**, Cilt: 0 Sayı: 7, 2016, ss. 373-398

ÇEKİN Mesut Serdar, **Kişisel Verilerin Korunması Hukuku**, İstanbul: On İki Levha yayıncılık, 2020

ÇEKİN Mesut Serdar/BERKTAŞ Ahmet Esad/AKINCI M. Furkan, **Veri Hukuku,** İstanbul: On İki Levha Yayıncılık, 2023

ÇELİKEL Serdar, **Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri**, Ankara: Seçkin Yayıncılık, 2022,

ÇETİN Hakan, "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi", **Akdeniz İ.İ.B.F. Dergisi**, Cilt: 14 Sayı: 29, 2014, ss. 86-105

DAL Ufuk, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti" **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı: 1, 2019, 21-33

DEDE Ramazan, **Kişisel Verilerin Korunması Kanunu Bakımından Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, Yüksek Lisans Tezi, İstanbul: Altınbaş Üniversitesi, 2022

DE HERT Paul/ PAPAKONTANTİNOU Vagelis, "The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on its Global Ambition", **Computer Law & Security Review,** Cilt: 30 Sayı: 6, 2014, ss. 633-642

DEĞİRMENCİ Olgun, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **TBB Dergisi**, Sayı: 58, 2005, ss. 195-208

DEHON Estelle/CAREY Pater, "Fair, Lawful and Transparent Processing", **Data Protection: A Practical Guide to UK and EU Law**, Editör: Peter Carey, Oxford: Oxford University Press, 2018, ss. 42-66

DEMİRCAN Tunç, **Bilişim Alanında Suçlar**, İstanbul: Legal Kitabevi, 2016

DEMİRBAŞ Timur, **Ceza Hukuku Genel Hükümler,** Ankara: Seçkin Yayıncılık, 2022

DENLEY Andrew/FOULSHAM Mark/HITCHEN Brian, **GDPR, How to Achieve and Maintain Compliance,** New York: Routledge, 2019

DEVELİOĞLU Hüseyin Murat, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması**, İstanbul: On İki Levha Yayıncılık, 2017

DOĞAN Bayram, **Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı**, Ankara: Adalet Yayınevi, 2022,

DOĞAN Koray, "Tüzel Kişilerin İdari Para Cezası Sorumluluğunda İsnadiyet Sorunu", **D.E.Ü. Hukuk Fakültesi Dergisi**, Cilt: 17 Sayı: 1, 2015, ss. 1-77

DÖNER Ayhan, "Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 26, Sayı: 1, 2022, ss. 23-60

DÜLGER Murat Volkan, **Kişisel Verilerin Korunması Hukuku,** İstanbul: Hukuk Akademisi, 2020,

EMİNAĞAOĞLU Mete/ GÖKŞEN Yılmaz, "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,** Cilt 11, Sayı: 4, 2009, ss. 1-15

ERARSLAN TÜRKMEN Sevgi, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, İstanbul On İki Levha, 2019

ERDOĞAN Irmak, **Yapay Zeka ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri**, Ankara: Seçkin Yayıncılık, 2022

ERDOĞAN Yavuz, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi", **Erciyes Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 8 Sayı: 2, 2013, ss. 569-632

EROĞLU Fulya, "5411 Sayılı Bankacılık Kanununa Göre İdari Para Cezaları Sistemi" **Suç ve Ceza Dergisi**, Sayı: 4, 2009, ss. 9-22

ERSOY Uğur, "Ceza Hukukunun Gri Alanı: Tehlike Suçları", **TAAD**, Yıl: 11 Sayı: 41, 2020, ss. 27-64

European Data Protection Board, **Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)**, Version 2.0, 2019, (https://edpb.europa.eu/our-work-tools/general-

guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_publication_type%3A64&page=4 E.T. 13.02.2023)

European Data Protectıon Board, **Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR**, Version 2.1, 2021, (https://edpb.europa.eu/system/files/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf E.T. 26.10.2022)

European Union Agency for Cybersecurity, **Guidelines for SMEs on the Security of Personal Data Processing**, 2016, (https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing E.T. 04.12.2022)

EVANS A. C., "European Data Protection Law", **The American Journal of Comparative Law,** Cilt: 29, Sayı: 4, 1981, ss. 571-582

EVİK Vesile Sonay, **Görevi Kötüye Kullanma Suçları,** İstanbul: On İki Levha Yayıncılık, 2019

FLEISCHMANN Amy, "Personal Data Security: Divergent Standarts in the European Union and the United States", **Fordham International Law Journal**, Cilt: 19, Sayı: 1, 1995, ss. 143-180

GEÇER Ahmet Emrah, "Vergi Ceza Hukukunda Non Bis İn İdem İlkesi", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 65 Sayı:2, 2016, ss. 315-348

GEKO Melisa/TJOA Simon, "An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security", **The Central European Cybersecurity Conference,** No: 19, 2018, ss. 1-6

GELLERT Raphaël, "Comparing Definitions of Data and Information in Data Protection Law and Machine Learning: A Useful Way Forward to Meaningfully Regulate Algorithms?", **Regulation & Governance**, Cilt: 16 Sayı: 1, 2020, ss. 156-176

GERÇEKER Hasan, **Yorumlu & Uygulamalı Türk Ceza Kanunu**, Ankara: Seçkin Yayıncılık, 2020

GONZÀLEZ FUSTER Gloria, **The Emergence of Personal Data Protection as a Fundemental Right of the EU**, Switzerland: Springer, 2014

GÖÇMEN UYARER Sinem, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,** Ankara: Seçkin Hukuk, 2020

GÜLEÇ Yahya Berkol, "Teoride ve Pozitif Hukukta Suç – Kabahat Ayrımı", **Kabahat Hukuku Yazıları**, Editrör: Zeynel T. Kangal, İstanbul: On İki Levha Yayıncılık, 2017

GÜNDÜZ Fatma Ebru/GÜNDÜZ Hakan, "Kabahatler Kanunu'na Göre Cumhuriyet Savcısı ve Mahkemenin İdari Yaptırım Karar Verme Yetkisi", **Adalet Dergisi,** Sayı: 68, 2022, ss. 111-131

GÜNGÖR Nevzat, **İç Denetimde Bilgi Teknolojileri ve Siber Güvenlik**, Ankara: Gazi Kitabevi, 2021

GÜRSEL İlke, **İşçinin Kişisel Verilerinin Korunması Hakkı**, İzmir: Doktora Tezi, Dokuz Eylül Üniversitesi, 2016

HAFIZOĞULLARI Zeki/ÖZEN Muharrem, **Türk Ceza Hukuku Genel Hükümler**, Ankara: US-A Yayıncılık, 2011

HAKERİ Hakan, **Ceza Hukuku Genel Hükümler/Temel Bilgiler**, Ankara: Astana Yayınları, 2020

HALLİNAN Dara/BORGESİUS Frederik Zuiderveen, "Opinions Can be Incorrect (in our opinion)! On Data Protection Law's Accuracy Principle", **International Data Privacy Law,** Cilt: 10 Sayı: 1, 2020, ss. 1-10

HENKOĞLU Türkay, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara: Yetkin Yayınları, 2015

HENKOĞLU Türkay, "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", **Arşiv Dünyası Dergisi**, Sayı: 18-19, 2017, ss. 46-56

HILL David, **Data Protection, Governance, Risk Management and Compliance**, Boca Raton: CRC Press Taylor & Francis Group, 2009

HONDIUS Frits W., "A Decade of International Data Protection" , **Netherlands International Law Review**, Cilt: 30 Sayı: 2, 1983, ss. 103-128

Information Commissioner's Office, **Guide to General Data Protection Regulation**, 2019, (https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf E.T. 04.12.2022)

IŞIKA Sertaç, **Gönüllü Vazgeçme**, İstanbul: On İki Levha Yayıncılık, 2021

İÇEL Kayıhan, **Ceza Hukuku Genel Hükümler**, İstanbul: Beta Yayıncılık, 2018

İMANÇLI Canan, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu,** İstanbul: On İki Levha Yayıncılık, 2020

İNAN Atilla İnan/DEMİR İbrahim, **Açıklamalı Gerekçeli Kabahatler Kanunu**, Ankara: Türkiye Belediyeler Birliği, 2014

İNCEOĞLU Asuman Aytekin, **Bankacılık Kanunu'nda Yer Alan Suçlar**,İstanbul: Marmara Üniversitesi Yayımlanmamış Doktora Tezi, 2006

KAMA IŞIK Sezen, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış,** İstanbul: On İki Levha Yayıncılık

KANGAL Zeynel T., **Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2022,

KANGAL Zeynel, **Kişisel Verilerin Ceza ve Kabahat Hukukunda Korunması**, İstanbul: On İki Levha Yayıncılık, 2019

Kangal Zeynel, **Ceza Hukukunda Zorunluluk Durumu**, Ankara: Seçkin Yayıncılık, 2010

KARAGÖZ Mehmet Can, **Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, İstanbul: On İki Levha Yayıncılık, 2020

KARINÇU Sümeyra, **Kişisel Verilerin Korunması Kanunu Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmemesi Kabahati**, Yüksek Lisans Tezi, İstanbul: İstanbul Üniversitesi, 2019

KART Aslıhan/KETİZMEN Muammer, "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", **Kişisel Verileri Koruma Dergisi,** Cilt: 1 Sayı: 2**,** 2019, ss. 17-29

KAŞIKARA Mustafa Serhat, "Kabahatler Kanunu'nun Yer ve Zaman Bakımından Uygulanması", **Kabahatler Hukuku Yazıları – I,** Editör: Zeynel T. Kangal, İstanbul, On İki Levha Yayıncılık, 2017, ss. 101-148

KAYIHAN Şaban/ÜNLÜTEPE Mustafa, **Medeni Hukuk Bilgisi**, Ankara: Seçkin Yayıncılık, 2017, 4. baskı

KAYIHAN Şaban, **Kişiler Hukuku,** Ankara: Seçkin Yayıncılık, 2022

KATOĞLU Tuğrul, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 61, Sayı: 2, 2012, ss. 657-694

KELEP PEKMEZ Tuba, **Ceza Muhakemesinde Fiil**, İstanbul: On İki Levha Yayıncılık, Eylül 2019

KILINÇ Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**,, Cilt: 61 Sayı: 3, 2012, ss. 1089-1172

Kişisel Verileri Koruma Kurumu(2019a), **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, Ankara: KVKK Yayınları, 2019

Kişisel Verileri Koruma Kurumu(2019b), **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, Ankara: KVKK Yayınları, 2019

Kişisel Verileri Koruma Kurumu(2019c), **100 Soruda Kişisel Verilerin Korunması Kanunu**, Ankara: KVKK Yayınları, 2019

Kişisel Verileri Koruma Kurumu(2019d), **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,** Ankara: KVKK Yayınları, 2019, No: 1

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi,** Ankara: KVKK Yayınları: No 41, 2022

Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Temel Kavramlar**, (https://kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022)

Kişisel Verileri Koruma Kurumu, Veri ihlal bildirim formu (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 21.11.2022)

Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022)

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler,** (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 04.12.2022)

Kişisel Verileri Koruma Kurumu, **6698 Sayılı Kanun'da Yer Alan Terimler**, (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 27.10.2022)

Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, Ankara: KVKK Yayınları, 2018

Kişisel Verileri Koruma Kurumu, **Kanun Kapsamında Hak ve Yükümlülükler**, (https://www.kvkk.gov.tr/Icerik/2030/Rehberler E.T. 26.10.2022)

Kişisel Verilerin Korunmasına Dair Eski Kanun Tasarıları ve Gerekçeleri Üzerine Karşılaştırma (2008-2014) Editör: Tuğba Karaer ve Burcu Sarı, Yayın No: 18, Yayım Tarihi 06.02.2015 (www.kanunum.com E.T. 24.06.2022)

KIRBY Michael D., "Transborder Data Flows and the "Basic Rules" of Data Privacy", **Stanford Journal of International Law,** Sayı: 16, 1980, ss. 27-66

KOCA Mahmut/ÜZÜLMEZ İlhan, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", **D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan**, C.21, Özel Sayı, 2019, ss. 69-93

KOCA Mahmut/ÜZÜLMEZ İlhan, **Türk Ceza Hukuku Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2021,

KOCA Mahmut/ÜZÜLMEZ İlhan, **Türk Ceza Hukuku Özel Hükümler**, Ankara: Adalet Yayınevi, 2016

KONUKPAY Cenk/TABAK Uğur, "Kişisel Verilerin İşlenme Amacının Sonradan Değişmesi: Uyumluluk Kriterlerinin Uygulanması Sorunu", **Kişisel Verileri Koruma Dergisi**, Cilt: 3 Sayı: 2, 2021, ss. 15-33

KORFF Douwe, **Ec Study on Implementation of Data Protection Directive Comparative Smmary of National Laws,** Cambridge: Human Right Centre, 2002, (https://gegevensbeschermingsrecht.nl/onewebmedia/douwe.pdf E.T. 04.12.2022)

KORKMAZ İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, İkinci Baskı, Ankara: Seçkin Yayıncılık, 2019

KÖSE AYSUN Melike, **Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135),** Ankara: Seçkin Yayıncılık, 2021

KÜLÇÜR İzzet Erdem, **Ceza Hukukunda Yer Bakımından Uygulama**, İstanbul: On İki Levha Yayıncılık, 2017

KÜZECİ Elif (2019a), **Kişisel Verilerin Korunması,** Ankara: Turhan Kitabevi, 2019

KÜZECİ Elif (2019b), "6698 Sayılı Kişisel Verilerin Korunması. Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", **İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi,** Cilt 16, Sayı 63, 2019, ss. 947-993

LAMBERT Paul, **Understanding the New European Data Protection Rules**, Boca Raton: CRC Press,, 2017

LENHARD Thomas H., **Data Security, Technical and Organizational Protection Measures against Data Loss and Computer Crime**, Wiesbaden: Springer, 2021

MADEN Mehmet, "Bir Tehlike Suçu Olarak "Gürültüye Neden Olma" (TCK, m. 83) ve Tehlike Suçlarına İlişkin Genel Tespitler", **Ankara Hacı Bayram Üniversitesi Hukuk Fakültesi Dergisi**, C. XXV, Y. 2021, ss. 431-470

MCCUMBER John, **Assessing and Managing Security Risk in IT Systems: A Structured Methodology**, Boca Raton: Auerbach Publications, 2005

MEMİŞ Tekin, "Veri Sorumlusu ile Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", **Beykent Üniversitesi Hukuk Fakültesi Dergisi,** Cilt: 3 Sayı: 6, Aralık 2017, ss. 9-23

MİRONENKO ENERSTVEDT Olga, **Avitation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles,** Cham Switzerland: Springer International Publishing, 2017

OECD, **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** France: OECD Publication Service, 2001

Oxford University, **The Concise Oxford Dictionary of English Etymology**, Editör: T. F. Hoad, New York: Oxford University Press, 1996

Oxford University, **The Oxford Dictionary of English Etymology**, Editör: C.T. Onions, New York: Oxford University Press, 1966

OTACI Cengiz/KESKİN İbrahim, **Türk Kabahatler Hukuku**, Ankara: Adalet Yayınevi, 2010

ÖZBEK Veli Özer/DOĞAN Koray Doğan/BACAKSIZ Pınar(2022a), **Türk Ceza Hukuku Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2022, on ikinci baskı

ÖZBEK Veli Özer/DOĞAN Koray Doğan/BACAKSIZ Pınar(2022b), **Türk Ceza Hukuku Özel Hükümler**, Ankara: Seçkin Yayıncılık, 2022

ÖZCAN Göknil, **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, İstanbul: On İki Levha, 2020

ÖZKAN Oğulcan, **Kişisel Verilerin Korunması**, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi, 2020

ÖZEN Mustafa,"5403 Sayılı Toprak Koruma ve Arazi Kullanımı Kanunu'nda Düzenlenen Kabahatler", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, 2015, C. 5 S. 1, ss. 203-226

ÖZEN Mustafa, **İdari Ceza Hukuku**, Ankara: Adalet Yayınevi, 2013

ÖZENÇ UÇAK Nazan, "Bilgi Üzerine Kuramsal Bir Yaklaşım", **Bilgi Dünyası**, Cilt: 1, Sayı: 1, 2000, ss. 143-159

ÖZER Yusuf Manzur, **Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler ve Hukuki Engeller**, İstanbul: On İki Levha Yayıncılık, 2020

ÖZOCAK Gürkan, **Türk Ceza Hukukunda Suça Teşebbüs**, Ankara: Seçkin Yayıncılık, 2018

ÖZTÜRK Bahri/ ALTINOK ÇALIŞKAN Elif/SEYHAN Serhan, **Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı**, Ankara: Seçkin Yayıncılık, 2021

ÖZTÜRK Bahri/ERDEM Mustafa Ruhan, **Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku,** Ankara: Seçkin Yayıncılık, 2021

ÖZTÜRK Şerif Ahmet, "Bankacılık Kanunu'nda Düzenlenen Kabahatler", **Kabahat Hukuku Yazıları -II**, Editör: Zeynel Kangal, İstanbul: On İki Levha Yayıncılık, 2018, ss. 161-205

PEHLİVAN Ali, **Kabahatler Hukukunun Genel Esasları**, İstanbul: Beta Basım Yayın, 2020

PEKMEZ Cüneyt, "Overview of the Definitions of Data controller and Data Processor within the Scope of the Turkish Code of Personal Data Protection (TCDP)", **Annales de la Faculté de Droit d'Istanbul,** Cilt: 0 Sayı: 67, 2018, ss. 47-63

PURTOVA Nadezhda, "The Law of Everything, Broad Concept of Personal Data and Future of EU Data Protection Law", **Law, Innovation and Technology**, Cilt: 10, Sayı: 1, 2018, ss. 40-81

RENÇBER Altan, **Kabahat Genel Teorisi Açısından Vergi Kabahatleri**, İstanbul: On İki Levha Yayıncılık, 2017

ROMANSKY Radi P./ NONINSKA Irina S., "Challenges of the Digital Age for Privacy and Personal Data Protection", **Mathematical Biosciences and Engineering**, Cilt: 17 Sayı: 5, 2020, ss. 5288-5303

ROSENBERG Daniel, "Data Before the Fact", **"Raw Data" is an Oxymoron**, Edited by Lisa Gitelman, London: MIT Press, 2013, ss. 15-41

SADOWSKI Jathan, "When Data is Capital: Datafication, Accumulation, and Extraction", **Big Data & Society**, 2019, ss. 1-12

SAYAR İbrahim Barış, "The Administrative Fines Regime of the General Data Protection Regulation and Its Impact", **Kişisel Verileri Koruma Dergisi,** C. 3 S. 1, 2021, ss. 1-16

SCHREIBER Arye, "Mere Access to Personal Data: Is It Processing?", **International Data Privacy Law**, 2020, Cilt 10, Sayı: 3, ss. 269-277

Selected Foreign National Data Protection Laws and Bills: Volume 1, Editor: Charles K. Wilk, Washington: U.S. Department of Commerce, Office of Telecommunications OT Special Publication, Cilt: 78 No: 19, 1978

SELZER Annika, "The Appropriateness of Technical and Organisational Measures under Article 32 GDPR", **European Data Protection Law Review**, Vol. 7, No. 1, 2021, ss. 456-470

SERRADO Joao/ PEREİRA Ruben Filipe/DA SİLVA Miguel Mira/ BİANCHİ Isaías Scalabrin, "Information Security Frameworks for Assisting GDPR Compliance in

Banking Industry", **Digital Policy, Regulation and Governance**; Cilt: 22 Sayı: 3, 2020, ss. 227-244

SERT Şeyma, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Ankara: Seçkin Yayıncılık, 2019

SEVİMLİ Ahmet, "Kişisel Verilerin Korunması Kanunu'ndaki Temel Kavramların İşçi-İşveren İlişkisindeki Karşılıkları", **İnşaat Sanayii Dergisi,** 2018, ss. 74-77

SOLOMON Michael G./ CHAPPLE Mike, **Information Security Illuminated**, Massachusetts: Jones and Barlett Publishers, 2005

ŞENTÜRK Aysan, **Veri Madenciliği**, Bursa: Ekin Basım Yayın, 2006

TAN İbrahim, "Sporda Şiddete Neden Olabilecek Açıklamalarda Bulunma Kabahati", **Kabahat Hukuku Yazıları – II,** Editör: Zeynel Kangal, İstanbul: On İki Levha Yayıncılık, 2018

TAN Mehmet, **Türk Ceza Kanunu Genel Hükümler**, Ankara: Seçkin Yayıncılık, 2011

TANSUĞ Çağla, İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması, İstanbul: On İki Levha Yayıncılık, 2023

TAŞTAN Furkan Güven, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul: On iki Levha Yayıncılık, 2019

TEERWANGNE Cécile de, "Article 5. Principles Relating to Processing of Personal Data", **GDPR: A Commentary**, Editörler: Lee A. Bygrave, Luca Tosoni ve Christopher Docksey, New York: Oxford University Press. 2020, ss. 309-320

The Swedish Data Bank Statute and Regulation of May 11, 1973, Çeviren: Finn Henriksen, Library of Congress Law Library, Cilt: 73 No: 2, 1973

TOP Elçin, "Yemek Sepeti'nden siber saldırı iddialarına ilişkin açıklama: Veri sızıntısı yok", Euronews, 16.11.2021. (https://tr.euronews.com/2021/11/16/yemek-sepeti-nden-siber-sald-r-iddialar-na-iliskin-ac-klama-veri-s-z-nt-s-yok# E.T. 07.11.2022)

TÖNGÜR Ali Rıza/ÇETİNTÜRK Ekrem, **Ceza Hukuku Genel Hükümler**, Ankara: Adalet Yayınevi, 2020, birinci baskı

TURAN Metin, **Kişisel Verilerin Korunması,** Ankara: Seçkin Yayıncılık, 2021, 4. Baskı,

Türkiye Cumhuriyeti Adalet Bakanlığı, İnsan Hakları Eylem Planı, 2021, (https://insanhaklarieylemplani.adalet.gov.tr/ E.T. 17.02.2023)

UĞUR Hüsamettin, "Kabahatler Kanunu ve 5252 Sayılı Kanun'a Göre İdari Para Cezası ve Yargıtay Uygulaması, **TBB Dergisi**, Sayı: 85, 2009, ss. 189-219

UNCULAR Selen, **İş İlişkisinde İşçinin Kişisel Verilerin Korunması**, Ankara: Seçkin Yayıncılık, 2018

USLU Ferhat/KUTKAN Oğuzcan, Kabahatler Hukukunda Tüzel Kişilerin Sorumluluğu, **D.E.Ü. Hukuk Fakültesi Dergisi**, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı,2017, ss. 2803-2819

ÜNSAL Burçak/ÖZDEMİR Kaan, "Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) Kapsamında Veri Kayıt Sistemi", **İstanbul Barosu Dergisi**, Cilt: 93 Sayı: 3, 2019, ss. 254-257

ÜNSAL ÖZDEN Sevgi/UZ İdil/KARAMUSTAFAOĞLU Mert, "Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği", **Kişisel Verileri Koruma Dergisi,** Cilt: 3, Sayı: 1, 2021, ss. 17-40

VAN ALSENOY Brendan, **Data Protection Law in Eu: Roles, Resposibilities, and Liability,** Cambridge: Intersentia, 2019

VOİGT Paul/ VON DEM BUSSCHE Axel, **The EU General Data Protection Regulation**, Cham: Springer, 2017

VON SOLMS SH BASIE/ VON SOLMS Rossouw, **Information Security Governance**, New York: Springer, 2009

WOLTERS P. T. J., "The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility", **International Data Privacy Law,** Cilt: 7, Sayı: 3, 2017, ss. 165-178

WONG Rebecca, **Data Security Breaches and Privacy in Europe**, London: Springer London, 2013

YAKIŞIR Ceren, **Türk Ceza Kanunu'nda Kişisel Verilerin Basın Yoluyla Açıklanması Suçu**, İstanbul: On iki Levha Yayıncılık, 2019

YALÇIN İsmail, **Tüm Yönleriyle Kabahatler Hukuku**, Ankara: Seçkin Yayıncılık, 2007, birinci baskı

YAMAKOĞLU Efe, **Bilişim Teknolojilerinin Kullanılmasının İş Sözleşmesinin Taraflarının Fesih Hakkına Etkisi**, İstanbul: On İki Levha Yayıncılık, 2020
YILMAZ Berna Ayşen, **Yardım veya Bildirim Yükümlülüğünün Yerine Getirilmemesi Suçu**, Ankara: Adalet Yayınevi, 2020

YOSİF Umniyahasghar, "Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler", **Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi,** Cilt: 4 Sayı: 1, ss. 1-22

YURTCAN Erdener, **Yargıtay Kararları Işığında Kabahatler Kanunu ve Uygulaması**, İstanbul: Aristo Yayınevi, 2020, 4. baskı

YURTLU Fatih, **İhmali Suçlar,** Ankara: Seçkin Yayıncılık, 2022

YÜCEDAĞ Nafiye, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", **Kişisel Verileri Koruma Dergisi,** Cilt: 1 Sayı: 1, 2019, ss. 47-63

ZAFER Hamide, **Ceza Hukuku Genel** Hükümler, İstanbul: Beta Yayıncılık, 2010

ZİNS Chaim, "Conceptual Approaches for Defining Data, Information and Knowledge", **Journal of the American Society For Information Science and Technology**, Cilt: 58, Sayı: 4, 2007, ss. 479-493

ZOR Abdulhamid, **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, İstanbul, On İki Levha, 2020

KARARLAR:

Kişisel Verileri Koruma Kurulu 13.02.2020 tarihli 2020/124 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6886/2020-124 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 03.03.2020 tarihli ve 2020/191,192,193,194 sayılı kararları (https://www.kvkk.gov.tr/Icerik/6762/2020-191-192-193-194 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli 2019/23 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5464/2019/52 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.01.2020 tarihli 2020/32 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6700/2020-32 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu 24.11.2020 tarihli 2020/905 sayılı kararı (https://kvkk.gov.tr/Icerik/6862/2020-905 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu 27.04.2021 tarihli 2021/426 sayılı kararı (https://kvkk.gov.tr/Icerik/6981/2021-426 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5423/2018-131 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu 2020/307 sayılı karar (https://www.kvkk.gov.tr/Icerik/6895/2020-307 E.T. 27.10.2022)

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/273 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6710/2019-273 E.T. 27.10.2022)

Kişisel Verileri Koruma Kurulu'nun 30.06.2020 tarihli ve 2020/507 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6926/2020-507273 E.T. 27.10.2022)

Kişisel Verileri Koruma Kurulu'nun 11.08.2021 tarihli 2020/608 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6927/2020-608 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 30.10.2019 tarihli 2019/316 sayılı karar (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 30.10.2019 tarihli 2019/316 sayılı karar. (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 2019/47 sayılı karar (https://www.kvkk.gov.tr/Icerik/5462/2019/47 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 2020/379 sayılı karar (https://www.kvkk.gov.tr/Icerik/6911/2020-379 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 2020/307 sayılı karar (https://www.kvkk.gov.tr/Icerik/6895/2020-307 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 2020/255 sayılı karar(https://www.kvkk.gov.tr/Icerik/6894/2020-255 E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu'nun 09.02.2021 tarihli ve 2021/111 sayılı kararı (https://www.kvkk.gov.tr/ E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu 30.01.2020 tarihli ve 2020/71 sayılı kararı (https://www.kvkk.gov.tr E.T. 26.10.2022)

Kişisel Verileri Koruma Kurulu'nun 19.03.2020 tarihli ve 2020/226 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6893/2020-226 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 13.02.2020 tarihli ve 2020/120 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6923/2020-120 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 01.10.2019 tarihli ve 2019/294 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6556/2019-294 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 03/02/2021 tarihli ve 2021/85 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7112/2021-85 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu 31.05.2019 tarihli ve 2019/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5494/2019-159 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu, 2020/66 sayılı kararı Kişisel Verileri Koruma Kurulu 27.01.2020 tarihli ve 2020/66 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6873/2020-66 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu 12.03.2020 tarihli ve 2020/212 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/6892/2020-212 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli ve 2021/891 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7045/whatsapp-uygulaması-hakkında-yurutulen-resen-ıncelemeye-ılıskın-kamuoyu-duyurusu E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 1.12.2020 tairhli ve 2020/915 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6872/2020-915 E.T. 25.02.2023)

Kişisel Verileri Koruma Kurulu'nun 1.12.2020 tairhli ve 2020/915 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6872/2020-915 E.T. 5.02.2023)

Kişisel Verileri Koruma Kurulu 25.03.2019 tarihli ve 2019/81 sayılı ile 31.05.2019 tarihli ve 2019/165 sayılı kararları (https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 E.T. 26.02.2023)

Kişisel Verileri Koruma Kurulu'nun 28.06.2018 tarihli ve 2018/169 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5366/2018-69 E.T. 26.02.2023)

Kişisel Verileri Koruma Kurulu'nun 09.12.2021 tarihli 2021/1243 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7274/2021-1243 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarihli 2021/889 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7139/2021-889 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 02.11.2021 tarihli 2021/1111 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/7266/2021-1111 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 06.01.2022 tarihli ve 2022/13 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7179/2022-13 E.T. 28.02.2023)

Kişisel Verileri Koruma Kurulu'nun 06.07.2021 tarihli 2021/670 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7136/2021-670 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarihli 2018/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/4110/2018-10 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 21.12.2017 tarihli ve 2017/61 sayılı ilke kararı, 30312 sayılı 25 Ocak 2018 tarihli Resmi Gazete'de yayımlanmıştır.

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/269 sayılı kararı (https://kvkk.gov.tr/Icerik/5534/2019-269 E.T. 12.02.2023)

Kişisel Verileri Koruma Kurulu'nun 11.04.2019 tarihli ve 2019/104 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5450/2019-104 E.T. 12.02.2023)

Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/144 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5487/Cathay-Pasific-Airway-Limited-Hakkinda-Kisisel-Verileri-Koruma-Kurulunun-16-05-2019-Tarih-ve-2019-144-Sayili-Karar-Ozeti E.T. 12.02.2023)

Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/143 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5479/2019-143 E.T. 12.02.2023)

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.02.2023)

Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli 2019/122 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/5461/2019/122 E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarih ve 2020/172 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6890/2020-172 E.T. 21.11.2022)

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 02.03.2023)

Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/187 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6891/2020-187 E.T. 19.11.2022)

Kişisel Verileri Koruma Kurulu'nun 05.12.2018 tarihli ve 2018/143 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5364/2018-143 E.T. 19.11.2022)

Kişisel Verileri Koruma Kurulu'nun 02.11.2021 tarihli 2021/1111 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7266/2021-1111 E.T. 13.11.2022)

Kişisel Verileri Koruma Kurulu'nun 16.04.2020 tarihli ve 2020/286 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6763/2020-286 E.T. 12.11.2022)

Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli 2021/1304 sayılı ilke kararı, 20 Ocak 2022 tarihli 31725 Sayılı Resmi Gazete.

Kişisel Verileri Koruma Kurulu'nun 18.01.2022 tarihli 2022/31 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7292/2022-31 E.T. 05.03.2023)

Kişisel Verileri Koruma Kurulu'nun 02.12.2021 tarihli 2021/1217 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7271/2021-1217 E.T. 05.03.2023)

Kişisel Verileri Koruma Kurulu'nun 02.04.2020 tarihli ve 2020/255 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6894/2020-255 E.T. 05.03.2023)

Kişisel Verileri Koruma Kurulu'nun 22.07.2022 tarih 2020/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6790/2020-559 E.T. 12.12.2022)

Kişisel Verileri Koruma Kurulu'nun 14.05.2020 tarihli ve 2020/379 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6911/2020-379 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 27.02.2020 tarihli ve 2020/167 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6738/2020-167 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 31.05.2019 tarihli ve 2019/159 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5494/2019-159 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli ve 2021/1324 sayılı Kararı (https://kvkk.gov.tr/Icerik/7168/2021-1324 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 06.05.2021 tarihli ve 2021/470 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6982/2021-470 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 15.12.2020 tarihli ve 2020/957 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7020/2020-957 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 05.05.2020 tarihli ve 2020/345 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7027/2020-345 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/144 sayılı Kararı (https://kvkk.gov.tr/Icerik/5480/2019-144 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 05.05.2020 tarihli ve 2020/336 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6910/2020-336 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.01.2020 tarihli ve 2020/32 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6700/2020-32 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli ve 2019/23 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5464/2019/52 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 02.05.2019 tarihli ve 2019/122 sayılı Kararı, (https://www.kvkk.gov.tr/Icerik/5461/2019/122 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 27.09.2019 tarihli ve 2019/254 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5535/2019-254 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarihli ve 2019/269 sayılı Kararı (https://kvkk.gov.tr/Icerik/5534/2019-269 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 27.08.2019 tarihli ve 2019/255 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5537/2019-255 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 05.12.2018 tarihli ve 2018/143 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5364/2018-143 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 28.05.2020 tarihli ve 2020/429 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6778/2020-429 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 09.07.2020 tarihli ve 2020/532 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7032/2020-532 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/465 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7031/2020-465 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/143 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/5479/2019-143 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli ve 2018/131 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5423/2018-131 E.T. 04.03.2023)

Kişisel Verileri Koruma Kurulu'nun 30.10.2019 tarihli ve 2019/136 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 04.03.2023)

Kişisel Verileri Koruma Kurulu'nun 22.05.2020 tarihli ve 2020/414 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6915/2020-414 E.T. 04.03.2023)

Kişisel Verileri Koruma Kurulu'nun 30.09.2021 tarihli ve 2021/989 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7143/2021-989 E.T. 04.03.2023)

Kişisel Verileri Koruma Kurulu'nun 30.10.2019 tarihli ve 2019/316 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6876/2019-316 E.T. 04.03.2023)

Kişisel Verileri Koruma Kurulu'nun 16.04.2020 tarihli ve 2020/286 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6763/2020-286 E.T. 05.03.2023)

Kişisel Verileri Koruma Kurulu'nun 24.11.2020 tarihli ve 2020/905 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6862/2020-905 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 27.04.2021 tarihli ve 2021/427 sayılı kararı. (https://www.kvkk.gov.tr/Icerik/6981/2021-427 E.T. 05.03.2023)

Kişisel Verileri Koruma Kurulu'nun 06.02.2020 tarihli 2020/86 sayılı kararı (https://www.kvkk.gov.tr/Icerik/6732/2020-86 E.T. 14.02.2023)

Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarihli 2019/9 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu E.T. 15.02.2023)

Kişisel Verileri Koruma Kurulu'nun 24.12.2018 tarihli ve 2018/156 sayılı kararı (https://www.kvkk.gov.tr/Icerik/5425/2018-156 E.T. 14.02.2023)

Kişisel Verileri Koruma Kurulu'nun 16.05.2019 tarihli ve 2019/144 sayılı Kararı (https://kvkk.gov.tr/Icerik/5480/2019-144 E.T. 11.03.2023)

Kişisel Verileri Koruma Kurulu'nun 23.12.2021 tarihli ve 2021/1324 sayılı kararı (https://www.kvkk.gov.tr/Icerik/7168/2021-1324 E.T. 07.11.2022)

Kişisel Verileri Koruma Kurulu'nun 25.03.2021 tarihli ve 2021/311 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7001/2021-311 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 24.11.2020 tarihli ve 2020/905 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6862/2020-905 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 20.04.2021 tarihli ve 2021/407 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6993/2021-407 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 07.05.2020 tarihli ve 2020/357 sayılı Kararı (https://kvkk.gov.tr/Icerik/7014/2020-357 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/466 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/6995/2020-466 E.T. 12.06.2023)

Kişisel Verileri Koruma Kurulu'nun 16.06.2020 tarihli ve 2020/463 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/7030/2020-463 E.T. 12.06.2023)

Danıştay Kararı - 13. D., E. 2014/1921 K. 2019/3591 T. 13.11.2019 (lexpera.com.tr E.T. 20.11.2022)

Danıştay Kararı - 13. D., E. 2019/2694 K. 2021/1471 T. 20.4.2021 (Lexpera.com.tr E.T. 20.02.2023)

Yargıtay Kararı - 19. Ceza Dairesi 2018/2119 E. 2018/5852 K. (https://www.lexpera.com.tr/ictihat/yargitay/19-ceza-dairesi-e-2018-2119-k-2018-5852-t-9-5-2018 E.T. 08.02.2023)

Yargıtay Kararı - CGK., E. 2017/829 K. 2017/363 T. 4.7.2017 (https://www.lexpera.com.tr/ictihat/yargitay/ceza-genel-kurulu-e-2017-829-k-2017-363-t-4-7-2017 E.T. 11.03.2023)

Yargıtay Kararı - 19. CD., E. 2015/13639 K. 2016/16037 T. 20.4.2016 E.T. 03.06.2023 (www.lexpera.com.tr E.T. 03.06.2023)

Anayasa Mahkemesi Kararı, Esas Sayısı : 2014/74 Karar Sayısı : 2014/201 Karar Tarihi : 25.12.2014 R.G. Tarih-Sayı : 23.5.2015-29364

CJEU - C-210/16 - Wirtschaftsakademie (Facebook Fan page), (https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5127976
E.T. 27.10.2022)

Fashion ID GmbH & Co. KG ECLI:EU:C:2019:629 para. 70, Google Spain SL, Google Inc. ECLI:EU:C:2014:317 (https://curia.europa.eu/juris/liste.jsf?num=C-40/17
E.T. 26.10.2022)

Peter Nowak v. Data Protection Comissioner, 2017, ECLI:EU:C:2017:994,
(https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0434
E.T. 25.02.2023)

Case of Franz Fischer v. Austria (Application no. 37950/97) (https://hudoc.echr.coe.int/fre-press?i=001-59475 E.T: 12.06.2023)

ÖZGEÇMİŞ

[redacted]

TEZ ONAY SAYFASI

Üniversite	: T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	: SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	: Mehmet Semih ÖZTEKİN
Tez Başlığı	: Kişisel Veri Güvenliğine İlişkin Yükümlülüklerin Yerine Getirilmemesi Kabahati
Savunma Tarihi	: 22/06/2023
Danışman	: Prof. Dr. E. Eylem AKSOY RETORNAZ

JÜRİ ÜYELERİ:

Unvan, Ad-Soyadı İmza

Prof. Dr. E. Eylem AKSOY RETORNAZ

Prof. Dr. Çağla TANSUĞ

Doç. Dr. Kadir Berk KAPANCI

Prof. Dr. Ulun Akturan
Enstitü Müdürü