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

KİŞİSEL VERİLERİN CEZA HUKUKU YÖNÜNDEN KORUNMASI

YÜKSEK LİSANS TEZİ

Nil Melek GÜLTEKİN

Tez Danışmanları: Prof. Dr. Mehmet Emin ARTUK – Doç. Dr. Ümit KOCASAKAL

Mayıs 2012

ÖNSÖZ

Kişisel verilerin korunması hususunu incelediğim tezimi hazırlarken, tereddüde düştüğüm ve değerli bilgilerine ihtiyaç duyduğum zaman kıymetli yardımlarını ve zamanlarını benden esirgemeyen tez danışmanlarım ve hocalarım Sayın Prof. Dr. Mehmet Emin ARTUK ve Sayın Doç. Dr. Ümit KOCASAKAL'a, tez konumu belirlediğim süreçte, üzerinde fazla çalışılmamış bir alan olması sebebiyle beni kişisel verilerin korunması konusuna yönlendirerek bu konuyu seçmeme vesile olan, ofisinde yaptığım avukatlık stajı süresince ve sonrasında akademik hayata adım atarken değerli bilgilerini benden esirgemeyen ve her daim kıymetli desteğini hissettiğim hocam Sayın Prof. Dr. A. Köksal BAYRAKTAR'a, araştırma görevlisi olma yolunda önümü daha net görmemi sağlayarak hedefime ulaşmamda bana çok kıymetli desteklerini veren ve üzerimde büyük emekleri bulunan Sayın Prof. Dr. Mehmet HELVACI ve eşi Prof. Dr. Serap HELVACI'ya, Marmara Üniversitesi'nde araştırma görevlisi olarak çalışmaya başladığım tarihten itibaren kıymetli bilgilerini ve desteğini esirgemeyen hocam Sayın Doç. Dr. A. Caner YENİDÜNYA'ya, değerli fikirleri, bilgileri ve destekleriyle bana yardımcı olan Marmara Üniversitesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı araştırma görevlilerine, özellikle tezimin son aşamalarında hataların ve eksikliklerin düzeltilmesinde bana değerli zamanını ayıran ve emeğini esirgemeyen Av. Pelin PORTAKALKÖKÜ'ne ve son olarak; hayatım boyunca her koşulda ve attığım her adımda yanımda olarak beni destekleyen aileme sonsuz teşekkürlerimi sunarım.

Nil Melek GÜLTEKİN

İÇİNDEKİLER

ÖNSÖZ……...……ii
İÇİNDEKİLER……...……iii
KISALTMALAR……...……...……....viii
RÉSUMÉ……...……...xi
ABSTRACT…..……..……..…….....xvii
ÖZET……..…….……xxii

GİRİŞ.....1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE ULUSLARARASI İLE ULUSAL KAYNAKLARDA KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ.....6
A. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİ HUKUKU KAPSAMINDA ÖNEM ARZ EDEN BAZI KAVRAMLAR……....6
1. Kişisel Veri……...6
2. Kişisel Verinin İşlenmesi…….8
3. Veri Öznesi/İlgili Kişi……..……8
4. Özel Hayatın Gizliliği/Mahremiyet/Gizlilik…...…..……...……8
5. Veri Denetçisi……...……...……...9
B. KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ……..…9
II. KİŞİSEL VERİLERİN KORUNMASININ HUKUKİ YAPILANMASI…….11
A. ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI……11
1. Genel Bilgiler……...11
2. Ekonomik İşbirliği ve Kalkınma Teşkilatı Sözleşmesi (OECD Convention).....12
3. Avrupa Konseyi ve Kişisel Verilerin Korunması……..……15

a. Genel Bilgiler……...15
b. 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme……..16
c. Avrupa İnsan Hakları Sözleşmesi (AİHS)…….....18
4. Birleşmiş Milletler…….27
5. Avrupa Birliği'nde Kişisel Verilerin Korunması……..29
a. Genel Bilgiler……29
b. Avrupa Birliği Temel Haklar Şartı…….…..31
c. 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi.....32
B. BAZI ÜLKELERDE KİŞİSEL VERİLERİN KORUNMASI…..……36
1. Genel Bilgiler……....36
2. Kıta Avrupa'sında Kişisel Verilerin Korunması……..……38
a. Fransa……38
(1) Fransız Ceza Kanunu……..38
(2) 1978 Tarihli Veri Koruma Kanunu……....40
b. İsviçre……...43
(1) Genel Bilgiler……43
(2) İsviçre Federal Anayasası……..…….44
(3) İsviçre Medeni Kanunu…….……44
(4) İsviçre Ceza Kanunu…….……45
(5) Verilerin Korunmasına İlişkin Federal Kanun (LDP).……...46
c. Almanya……48
(1) Alman Ceza Kanunu……..49
(2) Alman Ceza Muhakemesi Kanunu (StPO) ……....51
(3) Alman Veri Koruma Kanunu……52
3. Anglo – Saxon Ülkelerde Kişisel Verilerin Korunması.……55
a. Amerika Birleşik Devletleri……..……....55
b. İngiltere……59
c. Kanada……...……...……61
d. Yeni Zelanda……...……...……...62
C. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI……..64
1. 1982 tarihli Türkiye Cumhuriyeti Anayasasında Kişisel Verilerin Korunması……....…….65

2. İlgili Kanun ve Yönetmeliklerde Kişisel Verilerin Korunması…..…….68
a. Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu.....68
b. Medeni Kanun ve Borçlar Kanunu……...69
c. İş Kanunu……..71
d. Bankacılık Kanunu ve Banka Kartları ve Kredi Kartları Kanunu……72
e. Noterlik Kanunu…….……...74
f. Adli Sicil Kanunu…….…….74
g. Nüfus Hizmetleri Kanunu…….75
h. Türkiye İstatistik Kurumu Kanunu ve Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik...76
i. Hasta Hakları Yönetmeliği…..……...78
j. Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik……..……80

İKİNCİ BÖLÜM

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. CEZA HUKUKU YÖNÜNDEN KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ÇALIŞMALAR……...……...……..83
A. Kişisel Verilerin Korunması Hakkında Kanun Tasarısı.....…….....83
B. DNA Verilerinin Tasarı ve Ceza Muhakemesi Kanunu Kapsamında Korunması …….....….102
1. Ceza Muhakemesi Kanunu'ndaki Düzenleme…….....104
2. DNA Verileri ve Milli DNA Veri Bankası Kanunu Tasarısı…….....….....107
II. 5237 SAYILI TÜRK CEZA KANUNUNDAKİ DÜZENLEMELER…...….....115
A. Genel Bilgiler……...……...……115
B. Türk Ceza Kanunu'nda Kişisel Verilere İlişkin Düzenlemelerin Tarihçesi.....118
C. Türk Ceza Kanunu'nda (TCK) Kişisel Verilere İlişkin Düzenlemeler……...121
1. TCK m. 135: Kişisel Verilerin Kaydedilmesi…….....121
a. Genel Bilgiler……...……...……...……121
b. Suçla Korunan Hukuki Değer……...……...…….……124
c. Suçun Unsurları……...…….……...……...126

(1) Maddi Unsurlar……..…….....…….....126
(a) Fiil……...……...……126
(b) Fail……...……...……...128
(c) Mağdur……...…….....129
(d) Konu……...…….....129
(e) Netice……...…….....131
(f) Suçun Nitelikli Unsurları…….……...……...132
aa. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetki Kötüye Kullanılmak Suretiyle İşlenmesi……...133
ab. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi……...……...……134
(2) Manevi Unsur……...…….....……...136
(3) Hukuka Aykırılık……...…….....138
d. Suçun Özel Görünüş Şekilleri……...…….148
(1) Teşebbüs……...…….....148
(2) İştirak……...…….....149
(3) İçtima……...…….....150
e. Yaptırım……...…….....156
f. Soruşturma Usulü, Görevli ve Yetkili Mahkeme, Dava Zamanaşımı….158
2. TCK m. 136: Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme...160
a. Genel Bilgiler……...……...…….....160
b. Suçla Korunan Hukuki Değer……...……...……161
c. Suçun Unsurları.……...…….....161
(1) Maddi Unsurlar……...…….....161
(a) Fiil……...…….....161
(b) Fail……...…….....164
(c) Mağdur……...…….....165
(d) Konu……...……...…….....165
(e) Netice……....…….....166
(f) Suçun Nitelikli Unsurları…...…….……...……...166
(2) Manevi Unsur……...…….....166
(3) Hukuka Aykırılık…….……...…….....167
d. Suçun Özel Görünüş Şekilleri……...…….169
(1) Teşebbüs……...…….....169

(2) İştirak……..…….....170
(3) İçtima……..…….....170
e. Yaptırım……..…….....179
f. Soruşturma Usulü, Görevli ve Yetkili Mahkeme, Dava Zamanaşımı....179
3. TCK m. 138: Verileri Yok Etmeme……...…….....180
a. Genel Bilgiler……..……...…….....180
b. Suçla Korunan Hukuki Değer……...……...…….183
c. Suçun Unsurları……..…….....184
(1) Maddi Unsurlar……..…….....184
(a) Fiil……..…….....184
(b) Fail……..…….....186
(c) Mağdur……..…….....187
(d) Konu……..…….....187
(e) Netice.....192
(f) Suçun Nitelikli Unsurları…….……...……193
(2) Manevi Unsur ……..…….....193
(3) Hukuka Aykırılık……..…….....194
d. Suçun Özel Görünüş Şekilleri…….……...……194
(1) Teşebbüs……..…….....194
(2) İştirak……..…….....195
(3) İçtima……..…….....195
e. Yaptırım……..…….....196
f. Soruşturma Usulü, Görevli ve Yetkili Mahkeme, Dava Zamanaşımı…197

SONUÇ……....……198
KAYNAKÇA……...……202
ÖZGEÇMİŞ……...…….....220

KISALTMALAR

AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
ADN	**:** L'acide désoxyribonucléique (Deoksiribonükleik asit)
AİHM	**:** Avrupa İnsan Hakları Mahkemesi
AİHS	**:** Avrupa İnsan Hakları Sözleşmesi
Ar. Gör.	**:** Araştırma Görevlisi
Art.	**:** Article (Madde)
AT	**:** Avrupa Topluluğu
av. J.-C.	**:** avant Jésus-Christ (Milattan Önce)
BC	**:** Before Christ (Milattan Önce)
BDSG	**:** Bundesdatenschutzgesetz (Federal Veri Koruma Kanunu)
bkz.	**:** Bakınız
BM	**:** Birleşmiş Milletler Örgütü
CE	**:** Communauté Européenne (Avrupa Topluluğu)
CMK	**:** Ceza Muhakemesi Kanunu
CNIL	**:** La Commission Nationale de l'Informatique et des Libertés (Enformatik ve Özgürlükler Milli Komisyonu)
CPT	**:** Code Pénal Turc
çev.	**:** Çeviren
DCRI	**:** Direction Centrale du Renseignement Intérieur (Merkezi İçişleri İstihbarat Yönetimi)
der.	**:** Derleyen
dn.	**:** Dipnot
DNA	**:** Deoksiribonükleik asit
E.	**:** Esas
EC	**:** European Community (Avrupa Topluluğu)
EEA	**:** Avrupa Birliği ülkeleri ve Norveç, İzlanda, Lihtenstein

EU	**:** European Union (Avrupa Birliği)
Europol	**:** European Police Office (Avrupa Polis Teşkilatı)
f.	**:** Fıkra
FDPIC	**:** Federal Data Protection and Information Commissioner (İsviçre Federal Veri Koruma ve Danışma Komiseri)
Fedpol	**:** The Federal Office of Police (Federal Polis)
FIS	**:** Federal Intelligence Service (Federal İstihbarat Servisi)
FOIA	**:** US Freedom of Information Act (Bilgi Edinme Özgürlüğü Kanunu)
GBT	**:** Genel Bilgi Toplama
GLBA	**:** Gramm-Leach-Bliley Act (Finansal Hizmetleri Modernleştirme Kanunu)
IP	**:** İnternet Protokol
ISCTurkey 2010	**:** 4. Uluslar arası Bilgi Güvenliği ve Kriptoloji Konferansı
JUDEX	**:** Système Judicaire de Documentation et d'Exploitation (Adli Belgeleme Ve Kullanma Sistemi)
K.	**:** Karar
K.n.	**:** Kanun numarası
KVKT	**:** Kişisel Verilerin Korunması Kanunu Tasarısı
LPD	**:** Loi Fédérale sur la Protection des Données (Verilerin Korunmasına İlişkin Federal Kanun)
m.	**:** Madde
M.Ö.	**:** Milattan Önce
MK	**:** Medeni Kanun
n.	**:** Numéro (Numara)
OECD	**:** The Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
OEEC	**:** Organisation for European Economic Co-operation (Avrupa Ekonomik İşbirliği Örgütü)
prg.	**:** Paragraf
PVSK	**:** Polis Vazife ve Selahiyet Kanunu
R.G	**:** Resmi Gazete
R.G.t.	**:** Resmi Gazete tarihi
s.	**:** Sayfa

S.	**:** Sayı
SIS	**:** Système d'Information Schengen (Schengen Enformasyon Sistemi)
STIC	**:** Système de Traitement des Infractions Constatées (Tespit Edilmiş İhlalleri Ele Alma Sistemi)
StPO	**:** Strafprozeßordnung (Alman Ceza Muhakemesi Kanunu)
t.	**:**Tarih
T	**:** Tarihli
T.C.	**:** Türkiye Cumhuriyeti
TBMM	**:** Türkiye Büyük Millet Meclisi
TCK	**:** Türk Ceza Kanunu
TPC	**:** Turkish Penal Code (Türk Ceza Kanunu)
U.K.	**:** United Kingdom (İngiltere)
UE	**:** Union Européenne (Avrupa Birliği)
v.	**:** Versus (Karşı)
vb.	**:** Ve benzeri
vd.	**:** Ve devamı
Vol.	**:** Volume (Cilt)

RÉSUMÉ

Dans les documents internationaux, dans le préambule de l'article 135 du Code Pénal Turc (CPT) et dans les législations nationales des pays qui sont examinés dans le cadre de ce travail, la notion de «données à caractère personnel » a été définie en tant que « toute informations relatives à une personne physique identifiée ou identifiable. » Dans ce cas, le nom d'une personne, le prénom, la photo, le numéro de téléphone, l'ADN, les données dactyloscopiques, sont traités comme des données personnelles. La Cour Européenne des Droits de l'Homme, a décidé que même la voix des personnes, doit être considérée comme des données personnelles. Certaines données personnelles, cependant, en raison de leur nature, ont été classées en tant que données personnelles sensibles et, dans presque tous les textes nationaux-internationaux il leur a été assuré une protection spéciale. Les origines raciales et ethniques des individus, la vie sexuelle, les opinions politiques, religieuses ou philosophiques, la santé ou l'information du casier judiciaire sont considérés comme des données personnelles sensibles.

Bien que les règlements concernant la protection des données personnelles aient gagné de l'importance après la Seconde Guerre Mondiale, le devoir des médecins de respecter le secret médical résultant du 5ème siècle av. J.-C. est l'un des premiers exemples de la protection des données personnelles. Cette obligation, qui prévoit que les médecins ne doivent pas divulguer les renseignements personnels qu'ils ont acquis au sein de leur profession, est l'une des premières étapes pour la protection des données personnelles.

L'importance de la protection des renseignements personnels a d'abord émergé aux États-Unis dans les années 1950 et 1960 avec l'arrivée des premiers ordinateurs et le début de stockage et de transferts de données. En particulier après la Seconde Guerre Mondiale, la crainte des pays européens de l'utilisation abusive des

données personnelles collectées et stockées a fait surgir des discussions sur la protection des données personnelles.

La principale évolution sur les données personnelles a commencé dans les années 1970. La plupart des études législatives dans les pays Européens ont débuté dans les années mi-soixante-dix et les lois protégeant les données personnelles ont été adoptées entre les années mi-soixante-dix et quatre-vingt-dix. La première législature sur la protection des données personnelles a été faite en Allemagne en fin des années soixante dans le cadre du "Plan d'Hesse», qui a finalement abouti en 1970 en tant qu'un projet de loi réglementant la fondation d'une banque de données centrale. Plus tard, en 1977 la Loi de Protection des Données a été adoptée en Allemagne, mais a été très critiquée parce que la tâche de protection des données avait été laissée au Ministre de l'Intérieur. Dans les années suivantes la Loi sur la protection des renseignements personnels a été promulgué aux États-Unis en 1974 et de même, des lois spéciales de protection des données personnelles ont été légiféré dans d'autres pays tels que, en Suède (1973), en France (1978), en Allemagne (1977), en Suisse (1984), au Royaume-Uni (1984) et au Canada (1985).

Quand il s'agit de ressources internationales, la Déclaration Universelle des Droits de l'Homme a été signé en 1948 et immédiatement après, la Convention Européenne des Droits de l'Homme a été signée en 1950 et est entré en vigueur en 1953. Bien qu'il n'y ait pas de réglementation claire sur la protection des données à caractère personnel dans la Convention, la Cour Européenne des Droits de l'Homme a noté dans de nombreuses décisions, que la protection des données personnelles est dans le cadre du droit au respect de la vie privée . Ainsi, les violations de protection des données ont été analysées dans l'article 8 de la Convention qui protège la vie privée et familiale.

Le 23 Septembre 1980, la Convention de l'OCDE, qui est un document non contraignant, a été signé et les principes énoncés par la Convention ont été acceptés comme directeurs de l'OCDE. Après la Convention de l'OCDE, la « Convention Pour la Protection des Personnes à l'Egard du Traitement Automatisé des Données à Caractère Personnel » a été signé en 1981 et a apporté aux pays signataire, l'obligation de mettre en œuvre la Convention dans leur droit interne. Cependant

l'étape la plus importante prise dans l'amélioration de la protection des données a été la « Ddirective 95/46/CE Relative à la Protection des Personnes à l'Egard du Traitement des Données Personnelles et la Libre Circulation de ces Données Formulées par l'Union Européenne. La directive a défini des principes de base concernant la protection des données et a pour but de parvenir à une norme commune pour être appliquée à tous les membres de l'UE. En outre, la directive a entraîné le principe de l'égale protection lors du transfert de données de pays non-UE à d'autres pays et a interdit le transfert de données aux autres pays qui n'ont pas l'égalité des normes de protection des données. A partir de cette date, les pays européens ont pris les mesures nécessaires pour atteindre les normes fixées par la directive dans leur droit interne.

En Turquie, en regardant les règlements sur la protection des données personnelles, contrairement à la plupart des autres pays, une loi spéciale qui protège les données personnelles n'existe pas. La Turquie, afin de préparer un projet de loi pour la protection des données personnelles a créé une Commission pour la première fois le 13 Septembre 1995, mais cette commission n'a pas terminé le travail et le projet n'a pas été achevé. Puis, le 8 Septembre 2000, une nouvelle commission a été créée et à la fin d'une préparation de trois ans, en 2003, le projet de la « Loi concernant la Protection des Données Personnelles » a été accepté sur la base des principes de la « *Directive 95/46/CE sur la protection des personnes à l'égard du traitement des données à caractère personnel et la libre circulation de ces données* » et la « *Convention pour la protection des personnes à l'égard du traitement automatisé des données personnelles* .» L'harmonisation a continué sur le projet de loi et enfin le projet a été envoyé au Premier Ministre le 22 Avril 2008. Actuellement, le projet de loi n'est pas encore entré en force et la Turquie ressent sérieusement l'absence d'un arrangement spécial pour la protection des données personnelles. Jusqu'à présent, la Turquie a retardé l'adoption de ce projet de loi et compte tenu de la date de la première création de la commission, la promulgation d'une loi distincte sur la protection des données personnelles qui est présente dans presque tous les autres pays a été reportée pendant près de vingt ans. Bien qu'en vertu du Code Pénal Turc, enregistrer, obtenir, donner ou distribuer les données personnelles d'une manière illégale et de ne pas détruire les données personnelles sont pénalisés, la nécessité de l'existence d'une loi distincte est toujours évidente. En

fait, cette loi serait complémentaire en termes de sanctions prévues dans le Code Pénal Turc et serait capital pour la prévention de telles violations. En effet, la diffusion et le transfert de données à caractère personnel est devenu assez facile grâce à la technologie, donc une que fois la violation a eu lieu, l'éradication des dommages est très difficile.

L'idée de créer une banque de données génétiques afin d'analyser les ADN et de garder les informations du profil ADN obtenu à partir de l'analyse a été discutée pendant de nombreuses années en Turquie. Cette question a été dans l'agenda pour la première fois en 1998 comme un projet de loi sous le nom de la « Loi Des Données D'ADN Et La Banque Nationale De Données D'ADN. » Le projet de loi a été renvoyé par le ministère de la Justice le 4 mai 2007. Plus tard, il a été renouvelé le 3 Octobre 2007 et envoyé au Premier ministre. Toutefois, elle a été rejetée par le Premier ministre le 14 Avril 2008. La loi n'est pas encore entrée en vigueur; ainsi, l'analyse de l'ADN, les procédures et les principes de ceux-ci, sont effectués dans les dispositions du Code de Procédure Pénale Turc.

Ces dernières années, parallèlement a l'évolution de la technologie, des systèmes d'information et du réseau internet, il y a une augmentation dans le monde entier et en Turquie en ce qui concerne l'enregistrement des données personnelles. Principalement ce qui inclut, les numéros de téléphones mobiles, les renseignements personnels donnés aux banques et l'information financière personnelle et les données de consommation recueillies par les coopérations spécifiques.

Le projet, qui a été préparé par le gouvernement turc en vue de remplir le processus d'adaptation de l'Union européenne, n'est pas entré en vigueur depuis de nombreuses années. Cette absence de législation a conduit à l'augmentation du partage et de l'enregistrement des données à caractère personnel d'une manière chaotique et incontrôlable et donc ceci a causé d'importantes atteintes aux droits et libertés fondamentaux des individus, qui sont protégés par la Constitution turque.

Afin de réduire et de prévenir tous ces problèmes et afin de punir et de dissuader ceux qui commettent de tels actes, des dispositions ont été prises et de

nouvelles infractions et des sanctions liées aux données personnelles ont été élevés dans le Code Pénal Turc.

En vertu du Code Pénal Turc, la notion de données personnelles ne signifie pas seulement des données qui peuvent être utilisés ou transférés par la technologie de l'information (TI). En effet, le préambule de l'article 135 du Code Pénal Turc que "Il n'ya pas de discrimination entre les données personnelles enregistrées sur un système informatique et des données personnelles enregistrées sur le papier." Donc, cette déclaration montre clairement que le concept de données à caractère personnel sous le Code Pénal Turc, peuvent être des données personnelles enregistrées sur les systèmes informatiques ainsi que sur papier ou tout type de matériel et par n'importe quel moyen. La seule chose qui compte est qu'il y est un enregistrement; la forme de l'enregistrement ou la nature du matériel utilisé pour l'enregistrement n'est pas pertinent. Ce principe s'applique également aux autres articles connexes, qui sont "la livraison ou l'acquisition illégale des données" (CPT art.136) et «Pas de destruction de données" (CPT art. 138).

Les articles qui réglementent la protection des données personnelles (CPT art. 135, 136 et 138) ne sont pas couverts en vertu du Code pénal turc précédent (n.765). Ce code a été abrogé et le nouveau de code pénal turc (n. 5237) est entré en vigueur en 2005.

Les articles qui réglementent la protection des données personnelles en vertu du Code Pénal Turc sont cités dans le deuxième chapitre intitulé « délits contre les personnes» et la neuvième section intitulée "délits contre la vie privée et le secret de la vie privée» L'article 135 (Enregistrement des données personnelles) du Code stipule que «(*1) Toute personne qui enregistre illégalement les données personnelles est condamné à un emprisonnement de six mois à trois ans. (2) Toute personne qui enregistre les concepts politiques, philosophiques ou religieux des individus, ou des informations personnelles relatives à leurs origines raciales, les tendances éthiques, les conditions sanitaires ou les connexions avec les syndicats est punie conformément aux dispositions du paragraphe ci-dessus.* » Selon le l'article 136 « *(1) Toute personne qui livre des données illégalement à une autre personne, ou les diffuse ou les obtient par des moyens illégaux est condamné à un emprisonnement*

de d'un an à quatre ans» et l'article 137 affirme que «*(1) Dans le cas de la commission des infractions définies aux articles ci-dessus: a) par un officier public ou d'influence due sur la base de la fonction publique, b) En exploitant les avantages d'une profession exercée et de l'art, la peine est augmentée de moitié* » Enfin, l'article 138 précise que ; « *En cas d'échec de détruire les données dans un système défini, malgré l'expiration du délai prescrit par la loi, les personnes responsables de cet échec sont condamnés à un emprisonnement de six mois à un an*. »

ABSTRACT

In international documents, in the preamble of the 135 th article of the Turkish Penal Code (TPC) and in national legislations of the countries which will be examined within the scope of this work, the concept of “Personal Data” has been defined as any information relating to an identified or identifiable individual. In this case, a person's name, surname, photo, phone number, DNA, fingerprint data, are treated such as personal data. The European Court of Human Rights, has decided that even the voice of people, shall be considered as personal data. Some personal data, however, due to their nature, have been classified as sensitive personal data and in almost all national-international texts such data has been provided special protection. Racial and ethnic origins of individuals, information about sexual lives, political, religious or philosophical views, health or criminal record information is considered as sensitive personal data.

Although regulations concerning the protection of personal data have gained importance after World War II, physicians’ duty of confidentiality arising BC 5th century is one of the first examples of personal data protection. This duty which predicts that physicians shall not disclose personal information they have acquired within their profession, is one of the first steps for the protection of personal data.

The importance of the protection of personal has first emerged in the United States in 1950s and 1960s with the arrival of the first computers and the beginning of personal data storage and transfers. Particularly after World War II, the apprehension of European countries of the misuse of personal data collected and stored brought discussions about the protection of personal data.

The main development on personal data has started in 1970s. In most countries legislative studies have started in mid-seventies and laws protecting personal data have been adopted between mid-seventies and nineties. The first legislative on data protection has been made in Germany in late sixties within the “Hesse Plan” which finally ended up in 1970 as a draft law regulating the foundation of a central data bank. Later, in 1977 the German Data Protection Act has been enacted but has been highly criticized because the task of data protection was left to the Interior Ministry. In subsequent years the U.S. has enacted the Privacy Act in 1974 and similar special acts protecting personal data have been legislated in other countries such as; Sweden (1973), France (1978), Germany (1977), Switzerland (1984), U.K. (1984) and Canada (1985).

When it comes to international resources, the Universal Declaration of Human Rights was signed in 1948 and immediately after that the European Convention on Human Rights was signed in 1950 and entered into force in 1953. Although there is no clear regulation on personal data protection in the Convention, the European Court of Human Rights noted in many decisions which we have analyzed within this study, that the protection of personal data was within the scope of the right to respect to private life. Thereby, data protection violations have been analyzed within the 8th article of the Convention which protects private and family life.

On 23 September 1980, the OECD Convention which is a non-binding document was signed and the principles set by the Convention have been accepted as OECD Guidelines. After the OECD Convention, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was signed in 1981 and has brought to signing countries the obligation of implementing the Convention in their domestic law. However the most important step taken in improving data protection law was the 95/46/EC Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data formulated by the European Union. The Directive has defined basic principles concerning data protection and has aimed to reach a common standard to be applied to all EU Members. In addition the Directive has brought the principle of equal protection when transferring data from non-EU countries to other countries and

has prohibited data transferring to other countries that do not have equal data protection standards. From this date, the European countries have taken necessary steps to reach the standards set by the Directive within their domestic law.

In Turkey, looking at the regulations on protection of personal data, contrary to most of other countries, a special law that protects personal data does not exist. Turkey, in order to prepare a bill for the protection of personal data created a commission for the first time on September 13, 1995, but this commission did not complete the work and the draft was not completed. Then, on on September 8, 2000, a new commission was founded and at the end of a three-year preparation, in 2003, the draft bill of the "Turkish Data Protection Act" based on the principles of the "95/46/EC Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data" and the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" came out. Further harmonization was made on the draft and then finally the draft bill was sent to the Prime Ministry on April 22, 2008. Currently, the bill has not yet passed into law yet, and Turkey feels seriously the lack of a special arrangement for the protection of personal data. So far, Turkey has delayed the enactment of this bill and considering the first date of establishment of the commission, the enactment of a separate law on the protection of personal data which is present in almost all other countries has been postponed for nearly twenty years. Although under the Turkish Penal Code unlawful recording of personal data, obtaining, giving or distributing personal data in an unlawful way and not to destroy personal data is penalized, the need for the existence for a separate law is still obvious. Actually, this law would be complementary in terms of the sanctions foreseen in the Turkish Penal Code and would be capital for the prevention of such violations instead of penalizing offenders because of the lack of necessary precautions. Indeed, dissemination and transfer of personal data has become quite easy thanks to the technology, so once the breach occurs, the eradication of the damage is hardly possible.

The idea of establishing a DNA data bank in order to analyze DNAs and keep the information of the DNA profile obtained from the analysis has been discussed for many years in Turkey. This issue came into agenda for the first time in 1998 as a draft bill under the name of Law of DNA Data and National Databank. The draft bill

was referred by the Ministry of Justice on 4 May 2007. Later than, it was renewed on 3 October 2007 and sent to the Prime Minister. However, it was rejected by the Prime Minister on 14 April 2008. The draft has not entered into force yet; thus DNA analysis, procedures and principles thereof, are carried out within the provisions of the Code of Criminal Procedure.

In recent years, depending on the development of technology, information systems and internet network, there has been a crucial increase around the world and in Turkey regarding the recording of personal data. Principally this includes; mobile phone numbers, personal information given to the banks and the personal financial information and consumer data gathered by specific co-operations.

The draft, which was prepared by Turkish Government in order to fulfill the adaptation process of European Union, has not entered into force for many years,. This lack of legislation has led to the increase of sharing and recording of personal data chaotically and uncontrollably and thus it has caused significant impair of fundamental rights and freedoms of individuals, which are protected by the Turkish Constitution.

In order to reduce and/or prevent all these problems and in order to punish and dissuade of those, who commit such actions, arrangements were made and new offences and penalties related to personal data were brought up in the Turkish Penal Code no.5237.

Under Turkish Penal Code, the concept of personal does not merely refer to data that can be used or transferred by information technology (IT) systems. Indeed, the preamble of the 135th article of the Turkish Penal Code states that “There is no discrimination between personal data recorded on an IT system and personal data recorded on paper.” So this statement clearly shows that the concept of personal data Under Turkish Penal Code, may be personal data recorded on information technology systems as well as recorded on paper or all kind of material and by any method. The only important thing is that there has been a recording; the form of the recording or the kind of material used for the recording is not relevant. This principle

also applies to other related articles which are “Unlawful delivery or acquisition of data” (TPC art.136) and “No destruction of Data” (TPC art. 138).

The articles protecting personal data (TPC art. 135, 136 and 138) were not covered under the previous Turkish Penal Code No.765. This code was abrogated and the new Turkish Penal Code No. 5237 has entered into force in 2005.

Articles protecting personal data under Turkish Penal Code are cited in the Second Chapter entitled “*Offenses Against Individuals*” and the Ninth Section entitled “*Offenses Against Privacy and Secrecy of Life*”. The 135th article (Recording of personal data) of the Code, states that “*(1) Any person who unlawfully records the personal data is punished with imprisonment from six months to three years. (2) Any person who records the political, philosophical or religious concepts of individuals, or personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates is punished according to the provisions of the above subsection.*” According to the 136th article “*(1) Any person who unlawfully delivers data to another person, or disseminates or obtains the same through illegal means is punished with imprisonment from one year to four years*” and the 137th article says that “*(1) In case of commission of the offenses defined in above articles; a) By a public officer or due influence based on public office, b) By exploiting the advantages of a performed profession and art, the punishment is increased by one half.*” Finally the 138th article states that “*In case of failure to destroy the data within a defined system despite expiry of legally prescribed period, the persons responsible from this failure are sentenced to imprisonment from six months to one year.*”

ÖZET

Kişisel veri kavramı, çalışmamız kapsamında incelenecek olan uluslararası belgelerde, incelenen bazı ülkelerin ulusal mevzuatlarında ve Türk Ceza Kanunu'nun kişisel verileri koruyan hükümlerinden kişisel verilerin kaydedilmesi suçunu düzenleyen 135 inci maddenin ilk fıkrasının gerekçesinde, belirli veya belirlenebilir nitelikte olan bir kişiye ilişkin veri olarak tanımlanmıştır. Bu durumda bir kişinin adı soyadı, fotoğrafı, telefon numarası, DNA'sı, parmak izi gibi veriler kişisel veri olarak değerlendirilmektedir. Hatta Avrupa İnsan Hakları Mahkemesi, kişilerin sesini dahi, ses renginden kişinin belirlenebileceğinden bahisle kişisel veri olarak değerlendirmiştir. Bazı kişisel veriler ise, arz ettikleri önem itibariyle hassas kişisel veri kategorisinde değerlendirilmiş ve ulusal-uluslararası hemen hemen tüm metinlerde bu tür verilere özel bir koruma sağlanması gerektiği belirtilmiştir. Bu kapsamda genel olarak bireylerin ırki ve etnik kökenlerine ilişkin, cinsel yaşamlarına ilişkin, siyasi, dini veya felsefi görüşlerine ilişkin, sağlık bilgilerine veya adli sicil bilgilerine ilişkin veriler hassas nitelikte kişisel veriler olarak kabul edilmektedir.

Kişisel verilerin korunmasına ilişkin düzenlemeler, daha ziyade II. Dünya Savaşı'ndan sonra önem kazanmış olsa da, M.Ö. 5. yüzyılda ortaya çıkan hekimin sır saklama yükümlülüğü kişisel verilerin korunmasına ilişkin en eski örneklerden biridir. Hekimlerin, meslekleri kapsamında bireylerin sağlığıyla ilgili olarak öğrendikleri bilgileri başka kimselerle paylaşmamalarını öngören bu yükümlülük, kişisel verilerin dolaylı olarak korunmasının ilk adımlarından birisidir.

Günümüzde anlaşıldığı haliyle kişisel veri kavramının gelişmesi ve korunmasının önem arz etmeye başlaması ise, ellili ve altmışlı yıllarda, bilgisayarların ilk ortaya çıkışları ve buna bağlı olarak ilerleyen dönemlerde teknolojinin hızla gelişerek bireylere ilişkin verilerin tutulmaya, yayılmaya ve transfer edilmeye başlanması ile Amerika Birleşik Devletleri'nde (ABD) gündeme

gelmiştir. Özellikle toplanan ve depolanan kişisel verilerin kötüye kullanılması endişesi, II. Dünya Savaşı'ndan sonra Avrupa ülkelerinde de etkisini yoğun bir şekilde hissettirerek bu savaşın yıkıcı etkilerinin psikolojik olarak devam etmesi sebebiyle kişisel verilerin korunmasına yönelik tartışmaları beraberinde getirmiştir.

Genele bakıldığında, kişisel veri hukukuna ilişkin esas gelişme yetmişli yıllarda yaşanmıştır. Kişisel verilerin korunmasına ilişkin yasal çalışmalar ülkelerin çoğunda 70 li yıllarda başlamış, bu çalışmaların kanunlaşmaları ise bazı ülkelerde 70li, bazılarında ise 80li-90lı yıllarda gerçekleşmiştir. Bu alanda yapılan ilk yasal düzenleme 60 lı yılların sonuna doğru Almanya'da "Hesse Planı" olarak adlandırılan ve federe düzeyde merkezi bir veri bankası kurulmasına ilişkin olan 1970 tarihli kanun tasarısıdır. Daha sonra 1977 yılında Federal Almanya Veri Koruma Kanunu kabul edilmiş, ancak bu kanun verileri koruma görevini İçişleri Bakanlığı'na bıraktığından oldukça eleştirilmiştir. İlerleyen yıllarda ise, Amerika'da "Privacy Act" adıyla 1974 yılında kişisel verilerin korunmasına ilişkin özel bir kanun çıkarılmış, kişisel verileri koruyan benzer özel kanunlar İsveç'te 1973, Fransa'da 1978, Almanya'da 1977, İsviçre'de ve İngiltere'de 1984 tarihinde, Kanada'da 1985 tarihlerinde çıkarılmıştır.

Uluslararası kaynaklara baktığımız zaman ise, 1948 yılında İnsan Hakları Evrensel Bildirgesi imzalanmış, hemen ardından 1950 tarihinde imzalanan Avrupa İnsan Hakları Sözleşmesi 1953 yılında yürürlüğe girmiştir. Her ne kadar Sözleşme'de kişisel verilerin korunmasına ilişkin açık bir düzenleme bulunmasa da, Avrupa İnsan Hakları Mahkemesi vermiş olduğu pek çok kararında kişisel verilerin korunmasının özel hayatın gizliliğinin korunması kapsamında kaldığını belirtmiştir. Bu itibarla kişisel verilerin korunması hususunda yapılan ihlaller Sözleşme'nin özel hayatın ve aile hayatının gizliliğinin korunmasını düzenleyen 8 inci madde kapsamında incelenmiştir.

23 Eylül 1980 tarihinde, çalışmamızda incelediğimiz OECD Sözleşmesi kabul edilerek kişisel verilerin korunmasında temel rehber ilkeler benimsenmiş, ancak bağlayıcı bir sözleşme niteliğinde olmamıştır. OECD Sözleşmesi'nin hemen ardından ise, 1981 tarihli ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme yapılmış, bu sözleşmeyi

imzalayan devletlere sözleşmeyi iç hukuklarına aktarma yükümlülüğü getirilmiştir. Ancak kişisel verilerle ilgili en önemli adımlardan biri 1995 yılında Avrupa Birliği tarafından hazırlanan 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi ile atılmıştır. Bu Yönerge ile kişisel verilerin korunmasına ilişkin Avrupa Birliği'ne üye tüm ülkelerde geçerli olacak temel esaslar belirlenmiş, veri aktarımı yapılırken eşdeğer koruma prensibi getirilerek, AB üyesi olmayan ülkelere veri aktarımı yapılırken AB standartlarında koruma sahibi olmayan diğer ülkelere kişisel verilerin aktarılması yasaklanmıştır. Bu tarihten itibaren de, Avrupa ülkeleri bu Yönerge ile belirtilen standartları kendi ülkelerindeki iç hukuka aktarmaya başlamışlar, kendi veri koruma kanunlarını bu seviyeye yükseltmişlerdir.

Türkiye'de ise, kişisel verilerin korunmasına ilişkin düzenlemelere bakıldığında, diğer ülkelerde olduğu gibi kişisel verileri koruyan özel bir kanunun bulunmadığı görülmektedir. Türkiye'de, kişisel verilerin korunmasına ilişkin bir tasarı hazırlamak üzere ilk defa 13 Eylül 1995 tarihinde bir komisyon oluşturulmuş, ancak bu komisyon çalışmalarını tamamlayamamıştır. Bunun üzerine 8 Eylül 2000 tarihinde yeni bir komisyon kurulmuş, bunun neticesi olarak da, üç senelik bir çalışma sonunda 2003 tarihinde, 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme ve 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi esas alınarak "Kişisel Verilerin Korunması Kanunu Tasarısı" (KVKT) hazırlanmıştır. Ancak bu dönemde yasalaşmayan bu tasarı üzerinde ilave çalışmalar yapılarak 22 Nisan 2008 tarihinde son haliyle Başbakanlık'a gönderilmiştir. Mevcut durumda, tasarı henüz kanunlaşmamıştır ve Türkiye kişisel verilerin korunmasına ilişkin özel bir düzenlemenin eksikliğini ciddi şekilde hissetmektedir. Türkiye, bugüne kadar bu tasarının yasalaşmasını geciktirmiş, ilk komisyonun kuruluş tarihi dikkate alındığında, diğer ülkelerin hemen hemen hepsinde mevcut olan ve kişisel verilerin korunmasına ilişkin ayrı bir kanun çıkarmayı yaklaşık yirmi yıldır ertelemiştir. Mevcut durumda, Türk Ceza Kanunu'nda her ne kadar kişisel verilerin hukuka aykırı olarak kaydedilmelerine, ele geçirilmelerine, yayılmalarına, ifşa edilmelerine veya kanunun öngördüğü süreler geçmesine karşın silinmemesine ilişkin cezai yaptırımlar öngörülmüş olsa da, ayrı bir kanunun varlığına ihtiyaç duyulduğu muhakkaktır. Nitekim bu kanun, Türk Ceza Kanunu'nda öngörülmüş olan yaptırımlar açısından da tamamlayıcı nitelikte olacak, kişisel verilerin korunamayıp faillerin cezalandırılmasındansa, verilerin baştan

korunarak bu tür ihlallerin önlenmesine vesile olacaktır. Gerçekten, kişisel verilerin yayılması ve transfer edilmesi teknoloji sayesinde son derece hızlı olduğundan, bir kez ihlal gerçekleştirildikten sonra verilen zararın tamamen yok edilmesi pratikte oldukça zordur.

DNA analizi yapmak ve yapılan analizler sonucunda elde edilen DNA profil ve bilgilerinin tutulması için bir DNA veri bankası kurulması fikri uzun senelerdir Türkiye'de tartışılmaktadır. İlk olarak 1998 yılında gündeme gelen bu husus, DNA Verileri ve Millî DNA Veri Bankası Kanunu Tasarısı adı altında, 4 Mayıs 2007 tarihinde Adalet Bakanlığı tarafından sevk edilmiş olup, 3 Ekim 2007'de yenilenerek Başbakanlığa gönderilmiş, ancak 14 Nisan 2008 tarihinde Başbakanlık tarafından iade edilmiştir. Tasarı, günümüzde halen yasalaşabilmiş değildir, bu sebeple yapılan DNA analizleri ve buna ilişkin usul ve esaslar Ceza Muhakemesi Kanunu'nun aşağıda inceleyeceğimiz ilgili maddelerine göre yapılmaktadır.

Son yıllarda, dünyada ve Türkiye'de özellikle teknolojinin, bilişim sistemlerinin ve internet ağının gelişmesi dolayısıyla kişisel verilerin kaydedilmesinde ciddi artışlar olmuş, özellikle cep telefonu numaraları, bankalara verilen şahsi bilgiler, bazı şirketler tarafından toplanan ve kişilerin ekonomik durumlarını veya kullandıkları ürünleri, markaları kaydeden gerçek ve tüzel kişilerin sayısı önemli oranda artmıştır.

İşte Avrupa Birliği'ne uyum süreci açısından yukarıda değinilmiş olan anlaşmalar çerçevesinde Türkiye'nin hazırlamış olduğu Kişisel Verilerin Korunması Hakkında Kanun Tasarısı yıllardır yürürlüğe girmemiş, adeta bu kişisel veri kayıtlarının ve paylaşımının düzensiz ve kontrolsüz bir biçimde artmasına ve dolayısıyla bireylerin Anayasa tarafından korunmakta olan temel hak ve özgürlüklerinin bu alanda ciddi şekilde ihlal edilmesine yol açılmıştır. Tüm bu sorunları azaltmak ve engelleyebilmek, bu tür eylemlerde bulunanları cezalandırmak ve yine bu tür eylemlerde bulunacakları caydırabilmek adına, 5237 Sayılı Türk Ceza Kanunu'nda kişisel verilerle ilgili düzenlemelere gidilmiş, bu alanda yeni suçlar ve cezalar ihdas edilmiştir.

Türk Ceza Kanunu açısından "kişisel veri" kavramına bakıldığında, veriyi oluşturan bilgilerin mutlaka bilişim sisteminde kullanılabilen ve yine yalnızca bilişim sistemi vasıtasıyla aktarılabilen bilgiler olması şart değildir. Nitekim çalışmamızda üzere, kişisel verilerin kaydedilmesi suçunu düzenleyen 135 inci maddenin gerekçesinde *"kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir."* ifadesi yer almaktadır. Bu tanımlamadan da açıkça anlaşıldığı üzere, bahsedilen kişisel veriler elektronik ortamdaki ve bilişim sistemleri içerisinde kullanılabilen veriler olabilecekleri gibi, yazıyla veya başka herhangi bir şekilde kaydedilmiş veriler de olabilir. Bu husus kişisel veriler ile ilgili olan diğer maddeler (TCK m.136, 137, 138) için de geçerlidir.

2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun 135, 136, 137 ve 138 inci maddelerinin düzenlenmiş olan kişisel verilerin kaydedilmesi (m.135), hukuka aykırı olarak verilmesi veya ele geçirilmesi(m.136), bu suçların nitelikli halleri (m.137) ve hukuka uygun olarak kaydedilmiş olan kişisel verileri yok etmeme (m. 138) suçlarının, mülga 765 sayılı Türk Ceza Kanunu'nda karşılığı bulunmamaktaydı.

Kişisel verileri koruyan suçlar Türk Ceza Kanunu'nun "Kişilere Karşı Suçlar" başlıklı İkinci Kısmın "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde düzenlenmiştir. Kişisel verilerin kaydedilmesi suçu, TCK'nın 135 inci maddesinde ***"****(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."* şeklinde, TCK'nın 136 ncı maddesinde *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır"* şeklinde TCK'nın 138 inci maddesi ise TCK'nın 138 inci maddesinde "*Kanunların belirlediği süreler geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir"* şeklinde düzenlenmiştir. 137 nci maddede ise "*(1) Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın*

sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi hâlinde, verilecek ceza yarı oranında artırılır” şeklinde nitelikli haller düzenlenmiştir.

GİRİŞ

Gelişmekte olan dünyada, 1950 li ve 1960 lı yıllarda teknolojinin gelişmeye başlaması ve ilk bilgisayarların ortaya çıkmaya başlaması ile bireylerin kişisel verilerinin toplanmaya başlanmasıyla birlikte kişisel verilerin korunması meselesi tartışılmaya başlanmıştır. Özellikle yurtdışında, 60 lı yıllarda Amerika Birleşik Devletleri'nde[1] vatandaşlara kredi veren bankaların kredi verecekleri kişileri belirlemek için vatandaşların kişisel verilerinin toplanacağı bir merkezin kurulmasını talep etmeleri, ABD ordusunun pek çok kişinin kişisel verilerini herhangi bir kanuni dayanağı olmamasına rağmen depoladığının ortaya çıkması, bu konuda tartışmaları ateşleyen ilk vakalardan olmuştur[2]. Nitekim II. Dünya Savaşı'ndan sonra toparlanmaya ve yaralarını sarmaya başlayan Avrupa'da da, kişisel verilerin toplanmasına ilişkin öneriler özellikle Almanya ve İsveç'te büyük bir kamuoyu tepkisiyle karşılanmıştır[3]. Gerçekten II. Dünya Savaşı'nın niteliği düşünüldüğünde, Avrupa'da kişileri şahsi özellikleriyle belirlenebilir kılan kişisel verilerin tutulmasına karşı tepki göstermeleri anlayışla karşılanabilir.

II. Dünya Savaşı'ndan hemen sonra, 1948 yılında İnsan Hakları Evrensel Bildirgesi imzalanmış, hemen ardından 1950 tarihinde imzalanan Avrupa İnsan Hakları Sözleşmesi ise 1953 yılında yürürlüğe girmiştir. Bu belgeler kapsamında kişisel verilerin korunması hususu açıkça yer almamış olsa da, özel hayatın gizliliğinin korunması kapsamında kişisel verilerin de bu kapsama gireceği Avrupa İnsan Hakları Mahkemesi tarafından kabul görmüş ve Mahkemenin pek çok kararına konu edilmiştir. İlerleyen dönemlerde, 1970 li yıllarda Avrupa ülkelerinin çoğunda kişisel verilerin korunmasına ilişkin özel kanunlar hazırlanmasına ilişkin çalışmalar başlamış, pek çok ülkede bu yıllarda kişisel verilerin korunmasına ilişkin ilk

[1] Çalışmanın bundan sonrasında ABD olarak anılacaktır.
[2] **Şimşek**, **Oğuz**, Anayasa Hukukunda Kişisel Verilerin Korunması, 1. Baskı, Şubat 2008, s. 7.
[3] **Küzeci**, **Elif**, Kişisel Verilerin Korunması, Ankara 2010, s. 106-108, **Şimşek**, s. 7.

kanunlar çıkarılmıştır. Bu gelişmeler, 23 Eylül 1980 tarihinde Ekonomik İşbirliği ve Kalkınma Teşkilatı (The Organisation for Economic Co-operation and Development) Sözleşmesi'nin kabul edilerek kişisel verilerin korunmasında rehber ilkelerin benimsenmesi ile devam etmiş, ancak metnin bağlayıcı niteliği olmaması sebebiyle ülkeler açısından uygulanması zorunlu ortak bir standart getirememiştir. OECD Sözleşmesi'nin hemen ardından kabul edilen 1981 tarihli ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme[4] atılan önemli bir adım olmuştur, zira imzalayan devletler açısından bağlayıcılığı bulunan bir metin olarak düzenlenmiştir. Kişisel verilerin korunması bakımından yapılan en önemli düzenlemelerden biri de 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi'nin 1995 yılında Avrupa Birliği tarafından çıkarılması olmuştur. Bu Yönerge kapsamında Avrupa ülkelerinde uygulanacak ortak standart belirlenmiş, diğer ülkelere veri aktarılırken eşdeğer koruma aranması esası kabul edilmiştir.

Dünya'da tüm bu gelişmeler olurken ise, Türkiye ne yazık ki kişisel verilerin korunması konusunda kanuni düzenlemeler açısından son derece geride kalmış, 1981 tarihli ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'yi 28.01.1981 tarihinde imzalamış olmasına rağmen halen onaylamamıştır. Zira bu Sözleşme'nin onaylanabilmesi için kişisel verilerin korunmasına ilişkin özel bir kanun çıkarılması gerekmektedir ve Türkiye'de hala böyle bir kanun çıkarılmamış, çıkarılmasına ilişkin zayıf adımlar atılarak bazı tasarılar hazırlanmıştır. 108 Sayılı Sözleşme'yi imzalayan toplam 46 ülke bulunmaktadır ve günümüzde Türkiye haricinde Sözleşme'yi onaylamayan ülkeler yalnızca iki tane olup, bunlar da zaten Sözleşme'yi 2001 ve 2011 gibi yakın bir zamanda imzalayan Rusya ve Ermenistan'dır.

Mevcut durumda, Türkiye'de bazı kanunlarda kişisel verilerin korunmasına ilişkin birtakım hükümler bulunmaktadır. Türk Ceza Kanunu'nda da bazı eylemler suç olarak düzenlenmiş olup, bu fiilleri işleyenler cezalandırılmaktadır. 2010 tarihinde yapılan referandumdan sonra, 1982 tarihli Türkiye Cumhuriyeti Anayasası'nda özel hayatın gizilliliğinin korunmasını düzenleyen 20 nci maddeye bir fıkra eklenmek suretiyle kişisel verilerin korunması açık olarak anayasal güvence

[4] Çalışmanın bundan sonrasında 108 Sayılı Sözleşme olarak anılacaktır.

altına alınmıştır. Ancak Türkiye'nin kişisel verilerin korunması hususunu diğer ülkeler kadar ciddiye almaması, bu konuda yeterli çalışmaları yapmaması ve dolayısıyla hala kişisel verileri koruyan özel bir kanunu bulunmayan çok az ülkeden biri olması, hem kendi vatandaşlarının haklarının ülke içinde korunması açısından önemli sorunlar doğurmaktadır. Avrupa Birliği'ne üye tüm ülkelerin ortak bir koruma standardı tutturabilmek adına mevzuatlarını sürekli geliştirmeleri ve eşdeğer koruma esasının kabul edilmiş olmasının sonucu olarak, ilerleyen dönemlerde, Türkiye'nin bu ülkelerle yapılacak veri aktarımı konusunda sıkıntılı bir süreçten geçmesi muhtemeldir. Zira artık kişisel veriler hayatımızın her alanında kullanılmakta, özellikle internet üzerinden yapılan alışverişlerde ve organize suçla mücadelede büyük önem arz etmektedirler. Bu itibarla, ileride suçla mücadele kapsamında ortak bir çalışma yürütülmesinin söz konusu olduğu bir durumda veya Türkiye diğer ülkelerde bu bağlamda tutulan kişisel verilere ulaşmak istediği zaman, eşdeğer koruma bulunmadığı gerekçesiyle reddedilecektir. Eşdeğer koruma prensibine göre, Avrupa Birliği'ne üye ülkeler, yakaladıkları ortak standarda sahip olmayan ve AB üyesi olmayan ülkelere kişisel veri aktarmamaktadırlar. ABD'de, bu konuda yaşanabilecek sorunlar, Safe Harbor gibi birtakım düzenlemelerle aşılmaya çalışılmış ve bu alanda yeni düzenlemeler yapılmaya devam edilmiştir. Ancak Türkiye'nin bu yöndeki çabaları düşüncemize göre yetersiz kalmaktadır.

İşte çalışmamızda, temel hedefimiz, uluslararası kaynakları ve bazı ülkelerdeki düzenlemeleri ve Türkiye'de Ceza Kanunu'nda bu alanı düzenleyen hükümleri ve tasarıları inceleyerek Türkiye'de ulaşılması gereken standardı ortaya koymak ve bu ülkelerin sahip oldukları kişisel verilerin korunmasına ilişkin standardın Türkiye'de kişisel verilerin korunması açısından yol gösterici olmasını sağlamaktır.

Çalışmamızın Birinci Bölümünde, kişisel veri kavramı ve bu bağlamda çalışmamızda kullanılacak olan bazı önemli kavramlar açıklandıktan sonra, kişisel verilerin korunmasının tarihçesi kapsamında kişisel veri hukukunun günümüzden bugüne yaşadığı gelişmelere değinilecek, takiben Kişisel Verilerin Hukuki Yapılanması başlığı altında sırasıyla kişisel verilerin korunmasına ilişkin önemli uluslararası kaynaklar, bazı ülkelerdeki düzenlemeler ve Türk hukukunda kişisel verilerin korunmasına ilişkin kanun ve yönetmelikler incelenecektir.

Bu bölümde, Uluslararası Hukukta Kişisel Verilerin Korunması başlığı altında Ekonomik İşbirliği ve Kalkınma Teşkilatı Sözleşmesi (OECD Convention), 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa İnsan Hakları Sözleşmesi'nin kişisel verilere ilişkin önemli kararları, Birleşmiş Milletlerin Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeleri, Avrupa Birliği Temel Haklar Şartı ve 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi incelecek, bu kaynakların kişisel verilerin korunması hukukuna ilişkin getirdikleri önemli ilkeler değerlendirilecektir. Bazı Ülkelerde Kişisel Verilerin Korunması başlığı altında ise, Fransa, İsviçre, Almanya, İngiltere, ABD, Kanada ve Yeni Zelanda'da bu alanda mevcut düzenlemeler incelenecek, bu ülkelerde kişisel verilerin korunmasını düzenleyen özel kanunlar ve ülkelerin ceza kanunları üzerinde durulacaktır. Bu bölümde son olarak, Türk Hukukunda Kişisel Verilerin Korunması başlığı altında ise, 1982 tarihli Türkiye Cumhuriyeti Anayasası'nda ve bazı kanun ve yönetmeliklerde kişisel verilerin korunmasına ilişkin hükümlere yer verilecektir.

Çalışmamızın Türk Ceza Hukukunda Kişisel Verilerin Korunması başlıklı İkinci Bölümünde ise, Türkiye'de kanunlaşma ihtimali yüksek olan tasarılar ve Türk Ceza Kanunu'nda kişisel verileri koruyan hükümler incelenecektir. İlk olarak Ceza Hukuku Yönünden Kişisel Verilerin Korunmasına Yönelik Çalışmalar başlığı altında, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı incelenecektir. Tasarılar incelenirken, önemli olan ve tasarıların kanunlaşmaları halinde uygulamada birtakım sorunlar doğurabilecek hükümler ele alınacak ve bizce yapılması gereken değişikliklere değinilecektir. DNA veri bankasının oluşturulmasına ilişkin tasarı incelenmeden önce, Türk Ceza Muhakemesi Kanunu'nda yer alan ve şüpheli ile diğer kişilerin DNA'larının incelenmesine ilişkin kanun maddelerine de değinilecek, böylece günümüzde DNA'nın tutulmasına ilişkin mevcut uygulama değerlendirilecektir.

Son olarak, Türk Ceza Kanunu'ndaki Düzenlemeler başlığı altında, öncelikli olarak kişisel verilerin korunmasını düzenleyen suçların Türk Ceza Kanunu Tasarılarında yer alan tarihsel gelişimine değinilecektir. Bunun ardından, Türk Ceza

Kanunu'nda, "Kişilere Karşı Suçlar" başlıklı İkinci Kısmın "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde yer alan ve özel hayatın gizliliği kapsamında kişisel verilerin korunmasını düzenleyen suçlar incelenecektir. Bu suçlar, TCK'nın 135 inci maddesinde düzenlenen "Kişisel verilerin kaydedilmesi", TCK'nın 136 ncı maddesinde yer alan "Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme" ve TCK'nın 138 inci maddesindeki "Verileri Yok Etmeme" dir.

Netice itibariyle, çalışmamız kapsamında, Türkiye'de kişisel verilerin cezai korunmasına ilişkin mevcut çalışmaların yetersiz olduğunu ve bu konuyu detaylarıyla inceleyen kaynakların yok denilecek derece az olduğunu belirtmek gerekir. Türkiye'de kişisel verilerin korunmasına fazla önem atfedilmemesinin bir yansıması olarak gördüğümüz bu duruma ek olarak, Türk Ceza Kanunu'nda düzenlenen suçların uygulamasının son derece sınırlı olduğunu da görmekteyiz.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE ULUSLARARASI İLE ULUSAL KAYNAKLARDA KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ

A. KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİ HUKUKU KAPSAMINDA ÖNEM ARZ EDEN BAZI KAVRAMLAR

1. Kişisel Veri

Kişisel veri kavramı, uluslararası belgelerde, incelenen ülkelerin ulusal mevzuatlarında ve Türk Ceza Kanunu'nun kişisel verileri koruyan hükümlerinden kişisel verilerin kaydedilmesi suçunu düzenleyen 135 inci maddenin ilk fıkrasının gerekçesinde, belirli veya belirlenebilir nitelikte olan bir kişiye ilişkin veri olarak tanımlanmıştır. Bu durumda bir kişinin adı soyadı, fotoğrafı, telefon numarası, DNA'sı, parmak izi gibi veriler kişisel veri olarak değerlendirilmektedir. Hatta Avrupa İnsan Hakları Mahkemesi, kişilerin sesini dahi, ses renginden kişinin belirlenebileceğinden bahisle kişisel veri olarak değerlendirmiştir[5]. Bu itibarla, bir yerde kayıtlı olması şartı bulunmaksızın, belirli veya belirlenebilir bir kişiye ait olan her tür veri kişisel veri kapsamındadır. Nitekim 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin tanımlar başlıklı 2 nci maddesinde "belirli veya belirlenebilir bir kişiye ait her tür bilgi" ve 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi'nin tanımlar başlıklı 2 nci maddesinde kişisel veri "belirli veya belirlenebilir gerçek kişiye ait her tür bilgi" olarak tanımlanmıştır. Belirlenebilir kişi kavramı ise aynı maddede

[5] **P.G. and J.H. v. United Kingdom**, 44787/98, 25.09.2001. Ayrıntılı bilgi için çalışmamızın "**Avrupa İnsan Hakları Sözleşmesi**" başlığı altındaki bilgilere bakılabilir.

"doğrudan veya dolaylı olarak, özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine bir ya da birden fazla spesifik faktör referans alınarak, kimliği belirlenebilen kişi" olarak tanımlanmıştır.

Bazı kişisel veriler ise, arz ettikleri önem itibariyle hassas kişisel veri kategorisinde değerlendirilmiş ve ulusal-uluslararası hemen hemen tüm metinlerde bu tür verilere özel bir koruma sağlanması gerektiği belirtilmiş veya bu koruma doğrudan sağlanmıştır. Bu kapsamda bireylerin ırki ve etnik kökenlerine, cinsel yaşamlarına, siyasi, dini veya felsefi görüşlerine, sağlık bilgilerine veya adli sicil bilgilerine ilişkin veriler hassas nitelikte kişisel veriler olarak kabul edilmektedir[6].

Uluslararası belgelere ve farklı ülkelerin mevzuatlarına bakıldığında, veri (data), enformasyon (information) ve bilgi (knowledge) kavramlarının çoğu zaman birbirinin yerine kullanıldığı, bu konuda doktrinde ciddi tartışmalar olduğu ve bu üç kavramın genelde spesifik bir tanımının yapılamadığı görülmektedir[7]. Bazı yazarlara göre, bu üç kavramın birbiri yerine kullanılması ciddi bir hata oluşturmaktadır, ancak, belirttiğimiz gibi, uluslararası kaynaklar incelendiğinde, kişisel veri kavramını kullanırken bu üç kavramın da kullanım alanı bulduğu görülmektedir. Kavramların tanımlarına bakıldığında, aslında verinin enformasyonun, enformasyonun ise bilginin hammaddesini oluşturduğunu söylemek mümkün olmakla beraber, kavramların tanımlarının dahi ülkeden ülkeye, hatta onları tanımlayan yazardan yazara değişiyor olması, bu üç kavramın net çizgilerle birbirinden ayrılmasını zorlaştırmaktadır[8]. Türk Dil Kurumu'ndaki tanımlara bakıldığında, verinin "bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done", enformasyonun "danışma, tanıtma/haber alma, haber verme, haberleşme", bilginin ise "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat" şeklinde tanımlandığı[9], bu tanımların da açık ve net olmaktan uzak olduğu görülmektedir. Nitekim, daha evvel ifade ettiğimiz gibi, bu kavramlar, tartışıldığı zaman bunların soyut bir zeminde kaldığı ve netice itibariyle birbirleri arasındaki farkın net bir şekilde ortaya konulamadığı

[6] 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'de ve 95/46/AT Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi'nde, çalışma kapsamında incelenmiş olan ülkelerin bazılarının Veri Koruma Kanunlarında bu kişisel verilerin hassas nitelikte kişisel veri olarak tanımlandıkları görülecektir.
[7] **Küzeci**, s. 9.
[8] **Küzeci**, s. 10.
[9] Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&view=gts, 12.05.2012.

görülmektedir. Bu sebeple, çalışmamızda bu üç terimi birbirinin yerine geçer nitelikte kullanmış bulunmaktayız. Zira incelediğimiz uluslararası kaynakların ve kanunların çoğunun yabancı dilde yazılmış olması itibariyle çalışmamızda bunların bazı kısımları Türkçeye aktarılırken kişisel veri kavramı için bu kavramların her üçü de kullanılmıştır.

2. Kişisel Verinin İşlenmesi

Kişisel verilerin işlenmesi ise, 95/46/AT Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi'nde, kişisel verilerin tabi tutuldukları her tür işlem olarak tanımlanmıştır. Örneğin kişisel verilerin kaydedilmesi, silinmesi, depolanması, kullanılması, ifşa edilmesi, umuma sunulması gibi her tür işlem kişisel verinin işlenmesi kapsamında değerlendirilir.

3. Veri Öznesi/İlgili Kişi

Kişisel verilerin korunması ile ilgili olarak, önem arz eden iki kavram da "veri öznesi (data subject)" ve "ilgili kişi" dir. Veri öznesi, 95/46/AT Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi'nin 2 nci maddesi ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'nin 2 nci maddesinde kişisel verinin ilgili olduğu, yani belirli ya da belirlenebilir kıldığı kişi olarak tanımlanmıştır. Bu kavramların her ikisi de çoğu metinde birbirinin yerine geçecek şekilde kullanılmakta olup, bu çalışma kapsamında da bu yol izlenmiş, kişisel verinin nitelediği kişi için hem veri öznesi hem de ilgili kişi kavramı kullanılmıştır.

4. Özel Hayatın Gizliliği/Mahremiyet/Gizlilik

Çalışmamız kapsamında, değinilmesi gereken diğer iki kavram ise, "özel hayatın gizliliği" ile "mahremiyet" kavramlarıdır. İngilizcede yer alan "privacy" kavramının, farklı ulusal mevzuatlarda farklı alanlarda kullanılabildiği ve dilimize çevrilirken kimi yazarların bunu "özel hayatın (ya da yaşamın) gizliliği" olarak kimilerinin ise "mahremiyet" olarak kullandığı görülmektedir[10]. Özellikle Anglo-

[10] **Küzeci**, s. 15.

sakson ülkelerin hukuklarında, kişisel verilerin korunması kavramı yerine "privacy" kelimesinin kullanıldığı görülmektedir[11]. Kişisel verilerin korunması hukuku kapsamında, çalışmamızda, mahremiyet kelimesini "privacy" sözcüğünün yerine kullanmamakla beraber, bazı durumlarda, yabancı dilde olan kaynakların veya metinlerin anlam bütünlüğü açısından, "privacy" kelimesini karşılamak üzere "özel hayatın gizliliği" veya "gizlilik" kavramlarını beraber kullanmış bulunmaktayız.

5. Veri Denetçisi

Son olarak tanımlamak istediğimiz kavram ise, "veri denetçisi (data controller)" kavramıdır. Farklı ülkelerin veri koruma kanunlarında bahsi geçen bu ifade, verilerin işlenmesindeki amaç ve araçları belirleyen kişi veya örgütü ifade eder[12]. Ancak, bazı Türkçe metinlerde ve çalışmamızın ikinci bölümünde incelenecek olan ve Türkiye'de henüz kabul edilmemiş olan Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nda, veri denetçisi kavramı yerine veri kütüğü sahibi kavramının tercih edildiği görülmektedir. Bu itibarla veri kütüğü sahibi kavramının veri denetçisi kavramı ile birbirinin yerine geçecek şekilde kullanılabileceğini belirtmek gerekir.

B. KİŞİSEL VERİLERİN KORUNMASININ TARİHÇESİ

Kişisel verilerin korunmasına ilişkin düzenlemeler, daha ziyade II. Dünya Savaşı'ndan sonra önem kazanmış olsa da, M.Ö. 5. yüzyılda ortaya çıkan hekimin sır saklama yükümlülüğü kişisel verilerin korunmasına ilişkin en eski örneklerden biridir[13]. Hekimlerin, meslekleri kapsamında bireylerin sağlığıyla ilgili olarak öğrendikleri bilgileri başka kimselerle paylaşmamalarını öngören bu yükümlülük, kişisel verilerin dolaylı olarak korunmasının ilk adımlarından birisidir.

Günümüzde anlaşıldığı haliyle kişisel veri kavramının gelişmesi ve korunmasının önem arz etmeye başlaması ise, 1950 ve 1960'lı yıllarda,

---

[11] Nitekim, Amerika Birleşik Devletleri'nde ve Kanada'da, özel yaşamın korunmasına ilişkin çıkarılmış olan özel nitelikteki yasanın "*Privacy Act*" olarak anıldığı, buna karşın Almanya, Fransa, İsviçre gibi ülkelerde "*Data Protection Act (Veri Koruma Kanunu)*" olarak isimlendirildiği görülmektedir.

[12] **Küzeci**, s. 15.

[13] **Küzeci**, s. 105, **Şimşek**, s. 6.

bilgisayarların ilk ortaya çıkışı ve buna bağlı olarak ilerleyen dönemlerde teknolojinin hızla gelişerek bireylere ilişkin verilerin tutulmaya, yayılmaya ve transfer edilmeye başlamaları ile Amerika Birleşik Devletleri'nde (ABD) gündeme gelmiştir[14]. Özellikle toplanan ve depolanan kişisel verilerin kötüye kullanılması endişesi, II. Dünya Savaşı'ndan sonra Avrupa ülkelerinde de etkisini yoğun bir şekilde hissettirerek bu savaşın yıkıcı etkilerinin psikolojik olarak devam etmesi sebebiyle kişisel verilerin korunmasına yönelik tartışmaları beraberinde getirmiştir[15]. ABD'de o dönemde kişilerin kredi verilebilirliği sosyal açıdan büyük bir önem teşkil etmekte olup, kredi verilirken bilgisayarların hata yapmaması için vatandaşların verilerinin bir merkezde toplanması önerilince başlayan tartışmalar, ABD ordusunun pek çok kişinin kişisel verilerini topladığı ortaya çıkında iyice alevlenmiştir[16]. Benzer olarak, İsveç'te de, 60 lı yıllarda büyük bir vergi sicili oluşturularak vatandaşların nüfus bilgilerinin burada toplanmasına ilişkin bir çalışma başlatılmış, sonunda ABD'de ve İsveç'te bu tartışmalar ortak bir elektronik veri bankası kurulması ile sonlanmıştır[17].

Genele bakıldığında, kişisel veri hukukuna ilişkin esas gelişme 70 li yıllarda yaşanmıştır. Kişisel verilerin korunmasına ilişkin çalışmalar ülkelerin çoğunda 70 li yıllarda başlamış, bu çalışmaların kanunlaşması ise bazı ülkelerde 70li, bazılarında ise 80li-90lı yıllarda gerçekleşmiştir. Bu alanda Avrupa'da yapılan ilk düzenleme 60 lı yılların sonuna doğru Almanya'da "Hesse Planı" olarak adlandırılan ve federe düzeyde merkezi bir veri bankası kurulmasına ilişkin olan 1970 tarihli kanun tasarısıdır. Daha sonra 1977 yılında Federal Almanya Veri Koruma Kanunu kabul edilmiş, bu kanun ile verileri koruma görevini İçişleri Bakanlığı'na bırakıldığından çok eleştirilmiştir[18]. İlerleyen yıllarda ise, Amerika'da "Privacy Act" adıyla 1974 yılında kişisel verilerin korunmasına ilişkin özel bir kanun çıkarılmış, kişisel verileri koruyan benzer özel kanunlar İsveç'te 1973, Fransa'da 1978, Almanya'da 1998, İsviçre'de ve İngiltere'de 1984 tarihinde, Kanada'da 1985 tarihlerinde çıkarılmıştır.

Uluslararası kaynaklara baktığımız zaman ise, 1948 yılında İnsan Hakları Evrensel Bildirgesi imzalanmış, hemen ardından 1950 tarihinde imzalanan Avrupa

[14] **Şimşek**, s. 7.
[15] **Küzeci**, s. 106.
[16] **Şimşek**, s. 7.
[17] **Şimşek**, s. 7, **Küzeci**, s. 108.
[18] **Küzeci**, s. 109.

İnsan Hakları Sözleşmesi 1953 yılında yürürlüğe girmiştir. Her ne kadar Sözleşme'de kişisel verilerin korunmasına ilişkin açık bir düzenleme bulunmasa da, Avrupa İnsan Hakları Mahkemesi vermiş olduğu ve aşağıda ayrıntılı olarak inceleyeceğimiz pek çok kararında kişisel verilerin korunmasının özel hayatın gizliliğinin korunması kapsamında kaldığını belirtmiştir. Bu itibarla kişisel verilerin korunması hususunda yapılan ihlaller Sözleşme'nin özel hayatın ve aile hayatının gizliliğinin korunmasını düzenleyen 8 inci madde kapsamında incelenmiştir.

23 Eylül 1980 tarihinde aşağıda inceleyeceğimiz OECD Sözleşmesi kabul edilerek bu sözleşmeyle kişisel verilerin korunmasında temel rehber ilkeler benimsenmiş, ancak bu, bağlayıcı bir sözleşme niteliğinde olmamıştır. OECD Sözleşmesi'nin hemen ardından ise, yine bu çalışma kapsamında incelenecek olan 1981 tarihli ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme yapılmış, bu sözleşmeyi imzalayan devletlere sözleşmeyi iç hukuklarına aktarma yükümlülüğü getirilmiştir. Ancak kişisel verilerle ilgili en önemli adım, 1995 yılında Avrupa Birliği tarafından hazırlanan 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi ile atılmıştır. Bu Yönerge ile kişisel verilerin korunmasına ilişkin Avrupa Birliği'ne üye tüm ülkelerde geçerli olacak temel esaslar belirlenmiş, veri aktarımı yapılırken eşdeğer koruma prensibi getirilerek, AB üyesi olmayan ülkelere veri aktarımı yapılırken AB standartlarında koruma sahibi olmayan diğer ülkelere kişisel verilerin aktarılması yasaklanmıştır. Bu tarihten itibaren de, Avrupa ülkeleri bu Yönerge ile belirtilen standartları kendi ülkelerindeki iç hukuka aktarmaya başlamışlar, kendi veri koruma kanunlarını bu seviyeye yükseltmişlerdir.

II. KİŞİSEL VERİLERİN KORUNMASININ HUKUKİ YAPILANMASI

A. ULUSLARARASI HUKUKTA

1. Genel Bilgiler

Kişisel verilerin korunmasına ilişkin uluslararası hukukta pek çok düzenleme yapılmış, bunlardan bir kısmı yalnızca Avrupa Birliği'ne üye ülkeleri kapsarken, diğer bir kısmına ise Avrupa Birliği'ne üye olmayan diğer ülkeler de dahil

olmuşlardır. Nitekim gelişen teknoloji ile kişisel veri paylaşımının artması, hatta bunun bazı kişi ve kuruluşlar tarafından maddiyata dönüştürülebileceğinin fark edilmesi üzerine, bu alanda yapılan çalışmalara hız verilmiştir. Kişisel verilerin korunmasına ilişkin hükümler içeren uluslararası düzenlemelerin en önemli olanları arasında, Ekonomik İşbirliği ve Kalkınma Teşkilatı Sözleşmesi (OECD), 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, Avrupa İnsan Hakları Sözleşmesi, Avrupa Birliği Temel Haklar Şartı, 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi ve Birleşmiş Milletlerin düzenlediği Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler yer almaktadır.

İşte çalışmamızın bu bölümünde, hangilerinin Türkiye tarafından onaylandığı da belirtilerek uluslararası kaynaklar incelenecektir.

2. Ekonomik İşbirliği ve Kalkınma Teşkilatı Sözleşmesi (OECD Convention)

Uluslararası anlamda kişisel verilere ilişkin olarak ülkeler arasında birlik sağlanmaya çalışılması için ilk adımı atan OECD, 23 Eylül 1980 tarihinde "Özel Yaşamın Gizliliğinin ve Sınıraşan Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri" (OECD Convention) kabul etmiştir[19]. Her ne kadar uluslararası anlamda kişisel verilerin bir bütünlük içerisinde korunması amaçlanmış olsa da, imzalanan bu metin, rehber ilkeler olarak üye Devletlere yalnızca tavsiye niteliğinde olmaktan ibarettir ve bu itibarla metnin üye devletler açısından herhangi bir bağlayıcılığı bulunmamaktadır[20]. Sözleşme ile bu açıdan, üye devletlerin iç hukuku bakımından uyumluluk sağlanmak istenirken, devletlerin iç hukuklarına

[19] 1947 senesinde kurulan Avrupa Ekonomik İşbirliği Örgütü (Organisation for European Economic Cooperation - OEEC), temelde Amerika'nın finanse ettiği Marshall Planının uygulanması amacıyla kurulmuş olup, topluluğa Amerika ve Kanada'nın da katılmasıyla, 14 Aralık 1960 tarihinde imzalanan Ekonomik İşbirliği ve Kalkınma Teşkilatı Sözleşmesi'nin (**The Organisation for Economic Co-operation and Development Convention – OECD Convention**) 30 Eylül 1961 tarihinde yürürlüğe girmesiyle Ekonomik İşbirliği ve Kalkınma Teşkilatı resmen kurulmuştur. http://www.oecd.org/pages/0,3417,en_36734052_36761863_1_1_1_1_1,00.html, 20.02.2012.

[20] **Şimşek**, s. 13, **Küzeci**, s. 119, **Keele**, **Benjamin J.**, "Privacy By Deletion: The Need For A Global Data Deletion Principle", Indiana Journal of Global Legal Studies, Vol. 16, Issue 1, Winter 2009, s. 369, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1508025, 10.03.2012, **Murray**, **Patrick J.**, "The Adequacy Standart Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standart?", Fordham International Law Journal, Vol. 21, Issue 3, 1997, s. 953, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1563&context=ilj, 10.03.2012.

uyarlamalarında geniş bir çeşitliliğe neden olarak birörnek koruma sağlayamayacağı öne sürülerek eleştirilmiştir[21].

OECD'nin kabul etmiş olduğu Rehber İlkeler[22], kişisel veriyi belirli veya belirlenebilir bir kişiye ait olan tüm bilgiler olarak tanımlamış; kişisel verilerin korunmasına yönelik olarak 8 temel ilke kabul etmiştir ve bu ilkeler ilgili maddelerde belirtilmiştir. Rehber İlkeler, pek çok ülkenin iç hukukunda kişisel veri hukukunun kaynağını oluşturmuş, hatta Türkiye'de çıkarılması düşünülen Kişisel Verilerin Korunması Hakkında Kanunu Tasarısı'nın gerekçesinde bu ilkelere atıf yapılmıştır[23]. OECD, kişisel verilerin işlenmesi açısından şu ilkeleri getirmektedir[24];

1. İlke, "Veri Toplamanın Sınırlı Olması İlkesi" dir (md. 7). Bu ilkeye göre, kişisel verilerin toplanması sınırlı olmalı, bu tür veriler, veri süjesinin bilgisi ve rızası ile hukuka uygun olarak ve adil yöntemlerle elde edilmelidir.

2. İlke, "Veri Kalitesi İlkesi"dir (md. 8). Bu ilkeye göre, kişisel veriler kullanılış amaçlarına uygun olmalı ve bu amaç için gerekli olduğu ölçüde doğru, eksiksiz ve güncel olmalıdır.

3. İlke "Amacın Belirliliği İlkesi" dir (md. 9). Bu düzenlemeye göre, kişisel verilerin toplanma amacı, en geç toplanma anında belirlenmiş olmalıdır. Bu verilerin daha sonraki kullanımı, ancak bu amaçların gerçekleştirilmesi ile sınırlı olacak şekilde, bu amaçlarla bağdaştıkları sürece ve amacın değiştiği her seferin bildirilmesi koşullarıyla sınırlıdır.

4. İlke olan "Kullanımın Sınırlı Olması İlkesi" ne göre ise (md. 10), kanuni düzenlemeler ve veri süjesinin rızasının bulunması durumları haricinde, kişisel veriler ifşa edilemez, erişime açık bulundurulamaz ve 9 uncu maddede belirtilen toplama amaçları dışında kullanılamazlar.

---

[21] **Murray**, s. 953.
[22] Çalışmanın bundan sonrasında yalnızca "Rehber İlkeler" olarak anılacaktır.
[23] **Küzeci**, s. 120, **Keele**, s. 369.
[24] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, 20.02.2012.

5. İlke “Veri Güvenliği İlkesi” olup (md. 11), maddede, kişisel verilerin; kaybolma, izinsiz erişim, imha etme, kullanılma, değiştirilme veya ifşa edilme gibi risklere karşı uygun güvenlik önlemleriyle korunmaları gerektiği belirtilmiştir.

6. İlke “Açıklık İlkesi” dir (md. 12) ve bu kapsamda, kişisel verilere ilişkin gelişmeler, uygulamalar ve kurallar açısından genel olarak açıklık politikası bulunmalıdır. Kişisel verinin mevcudiyeti, niteliği ve temel kullanım amaçlarının yanı sıra veri denetçisinin kimliği ve mutat yerleşim yeri kolayca belirlenebilir olmalıdır.

7. İlke “Bireyin Katılımı İlkesi” dir (md. 13) ve bu ilke ile veri öznesi olan bireylerin hakları düzenlenmektedir. Buna göre birey; veri denetçisinden veya başka yoldan, veri denetçisinde, bireyin kendisini ilgilendiren kişisel verilerin bulunup bulunmadığı hususunun teyidini isteyebilir. Ayrıca, birey kendisini ilgilendiren kişisel verilerin kendisine makul bir sürede, gerekirse makul bir ücret karşılığı, makul bir usulle ve kolayca anlaşılır türde ulaştırılmasını isteyebilir. Kişinin kişisel verilerinin bulunup bulunmadığına veya kendisine ulaştırılmasına ilişkin taleplerinden birinin reddedilmesi halinde, kişi, bu reddin gerekçesini öğrenme ve bu ret kararına karşı hukuki yollara başvurma hakkına sahiptir. Son olarak kişilerin, kendilerine ilişkin kişisel verilere itiraz etmeleri ve itirazın haklı bulunması halinde bu kişisel verilerin silinmesini, düzeltilmesini, tamamlanmasını veya değiştirilmesini isteme hakkı mevcuttur.

8. İlke OECD Rehber İlkelerinde yer alan son ilke olup, “Hesap Verilebilirlik İlkesi” dir (md. 14). Bu ilkeye göre, veri denetçisi, yukarıdaki ilkelerin yerine getirilmesine dayanak teşkil eden tedbirlere riayet etmesi hususu ile ilgili olarak hesap verebilir durumda olmalıdır.

OECD’nin getirmiş olduğu bu ilkeler pek çok ülkede kişisel verilerin korunması hukukuna dayanak teşkil etmiştir ve OECD, teknolojinin gelişmesine bağlı olarak kişisel verilerin kullanım alanlarının genişlemesi sebebiyle buna ilişkin başka çalışmalara da imza atmıştır. Örneğin spam ile mücadele kapsamında (Report Of The Oecd Task Force On Spam: Anti-Spam Toolkit Of Recommended Policies

And Measures)[25], dijital ortamda kişilerin kimliğinin belirlenebilmesinin zorluğu göz önüne alındığında kişilerin olduklarını iddia ettikleri kişi olup olmadıklarının daha kolay anlaşılabilmesi amacıyla bu alanın düzenlenmesi için (OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication)[26], ağların ve bilgi sistemlerinin güvenliğinin sağlanmasına ilişkin yol gösterici nitelikte olan ilkelerin belirlenmesi için (OECD Guidelines for the Security of Information Systems and Networks)[27] gibi kişisel verilerin korunmasına ilişkin Rehber İlkeleri destekleyici pek çok çalışma yürütülmüştür.

3. Avrupa Konseyi ve Kişisel Verilerin Korunması

a. Genel Bilgiler

Avrupa Konseyi, Avrupa devletleri arasında birlik kurmak amacıyla 1949 yılında kurulmuş uluslararası bir teşkilattır[28]. Konsey, insan hakları, demokrasi ve hukuk devleti ilkesi kavramlarını korumak ve bu kavramların üye ülkelerde uyum içerisinde gelişmesini sağlamak için kurulmuştur[29]. Nitekim Avrupa Konseyi Statüsü'nün 3 üncü maddesine göre, Avrupa Konseyi üyesi olmak isteyen her devletin, hukuk devleti ilkesini benimsemesi, tüm vatandaşların temel haklar ve insan haklarından faydalanmalarına olanak vermesi ve Konseyin bu amacını gerçekleştirmesinde etkili ve samimi olarak işbirliği yapması gerekmektedir.

Avrupa Konseyi, yapmış olduğu çalışmalarla insan haklarının ve kişisel verilerin korunmasına önemli katkılarda bulunmuştur. Bu çalışmaların ilki, özel hayatın gizliliğini koruyan 8 inci maddesi çerçevesinde kişisel verileri koruyan Avrupa İnsan Hakları Sözleşmesi'dir. 4 Kasım 1950 tarihinde kabul edilen Avrupa

---

[25] **Report Of The Oecd Task Force On Spam: Anti-Spam Toolkit Of Recommended Policies And Measures**, http://www.oecd.org/dataoecd/63/28/36494147.pdf, 23.02.2012.
[26] **OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication**, http://www.oecd.org/dataoecd/32/45/38921342.pdf, 23.02.2012.
[27] **OECD Guidelines for the Security of Information Systems and Networks**, http://www.oecd.org/dataoecd/16/22/15582260.pdf, 23.02.2012.
[28] **Schwartz**, Paul M., "European Data Protection Law and Restrictions on International Data Flows", Iowa Law Review, Vol. 80, Issue 3, May 1995, s. 477, http://0-heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/ilr80&div=27&collection=journals&set_as_cursor=15&men_tab=srchresults, 07.03.2012.
[29]**Sepúlverda**, **Magdalena-Banning**, **Theo van-Gudmundsdóttir-Chamon**, **Christine**, **"**Human Rights Protection,Cases and Commentaries", Council of Europe, 2004, s. 130, http://www.wcl.american.edu/humright/hracademy/documents/Class2Reading3HRPortectionCasesandCommentaries.pdf?rd=1, 09.03.2012.

İnsan Hakları Sözleşmesi'ni, Türkiye 18 Mayıs 1954'te onaylamıştır[30]. Kişisel verilerin korunmasında bir sonraki adım 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme[31] olmuştur[32]. Daha sonra ise hızla gelişen biyoteknoloji alanında insan haysiyetini koruma amacıyla 1996 tarihli İnsan Hakları ve Biyotıp Sözleşmesi[33] kabul edilmiştir[34].

b. 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme

1981 tarihli ve 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme[35], AİHS'te açıkça yer verilmemiş olan kişisel verilerin korunması hakkını düzenlemektedir. 108 Sayılı Sözleşme'nin 23 üncü maddesine göre Avrupa Konseyi'ne üye olmayan devletler de bu sözleşmeyi imzalayabilirler ancak Sözleşme'nin 4 üncü maddesine göre, Sözleşme'yi imzalayan devletlerin, Sözleşme'nin hükümlerini iç hukuklarına aktarmakla yükümlüdürler[36].

108 Sayılı Sözleşme'nin ilk maddesinde, sözleşmenin amacı; sözleşmeye taraf her devletin, kişisel verilerin otomatik olarak işlenmeleri sırasında, milliyetine ve yerleşim yerine bakılmaksızın, kendi egemenlik alanı içerisinde bulunan her vatandaşın temel hak ve özgürlüklerini; özellikle özel hayatının gizliliğinin korunmasını sağlamak olarak ifade edilmiştir. Sözleşme 3 üncü maddesinin ilk fıkrası ile koruma kapsamına hem özel sektörü hem de kamu sektörünü dahil etmiş, 4 üncü maddede, Sözleşme'yi imzalayan devletlere Sözleşme'de öngörülen ilkeleri iç

---

[30] R.G. 19 Mart 1954, S. 8662, bkz. http://www.inhak-bb.adalet.gov.tr/aihs/aihs.htm, 26.02.2012, **Şimşek**, s. 19.

[31] "**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**". 1 Ekim 1985 tarihinde beş devletin onaylama işlemlerini tamamlamasıyla birlikte yürürlüğe giren sözleşmeyi, bugüne kadar 46 ülke imzalamış, bunlardan 43 ü ise sözleşmeyi onaylamışlardır. Sözleşmeyi 28/01/1981 tarihinde imzalayan Türkiye, 07/11/2001 yılında imzalayan Rusya ve 08/04/2011 tarihinde imzalayan Ermenistan henüz sözleşmeyi onaylamamış olan ülkelerdir.

[32] Türk hukukundaki yazarlar bu sözleşmeyi farklı isimlerle anmaktadır; Küzeci "108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme" ifadesini, Şimşek "108 Sayılı Kişisel Verilerin Korunmasına İlişkin Sözleşme" ifadesini, Başalp "108 Sayılı Avrupa Konseyi Konvansiyonu" ifadesini, Aksoy "108 Sayılı Avrupa Konseyi Sözleşmesi" ifadesini tercih etmektedir. Biz çalışmamızda, Küzeci'nin kullandığı ifadeyi kullanacağız.

[33] Türkiye ise bu sözleşmeyi imzaya açıldığı tarihte imzalayarak 3 Aralık 2003 tarihinde, 20 Nisan 2004 tarihli ve 25439 Sayılı Resmi Gazetede 5013 Sayılı Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunması Hakkında Kanun'u yayınlayarak onaylamıştır. **Küzeci**, s. 127, dn. 87.

[34] **Küzeci**, s. 127.

[35] Çalışmanın kalan kısmında 108 Sayılı Sözleşme olarak anılacaktır.

[36] Sözleşmenin tam metni için; http://conventions.coe.int/treaty/en/treaties/html/108.htm, 26.02.2012.

hukuklarına aktarma yükümlülüğü getirilmiştir. Sözleşme'nin 5 inci maddesinde ise bu ilkeler sayılarak otomatik işlemeye tabi tutulan kişisel verilerin; adil ve hukuka uygun bir şekilde toplanmaları ve işlenmeleri, belirli ve meşru bir amaç için saklanmaları ve bu amaca uygun olmayan şekilde kullanılmamaları, toplandıkları amaca uygun olarak ve sadece bu amaç için gerektiği kadar saklanmaları, doğru olarak ve gerektiğinde güncellenmeleri ve son olarak da veri sahibinin kimliğini yalnızca saklandıkları amacın gerektirdiği süre kadar belli edecek şekilde saklanmaları gerekmektedir.

108 Sayılı Sözleşme'nin 6 ncı maddesinde, hassas nitelikteki kişisel veriler için bir düzenleme getirilmiş, bireylerin ırki kökenleri, siyasi görüşleri veya dini inançlarını açıklayan ya da sağlıkları, cinsel yaşamları veya adli sicilleri ile ilgili kişisel verilerinin devletlerin iç hukukunda uygun güvenceler bulunmadığı sürece otomatik olarak işlenemeyecekleri belirtilmiştir. 7 nci maddede ise veri güvenliğine işaret edilerek, kişisel verilerin izinsiz veya kazara yok edilmeleri, kaybedilmeleri, değiştirilmeleri veya yayılmalarına ya da bunlara yetkisiz erişilmesine karşı korunmaları için uygun güvenlik önlemleri getirilmelidir. İlgili kişiler, kendileri ile ilgili otomatik olarak işlenmiş kişisel verilerin saklanıp saklanmadığını makul aralıklarla ve ölçüsüz bir bedel ödemek zorunda kalmaksızın kendilerine anlaşılır bir biçimde aktarılmasını isteyebilir, Sözleşme'nin 5 inci ve 6 ncı maddelerinde öngörülen temel ilkeleri ihtiva eden iç hukuk hükümlerine aykırı olarak toplanmış kişisel verilerin silinmelerini veya düzeltilmelerini talep edebilir ve bu talebin reddedilmesi halinde ise bu karara karşı etkili bir başvuru yoluna başvurabilirler[37]. Sözleşme, üye devletlere 5, 6 ve 8 inci maddelerde öngörülen ilkelere sınırlama getirilebileceğini öngörmüş, ancak bu sınırlamanın da sınırını belirterek, bu ilkelere ancak devletin veya kamunun güvenliği, devletin ekonomik çıkarlarının korunması, suçla mücadele amacıyla veya veri öznesi ya da başkalarının hak ve özgürlüklerinin korunması amacıyla ve demokratik bir toplumda gerekli ise sınırlama getirilebileceği belirtilmiştir[38].

Kişisel verilerin aktarımı ile ilgili olarak, 108 Sayılı Sözleşme, serbest aktarımı genel kural olarak düzenlemiş, Sözleşme'ye taraf ülkelerden birinin, taraf olan diğer ülkelerden birine yapılacak aktarımı yalnızca özel hayatın gizliliğinin korunması

[37] Bkz. 108 Sayılı Sözleşme, m.8.
[38] Bkz. 108 Sayılı Sözleşme, m.9.

sebebiyle yasaklayamayacağını veya özel bir izne tabi tutamayacağını öngörmüştür[39]. Ancak bu kurala iki istisna getirilmiştir ve bunlar; kişisel verinin aktarılacağı diğer ülkede eşdeğer koruma bulunmaması veya belirli kategorilerdeki kişisel veriler için özel koruma getirilmiş olması ya da veri aktarımının Sözleşme'ye taraf olmayan bir ülkeye yapılacak olmasıdır.

Sözleşme, 18 inci madde ile her ülkeden bir temsilcinin bulunduğu bir Danışma Komitesi kurulmasını öngörmüş, Komite'nin gerektiğinde 108 Sayılı Sözleşme'nin uygulanmasına veya değiştirilmesine ilişkin görüş bildireceğini veya raporlar hazırlayacağını düzenlemiştir. Nitekim Komite bu kapsamda pek çok çalışma yapmıştır[40].

108 Sayılı Sözleşme, kişisel verilerin korunmasına ilişkin önemli belgelerden biri olup, Sözleşme'yi imzalayan devletlere getirdiği yükümlülüklerle ve bunların iç hukuka aktarılmasına ilişkin bağlayıcı niteliği ile oldukça önemli bir konumdadır. Bu itibarla, Sözleşme'yi imzalayan ancak henüz onaylamamış olan Türkiye'nin en kısa sürede kişisel verilerin korunmasına ilişkin özel bir kanun çıkarması ve 108 Sayılı Sözleşme'yi onaylaması isabetli olacaktır.

c. Avrupa İnsan Hakları Sözleşmesi (AİHS)

İkinci Dünya Savaşı'nın yarattığı yıkımlardan sonra önem kazanan insan haklarının korunması hususunda, Birleşmiş Milletler Örgütü'nün kurulması ve ardından BM Genel Kurulu'nun 10.12.1948 tarihli kararıyla İnsan Hakları Evrensel Bildirgesi'nin kabul edilmesi ile ilk adımlar atılmıştır[41]. Ardından, 4 Kasım 1950 tarihinde Roma'da Avrupa İnsan Hakları Sözleşmesi imzalanmış ve Sözleşme 1953

---

[39] Bkz. 108 Sayılı Sözleşme, m.12.

[40] Komitenin bu çalışmalarına örnek olarak 108 Sayılı Sözleşme'de düzenlenen ilkelerin biyometrik verilerin toplanmasında ve işlenmesinde uygulanmasına ilişkin gelişme raporu (**Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data 2005**), http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf, 27.02.2012 ve Türkiye'nin imzaladığı ancak 108 Sayılı Sözleşmede olduğu gibi onaylamadığı 181 Sayılı Ek Protokol (**Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, **regarding supervisory authorities and transborder data flows CETS No.: 181)**, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=ENG, 27.02.2012, gösterilebilir.

[41] **Tezcan**, **Durmuş-Erdem**, **Mustafa Ruhan-Sancakdar**, **Oğuz-Önok**, **Rıfat Murat**, İnsan Hakları El Kitabı, 4. Baskı, Ankara 2011, s. 41.

yılında yürürlüğe girmiştir[42]. Ardından, bu Sözleşme'nin, Sözleşme'yi onaylayan ülkeler tarafından doğru bir şekilde uygulanmasını denetlemek amacıyla 1954 yılında Avrupa İnsan Hakları Komisyonu ve 1959 yılında Avrupa İnsan Hakları Mahkemesi (AİHM) kurulmuştur[43]. Türkiye de, bu Sözleşmeyi 1954 yılında onaylamıştır[44].

AİHS'nin Türk hukukundaki yerine bakıldığında, Anayasa'nın 90 ıncı maddesinden[45] yola çıkılarak, Sözleşme'nin Anayasa ile kanun arasında bir yere sahip olduğu görülmektedir. Anayasa'nın 90 ıncı maddesinde, milletlerarası antlaşmaların kanun hükmünde oldukları belirtilmiş olsa da, temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalar ile iç hukuktaki kanunlar arasında farklı hükümler bulunması halinde milletlerarası antlaşma hükümlerinin uygulanacağı belirtildiğinden, AİHS'nin de, kanunlardan farklı hükümler içermesi halinde, kanunlara nazaran öncelikli olarak uygulanacağı sonucu ortaya çıkmaktadır.

AİHS'de kişisel verilerin korunması hususu açıkça zikredilmemiş olsa da, bu konu Sözleşme'nin 8 inci maddesi kapsamında incelenmektedir, zira 8 inci madde "Özel Hayata ve Aile Hayatına Saygı Hakkını" korumakta, AİHM de kişisel verilerin korunmasını bu kapsamda değerlendirmektedir[46]. Çalışmamızda bu başlık altında, 8 inci maddeye kısaca değinilecek ve kişisel verilerin korunmasına ilişkin AİHM'in önemli gördüğümüz kararlarına yer verilecektir.

AİHS, özel yaşamın ve aile yaşamının korunmasına ilişkin maddeyi "1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. 2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin kanunla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir

---

[42] http://www.avrupakonseyi.org.tr/akih.htm, 06.05.2012.
[43] http://www.avrupakonseyi.org.tr/akih.htm, 06.05.2012.
[44] Türkiye, Sözleşmeyi 18 Mayıs 1954 tarihinde onaylamıştır. R.G.t., 19 Mart 1954, S. 8662, http://www.inhak-bb.adalet.gov.tr/aihs/aihs.htm, 07.05.2012.
[45] Bu husus, Anayasa'nın 90 ıncı maddesinde, "*Usulüne göre yürürlüğe konulmuş milletlerarası andlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. (Ek cümle: 7/5/2004-5170/7 md.) Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır.*" şeklinde düzenlenmiştir.
[46] **Tezcan-Erdem-Sancakdar-Önok**, s. 278, **Atak**, **Songül**, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", Türkiye Barolar Birliği Dergisi, Sayı 87, 2010, s. 103.

tedbir olması durumunda söz konusu olabilir" şeklinde düzenlemiştir[47]. Dolayısıyla, Sözleşme öncelikle, ilk fıkrada kişilerin özel hayatını, aile hayatını, konutunu ve yazışmalarını koruma altına almış, ardından ikinci fıkrada, kişilerin bu haklarının hangi gerekçelerle ve hangi koşullarda sınırlandırılabileceğini düzenlemiştir. Maddenin temel amacı, bireylerin özel ve aile hayatını keyfi müdahalelerden korumak olarak değerlendirilmektedir[48]. Bu kapsamda, AİHS'nin devlete yüklediği pozitif ve negatif yükümlülükler önem kazanmaktadır. Buna göre, devletin ilk yükümlülüğü negatif yükümlülük olup, bireyin özel hayatına ve aile hayatına keyfi olarak müdahale etmemektir. İkinci yükümlülüğü ise pozitif yükümlülük olup, bu yükümlülük kapsamında devlet, bireylerin bu haklarını kullanabilmeleri için uygun koşulları sağlamalı, kamu görevlileri veya bireylerin, başka kişilerin özel hayatına ve aile hayatına keyfi olarak müdahale etmesini önlemelidir[49].

AİHM'in kararlarına bakıldığında, Mahkemenin, kişilerin haklarının sınırlandırılmasının AİHS kapsamında kabul edilir olup olmadığını incelerken, temel olarak; müdahalenin kanunda öngörülmüş veya kanuna uygun olarak yapılıp yapılmadığını, sınırlamanın yöneldiği amacın meşru olup olmadığını, sınırlamanın demokratik bir toplumda gerekli olup olmadığını ve müdahalenin orantılı olup olmadığını değerlendirdiği görülmektedir[50]. Bu itibarla, AİHM'in önüne 8 inci madde kapsamında gelen davalarda, Mahkeme'nin ulaşacağı sonuç genel anlamda somut olayın koşullarına ve devletin o olay bakımından yükümlülüklerini yerine getirip getirmediğine bağlı olmaktadır[51].

AİHM, verdiği kararlarda, Sözleşme'yi yorumlamakta ve içtihat yaratmaktadır. Nitekim Mahkeme'nin pek çok kararında, önceki kararlarına atıf yapmak suretiyle, bazı ölçütleri artık benzer kararlarında da uyguladığı görülmektedir. Kişisel verilerin korunmasına ilişkin AİHM'in verdiği ilk ve en önemli kararlardan biri, devletin

---

[47] http://www.echr.coe.int/NR/rdonlyres/3BAA147F-29C9-48CE-AF64-FB85A86B2433/0/CONVENTION_TUR_WEB.pdf, 07.05.2012.

[48] **Bygrave**, **Lee A.**, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, Volume 6, 1998, s. 7, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf, 12.03.2012.

[49] **Zafer**, **Hamide**, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m. 132-134), 1. Baskı, Haziran 2010, s. 27-28, **Bygrave**, s. 8.

[50] **Tezcan-Erdem-Sancakdar-Önok**, s. 276.

[51] **Tezcan-Erdem-Sancakdar-Önok**, s. 277.

negatif yükümlülüğünün incelendiği Leander v. İsveç[52] davasıdır[53]. Bu davada, başvurucu, İsveç iç hukukunda personel kaydı tutulmasına izin veren bir kanuna göre kendisiyle ilgili olarak birtakım kişisel verilerin güvenlik amacıyla tutulduğunu, ancak kendisi hakkında toplanan bilgileri görme, yanlışsa düzeltme talebinin reddedildiğini, bu durumun da AİHS'nin 8 inci maddesini ihlal ettiğini ileri sürmüştür. Mahkeme ise, başvuruyu üç aşamada inceleyerek öncelikle müdahalenin meşru bir amaç için yapılıp yapılmadığını değerlendirmiş ve bunun sonucunda müdahale amacının 8 inci maddenin ikinci fıkrasında sayılan "ulusal güvenlik" olduğunu, bu itibarla meşru olduğuna kanaat getirmiştir[54]. Mahkeme daha sonra, yapılan müdahalenin kanuna uygun olup olmadığını değerlendirmiş, bu aşamada, kanunun yeterince açık hükümler içerdiğini, bu kapsamda hükümlerin hangi kişisel verilerin hangi amaçla tutulduklarını açıkça düzenlediğini, bu itibarla kanuna uygunluk kriterinin sağlandığını ifade etmiştir[55]. Mahkeme, yapılan müdahalenin ulusal güvenliğin korunması amacıyla demokratik bir toplumda gerekli olup olmadığını incelemiş ve müdahalenin orantılı olduğuna karar vererek demokratik bir toplumda gerekli olarak kabul etmiştir[56]. Sonuç olarak, Mahkeme, bu davada 8 inci madde kapsamında bir ihlal olmadığına karar vermiştir, ancak doktrinde, Mahkeme'nin bugünkü anlayışı ve yapısı gereği, kararı vermiş olduğu döneme nazaran daha ileride olduğu ileri sürülmüştür[57].

Gaskin v. İngiltere davasında[58] ise, devletin pozitif yükümlülüğü incelenmiş, başvuranın, kendisi hakkında, sosyal hizmetlerin bakımı altında geçirdiği çocukluğu süresince tutulan raporların tamamına ulaşamamasının, devletin pozitif yükümlülüğünü ihlal ettiği anlamına gelip gelmediği tartışılmıştır[59]. Mahkeme,

---

[52] **Leander v. Sweden**, 9248/81, 26.03.1987, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=leander%20%7C%209248/81&sessionid=94725631&skin=hudoc-en, 07.05.2012.

[53] **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 104, **Bygrave**, s. 10, **Ketizmen**, **Muammer**, Türk Ceza Hukukunda Bilişim Suçları, 1. Baskı, Ankara 2008, s. 200, **Akyürek**, **Güçlü**, **"**Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı", Suç ve Ceza Dergisi, Sayı 3 Temmuz-Ağustos-Eylül 2001, s. 47.

[54] **Leander v. Sweden**, prg.49.

[55] **Leander v. Sweden**, prg. 52-57.

[56] **Leander v. Sweden**, prg. 65-67.

[57] **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 105.

[58] **Gaskin v. the United Kingdom**, 10454/83, 07.07.1989, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=10454/83&sessionid=94823924&skin=hudoc-en, 09.05.2012.

[59] **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 106, **Bygrave**, s. 23.

kararda bu hususu incelerken, Johnston ve Diğerleri v. İrlanda[60] kararına atıf yaparak, sekizinci maddenin temel amacının bireylerin kamu kurumlarınca yapılabilecek keyfi müdahalelerden korunması olmasına rağmen, devletin, bireylerin özel hayatının efektif bir şekilde korunması için bir pozitif yükümlülüğünün de bulunduğunu belirtmiştir[61]. Hatta Mahkeme, davaya konu olan somut olayı Leander v. İsviçre kararına konu olan olay ile karşılaştırmış, iki dava arasındaki farkı tartışmıştır[62]. Mahkeme, sonuç itibariyle, devletin, kişiler hakkında yalnızca hukuka aykırı olarak kişisel veri tutmama değil, kişinin haberdar olup olmamasının doğrudan psikolojik durumunu etkileyecek nitelikteki kişisel verilere, ilgili kişilerin ulaşabilmesini sağlama yükümlülüğünün de bulunduğunu belirtmiştir.

Mahkemenin bir diğer önemli kararı Amann v. İsviçre'dir[63]. Bu kararında Mahkeme, kişilerin özel hayatının korunması kavramının, bireylerin özel hayatı ile ilgili bilgi toplanmasını ve madde geniş yorumlandığında kişisel verilerin korunmasına ilişkin Avrupa Konseyi'nin 108 Sayılı Sözleşmesi'nin konusunu teşkil eden, kişileri belirlenebilir kılan kişiye ait her tür bilgiyi kapsadığını ifade etmiştir[64]. Mahkeme ayrıca, olayda başvuran hakkında savcılıkta bir dosya tutularak, bu verilerin bir kamu kurumu olan İsviçre Federal Savcılığı tarafından fiş halinde saklanmasının, 8 inci madde anlamında özel hayatın gizliliğine bir müdahale oluşturmak için yeterli olduğunu belirtmiştir[65]. Mahkeme incelemesinin sonucunda, somut olayda tutulan fişlerin hukuka uygun olmadıklarını tespit ederek, İsviçre'nin kanuni düzenlemesini müdahaleye meşru bir hukuki dayanak oluşturabilecek nitelikte kabul etmemiştir.

Mahkeme, N.F. v. İtalya davasında[66] belirli bir çaba sarf edilmesi gerekmeden ulaşılabilen kişilere ait bilgilerin AİHS'in 8 inci maddesi kapsamında korunmadığını

---

[60] **Johnston and Others v. Ireland**, 9697/82, 18.12.1986, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Johnston%20%7C%20Others&sessionid=94824495&skin=hudoc-en, 09.05.2012.

[61] **Gaskin v. the United Kingdom**, prg.38.

[62] **Gaskin v. the United Kingdom**, prg.41.

[63] **Amann v. Switzerland**, 27798/95, 16.02.2000, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Amann&sessionid=94824495&skin=hudoc-en, 09.05.2012.

[64] **Ketizmen**, s. 201, **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 107.

[65] **Amann v. Switzerland**, prg.70.

[66] **N.F. v. Italy**, 37119/97, 02.08.2001, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=37119/97&sessionid=94824495&skin=hudoc-en, 09.05.2012.

belirtmiştir. Ancak kamuya açık olan ve herkes tarafından ulaşılabilir olan bilgiler hususunda, Mahkeme, Rotaru v. Romania davasında[67] önemli bir karar vermiştir. Buna göre, kişilere ait bu tür bilgiler her ne kadar kamuya açık olsalar da, bunların yetkili makamlar tarafından düzenli olarak toplanmaları ve dosyalanarak saklanmaları AİHS'nin 8 inci maddesi kapsamında ihlal oluşturmaktadır[68]. Olayda, istihbarat servisi tarafından başvuranın mensup olduğu gruba ve siyasi faaliyetlerine ilişkin bilgiler tutulmuş, başvuran dosyada yer alan bilgilerin yanlış olduğunu iddia ederek tazminat istemiş, istihbarat örgütü tarafından bir isim karışıklığının vuku bulduğu belirtilmesine rağmen ulusal mahkemeler tazminata hükmetmemişlerdir. AİHM ise, somut olayı inceledikten sonra, yapılan müdahalenin ulusal hukuka uygun olduğunu, ancak müdahalenin dayandığı metnin AİHS'ye uygun olmadığını, bu sebeple ihlal oluştuğunu ifade etmiştir[69].

P.G. ve J.H. v. İngiltere davasında[70], Mahkeme, kişilerin seslerinin kaydedilmesinin de özel hayatın gizliliği kapsamında korunacağını, zira kişilerin ses renginin kişiyi belirlenebilir kılan bir veri olduğunu, bu itibarla kişisel veri kapsamında değerlendirilerek AİHS'nin 8 inci maddesi çerçevesinde değerlendirilmesi gerektiğini belirtmiştir[71]. Mahkeme kararında, polislerin ifade alırken kişilerin sesini kaydetmesini 8 inci madde kapsamında müdahale olarak değerlendirmiş, ulusal hukukta bu hususta kanunda bireyleri koruyacak yeterince açık hüküm bulunmadığından yapılan kayıtların hukuka uygun olmadığını ve ulusal hukukun bu hususta keyfiliği ve kötüye kullanımı engelleyecek düzenlemeler ihtiva etmesi gerektiğini ifade etmiştir[72].

Mahkeme tıbbi verilerin de kişisel veriler kapsamında kaldığını ve bu itibarla 8 inci madde kapsamında korunmaları gerektiğini belirtmiştir. Örneğin Z. v.

---

[67] **Rotaru v. Romania**, 28341/95, 04.05.2000, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=28341/95&sessionid=94824495&skin=hudoc-en, 09.05.2012.
[68] **Zafer**, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, s. 34, **Akyürek**, s. 47.
[69] **Rotaru v. Romania**, prg. 59-62.
[70] **P.G. and J.H. v. United Kingdom**, 44787/98, 25.09.2001, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=44787/98&sessionid=94824495&skin=hudoc-en, 10.05.2012.
[71] **Zafer**, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması, s. 35.
[72] **P.G. and J.H. v. United Kingdom**, prg, 59-63.

Finlandiya davasında[73], başvuranın boşanmış olduğu eski eşine hem cinsel saldırı, hem de kasıtlı olarak HIV virüsünü bulaştırmaktan dava açılmış[74], savcılık tarafından verilen emirle başvuranın ve eski eşinin daha önce tedavi gördükleri hastanede polisler tarafından arama yapılmıştır. Aramada, başvuran ve eski eşiyle ilgili olarak HIV olduklarına ilişkin kayıtlara, başvuranın önceki rahatsızlıklarına ve ruhsal durumuna ilişkin kayda ve pek çok laboratuar testine el konulmuş, Mahkeme ise bu el konulan kayıtların tümünü dava dosyasına eklemiştir[75]. Davanın başvuranın eski eşinin aleyhine sonuçlanması ve bu kişinin mahkum olması üzerine, dava Helsinki Temyiz Mahkemesine taşınmış, temyiz mahkemesi ise kararı onayarak dosya kapsamının 10 yıl süreyle gizli tutulmasına karar vermiştir. Ancak bu süreçte, dava dosyası kapsamındaki belgeler baskına sızmış ve temyiz mahkemesinin kararı, bizzat mahkeme tarafından baskına faks çekilmiş, başvuranın adı ve soyadı açık bir şekilde yazılarak hastanede el koyulan belgeler, başvuranın eski eşinin kendisine HIV virüsünü bulaştırdığı ve HIV-pozitif olduğu baskında yer almıştır[76]. Mahkeme ise, tıbbi verilerin mahkemeye delil olarak sunulması ve polislerin bu verileri içeren kayıtlara el koymasında bir ihlal görmemiş, ancak başvuranın kişisel verilerinin 10 sene gibi kısa bir süre sonra kamuya açık hale gelmesi kararının ve başvuranın açık adı soyadı ile birlikte tıbbi verilerini barındıran temyiz mahkemesi kararının yayımlanmasının 8 inci madde kapsamında ihlal teşkil ettiğine karar vermiştir.

Benzer olarak, Panteleyenko v. Ukrayna davasında[77] da, Mahkeme, ceza yargılamasının sonucuna bir etkisi olmayacak psikiyatrik bilgilerin dava dosyası kapsamında toplanmasını ve bu bilgilerin hakim tarafından açık duruşma sırasında okuyarak duruşma salonunda bulunan diğer kimselere ifşa etmesini 8 inci madde kapsamında ihlal saymıştır[78].

---

[73] **Z. v. Finland**, 22009/93, 25.02.1997, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=22009/93&sessionid=94824495&skin=hudoc-en, 10.05.2012.

[74] **Polater**, **Yusuf Ziya**, Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması, 1. Baskı, Ankara 2010, s. 126, **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 115, **Akyürek**, s. 48.

[75] **Z. v. Finland**, prg. 30-32.

[76] **Z. v. Finland**, prg. 38-43.

[77] **Panteleyenko v. Ukraine**, 11901/02, 29.06.2006, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Panteleyenko&sessionid=94824495&skin=hudoc-en, 10.05.2012.

[78] **Panteleyenko v. Ukraine**, prg. 59-62.

Tıbbi verilerler ile ilgili bir diğer dava ise, M.S. v. İsveç davasıdır[79]. Bu davada, uğradığı iş kazası nedeniyle bel ağrıları için Sosyal Sigorta Kurumu'na tazminat davası açan başvuranın, daha önce tedavi gördüğü kliniğin Kurum'a gönderdiği raporda başvuranın bel rahatsızlığının daha önce geçirdiği bir rahatsızlıktan kaynaklandığı ve buna bağlı olarak geçmiş dönemlerde kürtaj olduğuna ilişkin bilgilerin yer alması, Mahkeme tarafından özel hayatın gizliliğini ihlal olarak nitelendirilmemiştir[80]. Mahkeme, burada, yapılan müdahalenin meşru amaç kapsamında olma ve demokratik bir toplumda gerekliliğe göre orantılı olma kriterlerine uyduğunu belirtmiştir[81].

Son olarak bu konuda önemli gördüğümüz ve Mahkeme'nin DNA verilerinin ve parmakizinin AİHS'nin 8 inci maddesi kapsamında korunup korunmayacağına ilişkin değerlendirme yaptığı dava, S. ve Marper v. İngiltere davasıdır[82]. Davaya konu olayda, S. İsimli başvuran Ocak 2001'de hırsızlık suçuna teşebbüsten yargılanmaya başlamış, bu kapsamda DNA örneği ve parmakizi alınmış, Haziran 2001'de ise beraat etmiştir[83]. Diğer başvuran Marper ise, Mart 2001'de arkadaşını darp ettiği gerekçesiyle gözaltına alınmış, bu kapsamda başvuranın DNA örneği ve parmakizi alınmış, başvuranın arkadaşıyla barışması üzerine hakkında dava açılmamıştır[84]. İlerleyen dönemlerde, başvuranlar kendileri ile ilgili tutulmuş olan kişisel verilerin, DNA örneklerinin ve parmakizlerini yok edilip silinmesini talep etmişler, ancak bu talepleri reddedilmiştir. Mahkeme, kararında DNA ve parmakizinin kişisel veri kapsamında kabul edilip edilmeyeceğini incelerken, DNA örneğinin yüksek kişisel niteliğinin yanı sıra, kişinin sağlığı ile ilgili de önemli ve hassas bilgiler ve buna ilaveten kişiye has ve benzeri olmayan bir genetik kod içerdiğini, bu sebeple kişinin yakınları ile de ilgili veriler ihtiva ettiğini, DNA

---

[79] **M.S. v. Sweden**, 20837/92, 27.08.1997, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=20837/92&sessionid=94824495&skin=hudoc-en, 10.05.2012.

[80] **Atak**, Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, s. 116, **Akıllıoğlu**, **Tekin**, "Kişisel Verilerin Korunması ve İdare", Maltepe Üniversitesi Hukuk Fakültesi Dergisi (1997/1998 – 2007-2008 Üniversitemizin ve Fakültemizin 10. Yıl Kuruluş Armağanı), 2008/Özel Sayı, s. 24.

[81] **M.S. v. Sweden**, prg. 38,43,44.

[82] **S. and Marper v. The United Kingdom**, 30562/04 ; 30566/04, 04.12.2008, kararın İngilizce tam metni için bkz. http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Marper&sessionid=95132622&skin=hudoc-en, 11.05.2012.

[83] **S. and Marper v. The United Kingdom**, prg.10.

[84] **S. and Marper v. The United Kingdom**, prg.11.

profilinin de benzer şekilde kişi ve kişilerin yakınlarıyla ilgili yüksek oranda hassas kişisel veri bulundurduğunu tespit etmiştir[85].

Parmakizi hususunda ise, Mahkeme, geçmiş dönemde kendisinin ve Komisyon'un verdiği kararlardan örnekler vermiş, P.G. ve J.H. v. İngiltere davasını da emsal göstererek, Mahkeme'nin fotoğraflar ve ses kayıtları için gösterdiği yaklaşımı, parmak izleri için de göstermesi gerektiğine kanaat getirdiğini belirtmiş, bu itibarla parmakizlerinin alınması yoluyla yapılan müdahalenin de AİHS 8 inci madde kapsamında bir müdahale olarak değerlendirileceğini ifade etmiştir[86]. Mahkeme, yapılan müdahalenin AİHS m. 8 kapsamında ihlal teşkil edip etmediğini araştırırken, DNA profili ve parmakizi alınması eyleminin cezai bir soruşturma kapsamında gerçekleştirilmiş olması sebebiyle meşru bir amaç taşıdığını kabul etmiştir. Ancak haklarında mahkumiyet kararı alınmamış olan kişilere ait bu denli hassas kişisel verilerin tutulmaya devam edilmesiyle, kamusal ve bireysel menfaatler arasında olması gereken adil ve orantılı dengenin sağlanamadığını, hükümetin bu noktada takdir marjını aştığını, bu itibarla yapılan müdahalenin orantısız olduğunu ve başvuranların özel hayatının gizliliğinin ihlal edildiğini belirtmiştir[87].

AİHM önüne gelen davalarda, davaya konu olayın konusunu kişisel verilerin teşkil ettiği durumlarda, yukarıda incelenen örnek kararlarda görüldüğü üzere, Mahkeme, kişisel verilerin tutulmasını veya ifşa edilmesini özel hayatın gizliliğinin korunması kapsamında değerlendirmiştir. Verilen kararlarda, genel olarak, öncelikle kişisel verilerin tutulmalarının veya ifşa edilmelerinin AİHS m.8 kapsamında müdahale teşkil edip etmediği değerlendirilmiş, müdahale teşkil ettiğinin belirlendiği hallerde ise öncelikle yapılan müdahalenin hukuka uygun olup olmadığı incelenmiş, bu inceleme yapılırken ulusal mevzuatta müdahaleye kaynak teşkil eden bir düzenlemenin mevcut olup olmadığına, şayet varsa, düzenlemede bireylerin kişisel verilerinin yeterli düzeyde korunmasını sağlayacak açık hükümlerin yer alıp almadığına bakılmıştır. Ardından, Mahkeme, yapılan müdahalenin demokratik bir toplumda gerekli olup olmadığını, bu bağlamda orantılı olup olmadığını belirlemiştir.

[85] **S. and Marper v. The United Kingdom**, prg.72-76.
[86] **S. and Marper v. The United Kingdom**, prg.82-86.
[87] **S. and Marper v. The United Kingdom**, prg.125.

4. Birleşmiş Milletler

Uluslararası güvenliği ve barışı korumak amacıyla İkinci Dünya Savaşı'ndan sonra, 1945 yılında 51 devlet ile kurulan Birleşmiş Milletler Örgütü'nün (BM) günümüzde 193 üyesi bulunmakta olup, bu kuruluş; ekonomik ve sosyal gelişmeler, çevrenin ve göçmenlerin korunması, insan hakları, terörle mücadele, silahsızlanma, cinsiyet eşitliği ve kamu sağlığı gibi alanlarda da daha iyi bir dünya yaratmak amacıyla faaliyet göstermektedir[88]. Nitekim 26 Haziran 1945 tarihinde imzalanan ve 24 Ekim 1945 tarihinde yürürlüğe giren BM Şartı'nın[89] 1 inci maddesinde[90] bu amaçlar ayrıntılı olarak belirtilmiştir.

Birleşmiş Milletler, İnsan Haklarına ilişkin genel çalışmaları kapsamında, 10 Aralık 1948 tarihli BM Evrensel İnsan Hakları Bildirisi'nde ve BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi'nde kişisel verileri de kapsamına alacak düzenlemelere gitmiştir[91]. Bunların yanı sıra, çalışmalarında getirdiği ilkelerin uygulanması hususunu denetleyen denetçilerin kişisel veriler üzerindeki hakimiyeti ve Birleşmiş Milletler bünyesinde çalışan personelin sağlıkları ile ilgili kişisel verilerinin korunmasına ilişkin çeşitli düzenlemeler de getirmiştir[92].

BM'nin doğrudan bu hususta temel çalışması ise 1990 yılında kabul edilen ve tavsiye niteliğinde olan "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler" dir[93]. İsminden de anlaşıldığı üzere, kişisel verilerin korunmasına ilişkin getirilen bu düzenleme Birleşmiş Milletlere dahil devletler için bağlayıcı olmayıp yalnızca yol gösterici niteliktedir ve kişisel verilerin

---

[88] Birleşmiş Milletler Örgütü, http://www.un.org/fr/aboutun/, 27.02.2012.
[89] http://www.un.org/fr/documents/charter/index.shtml, 27.02.2012.
[90] BM Şartı'nın Fransızca tam metni için bkz. http://www.un.org/fr/documents/charter/pdf/charter.pdf, 07.05.2012.
[91] BM İnsan Hakları Komitesi'nin getirmiş olduğu yorumla, kişisel verilerin BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17 nci maddesi kapsamında olduğu açıkça belirtilmiş, kişisel verilerin toplanması ve saklanmasının hukuki düzenlemeye tabi olması gerektiği belirtilmiştir. Ayrıntılı bilgi için bkz. **Küzeci**, s. 122-123.
[92] Ayrıntılı bilgi için bkz. **Vicien-Milburn**, **Maria**, "The United Nations And Personal Data Protection", Oktober 2005, s. 1, http://www.a-datum.ru/downloads/conferences/27th/The%20united%20nations%20and%20personal%20data%20protection.pdf, 28.02.2012, Birleşmiş Milletler tarafından 15 Ağustos 2000'de kabul edilen tıbbi standartlara ve yetkilere ilişkin düzenleme: "Medical standards and clearances", http://www.fsu.unlb.org/docs/related_documents/AI-2000-7.pdf, 28.02.2012.
[93] **Guidelines for the Regulation of Computerized Personal Data Files**, Genel Kurul tarafından 14 Aralık 1990 tarihinde kabul edilmiştir. Metnin tamamı için bkz. http://www.unhcr.org/refworld/pdfid/3ddcafaac.pdf, 28.02.2012.

korunması için yetkili ve bağımsız koruma organlarının kurulması gerekliliğini ifade eden uluslararası hukuk bağlamındaki ilk belgedir[94].

Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkelere[95] bakıldığında, kişisel verilerin korunmasına ilişkin olarak birtakım ilkelerin getirildiği görülmektedir. İlk ilke olan hukuka uygunluk ve dürüstlük ilkesine göre, kişisel veriler hukuka uygun ve dürüst bir şekilde toplanmalı ve işlenmeli, bu veriler BM Şartı'nda belirtilen amaç ve ilkelere aykırı olarak kullanılmamalıdırlar. İkinci ilke doğruluk ilkesidir ve buna göre kişisel verileri ihtiva eden dosyaların derlenmesinden veya saklanmasından sorumlu kişiler, kaydedilen verilerin doğruluğunu, güncelliğini ve uygunluğunu düzenli olarak kontrol etmekle yükümlüdürler. Üçüncü ilke amaçta belirlilik ilkesidir. Bu ilkeye göre; toplanan ve kaydedilen tüm kişisel verilerin amaçla ilintili ve amaca uygun olmalarının, bu kişisel verilerin ilgili kişinin rızası bulunmadıkça belirlenen amaç dışında kullanılmamasının ve kişisel verilerin tutulma sürelerinin belirtilen amaç için gereken süreyi aşmamasının sağlanması amacıyla, bir dosyanın (kişisel veri ihtiva eden) kullanılacağı amacın belirli ve meşru olması ve dosya oluşturulduğunda bunun ilgili kişinin bilgisine sunulması gerekmektedir. Dördüncü ilkeye göre ise, ilgili kişinin erişimi esastır. Kimliği hususunda kanıt sunabilen herkes, kendisiyle ilgili kişisel verilerin saklanıp saklanmadığını veya işlenip işlenmediği hususunda, makul olmayan bir bedel ödemeksizin ve makul olmayan bir süre beklemeksizin anlaşılır bir şekilde bilgilendirilmeli, verilerin aktarılması söz konusu olduğunda aktarıldığı yer ile ilgili olarak haberdar edilmeli ve hukuka aykırı, fuzuli veya gerçeğe aykırı bir veri girişi olması halinde, uygun düzeltme veya silme yapılmalıdır.

5 inci maddeye göre, keyfi veya hukuka aykırı olarak ayrımcılığa neden olabilecek ırk, etnik köken, din, cinsel yaşam, siyasi veya felsefi görüş ile ilgili kişisel veriler toplanmamalıdır. Ancak aynı maddede, bu genel kuralın istisnasını 6 ncı maddede sayılan hallerin oluşturacağı belirtilmiştir. 6 ncı maddede ise, ilk dört ilkeye, kanunda belirtilmesi ve uygun korumalar getirilmesi halinde, milli güvenlik, kamu düzeni, kamu sağlığı ve ahlakı veya başkalarının haklarının korunması amacıyla sınırlama getirilebileceği belirtilmiştir. 6 ncı maddenin ikinci fıkrasında ise 5 inci madde için özel bir düzenleme getirilerek, hassas kişisel verilerin

[94] **Şimşek**, s. 16.
[95] Çalışmanın devamında "Kişisel Verilere İlişkin BM Rehber İlkeleri" olarak anılacaktır.

toplanmamasına ilişkin kurala getirilecek sınırlamalarda, ilk dört ilke için öngörülmüş olan uygun korumalara ek olarak, ayrıca İnsan Hakları Evrensel Bildirgesi'nde belirtilen sınırlar dahilinde kalınması gerektiği belirtilmiştir.

7 nci maddede, veri güvenliği ilkesi gereğince, verilerin kaybolmamaları veya yok edilmemeleri, bunlara hukuka aykırı olarak erişilmemesi ve verilerin hukuka aykırı olarak kullanılmalarının önlenmesi için gerekli güvenlik tedbirlerinin alınması gerektiğine değinilmiştir. Koruma düzeyleri benzer olan iki veya ikiden fazla ülkede, kişisel verilerin o ülkelerin her birinin kendi sınırları içerisindeki gibi serbest bir dolaşımın benimsenmesi gerektiği ifade edilmiş, ancak karşılıklı korumanın söz konusu olmadığı durumlarda mahremiyetin korunması çerçevesinde bu serbest dolaşıma sınırlama getirilebileceği belirtilmiştir[96].

5. Avrupa Birliği'nde Kişisel Verilerin Korunması

a. Genel Bilgiler

Avrupa Birliği, İkinci Dünya Savaşı'ndan sonra, komşu ülkelerle süregelen kanlı çatışmaları önlemek, bölgeye barış getirmek ve Avrupa ülkelerini ekonomik, politik ve sosyal açıdan bir araya getirerek belirli bir birlik sağlamak üzere, 1950 li yıllarda temellerini oluşturmuştur[97]. Nitekim Belçika, Fransa, Almanya, İtalya, Lüksemburg ve Hollanda olan 6 kurucu ülke ile 1957 yılında Avrupa Ekonomik Topluluğu (European Economic Community) kurulmuş, 60 lı yıllarda Avrupa Birliği devletleri aralarındaki ticari ilişkilerde gümrük vergisini kaldırmış, gıda üretiminde ortak denetim uygulanacağı kararlaştırılmış, 1973 yılında ise bu birliğe İngiltere, İrlanda ve Danimarka da katılmıştır[98]. Daha sonra 1981 yılında Yunanistan'ın dahil olduğu Avrupa Birliği'ne, beş sene sonra İspanya ve Portekiz de katılmış, 1993 yılında ise Finlandiya, İsveç ve Avusturya da dahil olmuşlardır. 1986 yılında imzalanan Sözleşme ile Avrupa Tek Pazarı kurulmuş, bu kapsamda, gıda, hizmet, insan ve paranın AB üyesi ülkeler arasında serbest dolaşımı ilkesi benimsenmiş, 2002 yılında Euro'nun Avrupa Ülkelerinin çoğunluğunda kabul edilmesiyle ortak bir

[96] Bkz. "Kişisel Verilere İlişkin BM Rehber İlkeleri", m. 9.
[97] http://europa.eu/about-eu/eu-history/index_en.htm, 15.03.2012.
[98] http://europa.eu/about-eu/eu-history/index_en.htm, 15.03.2012.

para birimi kullanılmaya başlanmış, hatta ortak bir Anayasa oluşturulması için çalışmalar[99] yapılmıştır[100].

Bu çalışmalardan Avrupa Birliği Temel Haklar Şartı ve 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi çalışmamızın bu başlığı altında incelenecektir.

Ayrı bir başlık altında incelenmeyecek olan bir diğer çalışma ise, AB'nin telekomünikasyon alanında yaptığı düzenlemelerden olan 2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi'dir[101]. Bu yönerge her ne kadar kişisel verilerin korunmasına ilişkin genel hükümler içermekte ise de, gelişen teknoloji sebebiyle bazı alanlarda özel düzenlemeler yapılması ihtiyacının doğması sonucu ortaya çıkmıştır. Yönergenin düzenlediği temel alanlar, genel olarak; güvenlik, iletişimin gizliliği, trafik ve fatura verilerinin işlenmesinin sınırlandırılması, istenmeyen iletiler, çerezlerin (cookies) ve casus yazılımların (spyware) kullanılması, yer bilgilerinin anonim hale getirilmesi ve verilerin saklanması olarak sayılabilir[102]. Özel bir alanı ve belirli bir sektörü düzenleyen bu Yönerge'nin, 95/46/AT Yönerge'den önemli bir farkı; birinci maddesi ile tüzel kişilerin kişisel verilerini de koruma kapsamına almış olmasıdır. Elektronik İletişimin Korunması Yönergesi'nin gerekçesinin 10 uncu paragrafında, özel olarak düzenlenmeyen konularda 96/46/AT Sayılı Yönergenin uygulanacağı belirtilmiş, böylece bu Yönergenin özel alanı düzenleyen niteliğine de vurgu yapılmıştır.

---

[99] Avrupa Birliği'ne üye ülkelerin ortak bir Anayasaya sahip olmak amacıyla ortak bir Anayasa metni hazırlamak için bir araya geldikleri Roma'da süren tartışmalar sonucunda, Avrupa Birliği ülkeleri için ortak bir Anayasa metni üstünde uzlaşılmış, 29 Ekim 2004 tarihinde ise, Avrupa Anayasası olacak metin 25 üye ülkenin imzalaması ile kabul edilmiştir. Ancak metnin onaylanması aşamasında, onaylama için bazı ülkeler bu Anayasa metnini parlamentoda onaylarken, bazıları ülkelerinde referanduma gitmeye karar vermişlerdir. Referanduma gitmeye karar verip bunu gerçekleştiren ülkelerden olan Fransa'da, 29 Mayıs 2005 tarihinde yapılan referandumda, %54,87 oranında hayır oyu çıkmış, Hollanda'da 1 Haziran 2005 tarihinde yapılan (bağlayıcı olmayan) referandumda ise, %61,6 oranında hayır oyu çıkmıştır. Şimdiye kadar Avusturya (25.05.2005), Belçika (28.04.2005), Bulgaristan (11.05.05), Finlandiya (05.12.2006), Almanya (27.05.2005), Yunanistan (19.04.2005), Hırvatistan (20.12.2004), İtalya (06.04.2005) ve İspanya (18.05.2005) gibi ülkeler Avrupa Anayasası'nı onaylamışlardır, http://www.proyectos.cchs.csic.es/euroconstitution/Treaties/Treaty_Const.htm, 16.03.2012.

[100] http://europa.eu/about-eu/eu-history/index_en.htm, 15.03.2012.

[101] **Directive On Privacy And Electronic Communications**, (2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişim Korunması Yönergesi), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, 10.05.2012.

[102] **Küzeci**, s. 191.

b. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği vatandaşlarının temel haklarının şartlarını ve Avrupa Birliği'ne üye ülkelerin vatandaşlarına karşı sorumluluklarını düzenleyen Avrupa Birliği Temel Haklar Şartı[103], 7-8 Aralık 2000 tarihinde Fransa'nın Nice kentinde onaylanmıştır[104]. Temelde AB Anayasası'nın temeli olarak düşünülmüş, bu kapsamda 2004 yılında AB Anayasası'nın II. Bölümüne dahil edilmiştir[105]. AB Anayasa Antlaşmasının onaylanmaması üzerine, AB Temel Haklar Şartı hukuksal açıdan herhangi bir bağlayıcılık kazanamamış, ancak 1 Aralık 2009 tarihinde Lizbon Antlaşmasının yürürlüğe girmesiyle AB Temel Haklar Şartı hukuksal açıdan bağlayıcı hale gelmiştir[106].

AB Temel Haklar Şartı (I) Onur, (II) Özgürlükler, (III) Eşitlik, (IV) Dayanışma, (V) Vatandaşlık Hakları, (VI) Adalet ve (VII) Şartın Yorumlanmasını ve Uygulanmasını Düzenleyen Genel Hükümler olmak üzere toplam yedi bölümden oluşmaktadır[107].

AB Temel Haklar Şartı'nın "Onur" başlıklı I. bölümünde yer alan 1 inci maddede insanlık onurunun ihlal edilemeyeceği, insan onuruna saygı duyulması ve onun korunması gerektiği belirtilmiştir. Böylece AB Temel Hakları Şartı, korunacak en temel değer olarak insanlık onurunu ilk maddesinde açıkça koruma altına almıştır. Şartın "Özgürlükler" başlıklı II. bölümünde, 7 nci madde ile özel hayatın gizliliği korunması düzenlenmiş; 8 inci maddede ise ayrıca kişisel verilere yer verilerek bunların korunmasına ilişkin de ayrı bir hüküm sevk edilmiştir. 7 nci maddeye göre, "Herkes, özel ve aile yaşamına, konutuna ve iletişimine saygı gösterilmesini isteme hakkına sahiptir." Maddenin düzenlemesinin AİHS'nin 8 inci maddesi ile neredeyse aynı olduğu görülür. Aradaki fark ise, AİHS'nin 8 inci maddesinde haberleşme (correspondence) terimi kullanılmışken, AB Temel Hakları Şartı'nın 7 nci

[103] Çalışmamızın bundan sonrasında AB Temel Haklar Şartı olarak anılacaktır.
[104] http://www.ihd.org.tr/index.php?option=com_content&view=article&id=900:avrupa-birligi-temel-haklar-bildirgesi&catid=37:san-haklarylgeleri&Itemid=96, 21.03.2012.
[105] **Arsava**, **Füsun A.**, "AB'nin Anayasallaşma Sürecinde Temel Haklar Şartı", Ankara Avrupa Çalışmaları Dergisi, Cilt 3, No:2, Bahar 2004, s. 2, http://dergiler.ankara.edu.tr/dergiler/16/3/413.pdf, 21.03.2012, **Küzeci**, s.159, **Şimşek**, s.69.
[106] **Küzeci**, s.159.
[107] AB Temel Haklar Şartı'nın İngilizce metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF, 21.03.2012, Türkçe metni için bkz. http://www.ihd.org.tr/index.php?option=com_content&view=article&id=900:avrupa-birligi-temel-haklar-bildirgesi&catid=37:san-haklarylgeleri&Itemid=96, 21.03.2012.

maddesinde iletişim (communication) ifadesine yer verilmiş olmasıdır. Tabiidir ki, AİHS'nin imzalanmış olduğu 1950 tarihinden beri, teknolojik alanda önemli gelişmeler olmuş, bu anlamda son dönemlerde ortaya çıkan veya kullanımı artan diğer araçların da kapsama alınmak istenmiş; nitekim kişisel verilerin artan önemine bağlı olarak onları koruyan bağımsız bir madde de Şart'ta yer almıştır[108].

AB Temel Haklar Şartı'nın "Kişisel Verilerin Korunması" başlıklı 8 inci maddesinde "(1) Herkes kendisini ilgilendiren kişisel verilerinin korunması hakkına sahiptir. (2) Bu tür veriler belirli amaçlar için ve ilgili kişinin rızasına veya kanunla öngörülmüş diğer bir meşru temele dayanılarak adil bir şekilde işlenmelidir. Herkes kendisi hakkında toplanmış kişisel verilere erişme ve bunların düzelttirme hakkına sahiptir. (3) Bu kurallara uyulması bağımsız bir makam tarafından denetlenir." denilmektedir. Maddede yer alan "herkes" kavramının gerçek kişilerle birlikte tüzel kişileri de kapsayıp kapsamadığı madde metninde açıkça belirtilmemiş olması sebebiyle açıkça anlaşılamamaktadır. Ancak 95/46/AT Sayılı Yönerge ile birlikte değerlendirildiğinde maddenin korumayı hedeflediği temel kişilerin gerçek kişiler olduğu söylenebilir[109]. Nitekim AB Temel Haklar Şartı'nın 8 inci maddesine bakıldığında, üçüncü fıkrada belirtilen hususlar açısından da, madde, 95/46/AT Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi ile birlikte değerlendirilmeli, maddenin bu fıkrasındaki bağımsız denetim organı ile bu düzenlemeye (108 Sayılı Sözleşme m.286/2 ve 95/46/AT Sayılı Yönerge m.28) atıfta bulunulduğu düşünülebilir[110].

c. 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi

1995 yılında, Avrupa Birliği'nin kabul etmiş olduğu 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi[111], kişisel verilerin korunmasına ilişkin olan diğer uluslararası kaynaklar gibi kişisel verilerin toplanmasında belirli

---

[108] **Şimşek**, s. 69, **Küzeci**, s. 160.
[109] **Küzeci**, s. 161, **Şimşek**, s. 73.
[110] **Şimşek**, s. 74.
[111] Çalışmamızın bundan sonrasında 95/46/AT Sayılı Yönerge olarak anılacaktır. Yönergenin İngilizce tam ismi "**Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data**" olup, Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması ve bu Verilerin Serbest Dolaşımı" anlamına gelmektedir, Yönergenin İngilizce metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF, 15.05.2012.

sınırlamalar ve ilkeler getirmekte, verilerin güvenliğinin sağlanması ve AB üyesi olmayan ülkelere aktarımı gibi hususları düzenlemektedir[112]. Yönerge, 8 bölüm ve 34 maddeden oluşmakta olup, yönergede şu sekiz ilke sayılmaktadır: Hukuka ve dürüstlük kurallarına uygun işleme, Belirli, açık ve meşru amaçlar doğrultusunda işleme, Yeterli, ilgili ve aşırı ölçüde olmayacak verilerin işlenmesi, verilerin doğru ve güncel tutulması, Verilerin gerekli olandan daha uzun süre saklanmaması, Bireysel hak ve özgürlükler doğrultusunda işlenmesi, İşleme, muhafaza ve transfer aşamalarında güvenliğin sağlanmış olması, Eşdeğer, yakın veya daha üstün koruma sağlamayan ülkelere kural olarak transfer yasağı uygulanması[113].

95/46/AT Sayılı Yönerge ile tek Pazar düşüncesi altında gelişmekte olan ve bu amaçla çeşitli ticari faaliyetler geliştiren Avrupa Birliği üyesi ülkeleri arasındaki kişisel verilerin korunmasına ilişkin mevzuatların birbirine uyumlu hale getirilmesi ve böylece bu ülkelerin her birindeki asgari koruma ölçütünün belirlenmesi hedeflenmiştir[114]. Birinci maddede Yönergenin amacı belirlenmiş, ilk fıkrada üye devletlerin bireylerin temel hak ve özgürlüklerini, özellikle kişisel verilerin işlenmesine ilişkin alanda özel hayatın gizliliğinin korunmasını sağlamaları gerektiği belirtilmiş, ikinci paragrafta ise bu korunmanın sağlanması gerekçesiyle üye devletlerin verilerin özgür akışını engellememeleri gerektiği vurgulanmıştır. Üye devletler arasındaki ulusal mevzuat uyumunun önemine ise, Yönergenin 7 ve 8 Sayılı gerekçelerinde değinilmiş, kişisel verilerin korunması hususunda farklı düzenlemeler bulunmasının verinin bir üye devletten diğerine akışını engelleyebileceği ve bu tür durumların önlenmesi için sağlanan koruma düzeyinin tüm üye devletlerde eşdeğer olması gerektiği ifade edilmiştir[115].

Yönergenin 2 nci maddesinde yönergede kullanılacak kavramların tanımı yapılmış, kişisel veri kavramı diğer uluslararası kaynaklara benzer olarak "belirli veya belirlenebilir bir gerçek kişiye ilişkin her tür bilgi" olarak tanımlanmıştır. Tanımın bu kadar geniş tutularak gerçek kişilere ilişkin hemen hemen tüm bilgilerin

---

[112] **Keele**, s. 365.
[113] **Keser Berber**, **Leyla**, "Uluslararası Standartlar ve İyi Uygulama Kodları Işığında Kişisel Verilerin Korunması ve Kişisel Bilgi Yönetimi Sistemleri Oluşturulması", s. 2, http://www.docstoc.com/docs/91480740/ULUSLARARASI-STANDARTLAR-ISIGINDA-KISISEL-VERILERIN-KORUNMASI, 13.05.2012.
[114] **Küzeci**, s. 164-165.
[115] **Atak**, **Songül**, "Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri", Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Dergisi, Sayı 59-60, Temmuz Ağustos 2009, s. 202.

bu kapsama alınması eleştirilmiş, 29 uncu maddeye göre kurulan Verilerin Korunması Veri Koruma Grubu'nun (working party) biraz gecikmeli de olsa yayımladığı bir raporla kişisel veri tanımı dahil olmak üzere bazı tanımın çerçevesi belirlenmiştir[116]. Bu Veri Koruma Grubu, bağımsız bir danışma organı olarak faaliyet göstermekte olup, çeşitli konularda görüş belirtmekte ve yorum geliştirmekte, hem teoriye hem de uygulamaya yol gösterici nitelikte raporlar ve görüşler hazırlamaktadır[117]. Ancak bu rapor ve görüşler, Grubun danışma organı niteliğinde olması sebebiyle bağlayıcı değildir[118].

3 üncü maddede yönergenin uygulama alanı belirlenmiştir ve buna göre, yalnızca gerçek kişilere ait kişisel verilerin otomatik olarak kısmen veya tamamen işlenmesi bu kapsamda korunmaktadır. Buna karşın, bazı ülkelerin ulusal mevzuatlarını düzenlerken, tüzel kişilere ait kişisel verilerin korunmasını da bu kapsama aldıkları görülmektedir[119]. 8 inci maddede ise, kişilerin ırki ya da etnik kökenini, siyasi, dini veya felsefi inancını, sendika üyeliğini ortaya çıkaran kişisel veriler ile kişilerin cinsel yaşamına veya sağlığına ilişkin kişisel veriler, hassas kişisel veri olarak tanımlanmış, genel bir kural olarak bunların işlenmeleri yasaklanmıştır. Ancak aynı maddenin ikinci fıkrasında bu kurala istisna teşkil edecek durumlar düzenlenerek bu yasağın mutlak bir yasak olmadığı belirtilmiştir. Bu istisnalar arasında, veri öznesinin verinin işlenmesi için açık rıza vermiş olması, denetçinin ülkenin mevzuatı kapsamında iş hukukunun kendisine verdiği yetkileri kullanması, veri öznesinin fiziki veya hukuki olarak rıza gösteremeyecek durumda olduğu hallerde veri öznesinin veya bir başka kişinin hayati önem arz eden menfaatlerinin korunması için işlenmesi, veri öznesinin alenileştirdiği kişisel verilerin işlenmesi veya verilerin hukuki hakların korunması ya da uygulanması için işlenmesi durumları sayılmıştır.

---

[116] WP 136, 01248/07/EN, Opinion 4/2007 on the Concept of Personal Data (Kişisel Veri kavramına İlişkin Görüşler), 20.06.2007. Bu görüşe göre, kişisel veriler, gerçek kişilere ilişkin objektif nitelikteki ve görüşler ile değerlendirmeler gibi sübjektif nitelikleri de kapsayan her tür bilgiyi ifade etmektedir. **Atak**, Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, s. 206.

[117] **Küzeci**, s. 157.

[118] **Atak**, Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, s. 219.

[119] Bu konuda ayrıntılı açıklama için ve hangi ülkelerin bu şekilde düzenleme yaptığı ile ilgili bilgi için çalışmamızın "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" başlığı altına bakılmalıdır. Burada yalnızca, tüzel kişileri de koruma kapsamına dahil eden ülkelerden bazılarının İsviçre, Avusturya, Şili, Bulgaristan ve İtalya olduğunu belirtmek gereklidir.

Yönergede veri öznesine diğer uluslararası kaynaklarla benzer haklar verilmiş, 12 nci maddede veri öznesinin kendisiyle ilgili tutulmuş kişisel verilere ulaşabilme, kendisiyle ilgili işlenen kişisel veri bulunup bulunmadığını ve varsa işlemenin amacını ve işleme kapsamına giren verilerin hangi kategoriden veriler olduğunu öğrenme, işlenen kişisel verinin kendisine anlaşılır biçimde bildirilmesini isteme, işlenmesi yönerge hükümlerine uymayan kişisel verilerin silinmesini, düzeltilmesini veya işlemenin durdurulmasını isteme, imkansız olmadığı veya orantısız çaba gerektirmediği müddetçe kişisel verilerin ifşa edildiği üçüncü kişilerin bu madde uyarınca yapılan silme, düzeltme veya durdurmalardan haberdar edilmesini isteme gibi haklar tanınmıştır. 13 üncü maddede ise bu haklara getirilebilecek sınırlama gerekçeleri ulusal güvenlik ve savunma, kamu güvenliği, suçların veya meslek ahlak kuralları ihlallerinin önlenmesi, tespit edilmesi, araştırılması ve soruşturulması, bütçe ve vergi konuları dahil olmak üzere bir üye devletin veya Avrupa Birliği'nin ekonomik veya finansal menfaatinin bulunması, veri öznesinin veya başkasının hak ve özgürlüklerinin korunması olarak düzenlenmiştir.

Yönergenin 25 inci maddesinde, üçüncü ülkelere veri aktarımı hususu düzenlenmiş ve buna ilişkin temel ilkeler belirlenmiştir. İlk fıkrada, işlenmekte olan kişisel verinin veya işlenmesi amacıyla transfer edilen kişisel verinin diğer bir ülkeye transfer edilmesinin, bu diğer ülkenin bu Yönerge çerçevesinde eşdeğer koruma sağlanması şartına bağlı olduğu belirtilmiştir. İkinci fıkrada ise bu eşdeğer korumanın kişisel verinin aktarılması esnasındaki işlemleri de kapsar nitelikte olması gerektiği ve kişisel verinin niteliğine, amaca ve teklif edilen işleme süresine, verinin çıkış ülkesine ve varacağı nihai ülkeye, transfer edileceği diğer ülkede genel ve bölgesel hukukun kurallarına ve ülkedeki güvenlik önlemlerine özellikle önem atfedilmesi gerektiği ifade edilmiştir. Dördüncü fıkraya göre, Komisyon'un, aktarımın yapılacağı diğer ülkede eşdeğer koruma seviyesinin karşılanmadığını tespit etmesi durumunda üye ülkenin aktarımı önleme yükümlülüğü bulunmaktadır.

26 ncı maddede ise, verilerin aktarılacağı ülkede yeterli düzeyde ve eşdeğer koruma bulunmaması halinde dahi aktarımın yapılabileceğine ilişkin şu istisnalar getirilmiştir: İlgili kişinin aktarım için açık rızasının bulunması (m. 26/1,a), Aktarımın bir sözleşmenin ifası veya ilgilinin talebi ile sözleşme öncesi bir ilişkinin yürütülmesi için gerekli olması (m. 26/1,b), Aktarımın veri öznesinin çıkarlarının

korunması amacıyla, veri denetçisi ve üçüncü bir kişi arasında yapılan bir sözleşmenin sonuçlandırılması veya uygulanması için gerekli olması (m. 26/1,c), Aktarımın önemli bir kamusal çıkarın korunması veya hukuki taleplerin tesisi, uygulanması veya korunması için gerekli veya kanunen zorunlu olması (m.26/1,d), Aktarımın veri öznesinin hayati önem arz eden menfaatlerini korumak için yapılması (m.26/1,e) ve son olarak aktarımın herkese açık olan kamu sicillerinden yapılması ve veri koruma mevzuatının aradığı şartları taşıması[120].

Yönerge, gerçekten de zaman içinde amacına ulaşmış, aşağıdaki başlık[121] altında inceleneceği üzere Avrupa Birliği'ne üye ülkelerin veri koruma hukukunun uyumlu olması sağlanmış, uyum bulunmayan diğer ülkelerle ise Safe Harbor antlaşmaları[122] imzalanmıştır. Yönerge'de kişisel verilerin silinmesi ile ilgili bir ilke belirlenmemiş olması doktrinde önemli bir eksiklik olarak görülmüştür. Bunun sonucu olarak, AB üyesi ülkelerin toplanma amacının bireyin belirlenebilirliğini gerektirmediği durumlarda kişisel verileri anonimleştirmelerini, verilerin yanlış olduğu anlaşıldığında veya bu verilere itiraz edildiğinde ise silinmelerini gerektirecek bir düzenleme getirmelerinin Yönerge'ye uyum kapsamında yeterli olacağı belirtilmiştir[123]. Bu düzenleme ise, doktrinde yetersiz bulunmuş, kişisel verilerin silinmesi ile ilgili olarak daha belirli bir hüküm sevk edilmesi gerektiği ifade edilmiştir.

B. BAZI ÜLKELERDE KİŞİSEL VERİLERİN KORUNMASI

1. Genel Bilgiler

Dünyadaki diğer ülkelerin pek çoğunda, özel hayatın gizliliği kanunu veya kişisel verilerin korunmasına ilişkin kanun gibi isimler altında, bireylerin kişisel verilerinin korunması için özel kanunlar çıkarılmış ve yıllardan beri uygulanmıştır. Avrupa ülkelerinde ise, özellikle 1970 li yıllarda başlayan ve sonraki senelerde de devam eden tartışmalar, kişisel veriler hukukunun zenginleşmesini ve birtakım

[120] **Küzec**i, 174-175, **Atak**, Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, s. 216.
[121] Bkz. "Bazı Ülkelerde Kişisel Verilerin Korunması".
[122] Ayrıntılı bilgi için bkz. "Bazı Ülkelerde Kişisel Verilerin Korunması" ana başlığı altında "Amerika Birleşik Devletleri" alt başlığı.
[123] **Keele**, s. 365.

düzenlemelere gidilmesini sağlamıştır. Avrupa'da başlayan bu gelişmeler üzerine, Avrupa Birliği üyesi olmayan diğer ülkeler de zamanla bu alandaki mevzuatlarını mümkün olduğunca Avrupa Birliği üyelerinin tutturmuş oldukları standardı yakalamaya çaba göstermişlerdir. Zira 1995 yılında kabul edilen 95/46/AT Sayılı Yönerge ile Avrupa ülkelerinin tamamında kişisel veriler hukukuna ilişkin belirli bir standardın yakalanması öngörülmüş, bu standarda eşdeğer koruma sağlayamayan ülkelere kişisel veri aktarımı yapılması yasaklanmıştır. Bu bağlamda örneğin Avrupa Birliği üyesi olmayan ve kişisel veriler hukuku alanını tek elden düzenleyen bir kanunu bulunmayan Amerika Birleşik Devletleri'ndeki ticari kuruluşlar kişisel veri aktarımı hususunda birtakım sorunlar yaşamış ve çıkarılan kanunlarla bunlara çözüm aranmıştır.

Bu noktadan bakıldığında, Türkiye bu alanda son derece geri kalmış, 1981 yılında 108 Sayılı Sözleşme'yi imzaladığından beri bu sözleşmeyi iç hukukuna aktararak onaylamamış ve kişisel verilerin korunmasına ilişkin herhangi bir özel kanun çıkarmamıştır. Aşağıda inceleneceği üzere, Türkiye'de 1995 yılından beri kişisel verilerin korunmasına ilişkin bir kanun çıkarmak amacıyla çalışmalar yapılmış, birkaç defa buna ilişkin komisyon kurulmuş, nihayet bir kanun tasarısı hazırlanmış, ancak bu kanun tasarısı yıllardır tasarı aşamasında kalarak bir türlü kanunlaşamamıştır. Bu başlık altında incelenecek olan diğer ülkelerde ise, kişisel verilerin korunmasının önemi Türkiye'de olduğundan çok daha iyi anlaşılmış olup, bireylerin bu alanda korunmaları amacıyla gerekli kanuni düzenlemeler yapılarak bu konuya ilişkin kanunlar çıkarılmıştır. Bu da, Avrupa Birliği'ne üye olan ülkeler ve iç hukuklarında AB kişisel veri hukuku standardını yakalamış olan ülkeler bakımından, Türkiye'yi kişisel verilerde eşdeğer korumayı haiz olmayan bir ülke haline getirmiştir. İşte bu başlık altında da, kişisel veri hukuku açısından önemli gördüğümüz, AB'ye üye olan ve olmayan bazı ülkelerde çıkarılan kanunlar ve kişisel verilerin korunmasına ilişkin yapılan düzenlemeler incelenecektir.

2. Kıta Avrupası'nda Kişisel Verilerin Korunması

a. Fransa

(1) Fransız Ceza Kanunu

Fransız kişisel verileri koruma hukukunun önemli bir kısmı da Fransız Ceza Kanunu'nda yer almaktadır. Bu alanda işlenebilecek suçlar Fransız Ceza Kanunu'nun Kişilere Karşı Suçlar isimli İkinci Kitabının, İnsana karşı ihlaller isimli İkinci Başlığı'nın, kişilere karşı ihlaller isimli altıncı bölümünde düzenlenmiştir[124]. Fransız Ceza Kanunu'nun 226-16 ve devamı maddelerinde düzenlenen suçlara göre, kanun tarafından öngörülmüş olan usullere uyulmaksızın kişisel verileri işleyen veya işlenmesini sağlayan kişilere 5 yıla kadar hapis cezası ve 300.000 Euro para cezası verileceği öngörülmüştür (m.226-16). Benzer şekilde 1978 tarihli Kanun'nın 24 üncü maddesinde belirlenen usuller çerçevesinde, CNIL'in bu hususta koyduğu normlara ve sınırlamalara uymaksızın kişisel veri işleyen veya işlenmesini sağlayan kişilere yine aynı ceza verilir (m.226-16-1-A). Bu bölümde kişisel verilerin hukuka aykırı olarak işlenmesine yönelik belirlenen cezaların miktarı genelde aynıdır. Ancak bu maddeler açısından dikkat çekici olan önemli bir nokta, yukarıda belirtilen ve 226-16 ile 226-16-1-A maddelerindeki suçlarda, bu suçların "ihmali" olarak işlenmeleri halinde dahi, faillerin aynı cezayı alacaklarının madde metninde belirtilmiş olmasıdır.

Fransız Ceza Kanunu'nun diğer ilgili maddelerinde, yine 1978 tarihli Kanun'nun 34 üncü maddesindeki usullere uyulmadan kişisel veri işlenmesi veya işlenmesinin sağlanması (m.226-17), elektronik haberleşme hizmetleri sağlayıcısının kişisel verilerle ilgili ihlalleri CNIL'e bildirmemesi (m.226-17-1), kişisel verilerin hileli, dürüst olmayan veya hukuka aykırı yöntemlerle toplanması (m.226-18), veri öznesinin karşı çıkması ve bu karşı çıkmanın meşru (kanuni) temellere dayanmasına rağmen, kişisel verilerinin, pazarlama veya ticari amaçlı olarak işlenmesi (m.226-18-1), kanunlarla belirtilmiş haller dışında ve ilgili kişinin rızası bulunmaksızın, doğrudan veya dolaylı olarak ilgili kişilerin ırkları veya etnik kökenleri, siyasi, dini

[124] Fransız Ceza Kanunu, http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006417929&idSectionTA=LEGISCTA000006165309&cidTexte=LEGITEXT000006070719&dateTexte=20120304, 04.03.2012.

veya felsefi görüşleri, sendikal bağlantıları, sağlık durumları veya cinsel eğilimleri, mahkumiyetleri ve haklarında uygulanan güvenlik tedbirleri hakkındaki kişisel verilerin bilişim sistemlerine konması veya saklanması (m.226-19), kanunlarla öngörülmüş olan tarihi, istatistiki ve bilimsel amaçlar dışında, kişisel verilerin CNIL'e yöneltilen bildirim veya izin talebinde belirtilenden veya kanunların amaçla sınırlı olarak belirlediğinden daha uzun bir süre tutulmaları (m.226-20), kişisel verilerin yok edilmesi (m.226-21), paylaşılması halinde ilgili kişilerin özel hayatını ihlal edecek nitelikteki kişisel verilerin ilgili kişinin izni olmaksızın yetkisiz üçüncü kişilerin bilgisine sunulması (m.226-22), 1978 tarihli Kanun'da belirtilen veya CNIL tarafından saptanan koşullar sağlanmaksızın kişisel verilerin AB üyesi olmayan ülkelere transfer edilmesi (m.226-22-1) 5 yıla kadar hapis cezası ve 300.000 Euro para cezası ile cezalandırılır[125]. Yalnız, 226-22 nci maddede düzenlenen kişisel verileri yetkisiz kişilere ifşa edilmesi suçunun ihmal suretiyle işlenmesi halinde verilecek ceza 3 yıla kadar hapis cezası ve 100.000 euro para cezasıdır. 226-25 ve devamı maddelerinde ise, kişilerin genetik bilgilerinin kanunlarla belirtilen haller dışında kaydedilmesi, kişilerin genetik bilgileri hakkında bilgi edinmek amacıyla sağlık alanında yapılan bilimsel çalışmalardaki kişisel verilerin hukuka aykırı olarak geçirilmesi gibi kişilerin genetik bilgilerini korumaya yönelik suçlar ihdas edilmiştir[126]. Bu cezalara ilave olarak, faillerin, bu suçu işlemelerini sağlayan veya suçu işlemelerini kolaylaştıran kişilerin meslekten men edilmeleri, 5 yıl veya daha fazla süre ile ruhsatlı silah taşımalarının yasaklanması, bazı sivil ve aile haklarından yoksun bırakılmaları, haklarında verilen mahkumiyet kararının ilan veya ifşa edilmesine de karar verilebileceği düzenlenmiştir (m.226-31).

Fransız Ceza Kanunu'nda, kişisel verilerin korunması kapsamında düzenlenen suçların oldukça ağır cezalar öngördüğü görülmektedir. Bu bakımdan Türk Ceza Kanunu'nda düzenlenmiş olan ve aşağıda incelenecek olan suçlarla karşılaştırıldığında, Türkiye'de belirlenmiş olan cezaların daha az olduğu görülmektedir. Yalnız Fransız Ceza Kanunu açısından eleştirilebilecek önemli bir husus, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve saklanması hususunda,

[125] http://www.legifrance.gouv.fr/affichCode.do;jsessionid=6C9890927AC0CBE65600F0337B597A8B.tpdjo03v_1?idSectionTA=LEGISCTA000006165313&cidTexte=LEGITEXT000006070719&dateTexte=20120304, 04.03.2012.

[126] http://www.legifrance.gouv.fr/affichCode.do;jsessionid=6C9890927AC0CBE65600F0337B597A8B.tpdjo03v_1?idSectionTA=LEGISCTA000006165397&cidTexte=LEGITEXT000006070719&dateTexte=20120304, 04.03.2012.

hassas nitelikli kişisel veriler açısından herhangi bir ayrım yapılmamış olmasıdır. Hassas nitelikte kişisel verilerin hukuka aykırı olarak kaydedilmeleri veya işlenmeleri çok daha ciddi neticeler doğuracağından, bu hususun daha ağır bir ceza verilmesini gerektiren bir nitelikli hal olarak düzenlenmesi gerektiği kanaatindeyiz.

(2) 1978 Tarihli Veri Koruma Kanunu

Fransa, kişisel verilerin korunması ile ilgili olarak AB Direktifi'ni iç hukukuna 2004 yılına kadar aktarmamış olsa da, 1975 yılından itibaren bu alanda çeşitli çalışmalar yapmıştır. İlk olarak 1974 yılında, Fransa Cumhurbaşkanı, kişisel verilerin ve iletişim teknolojilerinin kullanımının yaygınlaşmasının kontrol edilmesi ve sınırlandırılmasının bireysel özgürlükler üzerindeki etkisinin araştırılması için özel bir komisyon[127] görevlendirmiştir. Bu komisyon, 6 Ocak 1978 tarihinde kabul edilen kanunla[128] resmi bir kuruluş halini almış, o günden bugüne değin bilişim ve bireylerin özgürlüğü alanında çalışan bir kuruluş olarak varlığını sürdürmüştür[129]. 1978 tarihli Kanun ile kurulmuş olan ve CNIL olarak adlandırılan bu kuruluşun temel amacı, kanunda da belirtildiği üzere, bilişimin vatandaşların hizmetine sunulması, ancak bunun bireylerin kimliğini, insan haklarını, özel hayatın gizliliğini ve bireysel ve kamusal özgürlükleri ihlal etmemesini sağlamaktır[130]. Kuruluşun en önemli özelliği bağımsız bir kuruluş olması ve devletin hiçbir makamından emir almamasıdır; bu anlamda CNIL bağımsız bir idari otoritedir[131].

1978 tarihli Kanun, 6 ağustos 2004 tarihinde çıkarılan kanun[132] ile önemli değişikliklere uğramış, bu değişiklikler ile AB Direktifi'nin getirdiği standartlar

---

[127] La Commission Nationale de l'Informatique et des Libertés (CNIL), Enformatik ve Özgürlükler Milli Komisyonu, http://www.cnil.fr/la-cnil/, 04.03.2012.

[128] 6 Ocak 1978 tarihli, bilişime, (bilişim) dosyalara ve özgürlüklere ilişkin kanun, Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, metnin tamamı için bkz. http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf, 04.03.2012. Çalışmanın bundan sonraki kısımlarında "1978 tarihli Kanun" olarak anılacaktır.

[129] **Simitis**, **Spiros**, "From the Market to the Polis: The EU Directive on the Protection of Personal Data", Iowa Law Review, Vol. 80, Issue 3, May 1995, s. 2, http://0-heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/ilr80&div=26&collection=journals&set_as_cursor=6&men_tab=srchresults, 05.03.2012.

[130] http://www.cnil.fr/la-cnil/qui-sommes-nous/, 04.03.2012.

[131] **Forest**, **David**, Droit des Données Personnelles, Paris 2011, s. 25.

[132] Kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin ve 6 Ocak 1978 kanunda değişiklik yapan kanun, Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, kanunun tam metni için bkz.

Fransız iç hukukuna aktarılmıştır. 1978 tarihli Kanunun bugünkü haline bakıldığında, CNIL'in hala etkili olduğu ve 2004 tarihli kanun ile yapılan değişikliklerle CNIL'in yaptırım yetkisinin artırıldığı, ancak güvenlik alanında ve emniyet teşkilatında mevcut dosyalara erişim hususunda izin verme yetkisinin daraltıldığı görülmektedir[133].

1978 tarihli Kanun'nun 2 nci maddesine göre, kanun, doğrudan veya dolaylı olarak kimliği belirli veya belirlenebilir olan gerçek kişileri kapsamakta olup, tüzel kişileri bu kanunun korumasının kapsamı dışında bırakmaktadır[134]. Kanun'da, 39 uncu madde ile ilgili kişilerin kendileri ile ilgili olarak toplanmış kişisel veriler hakkında doğrudan bilgilendirilmelerinin yanı sıra, 41 inci madde ile ilgili kişilerin, CNIL'den, adli kollukta, İçişleri Bakanlığı nezdindeki kuruluşlarda ve Schengen sisteminde[135] kendileriyle ilgili kişisel verilerin toplanıp toplanmadığının araştırılmasını talep etme hakkı düzenlenmiştir[136]. Fransız kişisel veri koruma hukukunun temel taşlarından biri, kişisel veri işleyene getirilen haber verme yükümlülüğüdür[137]. Buna göre, Fransa'da kişisel verilerin hukuka uygun olarak işlenebilmesi için, veri dosyalarının ne zaman açıldığı ve bu dosyaların içeriğinin neyi kapsadığı hakkında CNIL'in bilgilendirilmesi, özellikle hatalı verileri düzeltme hakkı başta olmak üzere, hakları konusunda veri öznelerinin bilgilendirilmeleri, kişisel verilerin gizliliğinin ve güvenliğinin sağlanması ve bunların yetkisiz üçüncü kişilerden korunması, CNIL'in denetlemelerine ve bilgi talebine riayet edilmesi ve son olarak bazı koşullarda kişisel verilerin işlenmesinden evvel CNIL'in izninin alınmış olması gerekmektedir[138]. 1978 tarihli Kanun'nun 68 ve devamı

---

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=, 04.03.2012.

[133] **Forest**, s. 25.

[134] **Forest**, s. 29.

[135] Adli kollukta **STIC** (Système de traitement des infractions constatées – Tespit edilmiş ihlalleri ele alma sistemi) ve **JUDEX** (Système judicaire de documentation et d'exploitation – Adli belgeleme ve kullanma sistemi), İçişleri Bakanlığı'nda **DCRI** (Direction centrale du renseignement intérieur – Merkezi içişleri istihbarat yönetimi) ve Schengen için **SIS** (Système d'information Schengen – Schengen enformasyon sistemi) sistemleri kullanılmaktadır. Ayrıntılı bilgi için bkz. **Forest**, s. 39-40.

[136] http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf, 04.03.2012.

[137] **Simitis**, s. 3

[138] **Hook**, **Elizabeth I.-Martin**, **Cécile-Ivanova**, **Suzette**, "Transborder Law: Application of the European Union Data Privacy Law to Multinational Corporations", International Law Practicum, Vol.21, No.2, Autumn 2008, s. 129, http://international.westlaw.com/result/default.wl?rp=%2fsearch%2fdefault.wl&rltdb=CLID_DB370529135145&sp=intmar-000&fn=_top&service=Search&action=Search&query=%22TRANSBORDER+LAW%3a+APPLICATION+OF+THE+EUROPEAN+UNION+DATA+PRIVACY+LAW%22&rs=WLIN12.04&db=INLP

maddelerinde, kişisel verilerin AB üyesi olmayan üçüncü ülkelere aktarılması ile ilgili kurallar düzenlenmiş, genel kural olarak da aktarım için eşdeğer koruma aranmıştır[139].

2006 yılında, Fransa'daki Amerikalı "Tyco Healthcare France" şirketi, yaptığı kişisel veri işlemesine dair bir sistem hakkında CNIL'i bilgilendirmiş, CNIL işlenen kişisel verilerin AB üyesi olmayan üçüncü üyelere aktarım prosedürü hakkında şirketten bilgi istemiş, şirket bunun üzerine istenen bilgileri göndermeyerek veri aktarımını durdurduğunu bildirmiş, ancak ilerleyen dönemlerde CNIL'in kontrolü üzerine aktarıma CNIL'in tarafından onaylanmamış bir prosedür ile devam edildiği ve yapılan kişisel veri işlemesinin CNIL'e sunulan işleme amaçları listesini büyük oranla aşıldığı fark edilmiş ve CNIL, Nisan 2007'de, yetkisini kullanarak şirkete 30000 Euroluk bir ceza kesmiştir[140].

Fransa'da kişisel verilerin korunması ile ilgili 02.10.2001 tarihli Onof, Nikon France'a karşı davasında önemli bir karar verilmiştir. Spaeter, Néocel'e karşı davasında, özel sektörde işverenlerin çalışanlarının iş saatlerindeki e-postalarını denetlemesine ilişkin genel kuralları belirlemiş olan ve bir işverenin çalışanının kontrol ettiği faaliyetlerine ilişkin bilgilendirdiği sürece özel e-postalarını ve telefon konuşmalarını takip edebileceğini belirten Fransız Temyiz Mahkemesi[141], Nikon v. France davasında tarihi bir karar alarak, çalışanların özel hayatlarının iş saatleri sırasında ve işyerinde de korunması gerektiğini, bu itibarla Frédéric Onof isimli çalışanının iş saatlerinde almış olduğu özel mailleri, Onof'un yokluğu esnasında okuyup kopyalayarak bu suretle çalışanının bilgisayarını iş dışında amaçlar için kullandığını tespit eden Nikon France şirketini mahkum etmiştir[142]. Bu davada Fransız Yargıtayı, AİHS'nin 8 inci maddesi ile korunan özel hayatın gizliliğine, bu alanındaki AİHM içtihat hukukuna ve o dönem yürürlükte olan Fransız İş

RAC&eq=search&srch=TRUE&rlt=CLID_QRYRLT9421036135145&fmqv=s&origin=Search&vr=2.0&method=TNC&cfid=1&mt=314&sv=Split&pbc=BC6E23F9, 04.03.2012.

[139] http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf, 04.03.2012.

[140] **Hook-Martin-Ivanova**, s. 129-130.

[141] Court de Cassation (Fransız Yargıtayı resmi web sitesi), http://www.courdecassation.fr/, 10.03.2012.

[142] **Suda**, **Yohei**, "Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States", Washington University Global Studies Law Review, Vol. 4, Issue 2, 2005, s. 257, http://0-heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/wasglo4&div=16&collection=journals&set_as_cursor=1&men_tab=srchresults&terms=yohei|suda&type=matchall, 10.03.2012.

Kanunu'nun L.120-2 maddesine[143] değinmiştir[144]. İş Kanunu'nun bu maddesi ile, çalışana getirilecek olan sınırlamanın orantılı olması gerektiğinden bahsedilmiş, Fransız Yargıtay'ı da bu maddeye değinerek Nikon France'ın çalışanına uyguladığı sınırlamanın orantılı olmadığına değinmiştir. Son olarak, Mahkeme, bir şirket her ne kadar çalışanlarının bilgisayarlarını iş dışında amaçlar için kullanmalarını yasaklamış olsa da, bu yasağın, çalışanların bilgisayarlarında yer alan kişisel mesajlarına ve kişisel bilgilerine izinsiz erişimlerini meşru kılmadığını belirtmiştir[145]. Nitekim bu kararın üzerine, Mart 2001'de CNIL, yayımladığı bir raporda, işverenlerin, çalışanlarına iş saatlerinde kullandıkları bilgisayarların şahsi kullanımına ilişkin bu denli geniş kapsamlı bir yasağın uygulanmasının orantısız olduğunu ve işverenler tarafından, çalışanların bilgisayarlarını, orantılı oranda şahsi işleri için kullanmalarına müsamaha gösterilmesi gerektiğini belirtmiştir[146].

b. İsviçre

(1) Genel Bilgiler

İsviçre'nin iç hukukunda kişisel verilerin korunmasına ilişkin yapılmış olan düzenlemelere bakılmadan evvel, İsviçre'nin bu alanda uluslararası kaynakların hangilerine taraf olduğuna kısaca değinmekte fayda görmekteyiz. Her ne kadar İsviçre Avrupa Birliği ülkelerinden biri olmayıp, bu sebeple 95/46/AT Sayılı Yönerge'yi imzalamamış olsa da, Avrupa Konseyi'ne üye olup 108 Sayılı Sözleşme'yi imzalamış, OECD Rehber İlkelerini kabul etmiş ve Avrupa İnsan Hakları Sözleşmesi'ni imzalayıp onaylamıştır[147]. Bu itibarla, 95/46/AT Sayılı Yönerge haricindeki temel uluslararı kaynakların çoğunu imzalayarak onaylamış, Yönerge'ye taraf olmamasının getirdiği eksiklikleri ise, Yönergenin AB üyesi olmayan üçüncü ülkelere veri aktarımı hususundaki katı kurallarını göz önüne alarak, iç hukukunu Yönergeye paralel olarak düzenleyerek gidermiştir. Nitekim Haziran 1999'da, Yönerge'nin 29 uncu maddesi kapsamında kurulan Veri Koruma Grubu,

---

[143] Fransız Yargıtay'ının kararı verdiği yıl olan 2001'de yürürlükte olan bu kanun, 1 Mart 2008 tarihinde yürürlükten kalkmış, günümüzde geçerli olan Fransız İş Kanunu'nun L1121-1 maddesi, eski kanunnın L.120-2 maddesini aynen karşılamaktadır.

[144] Fransız Yargıtay'ının 02.10.2001 tarihli kararının tam metni için bkz. http://www.privacynetwork.info/arresten/27.pdf, 04.03.2012.

[145] **Yohei**, s. 257.

[146] **Yohei**, s. 258.

[147] Privacy International, Switzerland - Privacy Profile, 23 Ocak 2011, https://www.privacyinternational.org/article/switzerland-privacy-profile#_ftn1, 09.03.2012.

İsviçre veri koruma hukukunun Yönergeye uygun olduğuna karar vermiş, Temmuz 2000'de ise Avrupa Konseyi, gelecekte İsviçre'ye yapılacak tüm veri transferlerini onaylamış, 20 Ekim 2004'te ise bu kararını kesinleştirmiştir[148].

(2) İsviçre Federal Anayasası

İsviçre'de kişisel verilerin korunmasına ilişkin temel güvence İsviçre Federal Anayasası'nın 13 üncü maddesi ile getirilmiştir. İsviçre Anayasası'nın "Gizli Alanın Korunması" başlıklı 13 üncü maddesinin birinci fıkrasına göre[149], herkes özel hayatının ve aile hayatının gizliliğine, konutuna, yazışmalarına, telekomünikasyon ve posta yoluyla kurduğu ilişkilere saygı gösterilmesi hakkına sahiptir[150]. İkinci fıkrada ise herkesin kendisi ile ilgili kişisel verilerin kötüye kullanımından korunma hakkına sahip olduğu belirtilmiştir.

(3) İsviçre Medeni Kanunu

İsviçre'de kişisel hakları koruyan hükümlerin yer aldığı bir diğer kanun ise İsviçre Medeni Kanunu'dur[151]. Bu kanunun 29 uncu maddesine göre, başkası tarafından ismi kullanılan kimseler bu kullanımı yasaklayan bir karar talep edebilirler ve ismi kullanan kişinin kusurlu olması durumunda tazminat talebinde bulunabilir. Aynı kanunun 43a maddesinin ilk fıkrasında, medeni halin kaydedilmesinde, Federal Konsey, kişisel verileri işlenen bireylerin kişilik haklarını ve anayasal haklarını korumakla yükümlü olduğu düzenlenmiş, diğer fıkralarda ise kişisel verilere hangi kuruluşların hangi usuller çerçevesinde internet üzerinde bireylerin kişisel verilerine ulaşabilecekleri belirtilmiştir. 45a maddesine göre de, Konfederasyonun her Kanton için merkezi bir veri tabanı işletmesi gerektiği, buna bağlı olarak kanunların çizdiği sınırlar çerçevesinde ve kantonlarla işbirliği halinde Federal Konsey'in işbirliği yöntemini, nüfus idaresi mercilerinin bu veri tabanına erişimlerini, verilerin

---

[148] https://www.privacyinternational.org/article/switzerland-privacy-profile#_ftn1, 09.03.2012.

[149] 101 Sayılı 18.04.1999 tarihli İsviçre Federal Anayasası (Constitution fédérale de la Confédération suisse), Anayasa metninin tamamının Fransızca metni için bkz. http://www.admin.ch/ch/f/rs/1/101.fr.pdf, İngilizce metni için bkz. http://www.admin.ch/ch/e/rs/1/101.en.pdf, 06.03.2012.

[150] Maddenin çevirisi Fransızca metninden yapılmıştır.

[151] 10 Aralık 1907 tarihli İsviçre Medeni Kanunu, kanunun İngilizce metni için bkz. http://www.admin.ch/ch/e/rs/2/210.en.pdf, Fransızca metni için bkz. http://www.admin.ch/ch/f/rs/2/210.fr.pdf, 07.03.2012.

korunması ve güvenliklerinin sağlanması için örgütsel ve teknik önlemleri, son olarak da arşivleme sistemini düzenler.

(4) İsviçre Ceza Kanunu

Kişisel verilerin korunmasına ilişkin İsviçre kanunlarında yer alan bir diğer düzenleme ise, İsviçre Ceza Kanunu'ndaki düzenlemedir[152]. Türk Ceza Kanunu'nun 132 ve 133 üncü maddelerinde düzenlenen "Haberleşmenin Gizliliğini İhlal" ve "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçları bakımından İsviçre Ceza Kanunu'nun ilgili maddeleri[153] adeta mehaz kanun özelliği taşırken, kişisel veriler açısından aynı durum söz konusu değildir, zira İsviçre Ceza Kanunu'nda bu husus yalnızca tek bir maddede ele alınmış ve düşüncemize göre yetersiz bir düzenleme yapılmıştır. Kanunun "179^{novies}" maddesine göre, hassas kişisel veri ihtiva eden bir dosyadan veya serbest erişime açık olmayan kişisel bir profilden izinsiz olarak kişisel veri ele geçiren kişi hakkında, şikayet üzerine, 3 yıla kadar hapis cezasına veya adli para cezasına hükmolunur.

İsviçre Ceza Kanunu'nun başka suçları düzenleyen bazı maddelerinde de kişisel verilerle ilgili koruma ihdas edilmiştir. Örneğin Kanun'un 321 inci maddesinde mesleki sırrın ifşası suçuna yer verilmiş, 321bis maddesinde ise, tıp ve sağlık alanında yapılacak bilimsel çalışmalar için kişisel verilerin ifşa edilebileceğine ilişkin bir istisna getirilmiş, ancak bu istisnanın uygulanabilmesi de uzmanlardan oluşan bir heyetin bu ifşaya izin vermesi, ifşa edilecek olan kişisel verinin veri öznesi ile arasındaki bağın kesilerek anonim hale getirilmesi ve veri öznesinin böyle bir durumda hakları konusunda bilgilendirilmiş olması gibi şartlara bağlamıştır. 354 üncü maddede adli sicil bilgilerine ilişkin kişisel verilerin hangi usul ve esaslarla, kim tarafından işlenebilecekleri belirtilmiştir. Aynı maddede, kantonlar arasındaki işbirliğini, hangi kategorilerdeki verilerin kaydedilebileceğini ve ne kadar süre ile tutulabileceklerini, kaydedilmiş olan verilere hangi yetkili makamların erişebileceğini ve hangi kişisel verilerin yalnızca özel vakalarda ifşa edilebileceğini ve ilgili kişilerin toplanmış olan kişisel verileri yok etme, düzeltme veya arşivleme

---

[152] 21 Aralık 1937 tarihli İsviçre Ceza Kanunu, kanunun İngilizce metni için bkz. http://www.admin.ch/ch/e/rs/311_0/index.html, Fransızca metni için bkz. http://www.admin.ch/ch/f/rs/311_0/index.html, 07.07.2012.

[153] İsviçre Ceza Kanunu, m.179 vd.

gibi usule ilişkin haklarını Federal Konsey'in düzenleyeceği belirtilmiştir. Ayrıca 355a maddesinde, Federal Polis (The Federal Office of Police – Fedpol) ve Federal İstihbarat Servisi (Federal Intelligence Service – FIS) nin Avrupa Polis Teşkilatı'na (European Police Office – Europol) hassas nitelikte olanlar da dahil olmak üzere, kişisel verileri aktarabilecekleri düzenlenmiş, 355f ve 355g maddesinde ise Schengen Antlaşması'nı imzalamış ülkeler arasındaki kişisel veri aktarımına ilişkin esas ve usuller düzenlenmiştir.

(5) Verilerin Korunmasına İlişkin Federal Kanun (LDP)

İsviçre'de kişisel verilerin korunmasına ilişkin özel bir kanun çıkarılmasına ilişkin çalışmalar ise, Avrupa ile paralel olarak, 1971-1977 yılları arasında başlamış, bunun akabinde 1984 yılında kişisel verilerin korunmasına ilişkin ilk kanun tasarısı sunulmuş, ancak gelen yoğun eleştiriler üzerine tasarı askıda kalarak, 1988 yılının Mart ayında yeni bir kanun tasarısı teklif edilmiş, bu tasarı da 19 Haziran 1992 tarihinde kabul edilmiş[154] ve Verilerin Korunmasına İlişkin Federal Kanun (LDP) 1 Temmuz 1993'te yürürlüğe girmiştir[155]. Kanunun amacı, ilk maddede, kişilik haklarının ve kişisel verileri işlenen bireylerin temel haklarının korunması olarak ifade edilmiş, ikinci maddede ise, kanunun hem gerçek kişileri hem de tüzel kişileri kapsadığı belirtilmiştir. LPD'nin 5 inci maddesine göre, kişisel verileri işleyen kişi bu verilerin doğruluğundan emin olmalı ve toplandıkları veya işlendikleri amaçlar bakımından doğru olmayan veya eksik olan kişisel verilerin silinebilmeleri ve düzeltilebilmeleri için gerekli tüm önlemleri almalıdır.

6 ncı maddenin ilk fıkrasında, kişisel verilerin yurtdışına aktarılması için eşdeğer koruma şartı aranmış, bu tür bir korumanın bulunmaması nedeniyle veri öznesinin kişiliği ciddi bir tehlike altına giriyorsa aktarımın yapılamayacağı belirtilmiş, ancak 6 ncı maddenin ikinci fıkrasında eşdeğer koruma bulunmamasına rağmen aktarmanın yapılabileceği yedi istisna hali düzenlenmiştir. Bunlara göre;

---

[154] 19 Haziran 1992 tarihli Verilerin Korunmasına İlişkin Federal Kanun, Loi fédérale sur la protection des données (LPD), kanunun İngilizce metni için bkz. http://www.admin.ch/ch/e/rs/2/235.1.en.pdf, Fransızca metni için bkz. http://www.admin.ch/ch/f/rs/2/235.1.fr.pdf, 06.03.2012. Çalışmanın bundan sonrasında, bu kanun LPD olarak anılacaktır.

[155] İsviçre Federal Veri Koruma ve Danışma Komiseri (Federal Data Protection and Information Commissioner – FDPIC) resmi web sitesi, http://www.edoeb.admin.ch/org/00828/01335/index.html?lang=en, 06.03.2012.

özellikle sözleşmesel olmak üzere eşdeğer korumanın sağlanacağına dair yeterli güvenceler bulunması, ilgili kişinin rıza göstermiş olması, veri işlemesinin bir sözleşmenin uygulanması veya sona erdirilmesi ile doğrudan bağlantılı olması ve veri öznesinin sözleşmenin tarafı olması, üstün kamu yararı bulunması veya kanunen öngörülmüş bir hakkın tesis edilmesi, uygulanması veya icra edilmesi için aktarımın yapılmasının kaçınılmaz olması, aktarımın ilgili kişinin vücut bütünlüğünün veya hayatının korunması için gerekli olması, veri öznesinin kişisel veriyi herkes tarafından ulaşılabilir kılmış olması ve işlenmesine rıza göstermediğini açıkça beyan etmemiş olması, aktarımın aynı yönetim bünyesinde faaliyet gösteren tüzel kişiler ile şirketler arasında olması ve bu yönetimde ilgili kişilerin korunması için yeterli koruyucu hükümlerin bulunması hallerinde, eşdeğer koruma olmasa dahi yurtdışına aktarımın yapılabileceği kabul edilmiştir. Eşdeğer koruma prensibine getirilen bu geniş istisnalar haricinde, özellikle İsviçre'nin 1 Ocak 2008 tarihinde yapmış olduğu değişikliklerden sonra, LPD'deki düzenlemelerin 95/46/AT Sayılı Yönerge'de öngörülmüş olan düzenlemeye paralel olduğu görülmektedir[156].

İsviçre'de kişisel verilerin korunmasına ilişkin hükümler ihtiva eden bir diğer kanun ise, İdarenin Şeffaflığına İlişkin Federal Kanun'dur. Bu kanun ile toplumun gerektiğinde idarenin resmi evraklarına ulaşabilmesinin sağlanması, böylece şeffaflığın sağlanabilmesi amaçlanmaktadır. Bu kapsamda idarenin resmi belgelerinde bireylere ait kişisel verilerin bulunması halinde, bu belgelere erişim sağlanabilmesi için temel kural, kişisel verilerin anonim hale getirilmeleridir. Şayet kişisel veriler anonim hale getirilemiyorlarsa, kanun LDP'yi işaret etmiş, sorunun LDP'nin 19 uncu maddesine göre çözümleneceğini söylemiş, bunun hacrinde oluşabilecek diğer sorunlar açısından da kişisel verilerin korunmasına yönelik hükümler sevk etmiştir.

İsviçre'de kişisel veri hukukuna çok ciddi standartlar getiren İsviçre Federal Temyiz Mahkemesi, son olarak 8 Eylül 2010 tarihinde oldukça önemli bir karara

---

[156] **Rihm**, **Thomas**, "New International Data Transfer Rules for Switzerland: Business Friendly by Respecting Employees' Privacy Rights", Employment & Industrial Relations Law, Vol. 18, No.2, s. 16, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(THOMAS+RIHM)&db=EMPIRL&rlt=CLID_QRYRLT2593415432155&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB2779545422155&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 06.03.2012.

imza atmıştır. Mahkeme bu kararda, İsviçreli bir servis sağlayıcı olan Logistep AG'nin, "Peer to peer" olarak adlandırılan paylaşım sitelerinde, eser sahiplerinin haklarını ihlal ederek, telif hakkıyla korunan eserleri paylaşan kişilerin IP adreslerinin ve hassas kişisel veri kategorisinde yer almayan diğer kişisel verilerinin toplanmasını sağlayan bir program ile toplayarak bu kişisel verileri telif hakkı sahiplerine satmasını LPD'nin dördüncü maddesindeki şeffaflık kuralına ve dolayısıyla hukuka aykırı bulmuştur[157]. Telif haklarıyla korunan eserleri internetteki paylaşım sitelerinde paylaşan kişiler hakkında, IP adresleri temel alınarak cezai takibat başlatılmış, dosya kapsamında IP adreslerinin sahiplerinin isimlerinin de tespit edilerek dava dosyasına girmesi ile, davaya taraf olan telif hakkı sahipleri, daha sonra öğrendikleri isimlere karşı tazminat davaları açmışlardır. İsviçre Federal Temyiz Mahkemesi ise, toplanan kişisel verilerin, toplandıkları amaçlar dışında işlendiklerini ve kullanıldıklarını, telif hakkı sahiplerinin telif haklarını koruma hakkının ve servis sağlayıcının ticari faaliyete girişmedeki menfaatinin bireylerin kişisel verilerinin gizli veri işlemeye maruz bırakılmaması gerekliliğinden daha önemli olmadığını belirtmiştir[158]. Ancak alınmış olan bu karar, telif hakkı sahiplerinin haklarının yeterince dikkate alınmamış olması ve kamunun menfaatine olan fikri ve sınaî hakları koruyan kanunun uygulanmasının sağlanması ile özel yaşamın gizliliğinin çakışan menfaatler bakımından yeterince tartışılmaması ve IP adreslerinin kişisel veri olarak addedilip addedilemeyeceği hususunun üzerinde yeterince durulmaması sebebiyle eleştirilmiştir[159]. Nitekim Alman Yüksek Bölge Mahkemesi, 3 Kasım 2010 tarihli kararında, ilave bilgiler olmadan doğrudan ait olduklarının kişiye bağlanamadıkları, kişisel verilerin özelliğinin ise belirli ya da belirlenebilir bir kişiye ait olması olduğu gerekçesiyle, IP adreslerinin kişisel veri olarak kabul edilemeyeceklerini belirtmiştir[160].

c. Almanya

Bu başlıkta, Almanya'da kişisel verilerin korunmasını düzenleyen kanunlar incelenecektir. Bu kanunlar incelenmeden önce, Federal Almanya Cumhuriyeti

---

[157] http://www.globallawwatch.com/2011/06/analysis-swiss-federal-court-decisions-raise-threshold-for-justification-of-data-processing/, 08.03.2012.

[158] http://www.globallawwatch.com/2011/06/analysis-swiss-federal-court-decisions-raise-threshold-for-justification-of-data-processing/, 08.03.2012.

[159] http://www.dataprotection.ch/en/news.asp?action=select&newsNO=57298&id=6213, 08.03.2012

[160] http://www.dataprotection.ch/en/news.asp?action=select&newsNO=57298&id=6213, 08.03.2012.

Anayasası'na bakıldığında, Anayasa'da kişisel verilerin korunmasına ilişkin özel bir düzenlemenin yer almadığı, ancak 10 uncu maddede[161] posta haberleşmesinin gizliliğinin korunduğu görülmektedir[162]. Ancak kişisel verilerin korunması hususu, Anayasanın "Yaşam hakkı, kişiliğin korunması, kişi özgürlüğü" başlıklı 2 nci maddesi kapsamında korunmaktadır[163]. Bu maddeye göre "(1) Herkes başkalarının haklarını ihlal etmemek, Anayasal düzene veya ahlak kurallarına aykırı düşmemek koşuluyla, kişiliğini serbestçe geliştirme hakkına sahiptir. (2) Herkes yaşam ve beden bütünlüğünün korunma hakkına sahiptir. Kişi özgürlüğüne dokunulamaz. Bu haklar ancak bir yasaya dayanılarak sınırlandırılabilir." Bu maddede geçen "kişiliğini serbestçe geliştirme hakkı" kişisel verilerin korunmasını da kapsamaktadır. Nitekim Avrupa İnsan Hakları Mahkemesi'nin de, kararlarında, kişisel verilerin korunmasının bireylerin kendilerini ve kişiliklerini serbestçe geliştirme hakkına dayandığını belirttiği görülmektedir[164].

Almanya'da kişisel verileri koruyan üç temel kanun vardır. Bunlardan birincisi Alman Ceza Kanunu, ikincisi Alman Ceza Muhakemesi Kanunu, üçüncüsü ise özel bir kanun niteliğinde olan Alman Veri Koruma Kanunu'dur. Bu başlık altında bu kanunların kişisel veriler ile ilgili kısımları incelenecektir.

(1) Alman Ceza Kanunu (StGB)

Alman Ceza Kanunu'nda (StGB) kişisel verilere, Kanunu'nun Kişisel Yaşam ve Gizli Alanın İhlali başlıklı 15 inci Kısımda yer alan 201, 202a ve 205 Sayılı paragraflarında yer verilmektedir[165]. Beyanın (yapılan açıklamanın) Güvenilirliğini İhlal başlıklı 201 inci paragrafın ilk fıkrasında, başkasının aleni olmayan konuşmalarını izinsiz olarak kaydeden veya kullanan veyahut kaydederek üçüncü

---

[161] Federal Almanya Cumhuriyeti Anayasası'nın "Mektup, posta ve telekomünikasyon gizliliği" başlıklı 10 uncu maddesi şu şekilde düzenlenmiştir: "*(1) Mektup ile posta haberleşmelerinin gizliliğine dokunulamaz. (2) Bu haklar ancak bir yasaya dayandırılarak sınırlandırılabilir. Bu hakların sınırlandırılması özgürlükçü demokratik temel düzeni veya Federasyon veya bir eyaletin varlık ve güvenliğini koruma amacını güttüğü takdirde, yasada sınırlamaların ilgiliye bildirilmemesi ve denetimin hukuk yolu yerine parlemento tarafından tayin edilen organ ve yardımcı organlarca yerine getirebileceğini belirtebilir.*" Anayasanın tam metninin Türkçesi için bkz. http://www.scribd.com/hsencan/d/51218711-Alman-Anayasas%C4%B1, 12.05.2012.

[162] **Akıllıoğlu**, s. 15.

[163] **Küzeci**, s. 261-263.

[164] **P.G. ve J.H. v. İngiltere**, prg. 56.

[165] **Ünver**, **Yener**, "Kişisel Verilerin Korunması", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2008/1, s. 175.

kişilerin kullanımına sunan kişilerin 3 yıla kadar hapis veya para cezası ile cezalandırılmaları öngörülmüştür. İkinci fıkrada ise, kendisine hitaben söylenmemiş ve aleni olmadığını bildiği açıklamaları dinleme cihazı ile dinleyen veya ilk fıkranın ilk bendi uyarınca kaydedilmiş aleni olmayan beyanların (açıklamaları) tamamını veya temel içeriğini aleni olarak ifşa eden veya ikinci bendi uyarınca kaydederek üçüncü kişilerin kullanımına sunulan beyanları dinleyen kişiler hakkında ilk fıkradaki cezaya hükmolunur. Kişilerin 2 inci bendin 1. cümlesi uyarınca cezalandırılabilmeleri için alenen yapılan ifşanın başkasının haklı yararlarını ihlal etmeye elverişli olması gerekmektedir. Şayet yapılan aleni ifşa üstün kamu yararını korumak için yapılmışsa eylem hukuka aykırı değildir. Üçüncü fıkrada nitelikli bir hal öngörülmüş, 1 inci ve 2 nci fıkradaki suçları bir kamu görevlisinin veya kamu hizmeti açısından özel olarak yükümlü kılınmış bir kişinin işlemesi halinde cezanın 5 yıla kadar hapis veya para cezası olacağı belirtilmiştir. Dördüncü fıkraya göre, suça teşebbüs de cezalandırılmaktadır ve beşinci fıkrada suçun işlenmesinde kullanılan kayıt ve dinleme cihazlarının müsadere edilebileceği ifade edilmiştir[166].

Alman Ceza Kanunu'nun verilerin gözetlenmesi başlıklı 202a paragrafının ilk fıkrasında, izinsiz olarak, aleni olmayan veya izinsiz erişime karşı özel olarak korunan verileri kendisi veya başkası için ele geçiren kişi üç yıla kadar hapis veya para cezasıyla cezalandırılır. İkinci fıkrada ise, ilk fıkra kapsamına giren kişisel verilerin yalnızca elektronik veya manyetik olarak transfer edilenler veya diğer doğrudan toplanamayan şekillerde depolanan veriler oldukları belirtilmiştir.

Son olarak Kanun'un 205 inci paragrafının ilk fıkrasında 201 ve 202 nci paragraflarda tanımlanan suçların şikayete bağlı oldukları belirtilmiş, mağdurun ölmesi halinde kanunun 77 nci paragrafının ikinci fıkrasında tanımlanan akrabaların da şikayet hakkının doğacağı, ancak bunun 202a paragrafında tanımlanan suç için geçerli olmadığı öngörülmüştür.

---

[166] 13 Kasım 1998 tarihli Alman Ceza Kanunu, (Strafgesetzbuch, StGB), Federal Law Gazette [Bundesgesetzblatt] Part I p. 945, p. 3322, Kanunun İngilizce tam metni için bkz. http://www.iuscomp.org/gla/statutes/StGB.htm, 11.05.2012.

(2) Alman Ceza Muhakemesi Kanunu (StPO)

Almanya'da kişisel veriler ayrıca Alman Ceza Muhakemesi Kanunu[167] (StPO) ile de korunmaktadırlar. Örneğin § 81a StPO da, şüphelinin muayenesinin istenebileceği, bunun neticesinde elde edilen kan tahlilleri veya vücuttan alınan diğer hücrelerin yalnızca bunların toplanmasını gerektiren ceza yargılaması veya bununla bağlantılı diğer ceza yargılamaları için kullanılabilecekleri, toplandıkları amaç için gerekli olmadıkları anda da mümkün olan en kısa sürede yok edilmeleri gerektiği belirtilmiştir[168].

§ 81g StPO'da ise, ağır cezayı gerektiren bir suç işleyen veya cinsel dokunulmazlığa karşı suçlardan birini işlediği iddia edilen sanıktan hücre dokusu alınmak suretiyle genetik inceleme yapılarak DNA-Kimlik Tespiti yapılabileceği; alınan hücre dokusunun yalnızca bu amaçla kullanılabileceği ve amacına hizmet ettikten sonra gecikmeksizin yok edilmeleri belirtilmiştir. İlgili kişinin rızasının bulunmaması halinde, hücre dokusu alınması kararı hakim tarafından, acil durumlarda ise savcılık veya soruşturmayı yürüten savcılık görevlileri tarafından verilebilirken, DNA-Kimlik Tespiti kararı yalnızca hakim tarafından verilebilmektedir. Rızası alınmış ilgili kişiler ise, toplanan bu verinin ne amaçla kullanılacağı hususunda bilgilendirilmelidirler. Maddenin beşinci fıkrasında, toplanan kişisel verilerin, Federal Kriminal Dairesi'nde (Bundeskriminalamt) bulunan veri bankasında saklanabilecekleri ve Federal Kriminal Dairesi Kanunu'nda belirtilen şekilde kullanılabilecekleri öngörülmüştür. Aynı fıkraya göre, bu veriler ancak cezai yargılamalar, tehdidin önlenmesi veya uluslararası hukuki dayanışma amaçlarıyla transfer edilebilecektir[169].

---

[167] 7 Nisan 1987 tarihli Alman Ceza Muhakemesi Kanunu, (Strafprozeßordnung, StPO), Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, p. 1319, Kanunun Almanca tam metni için bkz. http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, İngilizce tam metni için bkz. http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html, 11.05.2012.

[168] **Wolters**, **Gereon**, "Alman Ceza Usul Hukuku'nda Bedensel Muayene ve DNA Analizi", Ar.Gör. Fatih Gündoğdu (çev.), Fasikül Dergisi, Sayı 7, Haziran 2010, s. 38.

[169] Alman Ceza Muhakemesi Kanunu'nun ilgili maddeleri olan § 81a-§ 81g hakkında ayrıntılı bilgi için bkz. **Wolters**, s. 37-41.

(3) Alman Veri Koruma Kanunu

Almanya'da çıkarılan kişisel verilerin korunmasına ilişkin kanun, 95/46AT Sayılı Yönerge'nin esin kaynağı olmuş, ancak Fransa gibi, Almanya'nın da, veri koruma hukukunu Avrupa Birliği standartlarına taşıması oldukça uzun sürmüştür[170]. Kişisel verilerin korunmasına ilişkin ilk veri koruma kanunu 1977 yılında Federal Veri Koruma Kanunu[171] adıyla çıkarılmış, ancak 1998 tarihinde yeni bir kanunun yapılmasıyla bu kanun mülga olmuştur. Avrupa Birliği'nin vermiş olduğu süre 1998 tarihinde sona ermesine rağmen, 1998 tarihli Alman Veri Koruma Kanunu 2002 yılında yapılan değişikliklerle Avrupa Birliği standartlarına tam uyum sağlayan kanun haline getirilmiştir[172]. Federal Alman Veri Koruma Kanunu'nun (BDSG)[173] uygulanması Alman Federal Veri Koruma Komiseri tarafından sağlanmaktadır[174]. Kanun, Federal kamu kuruluşları ve özel kuruluşlar açısından uygulanmakta olup, online işlemler için Alman Telemedia Kanunu[175] uygulanmaktadır.

Alman Veri Koruma Kanunu, kişisel verilerin toplanabilmesi için genel kuralları belirlemekte ve kişisel verilerin hangi şartlarda, kimden veya nereden alınabileceklerini öngörmektedir. Kanuna göre, temel kural kişisel verilerin veri öznesinden ve veri öznesinin izniyle toplanması olup; kanunun 4 üncü paragrafı ile kanun tarafından öngörülmesi veya kanun tarafından izin verilmesi durumunda, verinin veri öznesinden toplanmasının orantısız çaba gerektirmesi durumunda veya ticari amaçlar veya idari görevlerin verinin başka kimseler veya kuruluşlardan toplanmasını gerektirdiği durumlarda, bu kurala istisna getirilmiştir. Kanunun 5 inci paragrafında da, veri öznesinin kendisi hakkında toplanan kişisel veriler, bu verilerin kim tarafından ne amaçla tutulacağı, işlenip işlenmeyeceği, kullanılıp

---

[170] **Hook-Martin-Ivanova**, s. 130.

[171] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz, BDSG), kanunun İngilizce tam metni için bkz. http://www.iuscomp.org/gla/statutes/BDSG.htm, 12.05.2012.

[172] **Hook-Martin-Ivanova**, s. 130.

[173] 20 Aralık 1990 tarihli Bundesdatenschutzgesetz, BDSG, (Federal Veri Koruma Kanunu), 14 Ocak 2003 tarihinde yeni bir metne kavuşturulmuş, (Federal Law Gazette I, 66), 14 Ağustos 2009 tarihli Kanun'un (Federal gazete I, p.2814) 1 inci maddesi ile değişikliğe uğramış, son hali 1 Eylül 2009'da yürürlüğe girmiştir. Kanunun İngilizce tam metni için bkz. http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile, Kanunun Almanca tam metni için bkz. http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf, 11.05.2012.

[174] **Hook-Martin-Ivanova**, s. 130.

[175] 26 Şubat 2007 tarihli Kanun (Federal Gazette I, p.176), kanunun İngilizce tam metni için bkz. http://www.cgerli.org/fileadmin/user_upload/interne_Dokumente/Legislation/Telemedia_Act__TMA_.pdf, 11.05.2012.

kullanılmayacağı hususunda bilgilendirilmesi gerektiği ve veri öznesinin izninin yazılı olarak alınması gerektiği belirtilmiştir. Nitekim Alman Anayasa Mahkemesi de, 1983 yılında vermiş olduğu bir kararda kişilerin kendileri hakkında toplanan verilerden haberdar olmalarının önemini vurgulamıştır[176]. Kanunun 4b paragrafında, yurtdışına veri transferi hususu düzenlenmiş olup, maddede, yurtdışına veri aktarılabilmesi için eşdeğer koruma şartının arandığı ve bu şartın aktarımın her safhasında bulunması gerektiği vurgulanmıştır.

Kanunun 20 inci paragrafı, kişisel verilerin düzeltilmesi, silinmesi ve bloklanması[177] hususunu düzenlemiştir. Buna göre, yanlış kişisel veriler düzeltilmeli, veri işleme sistemleriyle işlenen veya veri işleme sistemleri dışındaki yöntemlerle kaydedilen kişisel veriler, hukuka aykırı olarak kaydedilmişse veya denetçinin artık verileri topladığı için amaç için bu verilere ihtiyacı kalmamışsa veriler silinmelidir. Bunun dışında, kişisel verilerin hangi şartlarda bloklanmaları gerektiği de belirtilmiştir.

Alman veri koruma hukukunda, meşru amaç için olsa da, mümkün olduğunca az kişisel verinin toplanması ve işlenmesi ve kişisel verinin en kısa sürede anonim hale getirilmesi esası geçerlidir[178]. Kişisel verinin anonim hale getirilmesi, Alman Veri Koruma Kanunu'nun 3 üncü paragrafının altıncı fıkrasında tanımlanmış, buna göre, verinin anonimleştirilmesi, verinin tanımlı ya da tanımlanabilen herhangi bir

---

[176] Alman Anayasa Mahkemesi, 65 BverfGE 15 Kasım 1983 tarihli kararında bu hususu şu şekilde değerlendirmiştir: "*Eğer bir kimse kendisi hakkında belirli alanlarda hangi enformasyonun toplumsal çevresinde bilindiğini yeterli kesinlikte öngöremiyorsa ve iletilme ihtimali olan tarafları yeterince tahmin edemiyorsa, herhangi bir baskı ya da etki altında kalmadan hür bir şekilde planlama ya da karar verme hürriyetinden alıkonulmuş demektir. Enformasyona ilişkin self-determinasyon hakkı, vatandaşların bundan sonra kendileri hakkında kimlerin ne zaman ve hangi nedenle ne bildiklerini bilemeyecekleri bir duruma olanak veren toplumsal ve yasal düzeni engeller. Eğer bir kişinin ayrıksı davranışlarının sistemli bir şekilde enformasyon olarak saklanıyor, bu husus uygulanıyor ya da intikal ettiriliyor yönünde şüphesi varsa, o kişiyi bu tür bir davranışla ilgiyi üzerine çekmemeye gayret edecektir. Sivil girişime ya da toplantıya katılımın kaydedildiği ve bu yüzden kişisel bir risk oluşabileceği gözüyle bakıyorsa, muhtemel olarak bu haklarının kullanımından vazgeçecektir. Bu durum sadece kendi gelişmesine zarar vermeyecek aynı zamanda toplumun menfaatlerine de zarar verecektir. Çünkü self-determinasyon vatandaşlarının hareket ve katılımına dayalı olan özgür demokratik toplumun temel işlevsel koşuludur.*", aktaran; **Ketizmen**, s. 199.

[177] Bloklama, Kanun'un 4 üncü maddesinde verilerin kullanılamaz ve işlenemez hale getirilmesi olarak tanımlanmıştır.

[178] **Walden**, **Ian**, "Anonymising Personal Data", International Journal of Law and Information Technology, Summer 2002, s. 224-237, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=%22ANONYMISING+PERSONAL+DATA%22&db=INTJLIT&rlt=CLID_QRYRLT865515374145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB7284547364145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 28.02.2012.

kişiye atfedilebilmesinin orantısız bir gider, zaman ve çaba gerektirecek hale getirilmesidir. Nitekim Avrupa Konseyi, bir tavsiye kararında, kişisel verinin anonimleştirilmesinin, verinin tanımlı veya tanımlanabilir bir kişiye bağlanmasının makul olmayan bir zaman, gider ve çaba gerektirmesi olduğunu belirtmiştir[179]. Bunun yanı sıra, Kanun'un 30 uncu paragrafında, pazarlama veya kamuoyu araştırması sebebiyle toplanan kişisel verilerin ancak bu amaçlarla kullanılıp işlenebileceklerini, farklı amaçlarla kullanılıp işlenmelerinin ise yalnızca veriler anonimleştirildikten sonra mümkün olduğunu, ayrıca, kişisel verilerin toplandıkları araştırma projesinin amacı imkan tanıdığı anda anonimleştirilmeleri gerektiğini belirtmiştir. 32 nci paragrafta ise iş başvurusu amacıyla toplanan veya işverenlerin çalıştırdıkları kimselerle ilgili olarak topladıkları kişisel verilerin toplanma, işlenme ve kullanılma esasları belirlenmiştir.

43 üncü paragraf, idari para cezasını gerektiren eylemleri düzenlemiştir. Paragraf, 4 fıkradan oluşmakta olup, ilk fıkra 11, ikinci fıkra ise 6 bent içermektedir ve fiillerin hem kasten hem de taksirle işlenmeleri hali düzenlenmiş, bunlar için farklı para cezaları öngörülmüştür. İlk fıkrada, kasten veya taksirle; yapılması gereken bildirimin belirlenen sürede yapılmaması veya tüm bilginin sağlanmaması, belirlenen sürede veya şekilde resmi bir veri koruması yapılmaması, transfer edilen verinin tespit edilip kontrol edilmemesi, veri öznesinin hiç veya doğru veyahut gerektiği gibi bilgilendirilmemesi, kişisel verilerin hukuka aykırı olarak transfer edilmesi veya kullanılması, kişisel verilerin elektronik veya baskılmış adres-telefon numarası-branşlar-veya bunlara benzer şeylerin kaydedilmesi, bilginin yanlış aktarılması veyahut hiç aktarılmaması veya gerektiği gibi aktarılmaması veya bir önleme kullanılmaması ve icra edilebilir bir düzenlemeye aykırı davranılması idari cezasını gerektiren fiiller olarak düzenlenmişlerdir[180]. Bu fiiller için 50 000 Euro'ya kadar para cezası öngörülmüştür.

İkinci fıkrada ise, kasten veya taksirle, aleni olmayan kişisel verilerin izin alınmadan toplanması veya işlenmesi, aleni olmayan kişisel verilerin otomatiğe bağlanmış bir aracın hizmetine sunulması, aleni olmayan kişisel verilerin otomatik işleme sistemleri veya otomatik olmayan dosyalardan kişinin kendisi veya başkaları için izinsiz toplanması veya ele geçirilmesi, aleni olmayan kişisel verilerin yanlış

[179] **Walden**, s. 226
[180] **Ünver**, s. 181.

bilgi içermelerine rağmen transfer edilmeleri, kişisel verilerin transfer edildikleri amaçlar dışında kullanılması, 28 inci paragraf ihlal edilerek kişisel verilerin reklam, pazarlama veya kamuoyu araştırması için kullanılması veya işlenmesi, doğru bir şekilde, belirlenen sürede veya hiç bilgi verilmemesi veyahut eksik bilgi verilmesi idari para cezası gerektiren fiiller olarak tanımlanmıştır ve bunların işlenmesi halinde 250 000 Euro'ya kadar para cezası öngörülmüştür.

Kanun'un 44 üncü paragrafında ise teknik anlamda ceza hukukuna ilişkin hükümler düzenlenmiştir[181]. Paragrafın ilk fıkrasına göre, Kanun'un 43 üncü paragrafının ikinci fıkrasında belirlenen fiilleri ödeme karşılığında veya kendisine veyahut bir başkasına haksız çıkar sağlamak veya bir başkasına zarar vermek amacıyla kasten işleyen kişiler iki yıla kadar hapis veya adli para cezasına çarptırılırlar. İkinci fıkraya göre ise, bu tür fiillerin takibinin şikayete bağlı olduğu ve şikayetin veri öznesi tarafından Enformasyon Özgürlüğü ve Veri Koruması Federal Komisyonu'na[182] yapılacağı belirtilmiştir.

3. Anglo – Saxon Ülkelerde Kişisel Verilerin Korunması

a. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri, Avrupa Birliği kapsamına dahil olmadığından, kişisel verilerin korunmasına ilişkin Avrupa'da yaşanan gelişmelere dahil olamamış, kişisel verilerin korunması alanını biraz gecikmeli olarak düzenlemiştir. Özellikle Amerika Birleşik Devletleri'nde yazılı kanunlardan ziyade içtihat hukukuna dayanılması bu alandaki gecikmeyi kısmen de olsa açıklamaktadır. Dolayısıyla ABD'de özel hayatın gizliliği hakkını açık bir ifade ile koruyan kanunların bulunmaması, bu alanın ABD Anayasası'nda belirli bir madde ile doğrudan korunması yerine, böyle bir maddenin bulunmaması sebebiyle 1 inci, 4 üncü, 5 inci ve 14 üncü maddelerde dolaylı olarak korunmaya çalışılması, korumanın eksik kalmasına yol açmıştır[183]. Doktrinde, haklı olarak, ABD Anayasası'nın maddeleri ile

---

[181] **Ünver**, s. 181.
[182] Kurumun Almancası kanunda "Bundesbeauftragte für den Datenschutz" olarak geçmektedir.
[183] **Moshell, Ryan**, "…And Then There Was One: The Outlook For A Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection", Texas Tech Law Review, Vol. 37, Winter 2005, s. 373, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(MOS

doğrudan doğruya korunan bir hakkın özel hayatın gizliliğinin korunması hakkı ile çatışması halinde, özel hayatın gizliliği hakkının doğrudan doğruya Anayasal korumaya sahip olmamasının onu zayıf ve saldırıya açık hale getirdiği ifade edilmektedir[184]. Nitekim 1976 yılında ABD Temyiz Mahkemesi tarafından ele alınan ABD'ye karşı Miller davasında[185], Mahkeme, banka müşterilerinin bankalara vermiş oldukları kişisel verilerin idari makamlara aktarılmasının Anayasanın 4 üncü maddesinin koruması kapsamında kalmadığını ve müşterilerin bu bilgileri verdikleri zaman, ifşa edilmesi riskini kabul ettiklerini belirten bir karar almıştır.

ABD'de zamanla gelişen anlayışa göre, teknolojik gelişmelerin kişisel verileri daha kolay bulunur hale getirmesinin, bireylerin bu alanda kendi kişisel verileri ile ilgili olarak karar almalarını, böylece kişisel verilerin bireylerin sorumluluğunda olmasını sağlayacağı kabul edilmiştir. Böylece ABD hükümeti hususi düzenlemelerin daha iyi koruma getireceği esasını benimseyerek, merkezi olmayan, bölünmüş ve dar kapsamlı kanunlarla bu alanı düzenlemiştir[186].

Avrupa Birliği kişisel verilerin özel sektörde korunmasına ilişkin çeşitli düzenlemeler yaparken, ABD'de durum daha ziyade devletin kişisel verileri hukuka aykırı toplaması üzerinde durmuştur[187]. 1966 yılında çıkarılan Bilgi Edinme Özgürlüğü Kanunu[188] ile bireylere, hükümet nezdinde kendileri ile ilgili olarak toplanmış olan kişisel verilere ulaşabilmeleri hakkı tanınmış, takiben 1974 tarihli Özel Hayatın Gizliliği Kanunu[189] çıkarılarak, devletin bireylerle ilgili kişisel verileri toplamalarına sınırlama getirilmiştir[190]. Bu iki kanun birlikte değerlendirildiğinde, temel amacın kamu kuruluşları tarafından toplanmış olan kişisel verilerin devlet ve üçüncü şahıslar tarafından kötüye kullanılmasının engellenmesi olduğu

---

HELL)&db=TXTLR&rlt=CLID_QRYRLT18876875145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB496725055145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012., **Suda**, s. 231.

[184] **Suda**, s. 231.

[185] Kararın tam metni için, bkz. United States v. Miller, 425 U.S. 435 (1976), http://supreme.justia.com/cases/federal/us/425/435/case.html, 03.03.2012.

[186] **Moshell**, s. 375-376.

[187] Özellikle Vietnam Savaşı sırasında, ABD hükümetinin savaş karşıtı eylemcileri takip etmek amacıyla gizli takip yetkilerini (özellikle vergi, bankacılık ve telefon kayıtlarını takip) kötüye kullanması toplumda endişe yaratmıştır, **Suda**, s. 232.

[188] US Freedom of Information Act (FOIA), kanunun tam metni için bkz. http://uspolitics.about.com/library/bl_foia.htm, 03.03.2012.

[189] The Privacy Act of 1974, kanunun tam metni için bkz. http://www.justice.gov/opcl/privstat.htm, 03.03.2012.

[190] **Moshell**, s. 375-376, **Suda**, s. 232, **Murray**, s. 973.

görülmektedir, ancak ABD özel sektör için genel bir düzenleme yapmaktan kaçınarak, bu sektörde kişisel verilerin korunmasını rehber ilkelere ve hususi düzenlemelere bırakmıştır[191]. Her ne kadar ABD Temyiz Mahkemesi Reno v. Condon davasında kişisel verilerin özellikle özel sektörde üçüncü şahısları satılması hususunda önemli bir potansiyelin bulunduğunu vurgulamışsa da, daha sonraki senelerde de çıkarılan kanunlarla[192] özel sektörde kişisel verilerin üçüncü kişilere ifşa edilmesiyle ilgili olarak yer alan hükümler son derece sınırlı kalmış, özel sektörde kişisel verilerin korunmasına ilişkin genel anlamda bu hususu kapsayan bir kanun çıkarmak yerine bu hususta her sektör için ayrı ayrı kanunlar çıkarılmıştır[193].

Nihayet, Avrupa Birliği'nde kişisel verilerin korunmasına verilen önemin artması ve bu alanda çeşitli adımlar atılarak Rehber İlkeler ve sözleşmeler imzalanması, özellikle 95/46/AT Sayılı Yönerge'den sonra bu sözleşmeleri imzalayan ülkelerin de iç hukuklarında gerekli değişiklikleri yaparak ortak koruma hükümlerine uyum sağlamaları üzerine, kişisel verilerin eşdeğer koruma bulunmayan diğer ülkelere transfer edilmemeleri ile ilgili mevcut hükümler ABD'nin bu alanda daha koruyucu bir kanun çıkarması gereksinimini ortaya çıkarmıştır[194]. Sağladığı koruma Avrupa ülkelerindeki korumaya eşdeğer olmayan ABD'ye kişisel verilerin aktarılması ile ilgili tereddütler baş göstermiş, kişisel verilerin ABD'ye gönderilmemesi üzerine özel sektörde işletme maliyetleri artmaya başlamıştır[195]. Böylece 1999 yılında, müşterilerin finansal alandaki kişisel verilerinin korunması amacıyla federal düzeyde asgari koruma sağlayan ve ABD tarihinin özel hayatın gizliliğini koruyan en geniş federal kanunu olan Finansal Hizmetleri Modernleştirme

---

[191] **Moshell**, s. 377-378.

[192] Özel sektörde kişisel verilerin korunmasında belirli bir alanla sınırlı olmayan tek kanun olan Elektronik Haberleşmenin Gizliliği Kanunu (The Electronic Communications Act of 1986 – ECPA), motorlu araçlar departmanının yanı sıra diğer özel sektör departmanları açısından da uygulama alanı bulan Sürücünün Özel Hayatının Gizliliğinin Korunması Kanunu (Driver's Privacy Protection Act of 1994 – DPPA), Videolarda Özel Hayatın Gizliliğinin Korunması Kanunu (The Video Privacy Protection Act of 1988) ve 1984 tarihli Kablolu Komünikasyon Politikası Kanunu (The Cable Communications Policy Act) gibi, ayrıntılı bilgi için bkz. **Moshell**, s. 377-378, **Suda**, s. 234-235.

[193] **Moshell**, s. 377-378, **Suda**, s. 232-233, **Murray**, s. 977.

[194] **Loring**, **Tracie B.**, "An Analysis Of The Informational Privacy Protection Afforded By The European Union And The United States", Texas International Law Journal, Vol. 37, Spring 2002, s. 421 – 459, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(LORING)+%26+da(2002)&db=TXILJ&rlt=CLID_QRYRLT2779154574145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB1771456554145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012.

[195] **Loring**, s. 442.

Kanunu[196] çıkarılmıştır[197]. Bu kanun daha ziyade bankalar nezdinde bireylerin paylaşmış oldukları kişisel verilerinin korunmasına ve veri öznesinin rızası alınmaksızın üçüncü kişilere devredilememesi veya ifşa edilememesine ilişkin olup, müşterilerin izin vermiş oldukları bir işlemin gerçekleştirilebilmesi için zorunlu olan kişisel veri aktarımını bu kuralın istisnası olarak belirlemiştir[198].

95/46/AT Sayılı Yönerge'nin eşdeğer korumayı haiz olmayan ülkelere kişisel veri akışına izin verilmemesi neticesinde, ABD Ticaret Bakanlığı ve Avrupa Komisyonu tarafından "güvenli liman" anlamına gelen "Safe Harbor" Antlaşması hazırlanmış ve 2000 yılında Avrupa Birliği tarafından onaylanmıştır[199]. Yapılan antlaşmaya göre, ABD'deki özel sektörde yer alan şirketler, bu antlaşma ile belirlenen kurallara uygun olduklarına ilişkin kendilerini kaydettirmek için ABD Ticaret Bakanlığı'na gönüllü olarak başvurmakta, Bakanlık bu başvuruyu değerlendirmekte ve başvuran şirketin AB Direktifi kapsamında Safe Harbor Antlaşması ile getirilen şartlara uygun olup olmadığına karar vermektedir[200]. Safe Harbor'a katılmayı amaçlayan bir kuruluşun Safe Harbor Antlaşması'nda öngörülen yedi ilkenin tümünü uygulaması ve gizlilik politikasında Safe Harbor ilkelerine bağlı olduğunu alenen açıklaması gerekmektedir[201]. Şirketin uygun koşulları sağlaması halinde, 95/46/AT Sayılı Yönergesinin 25 inci maddesinde aranan kişisel verilerin üçüncü ülkelere aktarılması ile ilgili eşdeğer koruma şartı sağlanmış olmaktadır.

ABD'nin kişisel verilerin korunması ile ilgili olarak benimsediği sisteme genel olarak bakıldığında, kişisel verilerin kamu sektöründe korunmasını düzenleyen alanın, federal düzeyde, tek elden ve bütünü kapsayan kanunlarla düzenlendiği görülürken, özel sektör açısından bunun tam zıttı geçerli olup, özel sektördeki alanları ayrı ayrı düzenleyen kanunlar bulunmaktadır. Bu durum da, kişisel verilerin özel sektörde korunmasının tek elden değil, farklı kanunlarla ve belirli bir birlik sağlanamadan yürütülmeye çalışıldığını göstermektedir. Dolayısıyla, Avrupa Birliği'nin getirmiş olduğu düzenlemelere ve AB üyesi devletlerin bunu iç hukuklarında uygulamadaki azimlerine bakıldığında, ABD'deki kişisel verileri

---

[196] Financial Services Modernization Act, daha ziyade Gramm-Leach-Bliley Act (GLBA) adıyla bilinmektedir. Bkz. **Loring**, s. 442-448, **Moshell**, s. 378 vd.
[197] **Loring**, s. 442.
[198] **Moshell**, s. 378-381, **Loring**, s. 442-444.
[199] http://www.truste.com/pdf/EU_Data_Sheet.pdf, 03.03.2012.
[200] **Moshell**, s. 385-387.
[201] **Loring**, s. 452.

koruma hukukunun kamu sektöründe 95/46/AT Sayılı Yönergesinin üçüncü ülkelere aktarım için talep ettiği eşdeğer korumayı sağlayabildiği, ancak özel sektör için bunu söyleyebilmenin mümkün olmadığı görülmektedir. Ancak özel sektör açısından kişisel verilerin korunmasında kanunlar açısından bu denli dağınık ve belirsiz bir sistemin benimsenmiş olmasının getirdiği sorunlar, Safe Harbor Antlaşması ile önemli oranda bertaraf edilerek, bu Antlaşma'daki ilkeleri benimseyen ABD'deki özel sektör kuruluşlarının AB ülkeleri ile sorunsuz bir şekilde kişisel veri aktarımını gerçekleştirmelerine olanak tanınmıştır.

b. İngiltere

İngiltere'de, 1998 yılına kadar veri koruma hukukunda fazla ilerleme olmamış, o tarihe kadar 1984 tarihli Veri Koruma Kanunu uygulanmıştır. Bu kanunda da bireyler için, kendileri ile ilgili depolanan ve tutulan kişisel verilere erişme, yanlış verilerin düzeltilmesini ve silinmesini talep etme, kişisel verileri tutan kişinin bunları kötüye kullanması halinde tazminat talebinde bulunma gibi temel haklar öngörülmüş, ancak kişisel verileri esas olarak koruyan düzenleme 1998 yılında yapılmıştır[202]. 1998 tarihinde hazırlanan Veri Koruma Kanunu[203] 1 Mart 2000 tarihinde yürürlüğe girerek, Avrupa Birliği standartlarını da karşılayan bir düzenleme olarak mevzuatta yerini almıştır[204]. 1984 tarihli Kanun'da bulunmayıp, 1998 tarihli Kanun'a eklenen en önemli hususlardan biri, yeni Kanun'a ilave edilen 8 inci ilkeyle, eşdeğer koruma sağlanamadığı takdirde EEA[205] dışındaki ülkelere kişisel veri aktarımının yasaklanmış olmasıdır[206].

Veri Koruma Kanunu'nun ilk kısmında Kanun'da kullanılacak olan terimlerin tanımı yapılmış, hassas kişisel veriler kapsamına kişilerin ırk veya etnik kökenleri, siyasi görüşleri, dini veya benzer nitelikteki inanışları, sendikaya üye olup olmadığı, fiziksel veya ruhsal sağlık durumu, cinsel yaşamı ve adli sicil durumu hakkındaki verilerinin girdiği belirtilmiştir. Kanunun ikinci bölümünde yer alan 7 nci maddede ise, veri öznesinin hakları sayılmıştır ve diğer ülkelerdeki benzer kanunlarda olduğu

---

[202] **Grant**, **Hazel**, "Data Protection 1998 - 2008", Computer Law & Security Review, Vol. 25, Issue 1, 2009, http://www.sciencedirect.com/science/article/pii/S0267364908001696 s. 44 05.05.2012.
[203] Data Protection Act 1998, kanunun İngilizce tam metni için bkz. http://www.legislation.gov.uk/ukpga/1998/29/data.pdf, 13.05.2012.
[204] **Grant**, s. 44.
[205] EEA, Avrupa Birliği ülkeleri ve Norveç, İzlanda, Lihtenstein ülkelerini kapsar.
[206] **Grant**, s. 45.

gibi, kendisi hakkında tutulan kişisel verilere erişebilme, hangi amaçla tutuldukları veya işlendikleri hususunda bilgilendirilme, üçüncü taraflara ifşa edilip edilmeyecekleri, edileceklerse hangi amaçla edilecekleri hususlarında veri denetçisi tarafından bilgilendirilme gibi hakların sayıldığı görülmektedir. Maddede kişilerin bilgilendirilmeleri için bazı durumlarda veri denetçisinin makul bir ücret talep edebileceği ve bilgilendirilmek için yapılan başvurunun yazılı olması gerektiği belirtilmiştir.

Veri Koruma Kanunu'nun uygulanmasını sağlama görevi Veri Koruma Komiseri'ne (Data Protection Commissioner) verilmiştir. Buna göre veri işleyen sivil kuruluşların, veriyi işlemeden önce Enformasyon Komiserine (Information Commissioner) bilgi vermeleri gerekmektedir. Verilmesi gereken bilginin kapsamına, veri denetçisinin ismi ve adresi, şirket tarafından tayin edilen veri hukuku temsilcinin ismi ve adresi, ne tür kişisel verilerin işleneceği ve veri öznelerinin bundan nasıl etkilenecekleri, verinin hangi sebeple işleneceği, verilerin potansiyel alıcıları, verilerin hangi AB üyesi olmayan ülkelere doğrudan veya dolaylı olarak transfer edilme ihtimalinin bulunduğu girmektedir[207].

2007 senesine gelindiğinde, kişisel verilerle ilgili tartışmalar ve gelişen teknoloji ile birlikte yapılan ihlaller de önemli oranda artmıştır. Nitekim Enformasyon Komiseri Richard Thomas, 2007 yılında yaptığı açıklamada; "2007 senesi boyunca açıkçası korkunç bir ihlal listesi" olduğunu ifade etmiştir[208]. Şubat 2007'de Adalet Bakanlığı, mahkemelere, kişisel verilerin korunması hukukunu ihlal edenlerin cezalandırılmasında, bu tür suçları işleyenlere hapis cezası verilmesinde takdir yetkisi dahil olmak üzere, daha geniş yetkiler verileceğini açıklamıştır[209]. Nitekim Şubat 2007'de, İngiltere finansal hizmetler düzenleyicisi olan Finansal Hizmetler Yetkilisi (Financial Services Authority), Nationwide Building şirketine, şirketin çalışanının bilgisayarının çalınmasından sonra, söz konusu bilgisayarda onbir milyon müşterinin kişisel verileri olduğu ve şirketin bu verilerin korunmasında gerekli dikkat ve özeni göstermediği gerekçesiyle 980.000 £ değerinde bir ceza kesmiştir[210]. Benzer şekilde Eylül 2008'de ise, Enformasyon Komiseri Ofisi[211]

[207] **Hook-Martin-Ivanova**, s. 130.
[208] **Grant**, s. 47.
[209] **Hook-Martin-Ivanova**, s. 130.
[210] **Hook-Martin-Ivanova**, s. 131, **Grant**, s. 47.

Virgin Media Ltd şirketinin, 3000 müşterinin kişisel verilerinin kayıtlı olduğu bir CD yi kaybederek ihlal yaptığını tespit etmiştir. Bu tür ihlallerin önlenmesi amacıyla, Veri Koruma Kanunu'nda, şirketlerin ve tüm kuruluşların çalışanlarını, kişisel verilere erişimleri konusunda güvenilir kılmak için makul önlemler alma yükümlülüğü getirilmiştir[212].

Kanun'un cezai hükümleri ise, 55 inci madde ve devamında düzenlenmiş, ancak burada yalnızca hangi fiillerin ihlal teşkil edeceği düzenlenmiş ve bu fiillerin işlenmesi halinde para cezası öngörülmüştür. Diğer pek çok ülkedekinin aksine, bu Kanun'da kişisel verilerin hukuka aykırı olarak ele geçirilmeleri, ifşa edilmeleri, transfer edilmeleri gibi eylemlere hapis cezası yaptırımı bağlanmamıştır. Bunun yanı sıra, kişisel verilerin kasten veya taksirle veri denetçisinin izni bulunmaksızın ele geçirilmesi veya ifşa edilmesi veya kişisel verinin içerdiği bilginin başkalarına tedarik edilmesi ihlal teşkil eden fiiller olarak sayılmış, ancak ikinci paragrafta buna çok geniş istisnalar getirilmiştir. Buna göre, ele geçirme, ifşa veya tedarik etme eylemlerinin bir suçun önlenmesi veya tespit edilmesi için veyahut kanun hükmü veya mahkeme emriyle yapılması, kişinin bu eylemleri yapmakta hukuken yetkili olduğu inancının makul olması, kişide veri denetçisinin bu eylemlerden haberi olsa idi bunlara izin vereceği inancının bulunması ve bu inancın makul olması ve bu eylemlerin kamu menfaatleri dolayısıyla yapılmış olması hallerinde, yapılan eylemler ihlal teşkil etmezler. Kanun'un çıktığı dönemde, 55 inci madde kapsamında bu ihlalleri yapan kişilere karşı, Enformasyon Komiseri Ofisi'nin doğrudan para cezası kesme yetkisi bulunmamakta idi. Ancak önemli bir gelişme olarak, 9 Mayıs 2008 tarihinde çıkarılan Ceza Adaleti ve Göç Kanunu'yla, Enformasyon Komiseri Ofisi'ne, Kanun'un 55 inci paragrafını ihlal edenlere para cezası uygulama yetkisi verilmiştir[213].

c. Kanada

Kanada, eyalet sistemi ile yönetilen bir ülke olması sebebiyle, ülkede kişisel verilerin toplanması, kullanılması ve ifşa edilmesi hususunu düzenleyen özel hayatın

---

[211] Information Commissioner Office – ICO, resmi sitesi için bkz. http://www.ico.gov.uk/, 09.05.2012.
[212] **Grant**, s. 48.
[213] **Hook-Martin-Ivanova**, s. 131.

gizliliği ve kişisel verilerin korunmasına ilişkin kanunlar çeşitlilik göstermektedir. Kanada'daki özel hayatın gizliliğine ilişkin kanunlar, genelde kanuni takibat aşamalarındaki ifşaatı kanunun öngördüğü sınırlamaların dışında tutmaktadır.

Kanada'nın çeşitli eyaletlerinde, mevcut hukuki sistemde oldukça geniş olan ifşaat yükümlülüğünün sınırlandırılmasını öngörme amacı güden değişimler devam etmektedir. Bu kapsamda, gizli bilgilerin korunmasına ilişkin kurallar içeren Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu (Personal Information Protection and Electronic Documents Act) gibi kanunlar da yürürlüğe girmiştir[214].

Kanada, devlet kurumları tarafından kişisel bilgilerin toplanması, tutulması, kullanılması ve bu bilgilere ulaşılmasını düzenleyen Özel Hayatın Gizliliği Kanunu'nu 1985 yılında çıkarmıştır ve bu kanun ile Gizlilik Komiseri (Privacy Commissioner) kurumu Kanada hukukuna girmiştir. İlerleyen dönemlerde ülkenin eyalet sistemi ile yönetilen Kanada'nın farklı bölgelerinde, telekomünikasyon şirketleri, sigortacılık hizmeti ve finansal hizmet sağlayan şirketleri hedef alan bölgesel kanunlar çıkarmıştır. Bu dönem süresince, Kanada'daki işletmeciler Avrupa Birliği'nin benimsemiş olduğu prensipleri temel alan 10 ilkelik bir örnek kanun (Model Code for Protection of Information) hazırlamış ve her ne kadar Kanada'da kanuni bir zemine oturtulmamış olsa da bu prensipleri uygulamışlardır. 2000 tarihinde çıkarılan Kişisel Bilgilerin Korunması ve Elektronik Belgeler Kanunu (Personal Information Protection and Electronic Documents Act) ile daha önce işletmeciler tarafından kabul edilmiş olan örnek kanundaki ilkeler kabul edilmiş ve kanunlaşmışlardır[215].

d. Yeni Zelanda

Kanada'ya benzer bir şekilde, Yeni Zelanda'da, kişisel bilgilerin toplanması, kullanılması ve tutulması ile ilgili olarak birtakım kriterler koyan 1993 tarihli "Özel

---

[214] **Sullivan**, **James M.**, "IADC International Law Committee Survey of Electronic Discovery and Data Privacy Law, Defense Counsel Journal, Vol. 77, No.3, July 2010, s. 396, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(SULLIVAN)&db=DEFCJ&rlt=CLID_QRYRLT9391719534145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB4617418514145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012.

[215] **Moshell**, s. 423.

Hayatın Gizliliğine İlişkin Kanun" yürürlüğe girmiştir. Resmi bilgilerin ifşa edilmesi ise 1982 tarihli "Resmi Bilgi Kanunu" (merkezi hükümet kuruluşları için) ve 1987 tarihli "Yerel İdare Resmi Bilgi ve Karşılama Kanunu" (yerel hükümet için) ile düzenlenmiştir[216].

Özel Hayatın Gizliliğine İlişkin Kanun, ölmüş kişiler ve tüzel kişiler haricindeki kimliği tanımlanabilir kişiler hakkındaki kişisel bilgiler hakkında uygulanmaktadır, ancak bu kanunda kastedilen "bilgi"nin ne anlama geldiği açıkça ifade edilmemiştir. Yeni Zelanda Yargıtay Mahkemesi, bu konu ile ilgili olan "Harder v. Proceedings Commissioner" kararında, kişisel bilgilerin korunması kavramının insan hakları ve sosyal menfaat kavramlarıyla orantılı bir şekilde değerlendirilmesi gerektiğini ifade etmiştir[217].

Yeni Zelanda'daki kişisel bilgiler açısından ilginç olan bir konu, Yeni Zelanda Mahkemesi tarafından "Commissioner of Police v. Ombudsman" davasında tartışılmış olan, bir kişinin zihnindeki bilgilerdir. Bu hukuk sistemine göre, kişisel bilgiler, kayıt altına alınmamış bir şekilde bir kişinin hafızasında bulunabilirler ve bu husus, bu tür bilgilerin soruşturma aşamasında veya Mahkeme önünde delil olarak sunulmaları durumunda önem arz edebilmektedir[218].

Özel Hayatın Gizliliğine İlişkin Kanun'da toplam on iki adet ilke bulunmakta olup; bunlardan en önemlileri 1, 10 ve 11. ilkelerdir. Birinci ilkeye göre, kişisel bilgiler, ancak mercilerin görev ve faaliyetlerine ilişkin hukuka uygun amaçlarla ve bilgiyi toplamanın belirlenmiş olan amaç için gerekli olduğu durumlarda toplanabilirler. Onuncu ilkede ise amaca bağlılık ilkesi düzenlenmiş olup; toplanmış olan kişisel bilgilerin toplandıkları amaç dışında başka bir amaç için kullanılamayacakları, bunun istisnasını ise kişisel bilgilerin sahibi olan kişinin bizzat izin vererek bilgileri kamuya açık hale getirmesinin oluşturduğu, bunun haricinde bu bilgilerin soruşturma ve kovuşturma işlemlerinin yürütülmesinde kullanılabilecekleri belirtilmiştir. 11. ilke, kişisel bilgilerin başka kişilere, mercilere veya kurum ve

[216] **Sullivan**, s. 397.
[217] **Sullivan**, s. 397.
[218] **Sullivan**, s. 397.

kuruluşlara ifşa edilemeyeceğini düzenlemiş olup, onuncu maddede öngörülmüş olan istisnaların bu madde açısından da geçerli olduğunu ifade etmiştir[219].

Özel Hayatın Gizliliğine İlişkin Kanun bireylere Yeni Zelanda Mahkemelerinde fiilen kullanılabilecek haklar vermemekle birlikte, bunun istisnasını 6. ilkeye göre kişilerin bilgilerini ellerinde tutan mercilerdeki bu bilgilere ulaşabilme hakları oluşturmaktadır. 6. ilke haricinde, diğer ilkeler için uygulanan sisteme göre, bir kişi kişisel verilerinin korunması hakkının bu ilkelerin aleyhine olacak şekilde ihlal edildiğini düşünüyorsa, kanuni olarak yetkili kılınmış olan Gizlilik Komiseri'ne (Privacy Commissioner) bu hususta şikayette bulunur ve bu komiser bir soruşturma başlatarak taraflar arasında uzlaşma sağlamaya çalışır. Şayet uzlaşma sağlanamazsa, takibat Şikayetleri Değerlendirme Mahkemesi'ne (Complaints Review Tribunal) taşınabilmekte olup, komiserin veya mahkemenin bireyin özel hayatının gizliliğinin ihlal edildiğine kanaat getirebilmesi için Özel Hayatın Gizliliğine İlişkin Kanun'un ihlal edilmiş olması ve aynı zamanda birey açısından bir zarar veya kaybın bulunması gerekmektedir. Bu zarar veya kaybın mutlaka maddi anlamda anlaşılması gerekmeyip; önemli bir aşağılama, kişinin onurunu yitirmesi veya duygularının yara alması da zarar kapsamında kabul edilmektedir[220].

C. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

Türkiye'de kişisel verilerin korunması hususunu düzenleyen pek çok kanun ve yönetmelik bulunmaktadır. Bu konuya ilişkin Türk Ceza Kanunu'ndaki düzenlemeler ayrı bir kısımda inceleneceğinden, bu başlık altında, bu diğer düzenlemelere incelenecektir. Her ne kadar Türk hukukundaki düzenlemelerin tamamına burada yer verilemeyecek olsa da, önemli gördüğümüz kanun ve yönetmelikler değerlendirilecektir.

Bu düzenlemelerin başında Türkiye Cumhuriyeti Anayasası gelmekte olup, ilk etapta Anayasa'nın kişisel verilerin korunması hususunu düzenleyen maddeleri incelenecek, daha sonra Medeni Kanun ve İş Kanunu gibi diğer temel kanunlara değinilecek, son olarak ise bu alanı düzenleyen ve kişisel verilerin korunmasına katkıda bulunan yönetmelikler incelenecektir.

---

[219] **Sullivan**, s. 398.
[220] **Sullivan**, s. 399.

1. 1982 tarihli Türkiye Cumhuriyeti Anayasasında Kişisel Verilerin Korunması

1982 tarihli Türkiye Cumhuriyeti Anayasası'nda, 12 Eylül 2010'da yapılan Anayasa referandumundan evvel, kişisel verilerin korunması hakkı ile ilgili özel bir düzenleme yer almamakta, ancak bu hakkın korunması Anayasa'da yer alan bazı diğer hükümler kapsamında kabul edilmekteydi. Böylece kişisel verilerin korunması ile ilgili olarak belirli bir madde olmasa da, bu koruma Anayasal temelden yoksun değildi.

Diğer ülkelere bakıldığında, kişisel verilerin tartışılmaya başlanmasından çok önce düzenlenmiş ve kabul edilmiş olan Anayasaları olan ülkelerde buna ilişkin özel bir hükmün yer almadığı, ancak Anayasalarında yer alan başka maddelerin kapsamında kişisel verelere Anayasal koruma sağlandığı görülmektedir. Örneğin Kanada'da kişisel verilerin korunması hususu Anayasal dayanığını özel yaşamın gizliliğine dayandırırken, Fransa'da özgürlük hakkına, Almanya'da ise genel kişilik hakkına dayanmaktadır. Anayasaları daha yakın dönemde düzenlenmiş olan Portekiz, Hollanda ve İspanya gibi ülkelerde ise, kişisel verilerin korunması hakkı Anayasada özel bir maddede düzenlenmiştir[221].

2010'da yapılan referandumdan önce, temel bir hak ve özgürlük olan kişisel verilerin korunması hakkının dayanağını bulduğu kabul edilen madde, temelini insan onurunda bulan "kişinin dokunulmazlığı, maddi ve manevi varlığı"nı düzenleyen 17 nci maddedir[222]. Türkiye Cumhuriyeti Anayasası'na göre, "Her Türk vatandaşının bu Anayasadaki temel hak ve hürriyetlerden eşitlik ve sosyal adalet gereklerince yararlanarak millî kültür, medeniyet ve hukuk düzeni içinde onurlu bir hayat sürdürme ve maddî ve manevî varlığını bu yönde geliştirme hak ve yetkisine doğuştan sahip"tir (Başlangıç, 6 Sayılı Paragraf). Bu itibarla "Herkes, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir" (md.17/f.1) ve "kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tabi tutulamaz" (md.17/f.3) ve Anayasa'nın 2 nci maddesine göre

[221] **Küzeci**, s. 261 - 263.
[222] **Küzeci**, s. 267, **Şimşek**, s. 128, **Tahmazoğlu Uzeltürk**, Sultan, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, Sayı 93, Eylül 2010, s. 3151.

"Türkiye Cumhuriyeti... insan haklarına saygılı... demokratik bir hukuk devletidir." Dolayısıyla, kişisel verilerle ilgili özel bir düzenleme getirilmeden önce, insan onuru ve genel kişilik hakkı (md.17/f.1) kişisel verilerin korunmasının Anayasal temellerini oluşturmakta idi.

Kişisel verilerin korunması açısından kısmi koruma sağlayan ve bu konuyla bağlantılı olan diğer temel hak ve özgürlüklerin de bulunduğu kabul edilmektedir. Bunlardan biri, uluslararası düzenlemelerle de garanti altına alınmış olan ve Anayasa'nın 20 nci maddesinde yer alan özel hayatın gizliliği hakkını düzenleyen maddedir. Bu maddeye göre, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." Referandum ile getirilen düzenlemeden önce, Anayasa Mahkemesi'nin bir kararında belirttiği gibi[223], özel hayatının gizliliği kapsamında, kişilerin özel hayat alanına rızaları dışında girilmesi ve kişisel verilerine ulaşılması Anayasa'nın bu maddesini ihlal etmekte idi[224].

Kişisel verilerin korunması ile ilgili kısmi bir garanti getiren hükümlerin içinde, Anayasa'nın din ve vicdan hürriyetini koruyan 24 üncü maddesi ile buna bağlı olarak temel hak ve hürriyetlerin kullanılmasının durdurulmasını düzenleyen maddede, savaş, seferberlik, sıkıyönetim veya olağanüstü hallerde dahi kimsenin din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamayacağı ve bunlardan dolayı suçlanamayacağını öngören 15 inci maddedesi de yer almaktadır. Nitekim kişilerin dini görüşleri hassas kişisel veriler kapsamında yer almakta olup, bunun Anayasa'da sayılan istisnai hallerde dahi korunacağı belirtilmiştir. Anayasa Mahkemesi, nüfus kütüğünde bireylerin dininin kişisel veri olarak kaydedilmesini düzenleyen 1587 Sayılı Mülga Nüfus Kanunu'nun 43 üncü maddesine ilişkin olarak verdiği kararda[225], maddenin iptalinin gerekmeyeceğini, zira bu madde ile "kişinin dini kanaatlerinin değil, bilakis kamu yararı, kamu düzeni ve sosyal gereksinimlerle ilgili olarak göz önünde bulundurulmak üzere dininin ne olduğunun açıklanmasının söz konusu

---

[223] 06.01.1999 T, 1996/68 E., 1991/1 K. Sayılı Anayasa Mahkemesi kararı, R.G.t. 19.01.2001, S. 24292, kararın tam metni için bkz. http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=1458&content=, 13.05.2012.

[224] **Şimşek**, s. 142.

[225] 21.06.1995 T., 1995/17 E., 1995/16 K. Sayılı Anayasa Mahkemesi Kararı, karar metni için bkz. http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=1199&content=, 10.05.2012.

olduğunu" ve "bu kuralın zorlayıcı bir niteliği ve zorlama ile bir ilişkisi bulunmadığını" belirtmiştir[226]. Her ne kadar bu karara konu olan Nüfus Kanunu ilga edilmiş olsa da, 5490 Sayılı Nüfus Hizmetleri Kanunu'nun 7 nci maddesinde benzer bir hüküm yer almakta, aile kütüğünde kişilerin dininin de yer alacağı düzenlenmektedir. Kanaatimizce Anayasa Mahkemesi'nin bu hususta verdiği karar son derece isabetsizdir, zira kütükte kişilerin dininin ne olduğuna ilişkin bilgi bulunması gerekmesi, kişilerin kendileriyle ilgili bu kişisel veriyi açıklamak zorunda oldukları anlamına gelmektedir ki bu, yukarıda bahsedilen maddeler çerçevesinde Anayasa'ya aykırıdır.

Kişisel verilerin korunması ile ilişkili olabilecek diğer maddeler ise, Anayasa'nın 26 ncı maddesinde düzenlenen "düşünceyi açıklama ve yayma hürriyeti" ve 22 nci maddede düzenlenen "haberleşme hürriyeti" dir[227].

2010 yılında yapılan referandumdan sonra, 5982 Sayılı kanunla[228], Anayasa'nın özel hayatın gizliliğini düzenleyen 20 nci maddesine bir fıkra eklenerek bireylerin kişisel verilerinin korunması açık bir şekilde Anayasal güvence altına alınmıştır. Yirminci maddenin son fıkrasına göre, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." Maddeye eklenen bu fıkra doktrinde, kişisel verilerin korunması hakkının hangi şartlarda sınırlandırılabileceği belirtilmediği[229] ve kişisel verilerin işlenmesi hususunu denetleyecek bağımsız bir organ öngörülmediği[230] için

---

[226] **Şimşek**, s. 138-139.
[227] Ayrıntılı bilgi için bkz. **Şimşek**, s. 145-153.
[228] Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, K.n. 5982; R.G.t. 13.05.2010, S. 27580, kanunun tamamı için bkz. http://www.memurlar.net/haber/166939/, 10.05.2012.
[229] **Küzeci**, s. 266, **Uzeltürk**, s. 3155, "… *hem AB temel haklar şartı hem de Avrupa Konseyi Sözleşmelerinde ifade edilen kişisel verilerin hangi amaçlarla tutulabileceği Anayasa ile belirlenmemiştir. Yani kişisel verilerin sınırlanması sebepleri Anayasada belirtilmemiş ve bu alan tamamen kanun koyucuya bırakılmıştır… Örneğin İnsan hakları Avrupa sözleşmesinin 8/2. Maddesine göre bu alan sadece milli güvenlik, kamu emniyeti, memleketin ekonomik refahı, düzenin korunması, suçların önlenmesi, sağlığın veya ahlakın ve başkalarının hak ve özgürlüklerinin korunması sebepleriyle sınırlanabilir. Getirilen Anayasa hükmünde ise bu sebepleri kanun koyucu bir Anayasal çerçeve olmadan kendisi belirleyebilecektir*."
[230] **Küzeci**, s. 266.

eleştirilmiştir. Gerçekten de, Anayasa'nın temel hak ve özgürlüklerin gerektiğinde sınırlandırılmasını öngören 13 üncü maddesine göre, "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." Bu itibarla, 20 nci maddenin son fıkrasında yer alan kişisel verilerin korunması hakkının aynı fıkrada her ne kadar kanunla sınırlandırılabileceği öngörülmüş olup bu husus 13 üncü maddeye uygun olsa da, aynı maddede kişisel verilerin korunması hakkı açısından "Anayasanın ilgili maddelerinde belirtilen sebepler" bulunmamaktadır. Böyle bir durumda, kişisel verilerin korunmasının sınırlandırılması, 20 nci maddede de belirtildiği üzere ancak kanunla sınırlandırılabilecek ve her ne kadar bu maddede özel sınırlama sebepleri öngörülmüş olmasa da, yapılacak sınırlamalar yine 13 üncü maddedeki şartlarla bağlı olacaktır; ki bu da " Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamama" esasına dayanmaktadır.

2. İlgili Kanun ve Yönetmeliklerde Kişisel Verilerin Korunması

a. Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu

Kişisel verilerin korunması kapsamında, Türk Ceza Kanunu[231], kişisel verilerin hukuka aykırı olarak kaydedilmelerini (m.135), hukuka aykırı olarak ele geçirilmelerini, verilmelerini veya yayılmalarını (m.136) ve kanunla yükümlü kılınmış kişilerin yok etmeleri gereken kişisel verileri yok etmemelerini (m.138) suç olarak düzenleyerek, bu fiillerin işlenmesini yaptırıma bağlamış ve bu fiillerin belirli kişiler tarafından işlenmeleri halinde cezanın artırılmasını gerektiren haller öngörmüştür (m.137). Ceza Muhakemesi Kanunu'nda ise, kişisel verilerin korunması açısından önem arz eden maddeler, beden muayenesi ve vücuttan örnek alınması ile bunların saklanması, moleküler genetik incelemeler ve fizik kimliğin tespiti konularını düzenleyen 75 inci madde ile 81 inci maddeler arasında yer almaktadır. Bu maddelere ek olarak "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135 inci maddede de, yapılan tespit ve kayıtların tutulmaları il yok edilmelerine

[231] Türk Ceza Kanunu, K.n. 5237; R.G.t. 12.10.2004, S. 25611.

ilişkin düzenlemeler yer aldığından, bu madde de kişisel verilerin korunması bakımından son derece önem arz etmektedir.

Türk Ceza Kanunu'nun kişisel verilerin korunmasına ilişkin hükümleri aşağıda ayrı bir bölümde ayrıntılı olarak işleneceğinden, bu başlık altında bu maddeler hususunda açıklama yapılmayacaktır. İlgili Ceza Muhakemesi Kanunu hükümleri hakkında da, Türk Ceza Kanunu hükümleri incelenirken gerekli açıklamalar yapıldığından, bu başlık altında bu maddelere ilişkin de ayrıntıya yer verilmeyecektir.

b. Medeni Kanun ve Borçlar Kanunu

Doktrinde, Medeni Kanun'un[232] kişisel verilerin korunması hususunda güvence sağlayan maddelerinin, kişilik hakkını genel anlamda koruyan 24 ve 25 inci maddeleri olduğu belirtilmektedir[233]. Bu kapsamda genel anlamda kişisel veriler, kişilerin adı, resmi, özel hayatı ve sırları da bu kapsamda kabul edilmektedir[234]. 24 üncü maddeye göre, "Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir." Bireylerin kişisel verileri, MK. m. 24'te koruma altına alınmış "kişilik hakkı" kapsamında bulunduğundan[235], kişisel verilerine karşı bir saldırıda bulunulan kişi, hakimden koruma talep edebilecektir. Ancak 24 üncü maddenin ikinci fıkrasında bu korumaya bir istisna getirilmiş, "Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırı" olduğu belirtilerek, hukuka aykırılığı ortadan kaldıran sebepler olarak ilgili kişinin rızası veya daha üstün nitelikte özel veya kamusal yarar bulunması ya da kanunun verdiği yetkinin kullanılması durumlarında kişisel verilerin Medeni Kanun'un koruması kapsamında kalmayacağı ifade edilmiştir.

---

[232] Türk Medeni Kanunu, K.n. 4721; R.G.t. 08.12.2001, S. 24607.
[233] **Küzeci**, s. 276, **Başalp**, **Nilgün**, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 101.
[234] Bu konuda ayrıntılı bilgi için bkz. **Oğuzman, Kemal-Seliçi, Özer-Oktay Özdemir**, Saibe, Kişiler Hukuku, 10. Baskı, İstanbul 2010, s. 143-161; **Helvacı, Serap**, Gerçek Kişiler, 4. Baskı, İstanbul 2012, s.115-131.
[235] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 101.

MK. m.25'te ise[236], "Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir" denilmek suretiyle, bireylerin kişilik haklarına karşı bir saldırı bulunması veya bulunma tehlikesinin baş göstermesi durumunda bireylere dava hakkı tanınmıştır[237]. Bu itibarla, kişisel verilerine karşı hukuka aykırı bir saldırıda bulunulan, bulunulması tehlikesi olan veya bulunulmuşsa olumsuz etkilerine maruz kalmaya devam eden kişinin, kişilik hakları saldırıya uğramış olacağından, bu kişi MK'nun 25 inci maddesinde düzenlenmiş olan dava hakkını kullanabilecektir. Doktrinde bizim de katıldığımız bir görüşe göre ise, mevcut teknolojik gelişmeler dikkate alındığında, gerçekleşme tehlikesi bulunan hukuka aykırı saldırının tespit edilmesi son derece güç olacağından, Medeni Kanun kişisel verilerin korunması açısından tek başına yeterli olmayacak, bu sebeple kişisel verilerin korunmasına ilişkin özel bir kanun ile bu konudaki temel ilkelerin belirlenmesi yerinde olacaktır[238].

Borçlar Kanunu'nun[239] 58 inci maddesine göre ise, "Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hakim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir" ve dolayısıyla kişisel verileri hukuka aykırı olarak saldırıya uğrayan kişinin bu madde kapsamında manevi tazminat talep etme hakkı doğacaktır.

---

[236] Medeni Kanun'un 25 inci maddesi şu şekilde düzenlenmişir: "*Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.*
Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.
Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekaletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.
Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.
Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir."
[237] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 102.
[238] **Küzeci**, s. 278.
[239] Borçlar Kanunu, K.n. 6098; R.G.t. 04.02.2011, S. 27836.

c. İş Kanunu

İş Kanunu'nun[240] 75 inci maddesinde, işçilerin kişisel verilerinin korunması açısından işverenlere bazı yükümlülükler getirilmiştir. Maddenin ilk fıkrasına göre, "İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır." Bu fıkra açısından, işverene, işçilerinin kişisel verilerini içerecek bir özlük dosyası tutma yükümlülüğü getirilmekte, dolayısıyla işçilerin bu dosya kapsamına alınan kişisel verileri işverenin bilgisi ve denetimi altında bulunmaktadır. Aynı maddenin ikinci fıkrasında ise, işverenin bu kişisel verileri hukuka aykırı olarak kullanmaması için bir yükümlülük getirilmiştir.

75 inci ikinci fıkrasına göre, "İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür." Bu fıkra işverene, kaydetmiş olduğu kişisel verileri hukuka uygun olarak kullanma yükümlülüğü getirmekte, ancak hukuka aykırı kullanım durumunda işverenin nasıl bir yaptırıma tabi tutulacağı belirtilmemektedir ve işverenin bu sorumluluğu pek tabii işçi-işveren ilişkisi sona erdikten sonra da devam edecektir. Benzer şekilde, kimi zaman işe alım aşamasında, iş için başvuran kimseler özgeçmişlerini ve dolayısıyla kişisel verilerini işverene veya işverenin işe alım konusunda yetkilendirdiği kişiye ulaştırmaktadırlar. Bu noktada, kanaatimizce işe alınmayan kişiler açısından, kişisel veriler, bu kişilerin işe alınmayacaklarının kesinleşmesinden itibaren en kısa sürede yok edilmeli ve bu bilgiler de üçüncü kişilerle paylaşılmamalıdır[241]. Aksi halde Türk Ceza Kanunu'nun ilgili hükümlerinde düzenlenen suçların işlenmesi gündeme gelecektir.

İş Kanunu'nun 107 nci maddesinde işverenlerin yükümlülüklerine uymamaları halinde haklarında idari para cezası yaptırımı uygulanacağı belirtilmiş, ancak 75 inci madde bu hükümde yer almamıştır. Doktrinde bu durumda, 75 inci maddedeki yükümlülüklerine uymayan işveren hakkında da idari para cezası uygulanması

[240] İş Kanunu, K.n. 4857; R.G.t. 10.06.2003, S. 25134.
[241] Aynı yönde, bkz. **Küzeci**, s. 280.

gündeme gelebileceği belirtilmiştir[242]. Kanaatimizce işverenin işçilerine ait kişisel verileri hukuka aykırı olarak ifşa etmesi halinde zaten Türk Ceza Kanunu'nun 136 ncı maddesi uyarınca sorumlu olacak ve cezalandırılacaktır.

d. Bankacılık Kanunu ve Banka Kartları ve Kredi Kartları Kanunu

Kişisel verilerin korunması konusunu düzenleyen kanunlardan biri de 5411 Sayılı Bankacılık Kanunu'dur[243]. Bu kanunun 73 üncü maddesine göre kurul başkan ve üyeleri ile kurum personeli, fon kurulu başkan ve üyeleri ile fon personeli, bankaların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlilerinin sıfat ve görevleri dolayısıyla öğrendikleri müşteri sırlarını açıklayamazlar, kendileri veya başkaları yararına kullanamazlar[244]. Hükmün önemli bir özelliği ise, bu yükümlülüğün maddede sayılan kişiler açısından görevden ayrıldıktan sonra da devam edecek olmasıdır.

5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu'nda[245] da kişisel verilerin korunmasına ilişkin bir düzenleme getirilmiştir. Kanunun 23 üncü maddesinin ilk

---

[242] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 107.

[243] Bankacılık Kanunu, K.n. 5411; R.G.t. 01.11.2005, S. 25983.

[244] Bankacılık Kanunu'nun 73 üncü maddesine göre; "*Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tabidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.*

Bu Kanun hükümleri uyarınca Kurumun, yurt dışındaki muadili denetim mercileri ile düzenleyeceği mutabakat zabıtları çerçevesinde vereceği bilgi ve belgeler birinci fıkradaki sır kapsamında değildir. Kurul düzenleyeceği mutabakat zabıtları veya zabıtlar dışında elde edeceği sırların korunmasını sağlamakla görevlidir. Kurumun elde edeceği sır niteliğindeki bilgi ve belgeler, kuruluş ve faaliyet izni verilmesinde, faaliyetlerin denetiminde, düzenlemelere uyulup uyulmadığının izlenmesinde ve Kurul kararlarına karşı açılacak idarî davaların görülmesinde kullanılabilir. Kurumun bu fıkra kapsamında elde edeceği sır niteliğindeki bilgi ve belgeler hiçbir kişi, kurum ve kuruluşa verilemez. Mahkeme kararına bağlanmış sır kapsamına giren bilgilerin verilmesinden Kurum sorumlu tutulamaz.

Bankaların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri bankalara veya müşterilerine ait sırları, bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bankaların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.

Kredi kuruluşları ve finansal kuruluşların destek hizmeti kuruluşları ile aralarında akdedecekleri yazılı sözleşmeler çerçevesinde bu kuruluşların müşterilerinin risk durumlarının izlenmesi, değerlendirilmesi, kontrolü ve müşteri hizmetlerinin yerine getirilmesi nedeniyle yapılacak bilgi ve belge alışverişi ile hizmet temini ve ayrıca kredi kuruluşları ve finansal kuruluşların kendi aralarında doğrudan doğruya veya en az beş banka tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi bu hükmün dışındadır."

[245] Banka Kartları ve Kredi Kartları Kanunu, K.n. 5464; R.G.t. 01.03.2006, S. 26095.

fıkrasında, üye işyerlerinin, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamayacakları, saklayamayacakları ve kopyalayamayacakları, üye işyerlerinin, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamayacağı, satamayacağı, satın alamayacağı ve takas edemeyeceği belirtilmiştir. Maddenin ikinci fıkrasında ise kart çıkaran kuruluşların, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlü oldukları ifade edilmiştir. Aynı kanunun 31 inci maddesinde de kişisel verilerin korunmasına ilişkin bir düzenleme yer almakta olup, buna göre kurul üyeleri ile kurum personeli, görevleri sırasında öğrendikleri bilgileri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar[246].

Yukarıda ilgili maddelerine değinilmiş olan 5411 Sayılı Bankalar Kanunu ve 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu'nda her ne kadar "sır" dan bahsediliyor olsa da, müşteri sırrı kapsamında bazı kişisel verilerin de bulunabileceği muhakkaktır. Bu itibarla bu maddenin yalnızca "sır" koruma işlevini değil, aynı zamanda müşterilerin kişisel verilerini de koruma amacı bulunduğu kabul edilmelidir. Bu maddelerde öngörülmüş olan yükümlülüklerine aykırı hareket eden kimseler, TCK'nın 239 uncu maddesinde yer alan "Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması" suçundan sorumlu olacak, yükümlülüklerine aykırı hareket edenlerin fiillerinin konusunun kapsamına müşterilerin kişisel verilerinin de dahil olması halinde, bu kimselerin TCK'nın 136 ncı maddesine göre de sorumlulukları gündeme gelecektir.

---

[246] Kanunun 31 inci maddesine göre, "*Kurul üyeleri ile Kurum personeli, görevleri sırasında öğrendikleri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar.*
Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar, 29 uncu maddede yer alan kuruluşlar ile üye işyerleri, bunların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri sırları kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Kart çıkaran kuruluşların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır."

e. Noterlik Kanunu

Noterlikte yapılan işlemlerin niteliği değerlendirildiğinde, bireylerin kişisel verilerinin belki de işleme en çok konu edildiği yerlerden biri noterliklerdir. Buna bağlı olarak, noterliklerde kaydedilen veya çalışanların meslekleri dolayısıyla vakıf oldukları kişisel bilgiler azımsanmayacak miktardadır. Bu itibarla, bireylerin noterliklerde yaptıkları işlemler sonucunda kişisel verilerinin rızaları hilafına kaydedilmemesi veya yetkisiz başka kimselerle paylaşılmaması gerekmektedir ve bu başlık altında incelenen kanunda da noterlere birtakım yükümlülükler getirilmektedir.

1512 Sayılı Noterlik Kanunu'nun[247] 54 üncü maddesine göre "noter ve noterlik katipleri, görevleri dolayısıyla öğrendikleri sırları, kanunların emrettiği haller dışında açıklayamazlar." Bu maddede de her ne kadar "sır" dan bahsedilse de, maddenin kişisel verileri de koruduğunu kabul etmek gerekir, zira sır kapsamında kalan birtakım bilgi ve belgelerin muhtevasında kişisel bilgilerin de bulunması olasılığı oldukça yüksektir. Bu maddeye aykırı davranan kişiler ise Türk Ceza Kanunu'nun ilgili maddelerine göre sorumlu tutulacaklardır[248].

f. Adli Sicil Kanunu

Adli Sicil Kanunu'nda[249], bireylerin adli sicili ile ilgili olarak tutulan kayıtların gizliliğine ve silinmelerine ilişkin iki hüküm yer almaktadır. Kişilerin adli sicil bilgilerinin kendilerine ait kişisel veriler olduğu şüphesizdir ve bireylerin adli sicil bilgilerindeki kayıtlar, bir hukuka uygunluk sebebi bulunmadıkça gizli kalmalıdır, zira adli sicil kaydı bulunan bir bireyin bunun bilinmesini mümkün mertebe istememesi doğaldır. İşte bu kişisel verilerin korunması ve bireylerin zarar görmemeleri için bu kanunun 11 inci maddesinde adlî sicil ve arşiv bilgilerinin gizli olduğu, bu bilgilerin, görevlilerce açıklanamayacakları ve bu kanun hükümlerine göre verilerin verildiği kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamayacağı açıkça düzenlenmiştir. 12 nci maddede ise, adli sicil ve arşiv

[247] Noterlik Kanunu, K.n. 1512; R.G.t. 05.02.1972, S. 14090.
[248] Uygulanacak maddeler ile ilgili olarak bu çalışmada "5411 Sayılı Bankalar Kanunu ve 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu" başlığı altında yapılan açıklamaların son paragrafına bakılmalıdır.
[249] Adli Sicil Kanunu, K.n. 5352; R.G.t. 01.06.2005, S. 25832.

bilgilerinin hangi koşullarda silinecekleri açıkça belirtilmiştir. Bu itibarla bu kanunun getirdiği yükümlülüklere aykırı davranarak, 12 nci maddedeki şartlar oluşmasına rağmen adli sicil ve arşiv bilgilerini silmeyenler (TCK m.138) ile 11 inci maddedeki fiilleri işleyenler (TCK m.136) hakkında Türk Ceza Kanunu'nun ilgili hükümleri uygulanacaktır.

g. Nüfus Hizmetleri Kanunu

Nüfus Hizmetleri Kanunu[250] bireylerin nüfus bilgilerinin ve dolayısıyla kişisel verilerinin muhafazası ve kaydıyla ilgili olarak hükümler sevk ettiği gibi, bunların korunmasına ilişkin yükümlülükler de getirmiştir. Gerçekten de nüfus ile ilgili veriler kişisel verilerin temellerini oluşturmakta, bu kanunla vatandaşlık numarası, isim, soy isim, doğum yılı, doğum yeri, anne ve baba adı, yerleşim adresi, fotoğraf, medeni hal ve hatta din gibi bireylerle ilgili önemli kişisel verilerin kütüklere kaydedilmesi düzenlenmektedir. Bu itibarla, aralarında hassas kişisel verilerin de bulunduğu bu kadar çok kişisel verinin tutulmasına olanak veren bir kanunun, bu verileri tutanlara gizlilikle ilgili birtakım yükümlülükler getirmesi de kaçınılmazdır.

Kanunun 9 uncu maddesinin ilk fıkrasında nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgelerin gizli oldukları ve bunların, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemeyeceği belirtilmiştir. İkinci fıkrada ise, nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevlilerin de bu gizliliğe uymak zorunda oldukları ve bu yükümlülüğün kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam ettiği ifade edilmiştir. Bu yükümlülüklere uymayanlar ise Türk Ceza Kanunu'nun ilgili hükümlerince sorumlu tutularak cezalandırılacaktır.

[250] Nüfus Hizmetleri Kanunu, K.n. 5490; R.G.t. 29.04.2006, S. 26153.

h. Türkiye İstatistik Kurumu Kanunu ve Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik

Türkiye İstatistik Kurumu Kanunu'nun[251] 2 nci maddesinde, kanunda kullanılan terimlerin tanımları yapılmıştır. Buna göre, İstatistikî birim; "yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları", Gizli Veri; "istatistikî birimin doğrudan veya dolaylı bir şekilde sahip olduğu özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkan sağlayan bireysel veya tablo halinde saklı tutulan veriyi", Bireysel Veri ise; "hakkında bilgi toplanan istatistikî birimlerin özellikleri ile birlikte tanımlandığı veriyi" ifade etmektedir.

Kanunun 4 üncü maddesinde, kanunun uygulanmasında uyulacak ilkeler belirlenmiş, buna göre, üretilen istatistiklerin istatiski gizlilik esasına göre hazırlanıp uygulanacakları ve gizlilik ilkesine riayet edileceği belirtilmiştir. 7 nci maddede ise verilerin kullanılıp saklanmalarına ilişkin temel kurallar belirlenmiş, ancak maddenin son fıkrasında elektronik ortamda tutulan bilgilere ilişkin belgelerin, bu veri ve bilgilerin kesinleşip kullanıma açık hale gelmesine kadar saklanacakları ve bu sürenin sonunda imha edilecekleri belirtilmiştir.

13 üncü maddede ise, gizli veriler düzenlenmiş, gizli verilere yalnızca resmî istatistik üretiminde görev alanların, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilecekleri belirtilerek maddenin son fırkasında veri gizliliği ve güvenliğine ilişkin usûl ve esasların, ulusal ve uluslararası ilkeler doğrultusunda, ilgili kurum ve kuruluşların görüşleri alınarak çıkarılacak yönetmelikle düzenleneceği ifade edilmiştir[252]. Bu maddenin son fırkasına göre, 2006 yılında

---

[251] Türkiye İstatistik Kurumu Kanunu, K.n. 5429; R.G.t. 18.11.2005, S. 25997.

[252] 13 üncü maddeye göre, "*Gizli verilere yalnızca resmî istatistik üretiminde görev alanlar, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilirler.*

Bireysel verinin toplulaştırılması ile oluşturulan veri tablosunun herhangi bir hücresindeki istatistikî birim sayısının üçten az olması veya birim sayısı üç ve daha fazla olduğu halde bir veya iki istatistikî birimin hakim durumda olması halinde ilgili hücredeki veri gizli kabul edilir.

Resmî istatistiklerin üretilmesi için toplanan, işlenen ve saklanan verilerden gizli olanları, idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. Bu bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu kanunğa uymak zorundadır. Bu yükümlülük, görevlilerin görevlerinden ayrılmalarından sonra da devam eder.

Resmî istatistik üreten kurum ve kuruluşların yetkilileri tarafından, gizli verilerin hukuka aykırı erişimine, açıklanmasına veya kullanımına karşı her türlü önlem alınır.

Herkese açık kaynaklardan elde edilen veri veya bilgiler gizli kabul edilmez

Türkiye İstatistik Kurumu tarafından "Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik" [253] çıkarılmıştır ve Yönetmeliğin birinci maddesinde, yönetmeliğin amacı resmî istatistiklerde veri gizliliğine ve gizli verinin güvenliğinin sağlanmasına ilişkin usul ve esasları düzenlemek olarak düzenlenmiştir. Yönetmeliğin 8 inci ve 9 uncu maddelerinde, Kanun'un 13 üncü maddesinin ilk fırkasında yer alan düzenlemeye benzer bir ifade ile gizli verilere yalnızca resmî istatistik üretiminde görev alan kişilerin görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilecekleri belirtilmiş; resmî istatistiklerin üretilmesi için veri toplayan ve işleyen görevliler ile toplanan veriden üretilen istatistikleri saklamakla görevli personelin, gizli/bireysel veri ile gizli/bireysel veriye ulaşılmasını sağlayacak toplulaştırılmış veriyi istatistik üretim sürecinde görevlendirilenler dışında hiçbir organ, makam, merci veya kişiye veremeyecekleri ve bu yükümlülüklerinin görevleri sona erdikten sonra da devam edeceği ifade edilmiştir. Hatta maddenin üçüncü fıkrasında, gizli verilerin idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemeyeceği, istatistik amacı dışında kullanılamayacağı ve ispat aracı olamayacağı ifade edilmiştir.

Yönetmeliğin 10 uncu maddesinde, bireysel verilerin bilimsel amaçlı olarak kullandırılabilecekleri belirtilmiş, ancak bu husus birtakım şartlara bağlamıştır. Bu şartlara göre, bireysel verilerin bilimsel amaçlarla kullandırılabilmeleri için istatistikî birimlerin doğrudan tanınmasına yol açacak bölümleri gizlenmesi gerekmekte olup, yapılan analizlerin sonuçları, istatistikî birimin dolaylı olarak tanınmasına yol açacak bölümler gizlendikten sonra verilmesi öngörülmektedir. Aynı maddenin üçüncü fıkrasında ise çok önemli bir koruma getirilerek, bireysel verileri kullanma hakkını elde edenlerin, bu hakkı üçüncü şahıslara devredemeyecekleri ve elde ettikleri verileri hiçbir kişi veya kuruluşa veremeyecekleri, aksi davranışta bulunanların ise 5429 Sayılı Türkiye İstatistik Kanunu'nun, TCK'nın 258 inci maddesine

---

İstatistikî birimin, kendisine ait gizli verilerin açıklanmasına yazılı onay vermesi halinde, veri gizliliği ortadan kalkar.

Gizli veriler, ancak doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde diğer bilgilerle birleştirilerek yayımlanabilir.

(Ek fıkra: 25/11/2008 - 5813 S.K./2. md.) Dış ticaret istatistiklerinde dolaylı tanınma ile gizlilik kapsamına giren veriler için bu gizlilik hükümleri, istatistikî birimin kendisine ait verinin gizlenmesini talep eden yazılı başvurusu halinde uygulanır.

Veri gizliliği ve güvenliğine ilişkin usûl ve esaslar, ulusal ve uluslararası ilkeler doğrultusunda, ilgili kurum ve kuruluşların görüşleri alınarak çıkarılacak yönetmelikle düzenlenir."

[253] Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik, R.G.t. 20.06.2006, S. 26204.

göndermede bulunan 53 üncü maddesine göre cezalandırılacakları belirtilmiştir[254]. Nitekim kanunun 14 üncü maddesinde de yönetmeliğin bu maddesine benzer bir düzenleme yer almakta olup, bireysel verilerin, istatistikî birimlerin doğrudan veya dolaylı olarak tanınmasına yol açacak bölümleri gizlendikten sonra, münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izniyle verilebileceği ve bireysel verileri kullanma hakkı elde edenlerin, bu verileri üçüncü şahıslara veremeyecekleri belirtilmiştir.

Son olarak Yönetmeliğin 14 üncü ve 15 inci maddelerinde ise, Veri Gizliliği İhtisas Komisyonu'nun kurulmasına ve görevlerine ilişkin usul ve esaslar düzenlenmiş olup, Komisyon'un görevleri; veri gizliliği ve güvenliği konularındaki gelişmeleri takip etmek, veri gizliliği ve güvenliği konularındaki kurumsal stratejileri belirlemek ve resmî istatistik çalışmaları kapsamında hangi verinin gizli veri olduğu hususunda gerektiğinde görüş oluşturmak olarak belirlenmiştir.

i. Hasta Hakları Yönetmeliği

Sağlık alanındaki kişisel verilerin işlenmesine ve korunmasına ilişkin doğrudan veya dolaylı olarak çeşitli düzenlemeler içeren pek çok kanun ve yönetmelik vardır. Ancak bunlardan en önemlisini Hasta Hakları Yönetmeliği[255] oluşturduğu için, bu başlık altında daha çok bu yönetmelik üstünde durulacak, gerektiği yerlerde diğer yönetmeliklerden de kısaca bahsedilecektir.

Hastalara ilişkin sağlık bilgilerinin saklanmasına ve işlenmesine olanak veren en önemli düzenlemelerden biri "Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sisteminin kurulacağını" öngören Sağlık Hizmetleri Temel Kanunu'nun[256] 3/f hükmüdür. Buna göre, artık teknolojinin bu denli ilerleme kaydettiği günümüzde, hastaların sağlık durumlarına ilişkin kişisel veriler bilgisayar

[254] Türkiye İstatistik Kanunu'nda 53 üncü madde şu şekilde düzenlenmiştir: *Bu Kanunun 13 üncü Maddesinde yazılı kanunklara aykırı hareket eden kamu görevlileri, 5237 Sayılı Türk Ceza Kanununun 258 inci Maddesine göre cezalandırılır.*
TCK'nın "Göreve ilişkin sırrın açıklanması" başlıklı 258 inci maddesine göre, *(1) Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.*
(2) Kamu görevlisi sıfatı sona erdikten sonra, birinci fıkrada yazılı fiilleri işleyen kimseye de aynı ceza verilir.
[255] Hasta Hakları Yönetmeliği, R.G.t. 01.08.1998, S. 23420.
[256] Sağlık Hizmetleri Temel Kanunu, K.n. 3359; R.G.t. 15.05.1987, S. 19461.

ortamında ve hekimlerin kolayca erişebilecekleri bir düzen ve sistem içinde tutulmaktadırlar. Ancak bu kişisel verilerin bu ortamlarda tutulması, hekimlerin bunlara daha kolay erişebilmesini sağladığı gibi, dışarıdan yapılabilecek müdahalelere karşı da bu verileri daha savunmasız hale getirmiştir. Bu itibarla, Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesi gibi, sağlık alanındaki kişisel verilerin kaydedilmelerine ve saklanmalarına olanak veren diğer kanun ve yönetmeliklerle, verilerin saklanması için dayanak teşkil eden maddelere ek olarak bu verilerin korunması için de birtakım hükümler sevk edilmiştir.

Hasta Hakları Yönetmeliği'nin beşinci maddesinde yönetmeliğin uygulanmasında temel alınacak ilkeler belirlenmiş, buna göre maddede tıbbi zorunluluklar ve kanunlarda yazılı haller dışında, rızası olmaksızın kişinin kişilik haklarına ve kanun ile müsaade edilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamayacağı belirtilmiştir[257]. Yukarıda Medeni Kanun'u incelerken, bireylerin kişisel verilerinin korunmasının kişilik hakkı kapsamında olduğunu değinmiştik. Bu itibarla bu madde, doğrudan kişisel verilere açıkça değinmese de, bu madde ile yine kişisel verilere belirli bir koruma getirmektedir. Bunun yanı sıra, 16 ncı maddede, hastalara sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleme ve bir suretini alma hakkı getirmiş olup; bu kayıtların, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebileceği belirtilmiştir.

Hastaların mahremiyetinin korunması hususu yönetmelik 21 inci madde düzenlenmiş, hastanın mahremiyetine saygı gösterilmesinin esas olduğu, hastanın mahremiyetinin korunmasını açıkça talep edebileceği, her türlü tıbbi müdahalenin,

---

[257] 5. maddeye göre, "*Sağlık hizmetlerinin sunulmasında aşağıdaki ilkelere uyulması şarttır:*
a) Bedeni, ruhi ve sosyal yönden tam bir iyilik hali içinde yaşama hakkının, en temel insan hakkı olduğu, hizmetin her safhasında daima gözönünde bulundurulur.
b) Herkesin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkını haiz olduğu ve hiçbir merci veya kimsenin bu hakkı ortadan kaldırmak yetkisinin olmadığı bilinerek, hastaya insanca muamelede bulunulur.
c) Sağlık hizmetinin verilmesinde, hastaların, ırk, dil, din ve mezhep, cinsiyet, siyasi düşünce, felsefi inanç ve ekonomik ve sosyal durumları ile sair farklılıkları dikkate alınamaz. Sağlık hizmetleri, herkesin kolayca ulaşabileceği şekilde planlanıp düzenlenir.
d) Tıbbi zorunluluklar ve kanunlarda yazılı haller dışında, rızası olmaksızın kişinin vücut bütünlüğüne ve diğer kişilik haklarına dokunulamaz.
e) Kişi, rızası ve Bakanlığın izni olmaksızın tıbbi araştırmalara tabi tutulamaz.
f) Kanun ile müsaade edilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamaz."

hastanın mahremiyetine saygı gösterilmek suretiyle icra edileceği ifade edilmiştir[258].Yönetmeliğin 23 üncü maddesine göre ise "sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz ve kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz." Maddede ayrıca hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektireceği belirtilmiş, araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgilerinin rızası olmaksızın açıklanamayacağı belirtilmiştir.

Her ne kadar bu Yönetmelik ile hasta haklarının korunması ve dolayısıyla kişisel verilerinin korunması için faydalı olan hükümler yer alsa da, bünyesinde toplumdaki bireyler açısından son derece hassas ve önemli kişisel veriler barındıran sağlık bilgilerinin kanunla düzenlenmek yerine yönetmelikle düzenlenmiş olması doktrinde haklı olarak eleştirilmiştir[259].

j. Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik

Bilişim Teknolojileri Kurumu tarafından çıkarılan[260] Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında

---

[258] 21 inci maddeye göre, "*Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir.*
Mahremiyete saygı gösterilmesi ve bunu istemek hakkı;
a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,
b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini,
c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini,
d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını,
e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsi ve ailevi hayatına müdahale edilmemesini,
f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar.
Ölüm olayı, mahremiyetin bozulması hakkını vermez
Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır."
[259] **Küzeci**, s. 342.
[260] **Özdemir**, **Hayrunisa**, "İletişim Alanında Kişisel Verilerin Korunması", Bilişim Hukukunun Son 10 Yılı Sempozyumu, www.erzincan.edu.tr/gundem.php?al=86, 09.10.2011.

Yönetmeliğin[261] 1 inci maddesinde, yönetmeliğin amacı telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasların düzenlenmesi olarak tanımlanmıştır. Yönetmeliğin 3 üncü maddesinde ise tanımlara yer verilerek kişisel veriler/bilgiler; "Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi", trafik verisi; "bir şebekeden haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi", yer verisi ise; "Kamuya açık telekomünikasyon hizmeti kullanıcısına ait bir telekomünikasyon cihazının coğrafi konumunu belirleyen şebekede işlenen her türlü veriyi" ifade etmektedir.

Yönetmeliğin 9 uncu maddesinde ise abone veya kullanıcıların kişisel verilerinin ancak veri öznesinin izni ile işlenilebileceği ve kullanılabileceği belirtilmiş olup işlenen kişisel verilerin ve bu tür işlemlerin süresinin veri öznesine bildirileceği belirtilmektedir[262]. 10 uncu maddede ise, kimlerin trafik verilerini işleyebileceğine değinilmiştir[263]. 15 inci maddede, yer verilerinin hangi şartlarda işlenebilecekleri belirtilmiş, yer verilerinin "abonelerin aksi başvuruları olmadığı hallerde" işlenebilecekleri belirtilerek, böylece bu tür verilerin işlenmesi kaide, işlenmemesi ise istisna olarak düzenlenmiştir[264]. Kanaatimizce, bu tür verilerin işlenmemesi temel kural olarak belirtilmiş ve ancak abonelerin izin vermeleri halinde işlenebileceği düzenlenmiş olsaydı daha isabetli bir ifade olurdu. Yönetmeliğin 18 inci maddesine göre ise, "kötü niyetli veya rahatsızlık verici aramaların takibi

---

[261] Dayandığı Kanun: Telgraf ve Telefon Kanunu, K.n. 406, R.G.t. 06.02.2004, S. 25365.

[262] 9 uncu madde şu şekilde düzenlenmiştir: "*Telekomünikasyon hizmetlerini pazarlamak ya da katma değerli hizmetleri sağlamak amacıyla; abone veya kullanıcı kişisel bilgilerinin kullanılmasına izin verirse, işletmeci bu tür hizmetler ve pazarlama için gerekli kapsam ve sürede veriyi işleyebilir. Kullanıcı ve aboneler, kişisel bilgilerinin işlenmesi için verdikleri izinleri her zaman geri alabilirler. İşletmeci; abonenin veya kullanıcının onayını almak koşuluyla, telekomünikasyon hizmetlerinin pazarlanması ya da katma değerli hizmetlerin sağlanması amacıyla, işlenen kişisel bilgileri ve bu tür işlemin süresini abone ve kullanıcılara bildirecektir.*"

[263] 10 uncu maddeye göre, "*Trafik verilerinin işlenmesi yetkisi; işletmecinin yetkisi altındaki kişiler ile telekomünikasyon hizmetlerinin faturalama ve trafik idaresi, müşteri hizmetleri, yolsuzluk tespitleri, elektronik telekomünikasyon hizmetleri pazarlama veya katma değerli hizmet ile görevli kişilere münhasırdır.*"

[264] 15 inci maddeye göre, "*Abone ve kullanıcılarla ilgili yer verileri sadece abone ve kullanıcıların isimsizleştirildiği veya katma değerli bir hizmetin sağlanması için gereken kapsam ve sürede abonelerin aksi başvuruları olmadığı hallerde işlenebilir. İşletmeciler, işlenecek yer verisi tipini, işlemenin amaç ve süresi ile bu bilgilerin üçüncü şahıslara katma değerli hizmet sağlama amacıyla gönderilip gönderilmeyeceği hususlarında, aboneleri bilgilendirir. Aboneler, yer verilerinin işlenmemesi için her zaman başvuru yapabilirler.*"

amacıyla, abone tarafından yapılan başvuru üzerine, arayan abonenin kimliğini içeren bilgiler, 1 (bir) yıl süreyle saklanmalı ve ilgili mevzuata göre erişilebilir olmalıdır.” Abonenin savcılığa herhangi bir başvurusu olmaksızın, yalnızca rahatsızlık verici aramalara maruz kaldığı beyanına dayanılarak bir başka kişinin kimliğini içeren bilgilerin 1 yıl süreyle saklanmalarına ilişkin yapılan bir düzenleme kanaatimizce isabetsizdir, zira maddede yer alan düzenleme, kötüye kullanıma açık olup, getirilen bu kuralın hangi usullerle uygulanacağı dahi yönetmelikte belirtilmemiş, bu kaydı kimin tutacağına, bir yıl sonunda nasıl yok edeceğine ve yok etmemesi halinde nasıl bir yaptırımın uygulanacağına ilişkin hiçbir düzenleme getirilmemiştir.

İKİNCİ BÖLÜM

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

I. CEZA HUKUKU YÖNÜNDEN KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ÇALIŞMALAR

A. Kişisel Verilerin Korunması Hakkında Kanun Tasarısı

Kişisel verilerin korunmasına ilişkin Türkiye'deki düzenlemelere bakıldığında, diğer ülkelerde olduğu gibi kişisel verileri koruyan özel bir kanunun bulunmadığı görülmektedir. Türkiye'de, kişisel verilerin korunmasına ilişkin bir tasarı hazırlamak üzere ilk defa 13 Eylül 1995 tarihinde bir komisyon oluşturulmuş, ancak bu komisyon çalışmalarını tamamlayamamıştır. Bunun üzerine 8 Eylül 2000 tarihinde yeni bir komisyon kurulmuş, bunun neticesi olarak da, üç senelik bir çalışma sonunda 2003 tarihinde, 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme ve 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi esas alınarak "Kişisel Verilerin Korunması Kanunu Tasarısı" (KVKT) hazırlanmıştır[265]. Ancak bu dönemde kanun haline getirilmeyen bu tasarı üzerinde ilave çalışmalar yapılarak 22 Nisan 2008 tarihinde son haliyle Başbakanlık'a gönderilmiştir[266].

Tasarı toplam sekiz bölümden oluşmakta olup bunlar; "Amaç, kapsam ve tanımlar", "Genel kurallar", "Kişisel verilerin gerçek kişi ve özel hukuk tüzel kişileri tarafından işlenmesi", "Kişisel verilerin kamu tüzel kişileri tarafından işlenmesi", "Verilerin kişisel olmaktan çıkarılması, silinmesi, yok edilmesi ve bilimsel araştırma, istatistik ve planlama amacıyla kullanılması", "Kurumun kuruluş ve görevleri", "Kanun yolları, hukuki ve cezai sorumluluk" ve "Son hükümler" dir. Türkiye,

[265] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 107-108.
[266] **Küzeci**, s. 358.

bugüne kadar bu tasarının kanunlaşmasını geciktirmiş, ilk komisyonun kuruluş tarihi dikkate alındığında, diğer ülkelerin hemen hemen hepsinde mevcut olan ve kişisel verilerin korunmasına ilişkin ayrı bir kanunu çıkarmayı yaklaşık yirmi yıldır ertelemiştir. Mevcut durumda, Türk Ceza Kanunu'nda her ne kadar kişisel verilerin hukuka aykırı olarak kaydedilmelerine, ele geçirilmelerine, yayılmalarına, ifşa edilmelerine veya kanunun öngördüğü süreler geçmesine karşın silinmemesine ilişkin cezai yaptırımlar öngörülmüş olsa da, ayrı bir kanunun varlığına ihtiyaç duyulduğu muhakkaktır. Nitekim bu kanun, Türk Ceza Kanunu'nda öngörülmüş olan yaptırımlar açısından da tamamlayıcı nitelikte olacak, kişisel verilerin korunamayıp faillerin cezalandırılmasındansa, verilerin baştan korunarak bu tür ihlallerin önlenmesine vesile olacaktır.

Türkiye'nin bu kişisel verilerin korunmasına ilişkin tasarıyı bir an evvel Meclis'te tartışmaya sunması ve kanun haline getirmesi artık kaçınılmazdır, zira Avrupa'ya uyum kanunları çerçevesinde kanunlarında bu kadar değişikliğe ve uyuma giden bir ülkenin artık kişisel verileri sağlıklı bir şekilde düzenleyen bir kanun çıkarması zorunluluk halini almıştır. Söz konusu tasarı, bütününe bakıldığında, bazı maddelerde önemli farklılıklar bulunsa da, genel olarak 108 Sayılı Sözleşme ve 95/46 Sayılı Avrupa Topluluğu Veri Koruması Yönergesi'nden esinlenerek hazırlanmıştır. Ancak 108 Sayılı Sözleşme Türkiye tarafından 1981 yılında imzalanmış olsa da[267], iç mevzuatta gerekli düzenleme yapılmamış olduğundan onaylanamamıştır[268]. Bu nedenle, Tasarı yürürlüğe girdikten sonra önemli bir boşluk dolacak, diğer ülkelerle sağlanan bilgi alışverişi daha sağlam temellere oturtulacak ve böylece Türkiye, diğer ülkelerle eşdeğer koruma sağlayan bir kanuna sahip olması neticesinde bu ülkelerden ihtiyacı olan bilgileri de sağlayabilecektir[269]. Nitekim 2010 yılında düzenlenen "4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nda

[267] Sözleşmeyi Mayıs 2010'da imzalayıp Eylül 2010'da onaylayarak iç hukukuna dahil eden son ülke, Azerbaycan'dır. Mevcut durumda, Sözleşme'yi imzalayıp onaylayan ve iç hukukunda gerekli değişiklikleri yapan ülke sayısı 43 iken, imzalayıp onaylamayan ülke sayısı 3'tür. İmzalayıp onaylamayan bu ülkeler, Sözleşme'yi 2001'de imzalayan Rusya, 2011'de imzalayan Ermenistan ve 1981'de imzalayan Türkiye'dir. http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=09/01/2012&CL=ENG, 09.01.2012.

[268] **Küzeci**, s. 351.

[269] Kişisel verilerle ilgili düzenleyici yasalar bulunması artık internet üzerinden yapılan alışverişlerde kişilerin korunması açısından da önem kazanmıştır. Dolayısıyla uluslararası alanda internet üzerinden yapılan alışverişlerde diğer ülkelerle standart bir korumanın sağlanabilmesi için Türkiye'nin en kısa zamanda iç hukukunu kişisel verilerin korunması kapsamında uygun seviyeye çıkarması gerekmektedir.

(ISCTurkey 2010)" söz alan Ulaştırma Bakanı da bu hususun en kısa zamanda meclis gündemine tekrar taşınacağını ve gerekli adımların atılacağını belirtmiş, konferans sonucunda ISCTurkey 2010 Düzenleme Kurulu tarafından yayımlanan Sonuç Bildirgesi'nin 7 nci maddesinde "Yasalaşma çalışmaları süren Kişisel Verilerin korunması Kanunu Tasarısı'nın TBMM gündemine bir an önce alınmasının uygun olacağı ve kanunun önemli bir boşluğu dolduracağı" sonucuna varılmıştır[270].

Doktrinde, Sözleşme ile Yönergenin veri öznesi açısından sağlamaya çalıştıkları korumanın Tasarı ile sağlanmasının mümkün olmayacağı eleştirisi getirilerek, Tasarının veri öznelerinin haklarını korumaktan ziyade, kişisel verilerin işlenmesini, işleyenin lehine kolaylaştıracağı ve gerekçede bahsedilmiş olan kişisel veri öznesi ile kişisel veriyi işleyen arasındaki dengenin korunamayacağı ileri sürülmüştür[271]. Gerçekten de, Tasarının hükümlerine genel olarak bakıldığında, doktrinde getirilmiş olan eleştirilerin pek çoğunun haklı olduğu görülmektedir. Bunun yanı sıra, Tasarıda yer alan maddelerdeki veri öznesinin haklarını sınırlayan ifadelerin bir kısmı muğlak olup, Tasarının öngörmüş olduğu Kurul bağımsız olmaktan uzaktır ve veri öznesinin haklarına 108 Sayılı Sözleşmenin ve 95/46/AT Sayılı Yönerge'nin öngörmediği sınırlamalar getirilmektedir. Nitekim bu başlık altında Tasarının önemli gördüğümüz maddelerini ve bu maddelere yöneltilen eleştirileri inceleyeceğiz.

Tasarının, Yönerge ve Sözleşme'den önemli bir farkı, hem Yönerge'de hem de Sözleşme'de yalnızca "gerçek kişilerin" kişisel verilerinin korunmasından bahsedilmişken, Tasarı'nın 2 nci maddesinin ilk fıkrasında "kişilerin" korunmasından bahsedilmiş olmasıdır. Böylece Tasarı ile hem gerçek kişilerin hem de tüzel kişilerin kişisel verileri koruma kapsamına alınmış, bu husus doktrinde bazı yazarlar tarafından olumlu değerlendirilmişken[272], bazı yazarlar tarafından doğru

---

[270] 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey 2010) Sonuç Bildirgesi, http://www.biltekhaber.com/Web/Haber/HaberOku.aspx?haberID=2651, 08.01.2012.

[271] **Aksoy**, **Hüseyin Can**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Baskı, Ankara, Mart 2010, s. 117, **Beyli, Ceylin,** "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler", Bilişim Hukuku, Mete Tevetoğlu (der.), İstanbul, Aralık 2006, s. 72.

[272] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 109, TCK'nın 135 inci maddesinin gerekçesinde, maddenin kendisinde kişisel verilerle ilgili açık bir tanım yoken gerçek kişilerle ilgili kişisel verilerden bahsedilerek tüzel kişilerin bu maddenin kapsamında olmayacağı anlamı çıkmaması gerektiğini, Tasarının bu düzenlemesinin isabetli olduğunu ve TCK'nın ilgili maddelerinin gerçek kişilerin yanı sıra tüzel kişiler hakkında da uygulanabileceğini belirtmektedir.

bulunmayarak eleştirilmiştir[273]. Düşüncemize göre, gerçekten de, kişisel verilerin korunması hakkı gerçek kişilere mahsus bir hak olarak kabul edilmeli, tüzel kişiler için ticari sır kavramı benimsenmelidir. Zira tüzel kişiliğin bünyesindeki kişisel verilerin hukuka aykırı olarak işlenmesi halinde ilgili kişilerin kanunlaşacak olan bu Tasarı ve Türk Ceza Kanunu kapsamında başvuru hakları her zaman olacaktır. Bu itibarla, insan hakları kapsamında korunan ve gerçek kişilere mahsus olduğunu düşündüğümüz kişisel verilerin korunmasını düzenleyen bu Tasarının koruma alanı kapsamına, tüzel kişilerin dahil edilmemesi daha isabetli olacaktır. Bu noktada yabancı ülkelerin mevzuatına bakıldığında, Belçika, Finlandiya, Yunanistan, Almanya, İsveç, İngiltere, İrlanda, İspanya, Portekiz, Hollanda, Kanada ve Norveç yalnızca gerçek kişilere ilişkin bilgileri kişisel veri olarak kabul etmişken, İsviçre, Avusturya, Şili, Lüksemburg Bulgaristan ve İtalya'da kişisel verileri koruyan kanunların tüzel kişileri de ilgili mevzuatın kapsama aldığı görülmektedir[274].

İkinci maddenin ikinci fıkrasında, Tasarı hükümlerinin, "kişisel verilerin gerçek kişiler tarafından sadece kişisel veya birlikte oturanlarla ilgili faaliyetlerine ilişkin olarak işlenmesi halinde" uygulanmayacağı belirtilmiştir. Kanaatimizce bu

---

Şen, **Ersan** "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, Cilt:83, Sayı:3, 2009, s. 1202; "*… korunması gerekli kişisel veriler sadece gerçek kişilere değil, tüzel kişilere de ait olabilir. Gerçek kişilerden ayrı bir hukuki varlıkları ve kimlikleri bulunan tüzel kişilerin de kendi yapılarına özgü kişisel verilerinin olacağı tartışmasızdır. Kanun koyucu kişi ve kişisel kavramları ile yalnızca gerçek kişilere güvence sağlamayı hedeflememiştir. Belki 135. Maddenin ikinci fıkrasından hareketle bu sonuca ulaşılabilir, ancak suçun tanımını gösteren 135. Maddenin birinci fıkrası, korunan hukuki yararın mağduru olabilecek kişiler bakımından gerçek kişi- tüzel kişi ayrımı yapmamıştır. Bu nedenle tüzel kişiye ait verilerin korunması yönünden TCK m.135 ile 136'nın uygulama alanı bulabileceğini ifade etmek isteriz.*"

[273] **Aksoy**, s. 118; "*Her ne kadar, 2002/58/EC Sayılı direktif tüzel kişileri de kapsamaktaysa da, bu düzenleme elektronik haberleşme sektörüne özel olup, üye devletlere, 95/46/EC Sayılı Direktif'in uygulama alanını, tüzel kişileri de kapsayacak şekilde genişletme yükümlülüğü getirmemektedir. Bu çerçevede, 2002/58/EC Sayılı direktifin, elektronik haberleşme sektörünün özelliklerini dikkate alan istisnai bir düzenleme olduğu kabul edilmelidir. Nitekim kişisel veri kavramı, niteliği itibariyle gerçek kişilere ilişkin bir kavram olup, tüzel kişiler bakımından ticari sır kavramından bahsetmek daha isabetli olacaktır.*"

Şimşek, s. 207; "*Esasında bir gerçek kişiyi belirleyen veya belirlenebilir kılan bilgiler tüzel kişiye ilişkin bilgilerde bulunuyorsa, bunlar gerçek kişiyle olan ilişkisi nedeniyle zaten kişisel veri kavramına dahil olacaktır. Bunun yanı sıra, Tasarıda tüzel kişinin de verileri korunmakta ve bu garanti tüzel kişilerin korunması bakımından olumlu olarak değerlendirilmektedir. Ancak verilerin korunması hukukunda temel düşüncenin öncelikle kişisel verilerin veri işlemeye tabi tutulması sırasında gerçek kişi olarak insanın ve özgürlüklerinin korunması ve kişisel verilerin korunması hakkının güvence altına alınması olduğu gözden uzak tutulmamalıdır.*"

Küzeci, s. 364-365; "*… kişisel verilerin korunması başta özel yaşamın gizliliği hakkı olmak üzere temel hak ve özgürlüklerde kaynağını bulmaktadır ve bağımsız bir hak alanı olma yolunda gelişmektedir. Bu kapsama tüzel kişilerin de alınması kişisel verilerin korunmasının temel felsefesine aykırı olacağı gibi, korumanın zayıflaması tehlikesini de beraberinde getirecektir.*"

[274] **Aksoy**, s. 19, **Küzeci**, s. 367, **Atak**, Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, s. 205.

fıkrada bahsi geçen "birlikte oturanlar" ifadesi son derece muğlak kalmış, ciddi hak ihlallerine yol açabilecektir. Bu tür bir düzenlemeye gidilecekse, birlikte oturulan kişiler gibi geniş bir ifadeden ziyade yakın aile bireylerine değinilmeli, ancak bu kapsamda kalacak kişiler de kanunda açıkça sayılmalıdır[275].

Tasarının üçüncü maddesinde, tanımlar başlığı altında tasarıda geçen kavramlar tanımlanmıştır[276]. Buna göre; kişisel veri "Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler", kişisel verilerin işlenmesi ise "Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütününü" ifade etmektedir. Kişisel verilerin işlenmesinin bu şekilde tanımlanmış olması, 95/46/AT Sayılı Yönerge'nin ikinci maddesinde[277] yapılan tanıma göre dar kapsamlı olması ve teknik ilerleme karşısında işlevini ilerleyen dönemlerde yitirebilecek olması sebebiyle doktrinde eleştirilmiştir[278].

Tasarının 5 inci maddesinin ilk fıkrasında[279], kişisel verilerin işlenmesine ilişkin temel ilkeler belirlenmiş olup[280], maddenin ikinci fıkrasında buna bir istisna getirilmiştir. İkinci fıkraya göre, kişisel veriler, ilgili mevzuatta yeniden işlenme

---

[275] Aynı görüşte, bkz. **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1200.

[276] http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf, 08.01.2012.

[277] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 109; *"AT mevzuatı uyarınca işleme otomatik ya da otomatik olmayan prosedür yoluyla gerçekleştirilen kişisel verilerle ilintili olabilecek her türlü süreci içermelidir. Buna göre kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, saklanması, değiştirilmesi, okunması, sorulması, kullanılması, transfer yoluyla başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılan her türlü işlem ile bunun yanı sıra verilerin kombinasyonu ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleşen her türlü işlem çeşidi anlaşılması gerekecektir."*

[278] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 109.

[279] Tasarının "Kişisel Verilerin İşlenmesine İlişkin İlkeler" başlıklı 5 inci maddesinin 1. fıkrasında, *"(1) Kişisel verilerin;*
a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,
b) Belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi,
c) Toplandıkları amaçla bağlantılı, yeterli ve orantılı olması,
ç) Doğru olması ve gerektiğinde güncellenmesi,
d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi, zorunludur." denilmektedir.

[280] Benimsenmiş olan ilkelerin 95/46/AT Sayılı Yönerge'nin 6 ncı maddesinde benimsenmiş olan ilkelere paralel olduğu görülmektedir.

amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla tarihî, istatistikî veya bilimsel amaçlarla yeniden işlenebilir veya birinci fıkranın (d) bendinde öngörülen amaç için gerekli olan süreden daha uzun bir süre saklanabilirler. Bu fıkrada, kişisel verilere ilişkin amaçla sınırlı süre muhafaza etme ilkesine birtakım bilimsel, tarihi veya istatistikî çalışmalar kapsamında sınır getirilebileceği düzenlenmiş olup, amaç için tutulması gerekli olan süreden daha uzun sürenin ne demek olduğu ve bunun kim tarafından ve nasıl belirleneceği belirtilmemiştir. Doktrinde, ikinci fıkrada getirilen istisnanın da, ilk fıkradaki genel ilkelerle bağlı olduğu, dolayısıyla getirilen istisna açısından da amaç için gereken süre şartının bulunacağı ifade edilmiştir[281]. Fakat ikinci fıkradaki istisnanın ilk fıkradaki amaçla bağlılığın gerektirdiği süreden daha uzun olabileceği açıkça ifade edildiğinden ve bu nedenle ilk fıkranın (d) bendinde yer alan genel ilke bertaraf edildiğinden, bu görüşe iştirak etmemekteyiz. Bu noktada da, daha uzun süre tutulabilme kavramında ifade edilen sürenin ne anlama geldiği hususunun sınırlarının belirtilmesi gerektiği kanaatindeyiz.

Tasarının 6 ncı maddesinin birinci fıkrasında, kişisel verilerin ancak ilgili kişinin açık rızasıyla işlenebilecekleri belirtilmiş olup ikinci fıkrada kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin bir itirazda bulunması halinde verinin işlenemeyeceği ifade edilmiştir. Bu husus doktrinde, kişisel verilerin kişinin rızası hilafına işlenmemesinin temel bir hak olduğu ve dolayısıyla genel kural niteliğinde olduğu, bu itibarla "itirazda bulunma halinde işlenememe" yerine, "kişinin rızasını almadan işleyememe"ye vurgu yapılması gerektiği gerekçesiyle haklı olarak eleştirilmiştir[282]. Kanaatimizce, bu hususun yanı sıra, açık rıza ile ilgili olarak, hassas nitelikteki kişisel verilerin işlenebilmelerine imkan veren istisnai durumlarda da, her ne kadar yedinci maddenin ikinci fıkrasının (a) bendinde bu tür verilerin işlenmesine ilişkin rızanın yazılı olacağı belirtilmişse de, bu maddede de buna atıf yapılabileceği düşünülmelidir.

---

[281] **Küzeci**, s. 370; "*Bu noktada verilerin yeniden işlendikleri durumlarda da temel ilkelere uyulacağı ve verilerin tutulma sürelerinin bu kez de belirtilen istisna kapsamındaki amaçların gerçekleşmesi ile sınırlı olacağı unutulmamalıdır*."

[282] **Şimşek**, s. 208, **Küzeci**, s. 369, **İlkiz**, **Fikret**, "Kişisel Verilerin Korunması ve Kanun Tasarısı", Güncel Hukuk Dergisi, Sayı 67, Temmuz 2009, s. 16.

Altıncı maddede, kişilerin rızası olmadan kişisel verilerinin işlenemeyeceği belirtildikten sonra, üçüncü fıkrada buna dört tane istisna getirilerek bu hallerde hukuka uygunluğun bulunduğunun kabul edileceği belirtilmiştir. İşte hukuka uygunluğun varlığına delalet eden durumlardan biri de "Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işlemesinin zorunlu olması"dır. Veri öznelerini koruduğu iddia edilen bir kanunda böyle bir ifadenin yer alması son derece yanlıştır. Zira bu husus, Tasarının pek çok maddesinde olduğu gibi, muğlak biçimde kaleme alınmış, haklı çıkar ifadesinin ne demek olduğuna ve veri kütüğü sahibinin haklı çıkarları uğruna hangi kişisel verilerin işlenebileceğine hiç temas edilmemiştir. Kaldı ki düzenlemenin bu şekilde ifade edilmiş olması, sanki veri kütüğü sahiplerinin haklı çıkarları uğruna her tür veriyi işleyebilecekleri izlenimini uyandırmakta, bentte orantılılık ve amaca bağlılığa hiç değinilmemektedir. Düzenleme bu haliyle veri kütüğü sahiplerinin pek çok durumu kendi haklı çıkarları olarak yorumlayıp kişisel verileri gelişigüzel işlemelerinin önünü açacak ve ilgili kişiler için sağlanmak istenen korumayı önemli ölçüde baltalayacaktır[283]. Bu itibarla, düşüncemize göre, altıncı maddenin 3 üncü fıkrasının (b) bendi Tasarı kanunlaşmadan evvel madde metninden tamamen çıkarılmalıdır.

Tasarının 7 nci maddesinin ilk fıkrasında, "Kişilerin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel verilerin işlenemeyeceği" belirtilmiş olup, ikinci fıkrada bu kurala birtakım istisnalar getirilmiştir[284]. 95/46/AT

[283] Aynı görüşte, bkz. **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1203; "*Maddede yer alan 'veri kütüğü sahibinin kendi haklı çıkarları' ibaresi geniş kapsamlı ve belirsiz nitelikte olduğu gibi, kişinin rızası bulunmaksızın veri işlenmesine de bu yolla olanak sağlanmaktadır… veri kütüğü sahibinin kendi haklı çıkarları kavramının kapsamı son derece geniş olmakla birlikte söz konusu haklı çıkarların belirlenmesinde esas alınacak ilke ve esasların belirsizliği de hukuk devleti ilkesinden uzaklaşılmasına neden olabilir.*"

[284] Tasarının "Özel niteliği olan kişisel veriler" başlıklı 7 nci maddesinde **"***(1) Kişilerin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel veriler işlenemez.*

(2) Birinci fıkrada belirtilen kişisel verilerin, özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla, aşağıda sayılan hallerde işlenmesi mümkündür:

a) Kanunla yasaklanmayan hallerde kişinin yazılı rızasının alınması,

b) Hukukî veya fiilî nedenlerle rızasını açıklayamayacak durumda bulunan bir kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün idamesi için veri işlemenin zorunlu olması,

c) İlgili kişiye yeterli koruma imkanının sağlanması şartıyla, veri kütüğü sahibinin, bu Kanunla veya diğer kanunlarla tanınan hak ve yetkileri kullanabilmesi veya yükümlülükleri yerine getirebilmesi için veri işlemenin zorunlu olması,

Sayılı Yönerge'ye paralel olarak hazırlanan bu düzenlemede, Yönerge'den farklılık arz eden önemli bir husus olarak, hassas niteliği olan kişisel veriler kapsamında cinsel yaşamın sayılmamış olmasıdır. Doktrindeki bir görüşe göre, maddede özel olarak belirtilmemiş olan kişilerin cinsel yaşamlarına ilişkin kişisel veriler, "özel hayat" kapsamı içerisinde değerlendirilecektir[285]. Bu husus doktrinde özel yaşam ifadesinin pek çok kişisel veriyi kapsayabileceği ve bu sebeple bazı kişisel verilerin sahip olması gereken sağlam korumayı bu verilere sağlayamayacağı için eleştirilmiş, "özel yaşam" ifadesinin madde metninden çıkarılarak yerine "cinsel yaşam" ifadesinin getirilmesi gerektiği ileri sürülmüştür[286]. Gerçekten de, bu maddede, işlenemeyecek olan kişisel veriler oldukça geniş tutulmuş, amaç özel nitelikli kişisel verileri saymak iken, özel yaşama ilişkin tüm kişisel verilerin özel nitelikli kişisel veriler olacağına ilişkin bir düzenleme yapılarak özel yaşama ilişkin tüm kişisel verilerin ortaya koyduğu geniş kapsam sebebiyle, korunması daha mühim olan kişisel verilere bu kapsam içerisinde gereken sağlam koruma sağlanamayabileceğinden isabetsiz olmuştur. Dolayısıyla, düşüncemize göre, doktrinde ileri sürüldüğü gibi, "cinsel yaşam" ifadesinin "özel hayat" yerine kullanılması daha doğru olacak, Yönerge ile paralellik daha büyük oranda sağlanmış olacaktır. Nitekim 95/46/AT Sayılı Yönerge ve 108 Sayılı Avrupa Konseyi

---

ç) Vakıf, dernek, sendika ve siyasi partilerce, kuruluş amaçlarına ve tabi oldukları mevzuata uygun ve faaliyet alanlarıyla sınırlı olmak şartıyla, üye ve mensuplarına yönelik ve ilgili kişinin rızası olmadan üçüncü kişilere açıklanmamak kaydıyla veri işlenmesi,
d) İlgili kişi tarafından alenen açıklanmış olan veriler hakkında olması,
e) Hukuken bir hakkı tesis, kullanma veya korunması için veri işlemenin zorunlu olması,
f) Koruyucu hekimlik, tıbbî teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin;
1) Sağlık kurumları,
2) Sigorta şirketleri,
3) Sosyal güvenlik kurumları,
4) İşyeri sağlık birimi oluşturmakla yükümlü işverenler,
5) Sağlıkla ilgili okul ve üniversiteler,
tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altındaki bir başka kişinin gözetimi altında işlenmesi.
(3) Özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi halinde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, Kurul, özel niteliği olan kişisel verilerin işlenmesine karar verebilir.
(4) Suçun soruşturulmasına, koruma ve kontrol tedbirlerine ve ceza mahkumiyetlerine ilişkin özel nitelikteki kişisel veriler, ilgili kanunlarda yeterli koruma tedbiri bulunması kaydıyla, yetkili mercilerin kontrolü altında işlenebilir. Ancak, ceza mahkumiyetlerine ilişkin sicil sadece Adalet Bakanlığının kontrolü altında tutulabilir.
(5) İdarî nitelikteki yaptırımlar ve özel hukuk alanındaki mahkeme kararlarına ilişkin veriler de resmî mercilerin kontrolü altında işlenebilir.
(6) Vatandaşlık kimlik numarası veya benzeri karakteristik işaretlerin işlenme usul ve esaslarını belirlemek amacıyla yapılacak yönetmeliklerde Kurulun görüşü alınır." denilmektedir.

[285] **Şimşek**, s. 209, **Küzeci**, s. 372.

[286] **Küzeci**, s. 372.

Sözleşmesi'nde olduğu gibi, Fransa, Almanya ve Belçika'nın da veri koruma kanunlarına bakıldığında, hassas kişisel verilerin kapsamına cinsel yaşamın dahil edildiği görülmektedir[287].

Özel nitelikli kişisel verilerin belirlenmesinde olduğu gibi, bunların işlenemeyeceğine ilişkin istisnalar da gereğinden geniş tutulmuş, muğlak ve kanunilik ilkesinin gerektirdiği belirlilikten uzak ifadeler kullanılmıştır. Özellikle maddenin 3 üncü fıkrasında, "temel kamu yararının gerektirmesi" durumunda "yeterli koruma bulunması halinde" özel nitelikli kişisel verilerin işlenebilecekleri belirtilmiştir. Bu fıkrada geçen yeterli koruma belirsiz bir ifadedir[288]. Aynı fıkrada, işlemeye ilişkin kararı Kurul'un vereceği belirtilmiştir. İdari bir makama, "temel kamu yararı" gerekçesiyle ve "yeterli güvence" bulunması halinde gibi sınırları açık olmayan iki kavramın belirlenmesi hususunda, bu derece önemli kişisel verilerin işlenmesine ilişkin geniş bir takdir yetkisi verilmesi, düşüncemize göre uygun olmayıp, bu takdir yetkisinin sınırlandırılması gerekmektedir[289].

Yedinci maddenin dördüncü fıkrasında, suçun soruşturulmasına, koruma ve kontrol tedbirlerine ve ceza mahkumiyetlerine ilişkin özel nitelikteki kişisel verilerin, ilgili kanunlarda yeterli koruma tedbiri bulunması kaydıyla, yetkili mercilerin kontrolü altında işlenebileceği belirtilmiştir. Bu fıkra ile getirilen düzenlemenin doğal bir sonucu, soruşturmaya konu olmuş bir kimsenin kişisel verilerinin, henüz

---

[287] **Küzeci**, s. 373.

[288] Aynı yönde bkz. **Küzeci**, s. 374, **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1204-1205; "*Tasarının 7. maddesinin üçüncü fıkrasında yer alan temel kamu yararları ibaresi, kişi hak ve hürriyetlerine müdahale yönünden keyfi uygulamalara yol açabilecek özellik taşımaktadır. Kanun koyucu temel kamu yararı kavramından ne anlaşılması gerektiğini açıklamamıştır. Birçok nedenin bu kavram kapsamına dahil edilmesi ve bu yolla bireyin özel nitelik taşıyan verilerinin işlenmesi mümkün olabilir.*"

[289] **Şimşek**, s. 209, **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1207, **Küzeci**, s. 374; "*KVKKT'nin 7/3 hükmü ise adeta özel nitelikteki kişisel verilerin diğerlerine göre daha düşük bir seviyede korunmasına neden olmaktadır. Nitekim hükümdeki koşullar yeteli güvence sağlamadığı gibi, burada yer alan türde bir istisna kişisel verilerin işlenmesinde genel hukuka uygunluk sebepleri arasında da yer almamaktadır. Bütün bu nedenlerden ötürü Tasarının 7/3 hükmünün metinden çıkarılması en doğru yaklaşım olacaktır.*"

Şen, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1207; "*Kişisel Verileri Koruma Kurulu'na tanınan bu geniş kapsamlı yetki çerçevesinde Kurul gerekli gördüğü hallerde, özel nitelikli kişisel veriler kapsamında yer alan kişilerin ırk, siyasi düşünce, dini inançları ve özel yaşamları gibi bilgilerin kayda alınmasına tek başına karar verebilecektir. Kurulun tek başına karar verme yetkisi elbette keyfi uygulamaların doğmasına neden olabileceği gibi, keyfi uygulamalar sebebiyle Anayasa'da yer alan kişi dokunulmazlığı, özel hayatın gizliliği ve korunması, kişilerin düşüncelerini açıklama ve yayma hürriyeti ihlal edilecek, böylece telafisi güç ve imkansız zararlar doğabilecektir.*"

işlediğinden şüphelenilen suçtan mahkum olmadan evvel işlenmeleri olacaktır. Dolayısıyla bu tür bir durumda, kişi hakkında koruma tedbirleri uygulanmışsa veya soruşturma açılmışsa, buna ilişkin özel nitelikteki kişisel veriler masumiyet karinesinin ihlal edilmesine yol açabilecek şekilde işlenebilecektir. Kaldı ki, bu maddede söz edilen kişisel veriler de alelade kişisel veriler değil, kanun koyucu tarafından özel bir düzenleme gerektirdiğine kanaat getirilmiş ve ilave koruma sağlanmış "özel nitelikli kişisel veriler"dir. Bu itibarla, Tasarıda böyle bir düzenlemenin yer alarak henüz mahkum olmamış, hakkında yalnızca soruşturma açılmış bir kişinin kişisel verilerinin kaydedilmesine izin verilmesi ve buna koruma olarak yalnızca "ilgili kanunlarda yeterli korumanın bulunması"nın gösterilmesi, düşüncemize göre son derece isabetsiz, kötüye kullanıma açık ve masumiyet karinesine aykırı olmuştur[290].

Tasarının 8 inci maddesinde üçüncü kişilere veri aktarımına ilişkin usuller düzenlenmiş, bu hususa ilişkin kurallar konulmuş, ancak "Millî güvenliğin ve millî savunmanın sağlanması, suçun önlenmesi veya soruşturulması amacıyla yapılan istihbarî faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi için gerekli olması halinde de kamu kurum ve kuruluşlarınca kişisel veriler ilgili kamu kurum ve kuruluşuna aktarılabileceği" belirtilerek bu kurallara istisnalar getirilmiştir. Getirilen istisnalar yine oldukça geniş tutulmuş, ancak ilgili kişinin rızasının bulunması hali bu istisnalar arasında yer almamıştır. Kanaatimizce, bu husus sekizinci maddeye ilave edilmeli, ilgili kişinin açık rızası bulunması halinde verilerin üçüncü kişilere aktarılabileceği kabul edilmeli, ancak bu rızanın yazılı olması ve veri öznesinin bu hususta aydınlatılmış olması aranmalı, getirilen istisnaların ise sınırları belirlenmeli ve istisnalar dar tutulmalıdır[291]. Maddenin dördüncü fıkrasında, yine fazla esnek olarak değerlendirilebilecek bir ifade mevcut olup, buna göre, "kamu kurum veya kuruluşlarının görev alanlarıyla ilgili konularda yapacakları talep üzerine, gizlilik esaslarına göre görev yapan personelin bilgileri hariç olmak üzere, kişilerin nüfus kayıt örnekleri ve adresleri bildirilir." Düzenlemede, üçüncü kişi olarak değerlendirilen kamu kurum veya kuruluşlarına bildirilecek olan nüfus kayıt örnekleri ve adresler ile ilgili spesifik bir belirleme yapılmamış ve bu verilerin hangi

[290] Aynı yönde, bkz. **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1207.
[291] Aynı yönde, bkz. **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1209-1210.

durumlarda ne kadarının aktarılacağı belirtilmemiştir. Böylece bu fıkradan sanki görev alanı ile ilgili her talepte kamu kurum ve kuruluşlarına herkesin nüfus kayıt örnekleri ve adreslerinin tamamının verilebileceği anlamı çıkmaktadır.

Tasarının 11 inci maddesinde, aydınlatma yükümlülüğü düzenlenmiş olup, ilk fıkrada, kişisel verilerin elde edilmesi sırasında veri kütüğü sahibinin, ilgili kişilere; veri kütüğü sahibi ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere aktarılabileceği, veri toplamanın yöntemi, hukukî sebebi ve muhtemel sonuçları, kişisel verileri öğrenme hakkı, düzeltme hakkı konularında bilgi vermekle yükümlü olduğu düzenlenmiş, ikinci fıkrada ise kişisel verilerin, ilgili kişi dışındaki kaynaklardan edinilmesi halinde de ilgili kişiye yukarıdaki bilgilerle birlikte işleme konu olan veri kategorileri hakkında bilgi verileceği belirtilmiştir. Bu madde de doktrinde eleştirilmiştir. Maddenin ele alınış şekline bakıldığında veri kütüğü sahibinin kişisel verileri elde ettikten sonra ilgili kişiyi bilgilendireceği ifade edilmiştir ve böylece sanki kişisel veriler toplanırken ilgili kişinin rızası alınmayacakmış gibi bir anlam çıkmaktadır[292]. Halbuki aydınlatma yükümlülüğü ile ilgili olarak düzenlenen bir maddede, ilgili kişinin rızasına mutlaka atıf yapılması gerekmektedir, zira madde incelendiğinde, ilgili kişinin rızası alınmaksızın kişisel verilerinin toplanacağı, bilgilendirmenin ise ancak veriler toplandıktan sonra yapılacağı izlenimi oluşmaktadır.

Tasarının 12 nci maddesinde, herkesin, veri kütüğü sahibine başvurarak; kendisiyle ilgili kişisel verinin kaydedilip kaydedilmediğini öğrenmek, kaydedilmişse bunları talep etmek, verinin muhtevasının eksik veya gerçeğe aykırı olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini veya aktarımının engellenmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini istemek hakkına sahip olduğu belirtilmiş, ancak aynı maddenin 3 üncü fıkrasında bu hakka da bir sınırlama getirilmiştir. Buna göre, kanaatimizce yine son derece geniş bir kısıtlama ile milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, suçun önlenmesi veya istihbarat amacıyla yapılan faaliyetlerle ilgili olarak kanundan doğan bir görevin

[292] **Beyli**, s. 73; "*…maddeden anlaşılan, kişisel verilerin toplanması sırasında ilgili kişilerin rızasına başvurulmayacağı, sadece maddede sayılan hususlarda ilgili kişilere bilgi verileceğidir. Yani Tasarı, kişisel veri sahibi tüm gerçek kişilerin, önceden verilerinin toplanmasına rıza gösterdikleri gibi bir sonuç yaratmaktadır.*"

yerine getirilmesi veya ceza soruşturması veya kovuşturmasına zarar verilmesinin engellenmesi hallerinde veri öznesinin bu hakkının sınırlandırılabileceği öngörülmüştür. Bu maddeye getirilen sınırlama ile, veri öznesinin yalnızca bilgi edinme hakkının mı, yoksa hukuka aykırı verilerin silinmesini, yok edilmesini ve aktarımının engellenmesini isteme hakkının da mı kapsama dahil edilip edilmeyeceği açıkça belirtilmemiştir. Ancak maddenin kaleme alınış şeklinden anlaşıldığı kadarıyla, üçüncü fıkrada belirtilen durumlarda, birinci fıkrada sayılan tüm haklar sınırlandırılabilecektir. Bu noktada eleştirilmesi gereken önemli bir husus, üçüncü fıkrada sayılan durumların varlığı halinde dahi, verinin muhtevasının eksik veya gerçeğe aykırı olması halinde bunların düzeltilememesi, hukuka aykırı olması halinde silinememesini, yok edilememesi veya aktarımının engellenmesidir. Düşüncemize göre, milli güvenlik, milli savunma gibi üçüncü fıkrada benzerleri sayılmış istisnai durumlarda dahi, kişisel bir veri hukuka aykırı olarak bulundurulmakta ise, bu tür verilerin düzeltilmemelerini veya tutulmaya devam edilmelerini hukuka uygun hale getirecek bir istisnanın bulunması mümkün olmamalıdır[293].

2003 tarihinde düzenlenen ilk tasarının 8 inci maddesine göre, "özel kanunda açıkça öngörülmüş olması, üstün nitelikte bir kamu yararı, özellikle Devletin iç ve dış güvenliğinin korunması açısından gerekli olması, bilgi verilmesinin idari veya cezai bir soruşturmanın amacının gerçekleştirilmesini güçleştirmesi" hallerinde, veri öznesinin bilgi edinme hakkı sınırlandırılabilecek, ancak sınırlamaya konulan bir sınırlamaya göre; veri kütüğü sahibi kısıtlamanın sebebini ilgili kişiye yazılı olarak bildirecek idi[294]. Düşüncemize göre, veri kütüğü sahibine getirilen bu yükümlülük yerinde olup, veri kütüğü sahibinin keyfi davranmasını önleyecek niteliğe sahip bulunmaktaydı, bu itibarla tasarının son haline veri kütüğü sahibine bu yükümlülüğün getirilmesinin dahil edilmemiş olması ve bilgi edinme hakkının

[293] Bkz. aynı yönde **Küzeci**, s. 376-377; "*Ancak Tasarının genelinde görülen bir sorunun burada da geçerli olduğunu belirtmek gerekir: geniş kapsamlı istisnalar, hükmün uygulanmasını ciddi oranda sınırlamaktadır… Burada yer alan ifadelerin kapsamının son derece geniş olması bir yana, belirtilen hükümde yer alan hakların bir bölümü açısından dar sınırlamaların bile kabul edilebilir bir yanı bulunmamaktadır… Eğer bir bilgi yanlışsa ona dayanılarak varılacak sonuç da yanlış olacaktır. Böylesine bir durumun yalnızca ilgili kişiye değil, veriyi işleyene de zarar vereceği açıktır. Dolayısıyla yanlış bilginin düzeltilmesini engellemenin makul bir nedeni bulunmamaktadır.*" Bu madde bakımından Küzeci, getirilecek herhangi bir sınırlamanın makul olamayacağını, bu itibarla bu maddede herhangi bir sınırlama getirilmemesi gerektiğini vurgulamaktadır.

[294] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s. 115.

sınırlandırılabileceği durumların öngörülmesi ile yetinilmiş olunması yerinde olmamıştır.

Tasarının 13 üncü maddesi ise doktrinde haklı olarak en çok eleştirilen maddelerden biridir, zira veri öznesinin Tasarıda veya kanuni düzenlemelerle getirilen sınırlamalar haricinde mutlak olması gereken bilgi edinme hakkı bu madde ile ücret şartına bağlanmıştır. Şöyle ki, Tasarının 13 üncü maddesine göre, "başvurunun yapıldığı veri kütüğü sahibi, erişimine olanak sağladığı bilgi veya belgeler için başvuru sahibinden erişimin gerektirdiği maliyet tutarı kadar, Kurul tarafından her yıl Ocak ayında belirlenecek miktarda bir ücret talep edebilecek", böylece maddi olarak daha güçsüz durumda olan veri öznesine karşı büyük oranda avantajlı konumda olacaktır. Bu şekilde bir düzenleme yapılmış olması, veri öznesinin kendi kişisel verileri ile ilgili olarak bilgi edinmesini önemli ölçüde sınırlandırabilecek, maddi gücü bu ücreti ödemeye yeterli olmayan kişilerin başvurudan vazgeçmelerine sebep olarak bilgi edinme hakkını kullanılamaz hale getirebilecektir[295]. Nitekim bakıldığında, bu sistemi uygulayan başka ülkelerin de olduğu görülmektedir. Ancak bu ülkelerde, maddeye "makul ücret" kavramının eklenerek, veri öznesinden hakkaniyete aykırı bir miktar talep edilemeyeceğinin vurgulandığı, ancak Türkiye'de hazırlanmış olan tasarıda böyle bir ifadenin yer almadığı görülmektedir.

Tasarının 14 üncü maddesinde[296], kişisel verilerin yurt dışına aktarılması ile ilgili genel kurallar düzenlemiş, bu aktarımın nasıl yapılacağı, hangi durumlarda kimden izin alınacağı düzenlenmiştir. Maddenin 3 üncü fıkrasında ise, yine diğer maddelerde olduğu gibi, esnek bir ifade ile geniş kapsamlı bir istisna getirilmiştir. Üçüncü fıkraya göre, "yabancı ülkede bulunan veri kütüğü sahibinin, eşdeğer ve

---

[295] Aynı yönde bkz. **Aksoy**, s. 117, **Beyli**, s. 74.

[296] Tasarının "Yurtdışına Bilgi Aktarımı" başlıklı 14 üncü maddesinde *"(1) Kişisel veriler, ancak kişilik haklarının korunması açısından verinin istendiği yabancı ülkede eşdeğer ve etkin koruma bulunuyorsa yurtdışına aktarılabilir.*
5(2) Verinin istendiği ülkede eşdeğer ve etkin bir koruma olmasa dahi;
a) İlgili kişinin açık rızasının bulunması,
b) İlgili kişi ile veri kütüğü sahibi arasında bir sözleşmenin yapılması, sözleşme öncesi ilişkinin yürütülmesi veya sözleşmenin ifası için aktarımın gerekli olması,
c) Suçun önlenmesi veya bir hakkın tespiti, icrası veya korunması için aktarımın gerekli veya kanun gereği zorunlu olması,
ç) Veri konusu kişinin hayatı veya beden bütünlüğünün idamesi için aktarımın zorunlu olması,
d) Veri aktarımının, ilgili mevzuatın aradığı şartları yerine getirmek koşuluyla kamunun veya ilgisini ispat eden herkesin erişimine açık bulunan sicillerden yapılması,
hallerinde kişisel veriler yurtdışına aktarılabilir." denilmektedir.

uygun bir korumayı yazılı olarak taahhüt etmesi ve Kurulun izninin bulunması halinde de kişisel veriler yurtdışına aktarılabilir. Ancak, gecikmesinde sakınca bulunan veya telafisi güç veya imkansız zararların doğması ihtimali bulunan hallerde, veri kütüğü sahibi kişisel verileri yurtdışına aktarabilir." Maddede bahsi geçen Kurul, Tasarı'nın 2 nci maddesindeki tanımlar kısmında tanımlandığı üzere, Kişisel Verileri Koruma Kurulu'dur. Her ne kadar doktrindeki bazı yazarlar fıkranın yanlış kaleme alınmış olmasından kaynaklı bir sorun olduğunu, Kurul'un bilgiler gönderildikten sonra icazet vermesi değil, gönderilmeden önce izin vermesi gerektiğini savunsalar da, bu fıkra okunduğunda, fıkradan açıkça ortaya çıkan anlam, yurtdışına kişisel veri aktarımının eşdeğer koruma bulunması ve Kurul'un izni şartlarına bağlı olduğu, ancak gecikmesinde sakınca bulunan veya telafisi güç veya imkansız zararların doğması ihtimali bulunan hallerde bu şartların bulunmasına gerek olmaksızın Türkiye'deki veri kütüğü sahibinin istediği tüm kişisel verileri yurtdışına aktarabileceğidir. Tasarının 4 üncü maddesi kanunilik ilkesine vurgu yapmakta, Genel Gerekçe'de ise veri öznesinin korunmasından söz edilmektedir. Bu fıkrada yer alan ifadenin ise, ne kanunilik ilkesine ne de ilgili kişileri korumaya uygun olduğundan bahsetmek mümkün değildir. Bu düzenleme ile yine fıkranın ilk cümlesinde ilgili kişileri koruyucu bir ifade sevk edilmiş, ancak ikinci cümlede getirilen istisna ile ilgili kişinin hakları neredeyse yok sayılarak veri kütüğü sahibine çok geniş bir yetki tanınmıştır. Bu noktada yapılacak sınırlamada, kişisel verinin aktarımı için gecikmesinde sakınca bulunan veya telafisi güç veya imkânsız zararların doğması ihtimali bulunan hallerin neler olduğu, bu hallerin bulunup bulunmadığına herhangi bir merciin mi yoksa buna veri kütüğü sahibinin kendisinin mi karar vereceği, böyle bir durumda, ilgili kişilerin tüm kişisel verilerinin mi yoksa yalnızca amaçla bağlı olmak üzere bir kısım verilerinin mi aktarılacağı hususu, sınırlama getiren bu fıkrada yer almayarak büyük bir boşluk oluşturmaktadır.

14 üncü maddenin üçüncü fıkrasının son cümlesinde, bu halde veri kütüğü sahibinin, durumu yirmidört saat içerisinde Kurula bildireceği, Kurul'un, veri aktarımının bu Kanun hükümlerine uygun olup olmadığı hususunda inceleme yaparak bir karar vereceği belirtilmiştir. Bu ifadeden çıkan anlama göre ise, Kurul veriler aktarıldıktan sonra devreye gireceğine göre, böyle bir halin bulunup bulunmayacağına karar verecek olan kişi veri kütüğü sahibinin bizzat kendisi olacaktır ki; bu, her tür kötüye kullanımın önünü açmakta, veri öznelerini son derece

savunmasız hale getirmektedir. Durumu daha da vahim hale getiren husus ise, veri kütüğü sahibi, üçüncü fıkrada zikredilen bir durumun varlığının mevcut olduğuna inanarak, kişisel verileri, yurtdışında eşdeğer bir koruma bulunup bulunmadığına bakmaksızın kendi inisiyatifi ile yurtdışına aktardıktan sonra, Kurul'un yapılan veri aktarımının kanun hükümlerine uygun olmadığına karar vermesi halinde ne olacağının belli olmamasıdır. Kişisel veriler elektronik ortamda, eşdeğer korumaya sahip olmayan bir başka ülkeye aktarıldıktan sonra, yapılan aktarım hukuka aykırı ise veya Kurul gecikmesinde sakınca bulunan bir hal olmadığına karar verirse, artık o kişisel verilere Türkiye'den herhangi bir koruma sağlanması mümkün olmayacak; dolayısıyla bir kere aktarım yapıldıktan sonra, yurtdışında eşdeğer koruma yoksa, esas o zaman ilgili kişiler için telafisi imkansız zararlar doğacaktır[297]. Tasarı kanunlaşmadan evvel kanun koyucunun mutlaka bu maddeyi gözden geçirmesi, telafisi mümkün olmayan zararlı neticeler doğurma ihtimali son derece yüksek olan bu istisnayı Tasarı metninden çıkarması ve yurtdışına yapılacak aktarımlarda bu maddenin 2 nci fıkrasında düzenlenen istisnaları yeterli görmesi gerekmektedir.

Tasarının 22 nci maddesinin ilk fıkrasında ise, bazı maddeler açısından istisnalar getirilmiş, bu istisnai hallerde 22 nci maddede değinilen maddelerin uygulanmayacağı belirtilmiştir[298]. 22 nci maddede getirilen istisnaların bulunması halinde uygulanmayacak olan maddeler ise; hukuka uygunluk sebepleri (m.6), aydınlatma yükümlülüğü (m.11), veri kütüğü sicili (m.16), sicile kayıt başvurusu (m.17), ön inceleme (m.19) ile ilgili olanlardır. Bu maddeler, kişisel verilerin korunması açısından son derece önemli maddeler olmakla birlikte, bunların bu şekilde geniş ve sınırları belirsiz şekilde sınırlandırmaya tabi tutulmaları, ne yazık ki istisnaları kaide, kişisel verilerin korunmasını ise adeta istisna haline getirmiştir.

---

[297] Aynı yönde, bkz. **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1210.

[298] Tasarının 22 nci maddesinde, "*(1) Bu Kanunun 6 ncı, 11 inci, 16 ncı, 17 nci ve 19 uncu maddeleri aşağıda sayılan haller bakımından uygulanmaz:*
a) Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbarî faaliyetlerin yürütülmesi,
b) Kamu düzeninin korunması,
c) Suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlal eden eylemlerin soruşturulması veya kovuşturulması,
ç) Bütçe, vergi ve mali konulara ilişkin olarak Devletin önemli ekonomik veya malî çıkarlarının gerektirmesi,
d) Bu fıkranın (b), (c) ve (ç) bentlerinde belirtilen konularda, resmî mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi." denilmektedir.

22 nci maddenin ikinci fıkrası, düşüncemize göre sakıncalıdır. Zira bu fıkraya göre Tasarının "… 12 nci maddesinde belirtilen haklar, kişisel verilerin özellikle belli bir kişiye ilişkin tedbir veya karar alınmasına yönelik kullanılmadığı ve ilgili kişinin özel yaşamının gizliliğinin ihlal edilmesi riskinin bulunmadığı hallerde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, bilimsel araştırma veya istatistik oluşturma amaçları ile sınırlanabilecektir." 12 nci madde ise ilgilinin bilgi edinme hakkına ilişkindir. Fıkradaki ilk sorun "sınırlandırılabilir" ifadesine ilişkindir. Bu ifade geniş kapsamlı bir ifade olmakla birlikte, 12 nci maddede pek çok haktan bahsedildiği için, bunların hangisinin veya hangilerinin 22 nci madde ile sınırlandırılabileceğine ilişkin net bir bilgi verilmemektedir. Dolayısıyla maddenin bu haliyle kanunlaşması durumunda, bilimsel araştırma ve istatistik oluşturma amacıyla, veri özneleri 12 nci maddede kendilerine sağlanmış olan hakların tamamından da yoksun bırakılabileceklerdir ve bu sınırlamanın neye göre yapılacağı maddede belirtilmemiştir. Bu durumda örneğin belirli bir bilimsel araştırma açısından kişilerin yalnızca verinin hukuka aykırı olması halinde sildirme hakkı sınırlandırılabileceği gibi, benzer bir araştırma için ilgilinin hem verinin kaydedilip kaydedilmediğini öğrenme hem de sildirme hakkı sınırlandırılabilecektir ki; bunun uygulamada keyfiliğe yol açabileceği muhakkaktır. Son olarak değinilmesi gereken nokta ise, orantılılık ilkesidir. Bir bilimsel araştırma veya istatistik oluşturmanın önemi ile kişilerin kendi kişisel verilerinin akıbetini öğrenebilme haklarının korunmasının öneminin mutlaka orantılılık ilkesi çerçevesinde ele alınması ve kişisel veriler hakkında ilgilinin bilgi edinme hakkının ancak bu sınırlamanın orantılı olması koşuluyla yapılabilmesi gereklidir. Tasarı kanunlaşmadan evvel, mutlaka bu maddenin gözden geçirilmesi ve yapılacak sınırlamalarda bu paragrafta değinilen hususlara dikkat edilmesi gerekmektedir.

22 nci maddede sayılan hallerde sınırlandırılabilecekleri öngörülen hakların ne koşullarda sınırlandırılabilecekleri açıkça belirtilmemiş ve yine son derece geniş bir ifade tercih edilmiştir. Doktrinde ileri sürülen ve bizim de katıldığımız görüşe göre, bu madde kişisel verilerin korunması hakkının istisnalarını genel olarak düzenleyen bir madde olduğundan, bu düzenleme yapılırken Avrupa İnsan Hakları Sözleşmesi'nin 8 inci maddesinde öngörülmüş olan istisnalar ile bu istisnaların Avrupa İnsan Hakları Mahkemesi tarafından bugüne kadar içtihatlarla oluşturulan yorumu ve kişisel verilerin korunması hakkı Anayasal bir hak olarak

değerlendirildiğinden, Anayasanın 13 üncü maddesi de dikkate alınarak düzenlenmelidir[299].

Tasarının 26 ncı maddesinde, bir denetim organı olarak Kişisel Verileri Koruma Kurulu'nun kuruluş amacı düzenlenmektedir. Buna göre Kişisel Verileri Koruma Kurulu tasarıda verilen görevleri yapmak üzere oluşturulmuştur ve "kurul, yetkilerini bağımsız olarak kullanır. Hiçbir organ, makam, merci ve kişi Kurulun kararını etkilemek amacıyla emir ve talimat veremez." 26 ncı maddede ve Tasarının gerekçesinde bağımsızlığına vurgu yapılan denetim organının, 27 nci maddeye göre 7 üyesinin tamamının Bakanlar Kurulu tarafından seçilmesi, Kurul'un bağımsızlığını zedeleyen, hatta ortadan kaldırabilecek bir durumdur; zira üyelerin hepsinin yürütme organı olan Bakanlar Kurulu tarafından seçilmesi, ileride Kurul'un işleyişinde üyelerin etki altında kalmaları olasılığını artırabilecektir[300]. Kaldı ki, aynı maddenin son fıkrasına göre Kurul'un başkanı da Bakanlar Kurulu tarafından seçilmekte, böylece kurul tamamıyla Bakanlar Kurulu'nun bir uzantısı haline gelmektedir. Nitekim diğer ülkelerin veri koruma birimlerine veya kurullarına bakıldığında[301];

- Fransa'da 17 üyeden oluşan birimin 2 üyesi Senato'dan, 2 üyesi Ulusal Meclis'ten, 2 üyesi Ekonomik, Sosyal ve Çevre Konsey'inden, 2 üyesi Conseil d'Etat'dan (Danıştay), 2 üyesi Cour de Cassatition'dan (Yargıtay), 2 üyesi Cour des Comptes'dan (Sayıştay), 3 üyesi kişisel hürriyetler veya bilişim alanında uzman kişilerden kararname ile, 2 üyesi bilişim sistemleri alanında uzman kişilerden biri Senato Başkanı tarafından, biri de Meclis Başkanı tarafından seçilmekte[302],

---

[299] **Küzeci**, s. 378.

[300] Aynı yönde bkz. **Şimşek**, s. 212-213, **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1211-1212, **Uzeltürk**, s. 3154, Kanun Tasarısı Hakkında Türkiye Bilişim Vakfı Görüşü, 2003, s. 5, http://www.tbv.org.tr/TBV/Documents/BTHukuku/KisiselVerilerinKorunmasiKanunTasarisi-TBVGorus.pdf, 28.12.2011, **Kalaycı**, **Emre**, "Haberleşme Özgürlüğü ve Kişisel Bilgilerin Korunması", Elektrik Mühendisleri Odası İzmir Şubesi Aylık Bülteni, Temmuz 2008, s. 35-36, http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/200807_Emre.pdf, 02.01.2012; "*Nitekim Türkiye Bilişim Vakfı Genel Sekreteri Behcet Envarlı ile İnternet ve Hukuk Portalı Yürütme Kurulu Üyesi Av. Fikret İlkiz, bu konuda yapılan bir tartışma programında tasarının kişisel verilerin korunması amacıyla getirdiği yasaklara yasaklardan fazla geniş kapsamlı istisnalar getirilmesi hususunu ve Kişisel Verileri Koruma Kurulu'nun atanmasında tüm üyeleri atama yetkisinin yürütme erkinde olmasını eleştirmişler, bu koşullarda seçilmiş olan bir Kurul'un denetim görevini icra ederken bunu bağımsız bir şekilde yapamayacağını haklı olarak dile getirmişlerdir.*"

[301] **Başalp**, **Nilgün**, "Bağımsız Veri Koruması Kurumlarının Yapısı" Bilişim Hukukunun Son 10 Yılı Sempozyumu, www.erzincan.edu.tr/gundem.php?al=86, 14.03.2011.

[302] "Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée", madde 13, http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf, 08.01.2012.

- Avusturya'da tüm üyeleri Cumhurbaşkanı seçmekte olup, Cumhurbaşkanı'na sunulacak öneriyi hazırlayan Başbakan ise 6 üyeyi şu şekilde belirlemektedir; Avusturya Yüksek Mahkemesi Başkanı'nın önereceği üç hakimden biri, eyaletlerin önereceği adaylardan ikisi, İş ve İşçi Bulma Kurumu'nun önereceği üç adaydan biri, Avusturya Ticaret Odası'nın önereceği üç adaydan biri, seçilmekte olup, atanacak olan kişilerin hukuk eğitimi almış olmaları ve veri korumasında bilgi ve tecrübe sahibi olmaları gerekmekte[303],

- Almanya'da Federal Veri Koruma Yetkilisi en az 35 yaşında olmak şartıyla, Federal meclis tarafından bir defa yenilenebilirlik ile 5 yıllığına seçilmekte, Cumhurbaşkanı tarafından atanmakta ve İçişleri Bakanlığının idari gözetimine tabi olup şayet bu kişi geçici süre ile görevini sürdüremeyecek durumda bulunursa, İçişleri Bakanı bu göreve vekaleten bakmakta[304],

- İtalya'da "Garante" adı verilen veri koruması birimi kararlarını verirken bağımsız ve otonom hareket etmekte, 4 üyeden oluşan birimin 2 üyesi Bakanlar Kurulunca, diğer 2 üyesi ise Senato tarafından atanmakta, bu üyelerin hukuk veya bilişim sistemleri alanında uzman, bunlardan en az biri alanında da deneyim sahibi olmaları gerekmektedir[305].

Yukarıda sayılan örnek ülkelerde de görüldüğü üzere, denetimle görevli olan kurulların üye seçimlerinde, genelde üyeler bakımından çeşitliliğe yer verildiği ve üyelerin seçimine birden fazla kurumun dahil edildiği görülmektedir. Halbuki Tasarımızdaki düzenlemeye göre, Kurulun üyelerinin seçilmesi usulü göz önüne alındığında, çeşitlilikten söz etmek mümkün değildir, zira Kurul üyelerinin tamamı Bakanlar Kurulu tarafından atanmaktadır.

Tasarı ile ilgili olarak değineceğimiz son maddeler ise 34, 35 ve 36 ncı maddelerdir. Bu maddelerde, kişisel verilerin hukuka aykırı olarak kaydedilmeleri,

---

[303] "Federal Act concerning the Protection of Personal Data", §36, http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf, 08.01.2012.

[304] "Federal Data Protection Act (BDSG)", madde 22, yürürlük tarihi; 1 Eylül 2009, http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile , 08.01.2012.

[305] 30 Haziran 2003 tarihli "Personal Data Protection Code", madde 153, http://www.garanteprivacy.it/garante/document?ID=1219452, 08.01.2012.

ele geçirilmeleri, ifşa edilmeleri ve kişisel verileri silmekle yükümlü olanların bu verileri yok etmemeleri hususlarına değinilmiş, bununla ilgili olarak, aşağıda ayrıntılı olarak açıklayacağımız Türk Ceza Kanunu'nun ilgili hükümlerine göndermede bulunulmuştur. Buna göre, kişisel verileri hukuka aykırı olarak kaydeden kimseler TCK'nın 135 inci maddesi uyarınca, kişisel verileri hukuka aykırı olarak açıklayan, yayan, veren, aktaran veya ele geçiren kişiler TCK'nın 136 ncı maddesi uyarınca, görevleri gereği yok etmekle yükümlü oldukları kişisel verileri yok etmeyen kişiler ise TCK'nın 138 inci maddesi uyarınca cezalandırılacaklardır.

Tasarının 34 üncü maddesinin ilk fıkrasında, "hukuka aykırı olarak üçüncü fıkrada belirtilenler dışında kişisel verileri işleyen kişi, Türk Ceza Kanununun 135 inci maddesinin birinci fıkrasına göre cezalandırılacağı" belirtilmiş, ikinci fıkrada ise "Birinci fıkrada yazılı fiilin, bu Kanunun 7 nci maddesinde düzenlenen özel niteliği olan kişisel veriler hakkında işlenmesi halinde de birinci fıkrada belirtilen cezaya hükmolunacağı" düzenlenmiştir. Türk Ceza Kanunu'nun 135 inci maddesinde de, buna benzer bir düzenleme yer almakta olup, ilk fıkrada kişisel verilerin hukuka aykırı olarak kaydedilmesi durumunda failler açısından altı aydan üç yıla kadar hapis cezası öngörülmüş, ikinci fıkrada ise özel nitelikli kişisel veriler sayılarak, bunların hukuka aykırı olarak kaydedilmelerinin ilk fıkradaki hükme göre cezalandırılacağı belirtilmiştir. Aşağıda ilgili başlık altında bu konuya ilişkin eleştirilerimiz detaylı olarak yer alsa da[306], Tasarı'da da benzer bir hükme yer verilmiş olduğundan bu konuya kısaca değinilmesi yerinde olacaktır.

Hem Tasarı'nın yedinci maddesinin ikinci fıkrası, hem de TCK'nın 135 inci maddesinin ikinci fıkrası, özel nitelikteki kişisel verilerin kaydedilmesi hususunu zikretseler de, hiçbir işlevleri bulunmamaktadır. Zira özel nitelikteki kişisel verilerin hukuka aykırı olarak kaydedilmeleri TCK m. 135'te cezayı artıran nitelikli hal olarak düzenlenmesi gerekirken, maddede bu fiil açısından diğer kişisel verilerin kaydedilmesiyle aynı yaptırım öngörülmüştür. Hassas nitelikteki kişilerin diğer kişisel verilerin hukuka aykırı olarak kaydedilmesiyle aynı yaptırıma tabi tutulması son derece hatalı olup, bu hata Tasarı'daki hüküm (7 nci madde) ile tekrarlanmıştır. Bunun neticesinde ise, özel nitelikteki kişisel verilerin hukuka aykırı olarak kaydedilmesi ile diğer kişisel verilerin kaydedilmesi arasında kanun koyucu

[306] Bkz. "*5237 Sayılı Türk Ceza Kanunu'nda Kişisel Verilere İlişkin Düzenlemeler*" başlığı altında "*TCK m.135: Kişisel Verilerin Kaydedilmesi*" alt başlığı.

tarafından Türk Ceza Kanunu'nda hiçbir ayrım yapılmamış, Tasarı'da da aynı düzenlemenin getirilmesi isabetsiz olmuştur. Kanaatimizce, Tasarı kanun haline getirilmeden önce Türk Ceza Kanunu'nda bu hususla ilgili gerekli değişiklik yapılarak hassas nitelikli kişisel verilerin hukuka aykırı olarak kaydedilmesi fiilinin cezanın artırılmasını gerektiren nitelikli bir unsur olarak düzenlenmesi, Tasarı'daki ifadelerin de buna uygun olarak yeniden kaleme alınması gerekmektedir.

Sonuç olarak Tasarının geneline bakıldığında, veri öznelerinin haklarını koruma amaçlı düzenlenmiş olan bu Tasarının gerekli korumayı sağlamaktan oldukça uzak olduğu görülmektedir. Kişilerin haklarını korumaya yönelik getirilen her düzenlemede, korumayı düzenleyen maddenin alt fıkralarına mutlaka istisnalar getirilmiş ve Tasarının genelinde bu istisnalar birden fazla oldukları gibi, son derece muğlak ve geniş ifadelerle kaleme alınmışlardır. Her maddeye ayrı ayrı getirilen istisnalara ek olarak bir de genel istisnalar getiren ayrı bir madde (22 nci madde) de düzenlenmiştir. Tasarının bu haliyle kanunlaşması halinde, veri öznelerinin haklarından ziyade, kişisel verileri işleyenlerin haklarını korumaya yönelik bir kanun ortaya çıkmış olacak ve kişisel verilerinin özellikle elektronik ortamlarda işlenmesini ve yayılmasını denetlemekte zorlanan veri öznelerine çıkacak kanun ile belirli bir güvence getirilmiş olmaktan ziyade, bu tür verileri işleyenlerin eylemleri kanuni bir zemine oturtulmuş olacaktır. Bu itibarla Tasarının mutlaka gözden geçirilmesi, getirilmiş olan istisnaların daraltılması ve istisna getirilecekse bunların açık ve net ifadelerle düzenlenerek herhangi bir hukuka aykırılığa mahal vermeyecek bir zemine oturtulmaları gerekmektedir.

B. DNA Verilerinin Tasarı ve Ceza Muhakemesi Kanunu Kapsamında Korunması

DNA analizi yapmak ve yapılan analizler sonucunda elde edilen DNA profil ve bilgilerinin tutulması için bir DNA veri bankası kurulması fikri uzun senelerdir Türkiye'de tartışılmaktadır. İlk olarak 1998 yılında gündeme gelen bu husus[307], DNA Verileri ve Millî DNA Veri Bankası Kanunu Tasarısı adı altında, 4 Mayıs 2007 tarihinde Adalet Bakanlığı tarafından sevk edilmiş olup, 3 Ekim 2007'de

[307] **Atasoy**, **Sevil**, "DNA Bankasında Karar Zamanı", 19.11.2006, Hürriyet Gazetesi, http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=5464077&yazarid=145, 27.12.2011.

yenilenerek[308] Başbakanlığa gönderilmiş, ancak 14 Nisan 2008 tarihinde Başbakanlık tarafından iade edilmiştir[309]. Tasarı, günümüzde halen kanunlaşmış değildir, bu sebeple yapılan DNA analizleri ve buna ilişkin usul ve esaslar Ceza Muhakemesi Kanunu'nun (CMK) aşağıda inceleyeceğimiz ilgili maddelerine göre yapılmaktadır.

DNA veri bankası fikri, suçla mücadele açısından gerçekten faydalı olabilecek bir konu olmasına rağmen, hukuki açıdan ve kişilerin özel yaşamlarının gizliliğinin korunması bakımından doğru düzenlemelerle şekillendirilmezse son derece sakıncalı olabilecek bir durumdur. Bu sebeple analizler sonucunda elde edilecek olan ve kişisel veri niteliğindeki DNA verilerinin toplanması, kullanılması ve saklanması ile ilgili titiz bir çalışma yapılmalı, Avrupa Birliği standartlarına uyumsuzluk göstermeyecek, diğer ülkelerin düzenlemesine paralellik gösterecek bir düzenleme yapılmalıdır; zira kurulacak olan DNA veri bankası Türkiye'deki suçla mücadele açısından önem arz edeceği gibi, başka ülkelerle ortak yapılacak suçla mücadele operasyonlarına ve bu bilgilerle karşılıklı bilgi alışverişine de hizmet edecektir.

1995 yılında kurduğu veri bankası ile, DNA veri bankası kurulmasında öncü olan ülke İngiltere olmakla beraber, Portekiz, İtalya ve İspanya istisna olmak üzere, pek çok ülke de bu seyri takip etmiş ve kendi DNA veri bankalarını kurmuşlardır. İngiltere'de suçların öngördükleri hapis cezasına bakılmaksızın trafik kurallarını ihlal etmek gibi suç veya kabahatlerde dahi, daha az cezayı gerektiren suçlar işleyen bu kişilerin gelecek dönemlerde daha ciddi suçlar işleyebilecekleri düşüncesinden hareketle DNA profilleri alınarak veri bankasında muhafaza edilmektedir[310]. Avusturya ve Slovenya'da da İngiltere'deki sistem benimsenerek her suç tipinde faillerin DNA profili alınmaktadır. Ülkeler açısından veri bankası kurulurken karşılaşılan en büyük engel toplumun tepkisi olmaktadır, nitekim bazı ülkeler bu tepkilere karşılık veri bankasını düzenleyen kanunlarına bir takım sınırlayıcı hükümler koymuşlardır. Bazı ülkelerde ise yalnızca suçların faillerinden, bazılarında ise alınan hapis cezasının yalnızca belirli bir zaman sınırı üzerinde olanların DNA profili alınarak bir ayrım getirilmiştir. Örneğin Fransa'da yalnızca belirli suçlardan

[308] Tasarının son hali için bkz. http://www.kgm.adalet.gov.tr/gg/dna.pdf 20.12.2011.
[309] Cihan Haber Ajansı, "Başbakanlık Milli Dna Veri Bankası Kanunu Tasarısını İade Etti", 04.12.2011, http://www.sondakika.com/haber-basbakanlik-milli-dna-veri-bankasi-kanunu-tasarisi-3167637/, 26.12.2011.
[310] **Atasoy**, **Sevil**, "DNA Bankasında Karar Zamanı", 19.11.2006, Hürriyet Gazetesi, http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=5464077&yazarid=145, 27.12.2011.

mahkum olanların DNA profili alınırken, İsveç'te iki yıldan, Hollanda'da ise sekiz yıldan fazla hapis cezası alanların DNA profilleri alınıp bankalarda saklanmaktadır[311]. İsviçre'de ise, DNA verileri, 2000 yılında çıkarılan bir kararname ile basit şüpheye dayanılarak suç işlendiğinden veya suça iştirak ettiğinden şüphelenilen kişilerin DNA verileri herhangi bir kanuni dayanağı olmaksızın saklanmakta ve bu durum ciddi şekilde eleştirilmektedir[312].

İngiltere, Finlandiya, Avusturya ve Norveç elde ettikleri profilleri süresiz saklarken, diğer ülkelerin çoğunda profiller 5 ila 20 yıl arasında değişen sürelerde silinmektedir. Şüphelilerden alınan biyolojik örnekleri ileride yeni incelemelere olanak verecek şekilde muhafaza eden ülkelerden Avusturya, Finlandiya, İngiltere, Slovenya Danimarka, Macaristan ve İsviçre'nin aksine, diğer ülkelerde bu veriler imha edilmektedir[313].

Türkiye'nin henüz bir DNA veri bankası olmamakla birlikte, bu alanda yapılan çalışmaların ilerlemesi ve diğer ülkelerin bu hususta gösterdikleri gelişme neticesinde, yukarıda değinilen tasarının yakında kanunlaşacağı ve Türk Hukuku'nda yerini alacağı muhakkaktır. Bu başlık altında da, Türkiye'de mevcut durumda DNA analizinin hangi hukuki esaslara dayanılarak yapıldığı, tasarının kanunlaşması halinde ne gibi yenilikler getireceği ve tasarıdaki düzenlemelerin önemli görülen bazı kısımları değerlendirilecektir.

1. Ceza Muhakemesi Kanunu'ndaki Düzenleme

Anayasa'nın "Kişinin Hakları ve Ödevleri" başlıklı ikinci bölümünde yer alan "Kişinin Dokunulmazlığı, Maddî ve Manevî Varlığı" başlıklı 17 nci maddesinin ikinci ve üçüncü fıkralarına göre, "Tıbbî zorunluluklar ve kanunda yazılı haller dışında, kişinin vücut bütünlüğüne dokunulamaz; rızası olmadan bilimsel ve tıbbî deneylere tabi tutulamaz. Kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tabi tutulamaz." Dolayısıyla, vücuttan örnek alınması da kişinin vücut bütünlüğüne müdahale anlamına

---

311 **Atasoy**, **Sevil**, "DNA Bankasında Karar Zamanı".
312 **Akyürek**, s. 52.
313 **Atasoy**, **Sevil**, "DNA Bankasında Karar Zamanı".

geldiğinden, Ceza Muhakemesi Kanunu[314] kapsamında yapılacak müdahaleler, Anayasa'nın 13 üncü maddesi gereğince ancak kanunla düzenlenecek ve yapılan sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacaktır[315].

Türkiye'deki mevcut uygulamada DNA incelemesine ilişkin yapılan işlemler Ceza Muhakemesi Kanunu'nun ilgili hükümlerine göre yapılmaktadır. Kanunun 75 ve 76 ncı maddelerine göre, şüpheli veya sanığın ve mağdurun beden muayeneleri yapılabilmekte, bu muayene neticesinde vücuttan örnek alınabilmektedir[316]. Kanunda yapılan düzenlemeyle, bu husus, şüpheli veya sanığın muayenesi ve vücudundan örnek alınması ile diğer kişilerin beden muayenesi ve vücudundan örnek alınması olmak üzere ikiye ayrılmıştır[317]. Alınan bu örnekler üzerinde ise "Moleküler Genetik İncelemeler" başlığı ile düzenlenmiş olan 78 inci madde uyarınca DNA analizi yapılabilmektedir. Maddeye göre, "75 ve 76 ncı maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler yapılabilmektedir" ancak "alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır." 79 uncu maddede ise bu incelemenin yapılmasına karar verme yetkisinin münhasıran hakimde olduğu belirtilmiş olup, incelemelerin yapılması için atanacak olan bilirkişilerin "teknik ve teşkilat bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlü" oldukları öngörülmüştür. Bu konu ile ilgili olarak CMK'da yer alan son madde ise 80. maddededir ve bu maddede "75, 76 ve 78 inci Madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçlarının, kişisel veri niteliğinde olup, başka bir amaçla kullanılamayacakları; dosya içeriğini öğrenme

---

[314] Ceza Muhakemesi Kanunu, K.n. 5271; R.G.t. 17.12.2004, S. 25673.

[315] **Centel**, **Nur-Zafer**, **Hamide**, Ceza Muhakemesi Hukuku, 8. Baskı, İstanbul, Ekim 2011, s. 269 - 270.

[316] Ceza Muhakemesi Kanunu'nun 75 ve 76 ncı maddelerinin uygulanışı hakkında ayrıntılı bilgi için bkz. **Öztürk**, **Bahri-Erdem**, **Mustafa Ruhan**, Uygulamalı Ceza Muhakemesi Hukuku, 12. Baskı, Ankara, Kasım 2008, s. 622 - 634, **Öztürk**, **Bahri-Erdem**, **Mustafa Ruhan-Sırma**, **Özge-Saygılar**, **Yasemin F.-Alan**, **Esra**, Ana Hatlarıyla Ceza Muhakemesi Hukuku, 1. Baskı, Ankara 2010, s. 323-336.

[317] **Mahmutoğlu**, **Fatih Selami**, "Beden Muayenesi Ve Vücuttan Örnek Alınması", s. 2, https://docs.google.com/viewer?a=v&q=cache:n3ORpGq-MuMJ:cezahukuku.istanbul.edu.tr/ders-gerecleri/cmh/makale/bedenmuayenesi.doc+t%C4%B1bbi+muayene+fatih+selami+mahmuto%C4%9Flu&hl=tr&gl=tr&pid=bl&srcid=ADGEESjMfeKA8ljstyikRAlkKq1sUpT_pkNMKnJo_mOHiAqUYFXF-rAYlSPqTB_3K8Uyrxx55CgTVLYT7AaXkMSFbC6dELe_zgdHl3oSmDYszwqQZHQEr5f-iaNEVAEKLqD3qgJL2kOz&sig=AHIEtbRR10D8T20MWiH3Y4CyWbq2Ic3K3A, 06.05.2012.

yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyecekleri" ve "bu bilgilerin, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet savcısının huzurunda derhal yok edilecekleri ve bu hususun dosyasında muhafaza edilmek üzere tutanağa geçirileceği" düzenlenmiştir.

Gen analizi olarak adlandırılan inceleme dörde ayrılmakta olup; bunlar fenotip analizi, kromozom analizi, proteinkimyasal analiz ve DNA analizidir ve yukarıda incelenen Ceza Muhakemesi Kanunu maddelerinde düzenlenmiş olan moleküler genetik inceleme ile kastedilen ise DNA analizidir[318]. Nitekim DNA Verileri ve Millî DNA Veri Bankası Kanunu Tasarısı'nda "DNA verileri", "DNA analizi", "DNA profili" gibi terimler kullanılarak bu husus ortaya konmuş, buna ek olarak "Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik"[319] in 3 üncü maddesinde, moleküler genetik inceleme, "Gereken tür ve miktardaki biyolojik materyali kullanarak, kişiyi diğer kişilerden ayıran ve kalıtım kurallarına uygun olarak aktarılan hastalık dışındaki özelliklerinin moleküler düzeyde araştırılması" olarak tanımlanmıştır. Bu itibarla, "Ceza Muhakemesi Kanunu'nda ve Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik'te", "DNA Analizi" yerine moleküler genetik inceleme teriminin kullanılmış olması, aynı konuda düzenleme getiren kanunlar arasında terim farklılığı doğuracağı için doktrinde eleştirilmiştir[320]. Bu Yönetmeliğin 14 üncü maddesinde de yönetmeliğe göre toplanmış olan verilerin gizliliğine ilişkin özel bir madde sevk edilmiştir[321].

---

[318] **Altaş**, **Ebru**, "Bir Koruma Tedbiri Olarak Moleküler Genetik İncelemeler ve DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı", Ceza Hukuku Dergisi, Sayı:1 Nisan 2007, s. 79

[319] Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, R.G.t. 01.06.2005, S. 25832.

[320] **Özbek**, **Veli Özer**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", Ceza Hukuku Dergisi, Sayı:1 Nisan 2007, s. 71.

[321] Bu husus Yönetmeliğin 14 üncü maddesinde, "*Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.*

Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir. Olay yerinden elde edilen diğer delillere ilişkin hükümler saklıdır.

Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir.

Moleküler genetik incelemelerin özel kalıtsal karakterler hakkındaki açıklamayı içermediği bilinen kromozom bölgesi ile sınırlı kalmasına özen gösterilir." şeklinde düzenlenmiştir.

2. DNA Verileri ve Milli DNA Veri Bankası Kanunu Tasarısı

DNA Verileri ve Milli DNA Veri Bankası Kanunu Tasarısı'nda, tasarıda geçen terimlerin tanımları, tasarının ikinci maddesinde yapılmıştır[322]. Tasarının en fazla eleştirilen maddelerinden biri, üçüncü maddede "kanunilik ilkesi" olarak düzenlenen maddedir. Bu maddenin ilk fıkrasına göre, "DNA analizi, ancak bu Kanunda ve diğer kanunlarda öngörülen hallerde yapılabilmekte"dir, ancak ikinci fıkrada getirilen düzenleme ile "bu Kanunda ve diğer kanunlarda öngörülen esas ve usullere uygun olarak ve ancak meşru amaçlarla ilgili kişinin açık rızasıyla da DNA analizi yapılabilecektir." Burada DNA analizi açısından, kişilere bu tür bir analize rıza gösterme hakkı tanınmış, ancak bu rızanın ileride kanunlaşacak olan tasarıda ve diğer kanunlarda öngörülen esas ve usullere uygun olarak ve ancak meşru amaçlarla yapılabileceği vurgulanmıştır. Tasarının bu maddesinin temeli, aynı tasarının 2 nci maddesi ile atılmıştır, zira ikinci maddedeki tanımlardan biri "gönüllü"dür ve bu tanıma göre gönüllü, "kendi rızasıyla DNA profili elde etmeye yönelik biyolojik örnek veren kişiyi" ifade etmektedir.

Tasarının bu maddesi ile ilgili, haklı olarak eleştirilen iki önemli husus bulunmaktadır. Bunlardan birincisi, DNA analizinin DNA sahibi kişinin açık rızası ile yapılabilmesi hususudur. CMK'nın 79 uncu maddesinde bu tür bir incelemenin yapılmasına karar verilmesinin münhasıran hakimin yetkisinde olmasının, DNA analizi açısından "birey üstü" menfaatler korunduğuna işaret ettiğine, bu sebeple

---

[322] Tasarının 2 nci maddesinde, tanımlar şu şekilde düzenlenmiştir:
"*a) Banka: Millî DNA Veri Bankasını,*
b) Başkanlık: Millî DNA Veri Bankası Başkanlığını,
c) Başkan: Millî DNA Veri Bankası Başkanını,
ç) Biyolojik örnek: Kaynağını insan vücudundan alan, DNA profili elde etmeye uygun, kan, tükürük, doku, kemik, tırnak, saç ve benzeri oluşumları,
d) DNA: Deoksiribonükleik asidi,
e) DNA izolatı: Biyolojik örneklerden elde edilmiş DNA içeren yapıyı,
f) DNA analizi: DNA verisi elde etmek amacıyla DNA izolatı üzerinde yapılan bilimsel testi,
g) DNA profili: Bir kişiyi diğerlerinden ayırt eden DNA karakteristiklerinin tümünü,
ğ) DNA verisi: DNA analizi sürecinde elde edilen bilgilerin tümünü,
h) DNA veri tabanı: DNA analizi sonucu elde edilen kişiye özgü DNA profillerinin kodlandırıldığı bilgilerin tutulduğu veri tabanını,
ı) Gönüllü: Kendi rızasıyla DNA profili elde etmeye yönelik biyolojik örnek veren kişiyi, ifade eder."

bireyin rızasının yeterli olmadığı ileri sürülmüştür[323]. Gerçekten de, kişisel veriler arasında, DNA'nın önemli bir yere sahip olduğunu belirtmek gerekir. Kişilerin DNA'sı her bir hücresinde ve deri hücresi, kan, sperm, tükürük gibi vücut örneklerinin tümünde aynı olup, tek yumurta ikizleri hariç her insanın DNA'sı diğer insanlarınkinden farklıdır[324]. Bu durumda, DNA, kişisel verilerin en önemli özelliği olan sahibine atfedilebilme, sahibinin kimliği ile bağlantı kurulabilme koşulunu en iyi sağlayan verilerden biridir ve dolayısıyla toplanması ve saklanması somut, açık, belirli kurallarla belirlenmelidir. Bu itibarla haklı olarak, Tasarı'da, Ceza Muhakemesi Kanunu'nda olduğu gibi, DNA Analizinin bireyin rızasına bağlı olarak değil, ancak hakim kararıyla yapılabileceğine ilişkin bir düzenleme getirilmiş olması gerektiği savunulmuştur.

İkinci husus ise, rızanın "ancak meşru amaçlarla ilgili" olarak verilebilmesidir. Tasarıda meşru bir amaçtan bahsedilmiş olup, bu amacın ne olduğuna ilişkin belirli ve açık bir açıklama yapılmamıştır. Tasarının 3 üncü maddesinin gerekçesinin ikinci fıkrası ile ilgili olan kısmında[325], meşru amaç için "genel hukuk kurallarıyla

---

[323] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 72; "*Hükmün hakim kararını gerekli kılması, bizi artık burada birey üstü menfaatlerin korunması endişesinin bulunduğu sonucuna götürecek olursa bireyin izninin yeterli olmadığı kabul edilmelidir. Kanımızca aksi bir kabul CMK ile aranan bir koşulun herhangi bir şekilde şüpheli ya da sanığın muvafakatinin sağlanması suretiyle ortadan kaldırılması sonucunu doğurabilir.*"

[324] **Özdilek**, **Ali Osman**, "DNA'nın Kanıt Olarak Kullanılması", Montreal, Kasım 2002, http://www.hukukcu.com/bilimsel/kitaplar/dna_kanit.htm, 15.12.2011.

[325] Tasarının 3 üncü maddesinin gerekçesinde, "*Maddenin ikinci fıkrasında ise DNA analizi yapılması bakımından çok önemli bir kurala yer verilerek kişinin açık rızasıyla da DNA analizi yapılması esası kabul edilmiştir. Dikkat edilmesi gerekir ki, kişinin açık rızasının bulunması salt DNA analizi yapılması bakımından yeterli değildir. Başka bir anlatımla kişi, sadece kendi rızasının bulunduğunu göstermek suretiyle, DNA analizi yaptıramayacaktır. Bunun için Tasarıda "olmazsa olmaz" niteliğinde iki ana koşul öngörülmüş bulunmaktadır. Belirtmek gerekir ki bu koşullar kişinin açık rızasından önce aranması gereken koşullardır. Buna göre:*
a) Tasarıda veya diğer kanunlarda yer alan esas ve ilkelere uygun olarak rıza gösterilmelidir.
Bu ilke aynı zamanda Tasarının birinci fıkrasında belirtilmiş olan "kanunilik ilkesi"ni tamamlamaktadır. Başka bir anlatımla, kişinin "açık rızası" kanunilik ilkesini bertaraf edecek bir araç olarak kullanılamayacaktır. Belirtmek gerekir ki, açık rızanın bulunması halinde de aranan kanunilik ilkesi DNA analizi yapılması sonucunda elde edilen verilerin "kişisel veri" niteliğinde olmasının doğal bir sonucudur.
b) Rızanın meşru amaçlarla gösterilmiş olması gerekir.
Meşru amacın ne olması gerektiği, genel hukuk kurallarıyla tanımlanmış ve hukukî ilkelere kavuşturulmuş bir kavram niteliğindedir. Bu nedenle, hukukun cevaz vermediği bir amaçla kişinin rıza göstermiş olması halinde, bu rıza DNA analizi yapılması bakımından dikkate alınmayacaktır.
Dikkat edilmelidir ki, gösterilen rızanın hukuken korunan bir meşru amaç çerçevesinde bulunması gerekmektedir. Meşru amacın tanımlanmasında ve bu meşruluğun takdir edilmesinde, DNA analizini yapacak ve bu Tasarıda belirtilen kurum ve mercilerin belirli bir takdir yetkisi de bulunmaktadır. Zira yukarıda da belirtildiği gibi "meşruluk kavramı", hukukilik kavramı gibi genel olarak geçerli olabilecek bir terim değildir.
c) DNA analizinin Tasarıda belirtilen kurumlar ile yetkilendirilmiş laboratuvarlarda yapılması gerekir." denilmektedir.

tanımlanmış ve hukukî ilkelere kavuşturulmuş bir kavram niteliğinden" söz edilmiştir. Kişinin göstereceği açık rızanın meşru bir amacı olup olmadığının takdir edilmesinde, "DNA analizini yapacak ve bu Tasarıda belirtilen kurum ve mercilerin belirli bir takdir yetkisi de bulunduğu" düzenlenmiştir. Yapılan bu düzenleme ile birlikte, başlığı "kanunilik ilkesi" olan tasarının 3 üncü maddesinde, kanunilik ilkesi ile bağdaşmayan, muğlak bir ifadeye yer verilerek meşru amaçlarla verilecek olan açık rıza açısından bu 'meşru amaçlar'ın neleri kapsayacağı ile ilgili açık bir tanım yapılmamış, üstelik ilgili kişinin rızasının meşru bir amacının bulunup bulunmadığı hususunun takdiri birtakım kurum ve mercilere bırakılmıştır.

Tasarının 4 üncü maddesinde, DNA verileri ile ilgili temel ilkeler belirlenmiş, amaca bağlılık ilkesi vurgulanmış, verilerin toplanması, kullanılması ve aktarılması hususlarında ne yazık ki 3 üncü maddede olduğu gibi kanunda gösterilen "meşru amaçlar"dan bahsedilmiştir. Dolayısıyla her ne kadar bu madde ile getirilen temel ilkeler Avrupa Konseyi tarafından hazırlanmış olan 108 Sayılı Sözleşmede yer alan ilkelerle paralellik gösterse de[326], burada da meşru amaç ifadesi ile maddenin kapsamı yeterince açık bir şekilde belirtilmemiştir[327]. Özbek'e göre, bu sorun tasarıya, Kişisel Verilerin Korunması Kanunu Tasarısı'ndaki düzenlemeye benzer bir ifade koymak ve böylece DNA verilerinin 'ırk, renk, cinsiyet, politik inanç, sosyal ya da ekonomik durum ya da cinsel tercih'lerle ilgili olarak işlenmesinin, aktarılmasının veya kullanılmasının yasaklanması suretiyle giderilebilecektir[328].

Olay yerinden elde edilecek materyallerin incelenmesi için CMK'da açık hüküm bulunmamakla birlikte, CMK'nın 78 inci maddesinin ikinci fıkrasında moleküler genetik incelemenin "bulunan ve kime ait olduğu belli olmayan beden parçaları üzerinde de yapılabileceği" belirtilmiştir. Ancak "Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik" in 3 üncü maddesinde beden parçası "bir bedenin tamamlayıcı unsuru olan baş, gövde, kol, el, bacak, ayak gibi uzuv ve iç organları" olarak tanımlanmış olup olay yerinde bulunabilecek olan kıl, tüy, saç, sperm gibi materyaller bu tanımın

[326] **Altaş**, s. 102 - 103.
[327] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 72.
[328] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 72.

dışında kalmaktadır. Tasarının 5 inci maddesi[329] ise, bu sorunu giderebilecek bir şekilde, olay yerinden toplanacak olan materyallerin DNA incelemesi kapsamında kalacağına ilişkin açık bir düzenleme getirmiştir[330].

Tasarının 7 nci maddesi, DNA analizini yapabilecek laboratuvarların hangileri olduğuna ilişkin bir düzenleme getirmiş, ilk fıkranın c bendinde sayılan analizi yapabilecek laboratuvarlar arasına "bankanın olumlu görüşü ve Sağlık Bakanlığının izniyle diğer gerçek ve tüzel kişilere ait olanlar" da dahil edilmiştir. Bu madde, ilgili düzenlemenin kötüye kullanılabileceği endişesiyle haklı olarak eleştirilmiştir[331]. Gerçekten de, DNA analizinin yapılması özellikle yargılamalar açısından son derece önem arz eden bir husustur. Zira bu analiz sonuçları dava sonucunda verilecek olan karara doğrudan etki edebilmekte, yeri geldiğinde bir kişinin fail olarak saptanıp alacağı hapis cezası ile hürriyetinden yoksun bırakılmasına karar verilebilmektedir. Bu denli önemli neticeleri olabilecek analizlerin sıklıkla ve titizlikle denetimi yapılan laboratuarlarda yapılması, yapılabilecek hataların asgari düzeye indirilmesi gerekmektedir. Gerçek ve tüzel kişilere ait olan laboratuvarlara Sağlık Bakanlığı'nın söz konusu izni neye göre vereceği hususun belirtilmemiş olması da kanaatimizce sakınca doğurabilecek bir husustur.

Tasarının 8 nci maddesinde, DNA analizine tabi tutulan kişinin "analizi yapan kurumdan veya laboratuvardan yapılan işlemin sonuçları hakkında bilgi almak, bunlara ilişkin kayıtların düzeltilmesini veya güncelleştirilmesini istemek hakkına

---

[329] Tasarının 5 inci maddesine göre, "*(1) DNA analizi;*
a) 04/12/2004 tarihli ve 5271 Sayılı Ceza Muhakemesi Kanununda belirlenen esas ve usûller çerçevesinde vücuttan,
b) Bir suç sebebiyle olay yerinden veya suçla bağlantılı diğer yerlerden,
c) Kim olduğunu tespit etmek amacıyla;
1) Hukukî uyuşmazlıklarda,
2) Hukuki veya fiilî sebeplerle kimliğin tespit edilememesi halinde,
Kişilerin vücudundan, vücut parçalarından, eşyasından veya ölmüş kişilerden,
ç) Görevleri sebebiyle hayati risk taşıyanlardan,
d) Gönüllü kişilerden,
Alınan biyolojik örnekler üzerinde yapılabilir.
(2) Birinci fıkranın (c) bendinin (1) numaralı alt bendinde belirtilen hallerde, mahkeme kararıyla, (2) numaralı alt bendinde belirtilen halde ise, yetkili kolluk amirinin gözetimi altında DNA analizi yapılmak üzere biyolojik örnek alınabilir.
(3) DNA analizi yapılmak üzere laboratuvara gönderilecek biyolojik örnekler kodlanır, kime ait olduğu, analizi yapacak olan görevlilerden gizli tutulur.
(4) Biyolojik örneğin alınmasından laboratuvar sonuçlarının kaydına kadar geçen süreçte izlenecek kodlama sistemiyle ilgili esas ve usuller yönetmelikle belirlenir."
[330] **Altaş**, s. 73.
[331] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 75, **Altaş**, s. 94.

sahip olduğu" belirtilmekle beraber, üçüncü fıkrada bu hakka çok geniş bir sınırlama getirilmektedir. Bu düzenlemeye göre, "suç soruşturulması ve kovuşturulmasına ilişkin hükümler saklıdır." Getirilen sınırlama ile soruşturma ve kovuşturma safhalarında nasıl bir yol izleneceği, nasıl bir sınırlama getirileceği belirtilmemiş olup, adeta DNA analizi yapılan kişinin bu hakları kullanmasının hiç mümkün olmayabilmesine yol açabilecek bir ifade kullanılmıştır[332]. Benzer bir ifade 14 üncü maddede de bulunmakta, maddenin ilk fıkrasında "bu Kanun hükümlerine göre, Banka bünyesinde oluşturulan sistem, DNA veri tabanında tutulan profillerin karşılaştırılması, yurtdışına aktarılması veya eşleştirilmesi ile DNA verilerinin elde edilmesine ilişkin yapılan her türlü işlemler ile bunların sonuçlarının gizli" olduğu belirtilmiş, ancak ikinci fıkraya "Suç soruşturması ve kovuşturmasına ilişkin hükümler saklı" olduğu istisnası getirilmiştir. Burada yine 8 inci maddede olduğu gibi muğlak bir ifade kullanılmış, soruşturma ve kovuşturma safhasında nasıl bir uygulama yapılacağı belirtilmemiş, adeta bu bilgilere ilişkin gizliliğin tamamen ortadan kalkmasına yok açabilecek bir düzenlemeye gidilmiştir.

Tasarıdaki bir diğer sorunlu hüküm 11 inci madde[333] olup, bu madde belki de Tasarı'nın en önemli maddesi olarak dahi değerlendirilebilir. Zira DNA izolatlarının

---

[332] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 75.

[333] Tasarı'nın 11 inci maddesinin ilk fıkrasında şöyle denilmektedir: "*5 inci madde hükümlerine göre alınan biyolojik örnekler ile DNA izolatlarının saklanması ve yok edilmesinde aşağıdaki esaslar uygulanır:*
a) Ceza Muhakemesi Kanununda belirtilen esas ve usuller çerçevesinde, şüpheli veya sanığın vücudundan alınan biyolojik örneklerden elde edilen izolatlar ile buna ilişkin bilgilerden;
1) Ceza Muhakemesi Kanununun 80 inci maddesinin ikinci fıkrasına giren kararların kesinleşmesi halinde izolatlar ve bunlardan elde edilen bilgiler derhal yok edilir.
2) Ceza veya güvenlik tedbirine mahkumiyet ya da düşme kararı verilmesi halinde izolatlar, hükmün kesinleşmesinden sonra derhal yok edilir. Ancak, bu biyolojik örneklerden elde edilen bilgiler süresiz olarak saklanır.
3) Bu bent hükmünün uygulanmasında Cumhuriyet başsavcılıkları veya mahkemeler, karar ya da hükmün kesinleşmesini, DNA analizi yapan laboratuvarlara, karar veya hükmün kesinleşmesi tarihinden itibaren bir ay içerisinde bildirmekle yükümlüdür.
b) Bir suç sebebiyle olay yeri veya suçla bağlantılı diğer yerlerdeki biyolojik örneklerden elde edilen izolatlar ile buna ilişkin bilgilerden;
1) Biyolojik örneklerden elde edilen izolatlar ve bunlardan elde edilen bilgiler, Ceza Muhakemesi Kanununun 80 inci maddesinin ikinci fıkrası kapsamına girmesi halinde derhal yok edilir.
2) Ceza veya güvenlik tedbirine mahkumiyet ya da düşme halinde, biyolojik örneklerden elde edilen izolatlar, kanunlarda öngörülen cezanın alt sınırı beş yıla kadar olanlarda beş yıl; beş yıl ve daha fazla olanlarda ise on yıl süreyle saklanır. Ancak, biyolojik örneklerden elde edilen bilgiler süresiz olarak saklanır.
3) Bu bent hükmünün uygulanmasında Cumhuriyet başsavcılıkları veya mahkemeler, karar ya da hükmün kesinleşmesini, DNA analizi yapan laboratuvarlara, karar veya hükmün kesinleşmesi tarihinden itibaren bir ay içerisinde bildirmekle yükümlüdür.
c) Görevleri sebebiyle hayati risk taşıyanların biyolojik örnekleri, elde edilen izolatları ve buna ilişkin bilgilerden;

(biyolojik örneklerden elde edilmiş DNA içeren yapı) ve biyolojik örneklerin saklanması ve yok edilmesine ilişkin temel kuralları düzenlemektedir. 11 inci maddedeki ifade incelendiğinde, maddede öngörülmüş olan birtakım "biyolojik örneklerden elde edilen bilgilerin" süresiz olarak saklanacakları belirtilmektedir. Bu denli önemli kişisel veri teşkil eden materyallerin süresiz saklanması hususunun hukuka aykırı bir düzenleme olduğu kanaatindeyiz. Zira biyolojik örneklerden elde edilmiş olan bilgiler kaçınılmaz olarak biyolojik örneğin sahibi olan kişinin DNA'sı ile ilgili bilgiler içerecektir. Bu durumda, yukarıda da değinildiği üzere, bu bilgiler birer kişisel veri niteliğinde olacaktır ve bunların süresiz saklanması, kullanım amaçları ortadan kalktığında dahi kişisel verilerin tutulmaya devam edilmesi anlamına gelecektir ki; bu husus tasarının bizzat 4 üncü maddesi ile çelişmektedir. Kişisel verilerin toplanmaları ve tutulmaları hususunda Avrupa Birliği tarafından yapılmış olan sözleşmelerde vurgulanan en önemli prensiplerden biri amaca bağlılık ilkesidir. Bir kişisel verinin toplanma veya tutulma amacının sona ermesi durumunda o kişisel verinin derhal yok edilmesi gerekmektedir. Bu itibarla kanaatimizce 11 inci maddede öngörülmüş olan DNA izolatlarının yok edilmeleri usulü yeterli olmayıp, bunlardan kişileri birebir tanımlanabilir kılan biyolojik örneklerden elde edilmiş olan bilgilerin de tutulma amaçlarının sona ermesi halinde yok edilmeleri gerekecektir.

Tasarı'ya 3 Ekim 2007'de son hali verilmeden önce yapılmış olan önceki düzenlemede, DNA profillerinin saklanması (madde 12) ile biyolojik örnekler ile bu biyolojik örneklerden elde edilen izolatların saklanması (madde 10) farklı maddelerde düzenlenmiş, bu maddeye ilişkin de doktrinde birtakım eleştiriler getirilmişti. Eski düzenlemeye göre, biyolojik örnek ve izolatların saklanması CMK m.80/2'ye aykırı olarak mümkün kılınmış, m.80/2'nin tasarıdaki maddenin istisna olduğu düzenlenmiş, böylece işlevini yerine getiremeyecek bir madde ortaya çıkmıştı. Bu maddenin eleştirilmesinin en önemli nedenlerinden biri saklanan biyolojik örnekler ile bu biyolojik örneklerden elde edilen izolatların her zaman

---

1) Elde edilen biyolojik örnekler ile bu örneklerden elde edilen izolatlar laboratuvar sonucu alındıktan sonra derhal yok edilir.
2) DNA analizi sonucunda elde edilen bilgiler laboratuvarlarca ilgilinin veya ilgili kurumun istemi üzerine görevleri süresince saklanır ve daha sonra derhal imha edilir. İstemin bulunmaması halinde süresiz olarak saklanır.
ç) Gönüllülerin biyolojik örnekleri, elde edilen izolatları ve buna ilişkin bilgilerinden;
1) Elde edilen biyolojik örnekler ile bu örneklerden elde edilen izolatlar laboratuvar sonucu alındıktan sonra derhal yok edilir.
2) DNA analizi sonucunda elde edilen bilgiler laboratuvarlarca ilgilinin istemi üzerine derhal imha edilir, isteminin bulunmaması halinde, süresiz olarak saklanır."

DNA analizine tabi tutulabilecek olmaları ve dolayısıyla bunları saklamanın DNA verilerinin saklanması ile neredeyse eşit bir durum oluşturduğuydu[334]. Dolayısıyla tasarının mevcut halinden önceki düzenlemede, biyolojik örneklerle izolatların her daim DNA analizine tabi tutulabilecek olmaları ve bu sebeple her zaman DNA verilerine ulaşılabileceği ihtimali dahi sakıncalı görülmekte ve eleştirilmekte iken, tasarının mevcut halinde doğrudan DNA verilerinin, hem de süresiz olarak saklanmalarına ilişkin yapılan düzenleme, tasarının amacına ters düştüğü gibi, Anayasal normlar ve Avrupa İnsan Hakları Sözleşmesi'nin 8 inci maddesi ile güvence altına alınan özel hayatın gizliliği ilkesine de aykırıdır.

Tasarı ile ilgili olarak değerlendirilecek bir diğer husus ise, tasarının kanunlaşması durumunda DNA veri bankasında çalışacak olan uzmanların nitelikleri ve başkanın atanmasıdır. Tasarının 25 inci maddesine göre, "başkan müşterek kararnameyle[335], başkan yardımcısı ise Yürütme Kurulu üyeleri arasından Başkan tarafından atanır."[336] Tasarı gerekçesinde de özerkliğine vurgu yapılan bir kurumun Başkanı, Yürütme Kurulu ve Danışma Kurulu'nun yürütme organı tarafından oluşturulması ve atanması eleştiri konusu olmuştur. Türk Tabipleri Birliği, 17 Ocak 2007'de yayımladığı görüşünde, "kişisel verileri analiz edip saklayacak ve kişilerin suçluluğuna ya da suçsuzluğuna esas oluşturacak raporları hazırlayacak kurumun, çalışmalarında kanun ile verilmiş görevler dışında hiçbir makam ve merciden emir almaması, etkilenmemesi gerektiği" gerekçesiyle bu maddeyi eleştirmiş, bu

---

[334] **Özbek**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", s. 74; "*Bir başka sakınca biyolojik örnek ve izolatların saklanmasıdır. Böyle bir saklama DNA verilerinin saklanması ile neredeyse eşittir. Zira örnek ve izolatları her zaman DNA analizine tabi tutulabilir. Söz konusu Tasarı biyolojik örnek ve DNA analiz sonuçlarının kişinin beden tamlığı ve özel hayatının gizliliği haklarını sağlamak olduğu düşünüldüğünde biyolojik örnek ve izolatların da saklanmasına imkan tanıması ve m.10 ile bunun kapsamının genişletilmesi tümüyle amaca aykırı bir yaklaşımı ortaya koymaktadır.*"

[335] **Gözler**, **Kemal**, "*İlgili bakanın, başbakanın ve Cumhurbaşkanının imzalarının bulunduğu kararnamelerdir. İlgili bakanın başbakan olduğu durumlarda bu kararnamelerde iki imza (başbakan+Cumhurbaşkanı) bazen dış görevlere atamalarda dört imza (ilgili bakan+Dışişleri Bakanı+Başbakan+Cumhurbaşkanı) bulunur… bütün kararnameler, Bakanlar Kurulu kararnameleri ve ortak kararnameler de Cumhurbaşkanı tarafından imzalanmalıdır.*" http://www.anayasa.gen.tr/cumhurbaskani.htm, 27.12.2011.

[336] Benzer şekilde Yönetim Kurulu üyeleri de 28 inci maddeye göre müşterek kararname ile atanmaktadırlar. Danışma Kurulu ise 30 uncu maddede sayılan doğal üyelerden oluşmakta olup bu üyeler; "*Başbakanlık Müsteşarı veya görevlendireceği Müsteşar Yardımcısı, Yükseköğretim Kurulunun kendi üyesi olmayan ve tıbbî genetik veya moleküler biyoloji alanında uzmanlığa sahip öğretim üyeleri arasından belirleyeceği bir üye, Adalet Bakanlığı Kanunlar Genel Müdürlüğünden en az birinci sınıfa ayrılmış hakimler arasından belirlenecek bir üye, Türkiye Barolar Birliğinin mesleki kıdemi en az on yıl olan üyeleri arasından belirleyeceği bir üye, Türk Akreditasyon Kurumu Laboratuvar Akreditasyon Başkanlığından belirlenecek bir üye, Adalet Bakanlığı Adli Tıp Kurumu Başkanı, İçişleri Bakanlığı Jandarma Genel Komutanlığı Kriminal Daire Başkanı, İçişleri Bakanlığı Emniyet Genel Müdürlüğü Kriminal Polis Laboratuvarları Dairesi Başkanı*" dır.

koşullarda kurumun bağımsızlığından söz etmenin oldukça güç olacağını belirtmiştir[337].

Tasarı ile ilgili olarak değinilecek olan son husus ise, çalışmamızın temel konusunu teşkil eden kişisel verilerin Türk Ceza Kanunu'ndaki düzenlemesiyle doğrudan ilgili olan kısımdır. Tasarının Sekizinci Bölümünde yer alan, Ceza ve Usul Hükümleri başlığı altındaki 43 üncü maddede "Ceza Hükümleri", 46 ncı maddede ise "Soruşturma Usulü" düzenlenmiştir. 43 üncü maddede düzenlenmiş olan ceza hükümlerinde, Türk Ceza Kanunu'nun kişisel verilerle ilgili düzenlemeler getiren ve aşağıda ayrıntılı bir şekilde incelenecek olan 135 (Kişisel Verilerin Kaydedilmesi), 136 (Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme), 137 (Nitelikli Haller) ve 138 (Verileri Yok Etmeme) inci maddelerine atıf yapılmaktadır[338]. Tasarı getirmiş olduğu bu düzenleme ile tasarıda yer alan kurallara aykırı davranacak olan kişilerin fiillerinin, Türk Ceza Kanununda düzenlenmiş suçlar kapsamında olduğu durumlarda bu hükümlere göre cezalandırılmalarını güvence altına almıştır. Yine aynı maddenin son fıkrası ile, bu suçları işleyen kişiler bakımından, cezayı artıran ek bir nitelikli hal öngörülmüş, "bu maddede yazılı suçları işleyenler hakkında Türk Ceza Kanununa göre tayin edilecek hapis cezalarının yarı oranında artırılarak hükmolunacağı" hüküm altına alınmıştır. Tüzel kişilerin bu suçları işlemesi halinde ise, tasarının 45 inci maddesinde yine Türk Ceza Kanunu'na atıf yapılarak ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunacağı belirtilmiştir.

46 ncı maddenin ikinci fıkrasında ise, bankanın başkan, başkan yardımcısı, Yürütme Kurulu üyeleri ve diğer personelinin görevleri nedeniyle işledikleri suçlar ile kendilerine karşı işlenen suçlar bakımından Türk Ceza Kanununun uygulamasında kamu görevlisi sayılacakları belirtilmiştir. Bu itibarla TCK'nın 137 nci maddesindeki nitelikli haller aşağıda ayrıntılı olarak incelenecek olsa da, bu

---

[337] http://www.ttb.org.tr/index.php/Haberler/tye-milli-dna-veri-bankasnunu-tasar-473.html, 22.12.2011.

[338] 43 üncü maddeye göre, tasarının *"(1) … 7 nci maddesinin birinci fıkrası hükmüne aykırı olarak DNA analizi yapmaya yetkili olmadığı halde DNA analizi yapanlar Türk Ceza Kanununun 135 inci maddesinin birinci fıkrası hükmüne göre cezalandırılır. (2) Hukuka aykırı olarak DNA verilerini; açıklayan, yayan, bir başkasına veren, ele geçiren, aktaran veya kendileri ya da başkaları yararına kullananlar ile bu Kanunun 6 ncı maddesine aykırı hareket edenler, Türk Ceza Kanununun 136 ncı maddesi hükmüne göre cezalandırılır. (3) … 11 inci maddesinde yer alan biyolojik örneklerin saklanması veya yok edilmesine ilişkin hükümlere aykırı hareket edenler, Türk Ceza Kanununun 138 inci maddesi hükmüne göre cezalandırılır.*"

noktada, Türk Ceza Kanunu'nun kişisel verilerin hukuka aykırı olarak kaydedilmesi (m.135) ve verileri hukuka aykırı olarak verme veya ele geçirme (m.136) suçları açısından, 137 nci maddede fiili işleyenlerin kamu görevlisi olmasının öngörülmüş olan cezanın artırılmasını gerektiren nitelikli hallerden biri olduğuna değinmekte fayda vardır. Bu noktada kamu görevlisi sayılarak DNA verilerini hukuka aykırı olarak kaydeden veya hukuka aykırı olarak veren veya ele geçiren kişi bakımından ortaya iki nitelikli hal çıkmaktadır. Kanaatimizce tasarının kanunlaşması halinde, uygulama öncelikle failin TCK kapsamında 137 nci maddede öngörülen nitelikli halle beraber cezasının belirlenmesi, ardından tasarıda öngörülmüş olan nitelikli hal uyarınca bu cezanın artırılması şeklinde olmalıdır. Dolayısıyla veri bankasının başkan, başkan yardımcısı, Yürütme Kurulu üyeleri ve diğer personelinin, DNA verilerini hukuka aykırı olarak kaydetmesi (m.135) veya hukuka aykırı olarak vermesi veya ele geçirmesi (m.136) durumunda, failin cezası için önce ilgili madde uyarınca cezası belirlenecek, ardından TCK'nın 137 nci maddesi uyarınca kamu görevlisi oldukları için bu cezada yarı oranında artırım yapılacak, son olarak da tasarının 43 üncü maddesinin son fıkrası gereğince toplam ceza yarı oranında artırılacaktır.

II. 5237 SAYILI TÜRK CEZA KANUNUNDAKİ DÜZENLEMELER

A. Genel Bilgiler

Son yıllarda, dünyada ve Türkiye'de özellikle teknolojinin, bilişim sistemlerinin ve internet ağının gelişmesi dolayısıyla kişisel verilerin kaydedilmesinde ciddi artışlar olmuş, özellikle cep telefonu numaraları, bankalara verilen şahsi bilgiler, bazı şirketler tarafından toplanan ve kişilerin ekonomik durumlarını veya kullandıkları ürünleri, markaları kaydeden gerçek ve tüzel kişilerin sayısı önemli oranda artmıştır.

Kişisel verilerin kaydedilmesi devletin resmi kurumları tarafından yapılabildiği gibi[339], başkaca kurum ve kuruluşlar da bireylerin kişisel verilerini toplayabilmekte ve bunları saklayabilmektedir. Buna örnek olarak hastalarla ilgili gizli ve son derece önemli bilgileri kaydeden hastaneler, kişilerin DNA ve parmak izlerini toplayan,

[339] Buna örnek olarak GBT sistemi verilebilir.

bunlarla ilgili incelemeler yapan, ancak daha sonra bu verileri yok etmeyen adli tıp kurumları ve cep telefonu işletmecisi olan şirketler verilebilir.[340] Gerçekten de, özellikle cep telefonları alanında, günümüzde herhangi bir yerden alışveriş yapıldığında dahi, neredeyse tüm mağazalar kişilerin cep telefon numaralarını istemekte, sistemlerine kaydetmektedir. Benzer şekilde, bazı süpermarketlerin, birtakım indirimler sağlayacak olan kartlar verirken kişilerin cep telefonu, isim, soy isim, yaş, cinsiyet gibi bilgilerini kaydettikleri bilinmektedir. Daha vahim olarak, son yıllarda bireylerin sürekli olarak cep telefonu numaralarını vermediklerini iddia ettikleri yerlerden tacize varacak boyutlarda sık mesaj almaları ve aranmaları; bu durumun da kişisel verileri toplayan bazı kuruluşların bu bilgileri daha sonra başka kurum ve kuruluşlara sattıkları iddiasını gündeme getirmiş olmasıdır.

İşte Avrupa Birliği'ne uyum süreci açısından yukarıda değinilmiş olan anlaşmalar çerçevesinde Türkiye'nin hazırlamış olduğu Kişisel Verilerin Korunması Hakkında Kanun Tasarısı yıllardır yürürlüğe girmemiş, adeta bu kişisel veri kayıtlarının ve paylaşımının düzensiz ve kontrolsüz bir biçimde artmasına ve dolayısıyla bireylerin Anayasa tarafından da korunmakta olan temel hak ve özgürlüklerinin bu alanda ciddi şekilde ihlal edilmesine yol açılmıştır.

Tüm bu sorunları azaltmak ve engelleyebilmek, bu tür eylemlerde bulunanları cezalandırmak ve yine bu tür eylemlerde bulunacakları caydırabilmek adına, 5237 Sayılı Türk Ceza Kanunu'nda kişisel verilerle ilgili düzenlemelere gidilmiş, bu alanda yeni suçlar ve cezalar ihdas edilmiştir. Kanun'un "Kişilere Karşı Suçlar" başlıklı İkinci Kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde, 135 inci maddede "Kişisel verilerin kaydedilmesi", 136 ncı maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" ve 138 inci maddede "Verileri yok etmeme" suçları düzenlenmiş, 137 nci maddede ise cezanın artırılmasını gerektiren nitelikli haller sayılmıştır.

Yukarıda kişisel veri kavramının açıklandığı başlık altında ayrıntılı olarak incelenmiş olsa da, Türk Ceza Kanunu'nda düzenlenmiş olan suçların daha iyi anlaşılması bakımından kişisel veri kavramının bu kanun bakımından ne anlam ifade ettiği hususu üzerinde durmak gerekir. Kişisel verilerin kaydedilmesi suçunu

[340] **Dülger**, **Murat Volkan**, Bilişim Suçları, 1. Baskı, Kasım 2004 s. 266.

düzenleyen 135 inci maddede her ne kadar kişisel verinin ne olduğuna ilişkin açık bir tanım yapılmamış olsa da, madde gerekçesinde "söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanındığı" belirtilmiştir. Söz konusu sözleşmenin 2/a maddesinde ise sözleşmede geçen kişisel nitelikteki veriler ifadesi "kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade etmektedir."[341] Bu açıdan telefon numarası, banka hesap bilgileri, nüfus bilgileri, DNA analizi sonuçları, kan grubu gibi gerçek kişilere ilişkin olup, bu kişileri belirli veya belirlenebilir kılan tüm bilgiler kişisel veri Sayılırlar[342].

Türk Ceza Kanunu açısından "kişisel veri" kavramına bakıldığında, veriyi oluşturan bilgilerin mutlaka bilişim sisteminde kullanılabilen ve yine yalnızca bilişim sistemi vasıtasıyla aktarılabilen bilgiler olması şart değildir. Nitekim aşağıda görüleceği üzere, kişisel verilerin kaydedilmesi suçunu düzenleyen 135 inci maddenin gerekçesinde "kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir." ifadesi yer almaktadır. Bu tanımlamadan da açıkça anlaşıldığı üzere, bahsedilen kişisel veriler elektronik ortamdaki ve bilişim sistemleri içerisinde kullanılabilen veriler olabilecekleri gibi, yazıyla veya başka herhangi bir şekilde kaydedilmiş veriler de olabilir[343]. Bu husus kişisel veriler ile ilgili olan diğer maddeler (TCK m.136, 137, 138) için de geçerlidir.

---

[341] http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm , Erişim Tarihi: 05.01.2012.

[342] **Şener**, **Gülnihal Emine**, **"**Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu", Adalet Dergisi (T.C. Adalet Bakanlığı Yayın İşleri Daire Başkanlığı), 39. Sayı, Ocak 2011, s. 75 http://www.yayin.adalet.gov.tr/dergi/39.say%C4%B1/05%20-%20EM%C4%B0NE%20G%C3%9CLN%C4%B0HAL%20%C5%9EENER.pdf 21.09.2012.

[343] **Dülger**, s. 269, **Ketizmen**, s. 233, **Şener**, s. 76, **Değirmenci**, **Olgun**, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", TBB Dergisi, Sayı 58, 2005, s. 202,
Aksi görüş için; **Özbek**, **Veli Özer**, TCK İzmir Şerhi – Yeni Türk Ceza Kanununun Anlamı, Cilt 2 Özel Hükümler, Ankara, Şubat 2008, s. 950 – 951; "… *Ancak kanımızca kişisel veriler elektronik (CD gibi) ya da manyetik olarak (video kaset veya teyp kaseti gibi) veya doğrudan görülebilir olmayan bir ortamda kayda alınmış olmalıdır….. Bu nedenle verilerin okunması ya da dinlenmesi suretiyle kişinin hafızasına alınması ya da ezberlenmesi veyahutta kağıt üzerine yazmak kaydetmek olarak anlaşılmamalıdır.*"

B. Türk Ceza Kanunu'nda Kişisel Verilere İlişkin Düzenlemelerin Tarihçesi

5237 Sayılı Türk Ceza Kanunu'nun 135, 136, 137 ve 138 inci maddelerinin düzenlenmiş olan kişisel verilerin kaydedilmesi (m.135), hukuka aykırı olarak verilmesi veya ele geçirilmesi(m.136), bu suçların nitelikli halleri (m.137) ve hukuka uygun olarak kaydedilmiş olan kişisel verileri yok etmeme (m. 138) suçlarının, mülga 765 Sayılı TCK'da karşılığı bulunmamaktaydı. 5237 Sayılı TCK kabul edilmeden önce, 1997, 2000 ve 2003 yıllarında düzenlenmiş olan üç tasarıda da kişisel verilerin korunmasına yönelik hükümler yer almış olup, bu hükümler birtakım değişikliklere uğrayarak 5237 Sayılı kanun ile kanunlaşmışlardır.

1997 tarihli Türk Ceza Kanunu Öntasarısı'nda, kişisel verileri koruma amacıyla düzenlenmiş dört adet madde (m.193, m.194, m.195, m.196) bulunmakta idi. Öntasarının 193 üncü maddesinde[344] kanuna aykırı olarak kişisel verilerin toplanmasına ilişkin yaptırımlar düzenlenmiş, bu maddenin ilk iki fıkrasında yer alan suçların kasten işlenmeleri halinde hapis cezası öngörülmüş, suçların taksirle işlenmesi de aynı madde kapsamında düzenlenerek bu haller için para cezası öngörülmüştür.

Öntasarının 194 üncü maddesinde[345] ise, mevcut 5237 Sayılı TCK'nın 136 ncı ve 138 inci maddelerinde öngörülen suçlara benzer bir düzenleme yapılmış, her iki suç da aynı maddede toplanmıştır. Bu maddeye göre, ilk fıkrada kişisel verileri yetkisiz kişilere vermek, ifşa etmek, çeşitli şahsi maksatlarla kullanmak ve her ne

---

[344] "Kanuna aykırı olarak kişisel verileri toplamak" başlıklı 193 üncü maddede, "*1. Rızaları olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verileri bilişim sistemlerine yerleştiren veya işleyen kimseye altı aydan üç yıla kadar hapis cezası verilir.*

Veriler, hileli veya kanun ışı yollarla elde edildiğinde verilecek ceza üçte biri oranında artırılır.

2. Kanuna uygun olarak bilişim sistemlerine yerleştirilmek veya işlenmekle beraber muhafazaları için gerekli güvenlik tedbirlerinin alınmaması nedeni ile kişisel verilerin başkalarının ellerine geçmesine veya bozulmasına veya zarar görmesine neden olan kimse hakkında bir yıldan dört yıla kadar hapis cezası verilir.

Fiil taksirle işlendiğinde ellimilyon liradan ikiyüzmilyon liraya kadar ağır para cezası verilir.

3. Kanunun öngördüğü haller hariç, kişilerin ahlaki niteliklerini, siyasal, felsefi veya dini görüşlerini veya ırki kökenlerini veya sendikal bağlantılarını veya cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştiren veya işleyen kimseye bir yıldan iki yıla kadar hapis cezası verilir" denilmekteydi.

[345] "Verileri, yetkili olmayanlara verme, imha etmeme" başlıklı 194 üncü maddede, "*1. Kişisel verileri, yetkisiz kişilere veren, ifşa eden, çeşitli şahsi maksatlarla kullananlar ile her ne surette olursa olsun ele geçirenlere iki yıldan beş yıla kadar hapis cezası verilir.*

2. Kanunların tayin ettiği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmeyenlere altı aydan bir yıla kadar hapis cezası verilir" denilmekteydi.

suretle olursa olsun ele geçirmek suç olarak düzenlenmiştir. Aynı maddenin ikinci fıkrasında ise kanunların tayin ettiği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmeme fiili suç olarak düzenlenmiştir.

Öntasarının kişisel verilerin korunmasına ilişkin son iki maddesi 195 inci ve 196 ncı maddelerdir. 195 inci madde[346], 2000 tarihli Tasarıda da yer alan, ancak 5237 Sayılı TCK'da yer verilmemiş olan fişlikler ile ilgili maddedir. Bu maddede 193 ve 194 üncü maddelerde yer alan suçların fişliklere yerleştirilmiş veriler hakkında işlendiğinde de faile ceza verilmesi öngörülmüştür. Son olarak 196. maddede[347] ise tüzel kişilerin sorumluluğuna ilişkin bir düzenleme yapılmış olup, tüzel kişilerin bu fiillerden sorumlu olacakları belirtilmiştir.

2000 tarihli Türk Ceza Kanunu Tasarısı da, 1997 tarihindeki Öntasarı ile hemen hemen aynı olup, temel farklar; maddeler içindeki bazı kelimelerin değiştirilmiş olması ve 1997 tarihli Öntasarının 193 üncü maddesinde yer alıp, 2000 tarihli Tasarının 195 inci maddesine tekabül eden suçun ise başlığının değiştirilmiş olmasıdır[348].

2000 tarihli Tasarı'yı takiben, 2003 tarihinde bir tasarı daha hazırlanmıştır. 2003 tarihli Tasarı'da da, kişisel verilerin korunması "Hayatın Gizli Alanına ve Özel Hayata Karşı Suçlar" başlıklı Dokuzuncu Bölüm'de dört madde (m.197, m.198, m.199, m.200) halinde düzenlenmiştir. Maddelere bakıldığında, 197 nci maddede "Kanuna aykırı kişisel veriler" başlığı ile 2000 tarihli Tasarı'nın 195 inci maddesinin aynen muhafaza edildiği görülmektedir. 198 inci maddede ise "Verileri yetkili olmayanlara verme, imha etmeme" suçu düzenlenmiştir. Bu maddenin, 1997 tarihli Öntasarı'nın ve 2000 tarihli Tasarı'nın bu maddeye tekabül eden maddelerinden

---

[346] "Fişlikler" başlıklı 195 inci madde şu şekilde düzenlenmişti: "*193 ve 194 üncü maddelerde yer alan fiiller, her türlü fişliklere yerleştirilmiş veriler hakkında işlendiğinde faillere aynı cezalar verilir.*"

[347] "Tüzel kişilerin sorumluluğu" başlıklı 196 ncı maddede ise, "*193 ila 195 inci maddelerde yer alan suçlardan dolayı tüzel kişiler de sorumlu"* olacağı belirtilmişti.

[348] 1997 tarihli tasarının 193 üncü maddesinin başlığı "Kanuna aykırı olarak kişisel verileri toplamak" iken, 2000 tarihli tasarıda bu ifade "Kanuna aykırı kişisel veriler" olarak değiştirilmiş, 1997 tarihli tasarıda yer alan 193 üncü maddenin 3 üncü fıkrası şu şekilde değiştirilmiştir: "*Kanunun öngördüğü haller dışında, kişilerin ahlaki niteliklerini, siyasal, felsefi veya dinsel görüşlerini veya ırki kökenlerini veya sendikal bağlantılarını veya cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştiren veya işleyen kimseye bir yıldan iki yıla kadar hapis cezası verilir.*"
1997 tarihli tasarının 194 üncü maddesinin ikinci fıkrasında yer alan "*her ne suretle olursa olsun ele geçirenlere*" ifadesi ise, "*her ne suretle olursa olsun*" kelimeleri çıkarılarak "ele geçirenlere" şeklinde değiştirilmiştir.

önemli bir farkı, maddenin ikinci fıkrasına "yok etmekle yükümlü olanlar" ibaresinin eklenmiş olmasıdır. 1997 tarihli Öntasarı'nın 194, 2000 tarihli Tasarı'nın ise 196 ncı maddelerinde "verileri sistem içinde yok etmeyenler" şeklinde bir ifade kullanılmışken, 2003 tarihli Tasarı'nın 198 inci maddesinde "yok etmekle yükümlü olanlardan" bahsedilmiştir.

2003 tarihli Tasarı'nın "Fişlikler" başlıklı 199 uncu ve "Tüzel kişilerin sorumluluğu" başlıklı 200 üncü maddelerinde, herhangi bir değişiklik yapılmamış, 1997 tarihli Öntasarı ve 2000 tarihli Tasarı'daki ifadeler aynen alınmıştır.

Kişisel verilerin korunması ile ilgili suçlar açısından tasarılar ile kanunlaşan mevcut 5237 Sayılı TCK arasındaki önemli farklardan ilki, hem 1997 tarihli Öntasarıda, hem 2000 tarihli Tasarıda, hem de 2003 tarihli Tasarı'da, kişisel verilerin "kaydedilmesi"nden değil, "yerleştirilmesi veya işlenmesi"nden bahsedilmiş olmasıdır. İkinci fark ise, tasarılarda suçun işlenmesi için gerekli olan yerleştirme veya işleme fiillerinin ancak bilişim sistemleri bakımından söz konusu olabileceği belirtilmişken, 5237 Sayılı TCK'da böyle bir şartın aranmamış olmasıdır. Aşağıda detaylı olarak inceleneceği üzere, 5237 Sayılı TCK'nın 135 inci maddesinde düzenlenmiş olan kişisel verilerin kaydedilmesi suçu açısından herhangi bir bilişim sistemine kayıt şartı aranmamış olup; madde gerekçesinde de her tür hukuka aykırı kaydın, "bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmeden" bu suçu oluşturacağı hususu belirtilmiştir.

Tasarılarla 5237 Sayılı TCK arasında değinilebilecek bir diğer fark ise, tasarılarda yerleştirme veya işleme fiillerinin suçun seçimlik hareketleri olarak belirtilmiş olmasıdır. 5237 Sayılı TCK'da bu seçimlik hareketler yer almamakta, yalnızca "kaydetme"den bahsedilmektedir.

5237 Sayılı TCK'nın 136 ncı (Verileri hukuka aykırı olarak verme veya ele geçirme) ve 138 inci (Verileri yok etmeme) maddelerinde düzenlenmiş olan suçların 1997 tarihli Öntasarının 194 üncü; 2000 tarihli Tasarının 196 ncı, 2003 tarihli Tasarının ise 198 inci maddelerinde, bir arada düzenlenmiştir.

Son olarak; üç tasarıda da, kişisel verileri kanuna aykırı olarak bilişim sistemlerine yerleştirme veya işleme ile yerleştirmenin veya işlemenin kanuna uygun olarak yapılmasıyla beraber muhafazaları için gerekli güvenlik tedbirlerinin alınmaması nedeniyle kişisel verilerin başkalarının ellerine geçmesine veya bozulmasına veya zarar görmesine neden olanların, bu fiilleri taksirle işlemeleri halinin yine aynı maddede düzenlenmiş olduğu belirtilmelidir. Tasarılarda bu fiillerin taksirle işlenmeleri mümkün kılınmış iken, 5237 Sayılı TCK'da böyle bir düzenlemeye gidilmeyerek kişisel verilerle ilgili suçların taksirle işlenmeleri hali düzenlenmemiştir.

C. Türk Ceza Kanunu'nda (TCK) Kişisel Verilere İlişkin Düzenlemeler

1. TCK m. 135: Kişisel Verilerin Kaydedilmesi

a. Genel Bilgiler

Kişisel verilerin kaydedilmesi suçu, TCK'nın 135 inci maddesinde **"***(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.*

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır[349]." şeklinde düzenlenmiştir.

---

[349] 135 inci maddenin gerekçesi şu şekilde düzenlenmiştir:
"*Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır.*
Suçun konusu, kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir.
Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanınmıştır.
Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli

Türk Ceza Kanunu'nun 135 inci maddesinin ilk fıkrası ile hukuka aykırı olarak kaydedilen kişisel verilerin korunmasına ilişkin genel bir yaptırım öngörülmüş, ikinci fıkrada ise; sınırlı sayıda sayılan birtakım alanlardaki hassas nitelikteki kişisel verilerin kaydedilmesine ilişkin bir ifade getirilmiştir.

Doktrinde, kişisel verinin kanunda tanımlanmamış olması ve belli bir çerçeveye oturtulmayarak kapsamının geniş bırakılmış olması eleştirilmiş, bunun ceza hukukunun temel ilkelerinden olan "belirlilik ilkesi" ne ters düştüğü savunulmuştur[350]. Benzer düşüncede olan yazarlara göre de, "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" henüz tasarı aşamasında olup, kişisel verilerin nelerden oluştuğuna ve Anayasa'da temel hak ve özgürlükler arasında sayılabilecek olan kişisel verilerin saklanması ve kaydedilmesinin herhangi bir kanuni dayanağı bulunmamakta ve dolayısıyla bu madde kanunilik ilkesini ihlal edecek nitelikte olup, temel ilkelerin belirlendiği bir kanunun bulunmaması sakınca doğurabilecek bir hususdur[351]. Bazı yazarlara göre bu duruma; Anayasa'ya göre, ancak kanunla sınırlanabilecek olan bir Anayasal özgürlüğün nasıl sınırlandırılacağını düzenleyen hiçbir kanunun bulunmaması yol açmıştır[352]. Dolayısıyla Türk Ceza Kanunu'nda düzenlenen bu suçla da; kolluk güçlerinin tuttukları Genel Bilgi Toplama (GBT) kayıtlarını, istihbarat bilgilerini ve hastanelerdeki hastalara ilişkin kişisel verileri tutmak başlı başına suç haline gelme tehlikesiyle karşı karşıya kalmıştır[353]. Bu durumda hastanelerde tutulmakta olan kişisel verilerin kişilerin ırki kökenlerine ilişkin olması veya kolluk kuvvetlerince tutulan GBT kayıtlarında veya istihbarat bilgilerinde kişilerin hangi örgütlerin sempatizanı olduklarına ilişkin kayıtları tutmak bu madde ile suç haline getirilmiştir. Nitekim doktrinde bu durum eleştirilmiş olup; bu maddenin yürürlüğe girme tarihinin Kişisel Verilerin Korunması Hakkında

---

nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alın¬maktadırlar. Bu durumlarda, söz konusu suç oluşmayacaktır.
Maddenin ikinci fıkrasında, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine, ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kayda almak, suç olarak tanımlanmıştır. Ancak, bunlardan kişilerin ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır."

[350] **Dülger**, s. 271.

[351] **Yaşar**, **Osman-Gökcan**, **Hasan Tahsin-Artuç**, **Mustafa**, Türk Ceza Kanunu, Cilt 3, 1. Baskı, Ankara, Şubat 2010, s. 4116, **Şen**, **Ersan**, Yeni Türk Ceza Kanunu Yorumu, Cilt 1, İstanbul, Nisan 2006, s. 601, **Küzeci**, s. 286 - 287.

[352] **Yaşar-Gökcan-Artuç**, s. 4116.

[353] **Yaşar-Gökcan-Artuç**, s. 4116.

Kanun'un yürürlüğe gireceği tarihe kadar ertelenmesinin daha uygun olmuş olacağı yazarlarca savunulmuştur[354].

Bu sorunun kaynağı olarak doktrinde ortaya atılan bir diğer görüş ise, bu maddenin kaynağını teşkil eden Fransız Ceza Kanunu'ndaki düzenlemede kişisel verilerin korunmasına ilişkin suçların eksik norm şeklinde düzenlenmiş olmasıdır. Bu durumda Fransa'da, kişisel verilerin korunması ile ilgili olarak özel bir kanunun var olması sebebiyle, suç olarak düzenlenenin aslında bu kanundaki usul ve esaslara uyulmaması olduğu; ancak Türkiye'de böyle bir özel kanun henüz kanunlaşmamış olduğundan eksik norm olarak bağlantı kurulabilecek bir düzenleme bulunmadığı ileri sürülmüştür[355].

Doktrindeki bir diğer görüşe göre ise, asıl olan kıyas yasağıdır ve ceza kanunları kazuistik yöntemle düzenlenemeyeceklerinden, tipiklikte yer alan kavramların yorum yoluyla değerlendirilmesi mümkün olup bazı kavramlardan ne anlaşılması gerektiğine ilişkin hususların uygulamaya ve öğretiye bırakılmasının kanunilik ilkesine aykırılık teşkil eden bir tarafı yoktur[356].

Kanaatimizce, her ne kadar Türk Ceza Kanunu'nun niteliği itibariyle, kanunda kişisel verinin açık tanımının yapılması beklenemeyecek olsa da, kişisel verinin kaydedilmesini düzenleyen bir suçun ihdas edilmiş olması, kişisel veriden ne anlaşılması gerektiğini mümkün olduğunca açık bir şekilde belirleyen kanuni bir tanımın bulunmasını gerekli kılmaktadır. Aksi bir durum kişisel verinin tam olarak ne olduğunun kanunla belirtilmemiş olması sebebiyle, hangi verilerin bu suçun kapsamına dahil edileceği muğlak kalarak kanunilik ilkesi ihlal edilmiş olacaktır. Ancak burada hemen belirtmek gerekir ki, yukarıda incelenen ülkelerin mevzuatlarına ve kişisel verilerin korunmasını düzenleyen uluslararası metinlere bakıldığında, aslında kişisel verinin net bir tanımının yapılamadığı ve belirli veya belirlenebilir kişilere ait her verinin bu kapsamda kaldığı görülmektedir. Yine de, yukarıda belirttiğimiz görüşe paralel olarak, Türk Ceza Kanunu'nda kişisel verilerin korunması ile ilgili olarak ihdas edilmiş olan hükümlerin yürürlüğe girme tarihinin, kişisel verileri koruyan özel kanunun çıkış tarihine kadar ertelenmesinin hukuki

[354] **Yaşar-Gökcan-Artuç**, s. 4116.
[355] **Ketizmen**, s. 235.
[356] **Özbek**, TCK İzmir Şerhi, s. 948, **Şener**, s. 74.

açıdan daha yerinde olacağı kanaatindeyiz. Düşüncemize göre, özel bir kanun çıkmadan bu hükümlerin Türk Ceza Kanunu ile düzenlenmiş olması, bu suçlar için öngörülen yaptırımların uygulanmasının hukuken sağlam temellere dayanmasını imkansız kılmakta, mevcut durumda kişisel verinin Türkiye'de kanunla yapılmış bir tanımı bulunmaksızın öngörülen yaptırımların uygulanması kanunilik ilkesine ters düşmektedir.

b. Suçla Korunan Hukuki Değer

Özel hayatın gizliliği, Avrupa İnsan Hakları Sözleşmesi'nin 8 inci maddesi[357] ile Anayasa'nın 20 nci maddesinde[358] koruma altına alınmış; Türkiye'nin 28 Ocak 1981 tarihinde imzaladığı 108 Sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" ile de kişisel verilerin korunmasıyla birlikte yer almıştır[359].

Bu suç, Türk Ceza Kanunu'nun "Kişilere Karşı Suçlar" başlıklı İkinci Kısmında ve "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde düzenlenmiştir. Bu sistematikten açıkça anlaşıldığı üzere, kişisel verilerin kaydedilmesi suçu, kişilere karşı suçlardandır ve suçla kişilerin özel hayatın gizliliği korunmaktadır[360]. Özel hayatın gizliliği kavramı, 1987 tarihli Anayasa Mahkemesi kararında[361] "Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir.

---

[357] Bu maddenin Kişisel Verilerin Korunması açısından değerlendirilmesi aşağıda ayrı bir başlık altında incelenecektir.

[358] Anayasa'nın " Özel hayatın gizliliği" başlıklı 20 nci maddesi şu şekilde düzenlenmiştir:
"*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*
Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."

[359] **Yaşar-Gökcan-Artuç**, s. 4117, **Parlar**, **Ali-Hatipoğlu**, **Muzaffer**, Açıklamalı – Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 2. Cilt, 3. Baskı, Ankara 2010, s. 2087, Dülger, s. 268.

[360] **Parlar**, **Hatipoğlu**, s. 2087, **Soyaslan**, **Doğan**, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010, s. 342, **Arslan**, **Çetin-Azizağaoğlu**, **Bahattin**, Yeni Türk Ceza Kanunu Şerhi, 1. Baskı, Kasım 2004, s. 608, **Yaşar-Gökcan-Artuç**, s. 4117, **Dülger**, s. 268.

[361] 31.03.1987 T, 1986/24 E., 1987/8 K. Sayılı Anayasa Mahkemesi Kararı, R.G.t. 28.05.1987, S. 19473, kararın tam metni için bkz. http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=762&content=, 08.05.2012.

Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir." şeklinde tanımlanmıştır[362]. Mahkeme, kararında, özel hayatın korunmasının önemini de "Bu niteliği sebebiyledir ki, özel hayatın gizliliğine dokunulmaması, insan haklarına ilişkin beyanname ve sözleşmelerde korunması istenilmiş, ayrıca tüm demokratik ülke mevzuatında açıkça belirlenen istisnalar dışında bu hak devlet organlarına, topluma ve diğer kişilere karşı korunmuştur. insanın mutluluğu için büyük önemi olan özel hayata saygı gösterilmesi hakkı onun kişiliği için temel bir hak olup yeteri kadar korunmadığı takdirde kişilerin ve dolayısıyla toplumun kendini huzurlu hissedip güven içinde yaşaması mümkün değildir. Bu nedenlerle söz konusu gizliliği çeşitli biçimde ihlal eylemleri suç sayılarak ceza yaptırımlarına bağlanmıştır" ifadesiyle belirtmiştir.

Yukarıda ilgili bölümde incelediğimiz 1982 tarihli Türkiye Cumhuriyeti Anayasası'nda özel hayatın gizliliğini düzenleyen 20 nci maddeye kişisel verilerin korunmasına ilişkin bir fıkra eklenmiştir. Ancak bu fıkra eklenmeden önce de, Anayasa Mahkemesi, 1999 yılında verdiği bir kararda[363], kişisel verilerin korunması hususunun özel hayatın gizliliğinin korunmasıyla doğrudan ilgili olduğunu belirtmiştir[364]. Nitekim Danıştay 12. Dairesi 2006 yılında verdiği bir kararda[365], işe geliş gidişlerini denetlemek istediği çalışanlarının parmakizlerini alan bir belediyenin işlemini değerlendirirken, her ne kadar kararın konusu idari işlemin dava edilebilir olup olmadığı idiyse de, Tetkik Hâkimi uluslararası belgeler ve anayasal düzenlemeler ışığında kişisel verilerin korunmasının özel hayatın gizliliğinin korunması kapsamında değerlendirilmesi gerektiğini belirtmiştir[366]. Hatay İdare Mahkemesi de 2010 yılında verdiği bir kararında, uluslararası ve ulusal mevzuatı değerlendirerek kişisel verilerin korunmasının gerek evrensel gerek bölgesel insan hakları sözleşmelerinde özel yaşamın korunması çerçevesinde değerlendirildiğini belirtmiş, kamusal alanda dahi olsa, parmak izinin kişisel veri olduğu için özel

---

[362] **Ketizmen**, s. 197.
[363] 06.01.1999 T, 1996/68 E., 1991/1 K. Sayılı Anayasa Mahkemesi kararı, R.G.t. 19.01.2001, S. 24292, kararın tam metni için bkz. http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=1458&content=, 13.05.2012.
[364] **Ketizmen**, s. 208.
[365] 15.05.2006 T., 2005/6811 E., 2006/1959 K. Sayılı Danıştay 12. Daire Kararı, kararın tam metni için bkz. http://www.kararevi.com/karars/805368_danistay-e-2005-6811-k-2006-1959, 13.05.2012.
[366] **Akyürek**, s. 44.

hayatın gizliliğinin korunması kapsamında değerlendirilmesi gerektiğini belirtmiştir[367].

Kişisel verilerin öneminin anlaşılmaya başlanması üzerine, bu kavramın özel hayatın gizliliğinin korunması kapsamında değerlendirilmeye başlanmıştır. Çalışmamızın Avrupa İnsan Hakları Sözleşmesi'ni incelediğimiz başlığı altında, AİHM'in bu konuya ilişkin kararlarına yer verilmiş, Mahkeme'nin kişisel verilerin korunmasını AİHS m.8 kapsamında koruma altına aldığı ortaya konmuştur. Nitekim Avrupa Konseyi Parlementerler Meclisi, 1970 tarihli 428 Sayılı kararında tanımladığı özel hayatın gizliliği kavramına[368], 1998 tarihli kararı ile "kişinin kendisi hakkındaki verileri kontrol hakkı" nın da eklenmesi gerektiğini belirtmiştir[369].

c. Suçun Unsurları

(1) Maddi Unsurlar

(a) Fiil

Türk Ceza Hukukunda, suçlar hareketin sayısına göre tek hareketli veya birden fazla hareketli olmak üzere ikiye ayrılırlar. Suçun işlenmesi için kanun koyucunun tek bir hareketin yapılmasını yeterli gördüğü ve bu hareketin yapılmasıyla birlikte suçun tamamlandığı suçlara tek hareketli suçlar, tipiklikte birden fazla hareketin yapılması öngörülmüşse buna da birden fazla hareketli suçlar denir[370]. Kişisel verilerin kaydedilmesi suçu ise, maddede yalnızca "kaydetme" fiilinin işlenmesiyle suçun oluşacağı öngörülmüş olduğundan, tek hareketli suçlardandır.

---

[367] 06.07.2010 T., 2009/915 E., 2010/803 K. Sayılı Hatay İdare Mahkemesi kararı, karar metni için bkz. http://www.isciler.org/yazi/parmak-iziyle-mesai-takibi-yapilamaz.-mahkeme-karari, 12.05.2012.

[368] Özel Hayatın Gizliliğinin Korunması kavramı, kararın "*C. Measures to protect the individual against interference with his right to privacy*" başlığı altında, ikinci paragrafta, "kişinin kendi hayatını asgari müdahaleyle yaşaması" olarak tanımlanmıştır. Kararın tamamı için bkz. **Resolution 428 (1970); Containing a Declaration on Mass Communication Media and Human Rights**, http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/TA70/ERES428.htm, 08.05.2012.

[369] **Ketizmen**, s. 198.

[370] **Artuk**, **Mehmet Emin-Gökcen**, **Ahmet-Yenidünya**, **A. Caner**, Ceza Hukuku Genel Hükümler, 5. Baskı, Ankara 2011, s. 255, **Centel**, **Nur-Zafer**, **Hamide-Çakmut**, **Özlem**, Türk Ceza Hukukuna Giriş, 7. Baskı, İstanbul, Kasım 2011, s. 253, **Koca**, **Mahmut-Üzülmez**, **İlhan**, Türk Ceza Hukuku Genel Hükümler, 4. Baskı, Eylül 2011, s. 107-108, **Zafer**, **Hamide**, Ceza Hukuku Genel Hükümler, 2. Baskı, İstanbul, Ekim 2011, s. 174-175.

Suçlar hareketin şekline göre icrai ve ihmali suçlar olmak üzere ikiye ayrılırlar. İcrai suçlar, yapılmaması emredilmiş olan bir davranışın, yasaklanmış bir normun yapılması, dolayısıyla fiilin yapılmamasını emretmiş olan kuralın olumlu davranışla bozulmasıdır[371]. İhmali suçlar ise, icrai suçların aksine, hukuk kurallarının belirli bir emredici davranış öngörmüş olması, ancak bu hareketin yapılmayarak olumsuz bir davranışla suçun işlenmesi şeklinde oluşurlar[372]. Kişisel verilerin kaydedilmesi suçu, kişisel verilerin hukuka aykırı olarak kaydedilmesini yasaklamakta, bunun aksine bir fiil yapılarak hukuka aykırı kayıt yapıldığında bu eylemi cezalandırmaktadır. Bu itibarla, kişisel verilerin kaydedilmesi suçu icrai hareketle işlenen bir suçtur. Yukarıda değinildiği üzere, kaydetmekten maksat yalnızca bilişim sisteminde yapılacak bir kayıt değil; her tür kayıttır. Dolayısıyla kişisel verilerin bir bilişim sistemine veya veri taşıma aracına girilmesi ile bu kayıt gerçekleştirilebileceği gibi, bir kağıda el yazısıyla veya herhangi bir şekilde yazmak suretiyle kaydedilmesiyle oluşabilir[373]. Kişisel veriler ne şekilde kaydedilirlerse kaydedilsinler, kayıt yapıldığı an bu suç oluşmuş olur; yeter ki kayıt hukuka aykırı olarak yapılsın. Kişisel verinin hukuka aykırı olarak kaydedilmesi suçunun oluşması için mutlaka yeni bir verinin hukuka aykırı olarak kaydedilmesi şart olmayıp; daha önce hukuka uygun bir şekilde kaydedilmiş olan bir verinin, o kaynaktan alınarak hukuka aykırı olarak bir bilişim sistemine kaydedilmesi veya el yazısı ile kaydedilmesi durumunda da bu suç oluşacaktır[374].

Tipiklikte öngörülmüş hareketin devam edip etmemesine ilişkin yapılan değerlendirmede, suçlar ani hareketli ve mütemadi suçlar olmak üzere ikiye ayrılırlar. Hareket yapıldığı anda tamamlanan ve icrasının belirli bir süre devam etmesinin aranmadığı suçlara ani suç, tipiklikte belirtilen hareketin yapılmasıyla suçun tamamlandığı[375] ancak icrasının devam etmesi nedeniyle bitmediği ve failde

---

[371] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 259, **Demirbaş**, **Timur**, Ceza Hukuku Genel Hükümler, 7. Baskı, Ekim 2011, s. 212, **Centel-Zafer-Çakmut**, s. 245 - 246, **Gözübüyük, Abdullah Pulat**, Alman, Fransız, İsviçre ve İtalyan Ceza Kanunlariyle Muhakeyeseli Türk Ceza Kanunu Gözübüyük Şerhi, Cilt I, 5. Baskı, İstanbul 1988, s. 8, **Önder, Ayhan**, Ceza Hukuku Genel Hükümler, Cilt II-III, 2. Baskı, İstanbul 1992, s. 50-51, **Öztürk-Erdem**, s. 173.

[372] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 259, **Demirbaş**, s. 212, **Hakeri**, **Hakan**, Ceza Hukuku Genel Hükümler, 12. Tıpkıbasım, Ankara 2011, s. 140, **Önder, Ayhan**, s. 50-51, **Koca-Üzülmez**, s. 312, **Zafer**, Ceza Hukuku Genel Hükümler, s. 191 - 192.

[373] **Dülger**, s. 271, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 602 - 603, **Ketizmen**, s. 233, **Malkoç**, **İsmail**, Açıklamalı – İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu, 1. Cilt, Ankara 2007, s. 912.

[374] **Dülger**, s. 271.

[375] **Erem**, **Faruk-Danışman**, **Ahmet-Artuk**, **Mehmet Emin**, Ceza Hukuku Genel Hükümler, Ankara 1997, s. 353; "*… mütemadi suç, temadinin sonuna kadar, tamamlanmış olarak devam eder.*"

iradi olarak sürdürdüğü fiile son verme imkân ve iktidarının bulunduğu suçlara ise mütemadi suçlar denilmektedir[376]. 135 inci maddede öngörülen kaydetme hareketinin belirli bir süre devam etmesi aranmadığından ve kişisel verilerin hukuka aykırı olarak kaydedilmesiyle suç oluşmuş olacağından, bu suç ani bir suçtur.

(b) Fail

Kişisel verilerin kaydedilmesi suçunu düzenleyen 135 inci maddede, suçun faili için "kimse" terimi kullanıldığından, kanun fail açısından herhangi bir özellik aramamış, dolayısıyla herkesin bu suçun faili olabileceğini düzenlemiştir. Ancak failin kamu görevlisi olması açısından özel bir düzenleme getirilmiş, bu husus bir nitelikli hal olarak düzenlenmiştir[377]. Gerçekten de, TCK'nın 137 nci maddesinde, failin kamu görevlisi olması nitelikli bir hal olarak öngörülmüştür. Bu nitelikli hal 135 inci madde açısından da uygulanacak, bu husus 135 inci maddenin nitelikli halleri incelenirken ayrıntılı olarak açıklanacaktır. Bu durumda, bu suçun, fail açısından görünüşte özgü bir suç olduğu ortaya çıkmaktadır. Görünüşte özgü suçlarda, fiilin temel şekli herkes tarafından işlenebilirken, belirli özellikleri haiz kişiler tarafından işlenmesi o suçta cezanın artırılmasını veya azaltılmasını gerektiren bir nitelikli hal oluşturur[378]. İşte bu suç açısından da, 135 inci maddede, fail açısından, fiilin kişisel verileri hukuka aykırı olarak kaydeden "kimse" tarafından işlenebileceği belirtilmiştir. Ancak 137 nci maddede yer alan nitelikli hal ile bu suçun "kamu görevlisi tarafından" veya "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi halinde cezanın artırılacağı öngörülmüştür. Dolayısıyla kişisel verileri kaydetme suçu, fail açısından, temel şekli herkes tarafından işlenebilen, ancak belli kişiler tarafından işlendiğinde suçun nitelikli halinin oluştuğu bir görünüşte özgü suçtur.

---

[376] Mütemadi suçların tanımı konusunda doktrinde farklı görüşler bulunmaktadır. Örneğin Centel-Zafer-Çakmut'a ve Kunter'e göre mütemadi suçta devamlılık arz eden husus hem hareket hem neticedir, **Centel-Zafer-Çakmut**, s. 259; Artuk-Gökcen-Yenidünya'ya ve Koca-Üzülmez'e göre ise devam eden icra hareketleridir, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 269, **Koca-Üzülmez**, s. 110; Öztürk-Erdem'e ve Demirbaş'a göre ise devam eden neticedir, **Öztürk-Erdem**, s. 182 - 183, **Demirbaş**, s. 223.

[377] Türk Ceza Kanunu kapsamında, kamu görevlisi ifadesi ile kimlerin kastedildiği, kanunun 6 ncı maddesinde tanımlanmıştır. Buna göre, "*Kamu görevlisi deyiminden; kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi*" anlaşılmalıdır.

[378] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 296, **Koca-Üzülmez**, s. 101, **Zafer**, Ceza Hukuku Genel Hükümler, s. 136, **Öztürk- Erdem**, s. 166.

(c) Mağdur

Mağdur, suçun maddi konusunun sahibidir[379]. Bu suçun mağduru açısından maddede herhangi bir özellik gösterilmemiş olduğundan, mağdur herhangi bir birey olabilecektir. Her ne kadar doktrinde aksine görüş bulunsa da[380], kanaatimizce bu suçun mağduru yalnızca gerçek kişiler olabileceğinden, bu suç açısından mağdur, ancak konunun, yani kişisel verilerin sahibi olan gerçek kişi olabilecektir. Nitekim bu suçu düzenleyen kanun metninin ikinci fıkrasında, kişilerin "ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ilişkin" bilgilerden bahsedilmekte olup, bu tür bilgiler yalnızca gerçek kişilere ait olabilecek bilgiler olduklarından bu suçun düzenlenmesiyle korunmak istenenin gerçek kişiler olduğu anlaşılmaktadır. Ayrıca, suçu düzenleyen 135 inci maddenin gerekçesinde kişisel verinin tanımı yapılırken "gerçek kişiyle ilgili her tür bilgi" den bahsedilmektedir. Tüzel kişiler ise ancak suçtan zarar gören olabileceklerdir[381]. Bu noktada, suçtan zarar görenin, mağdur kavramına nazaran daha geniş olduğunun ve suçtan zarar görenden anlaşılması gerekenin, "bir suçun işlenmesiyle hukuken korunan menfaatleri doğrudan veya dolaylı olarak ihlal olan kimse" olduğunun[382] altını çizmek gerekir.

(d) Konu

"Hareketin yöneldiği kişi ya da şey suçun konusunu oluşturmaktadır."[383] Kişisel verilerin kaydedilmesi suçunun konusu kişisel verilerdir[384].

---

[379] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 313, **Toroslu**, **Nevzat**, Ceza Hukuku Genel Kısım, 16. Baskı, Ankara, Eylül 2011, s. 106.

[380] **Dülger**, s. 269, "*Ayrıca yasada bir ayrım yapılmadığı için bu suçun mağduru hem gerçek hem de tüzel kişiler olabilecektir*.", Aynı yönde bkz. **Soyaslan**, **Doğan**, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010, s. 346; "*Suçun … mağduru ise hem gerçek hem de tüzel kişiler olacaktır*."

[381] **Özgenç**, **İzzet**, Türk Ceza Hukuku Genel Hükümler, 6. Baskı, Ankara 2011, s. 205, **Koca-Üzülmez**, s. 102, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 313; "*Bir suçun mağduru, kural olarak işlenen suç ona karşı bir haksızlık teşkil ettiğinden suçtan zarar görendir… Buna karşılık belirli bir suçtan, onun mağdurundan başka, diğer kimseler de hukuken korunan bir haklarının ihlali dolayısıyla zarara uğramış olabilirler.*"
Aksi görüşte olup, ceza hukukunda tüzel kişilerin de mağdur olabileceğini savunan yazarlar; **Dönmezer**, s. 255, **Zafer**, Ceza Hukuku Genel Hükümler, s. 137, **Demirbaş**, s. 518, **Toroslu**, s. 107.

[382] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 313.

[383] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 309.

[384] Türk Ceza Kanunu'nun kişisel verilerle ilgili olarak düzenlenmiş suçları açısından kişisel veri kavramı ile ilgili olarak yukarıda "1. Genel Bilgiler" başlığı altında açıklama yapıldığından, burada bu husus üzerinde durulmayacaktır.

Kişisel veri, çalışmamızın önceki ilgili başlıklarında açıklandığı üzere, 108 Sayılı Sözleşme'de, "Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder" şeklinde tanımlanmıştır[385]. TCK'nın 135 inci maddesinin gerekçesinde ise, "Gerçek kişiyle ilgili her türlü bilgi" kişisel veri olarak tanımlanmıştır. Dolayısıyla, Türk Ceza Kanunu kapsamında, belli bir kişiye bağlanabilen veya o kişiye aidiyetini gösteren her tür bilgi kişisel veri kapsamındadır. Buna örnek olarak kişilerin ismi, telefon numarası, resmi, parmak izi, genetik bilgileri, adresi vb. bilgiler gösterilebilir. Bir kimsenin yapmakta olduğu iş gereği öğrendiği veya kaydettiği, kişilerin ekonomik harcamaları, telefon numaraları, iş faaliyetlerine ilişkin kişisel veriler de doğaldır ki bu kapsamda kalacaktır. Nitekim Yargıtay 11.Ceza Dairesi 11.07.2006 tarihli ve 5430/6541 Sayılı kararında, "Katılana ait şirkette satış müdürü olarak çalışan sanığın işten ayrılmadan önce kendi şirketini kurup, çalıştığı şirketin müşterilerine ait tüm verileri kendi şirketinde kullanmak üzere hukuka aykırı olarak aktardığı, iddia, tanık beyanları, istenmesi üzerine sanık tarafından elektronik posta ile gönderilen teklif mektubu, bilirkişi raporu ve tüm dosya kapsamıyla sabit olduğu halde yazılı şekilde hüküm kurulması" şeklinde bir değerlendirme yaparak bu kişisel verilerin de 136 ncı madde kapsamında kalacağını belirtmiştir[386].

Doktrindeki farklı bir görüşe göre, yalnızca gerçek kişiler hakkındaki değil, tüzel kişiler hakkındaki kişisel veriler de bu suçun konusunu teşkil edebilecektir[387]. Nitekim Kişisel Veriler Hakkında Kanun Tasarısı'nın ikinci maddesinde, kişisel verileri korunacak kişiler kapsamına gerçek kişilerin yanı sıra tüzel kişiler de dahil edilmiştir ve bazı yazarlar bunun isabetli olduğu kanısındadır[388]. Biz ise tasarıya ilişkin kısımda bu hususta görüşlerimizi ayrıntılı olarak açıkladığımızdan, burada veri öznesi olarak yalnızca gerçek kişilerin düşünülmesi gerektiğini, tüzel kişiler için ise ticari sır kavramının benimsenmesi gerektiğini belirtmekle yetineceğiz. Bu itibarla, düşüncemize göre bu suçun konusunu, 135 inci maddenin gerekçe

---

[385] **Ketizmen**, s. 228, dn. 99.
[386] **Malkoç**, s. 913.
[387] Ayrıntılı bilgi için çalışmamızın "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" başlığı altında, Tasarının ikinci maddesine değinildiği ve bu hususun detaylı bir biçimde farklı doktrinel görüşlerle açıklandığı kısıma bakılmalıdır.
[388] **Başalp**, Kişisel Verilerin Korunması ve Saklanması, s.109, **Şen**, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, s. 1202.

kısmındaki açıklama doğrultusunda, yalnızca gerçek kişilerin kişisel verileri oluşturabilecektir.

Suçlar, suçun işlenmesinin suçun konusuna zarar verip vermemesine göre ikiye ayrılırlar. Tipiklikte suçun işlenebilmesi için konu üzerinde zararın meydana gelmesi gerektiğinin belirtildiği hallerde zarar suçlarından, konuya bir zarar gelmesinin aranmadığı, hareketin yapılmasıyla konunun tehlike altına girmesinin yeterli sayıldığı hallerde ise tehlike suçlarından bahsedilir[389]. Tehlike suçları da, yapılan hareketin suç konusu üzerinde gerçekten tehlike yaratıp yaratmadığına ilişkin hakim tarafından araştırma yapılmasının öngörülüp öngörülmediğine bağlı olarak ikiye ayrılırlar[390]. Şayet kanun koyucu, işlenmiş olan fiilin suçun konusu üzerinde tehlike meydana getirip getirmediğinin hakim tarafından araştırılmasını öngörmüşse, buna somut tehlike suçu denilmektedir. Böyle bir araştırmanın yapılması öngörülmeyip, hareket yapıldığı an suç oluşuyorsa buna da soyut tehlike suçu adı verilmektedir.

Kişisel verilerin kaydedilmesi sebebiyle herhangi bir zararın ortaya çıkması aranmamaktadır. Dolayısıyla bu suç bir zarar suçu değil; bir tehlike suçudur. Zira kişisel verilerin kaydedilmesiyle suç oluşmakta, kişisel verileri kaydedilen kişinin bundan dolayı herhangi bir zarara uğraması aranmamaktadır. Madde metninde, kişisel verilerin hukuka aykırı olarak kaydedilmesi neticesinde, suçun konusunun zarara uğrama tehlikesinin doğup doğmadığının araştırılmasına ilişkin herhangi bir ibare olmadığından, bu suç soyut tehlike suçudur ve kayıt yapıldığı an suç gerçekleşir, ayrıca bir tehlikenin ortaya çıkıp çıkmadığı incelenmez.

(e) Netice

Kişisel verilerin kaydedilmesi suçunun, sırf hareket suçu olduğunu söylemek mümkündür. Sırf hareket suçlarında hareketin yapılmasıyla suç gerçekleşir ve tamamlanır. Bu itibarla sırf hareket suçlarında suçun tamamlanması için neticenin ortaya çıkmasına gerek yoktur; hareketin yapılmasıyla tipiklikte belirtilmiş olan ihlal

---

[389] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 311, **Demirbaş**, s. 226, **Centel-Zafer-Çakmut**, s. 255, **Koca-Üzülmez**, s. 105, **Zafer**, Ceza Hukuku Genel Hükümler, s. 175 - 176, **Öztürk- Erdem**, s. 183.

[390] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 312, **Centel-Zafer-Çakmut**, s. 256 - 257, **Demirbaş**, s. 226, **Zafer**, Ceza Hukuku Genel Hükümler, s. 176.

tamamlanır[391]. Doktrinde bu suçlara neticesi harekete bitişik suç da denmektedir[392]. Kişisel verilerin kaydedilmesi suçu açısından da, herhangi bir neticenin ortaya çıkmasına gerek olmayıp, kişisel verilerin hukuka aykırı olarak kaydı gerçekleştiği an suç oluşmuş olacaktır. Dolayısıyla, sadece kişisel verilerin kaydı suçun oluşması için yeterli olacak, ayrıca failin bu verileri kullanması veya bunlardan bir fayda sağlaması aranmayacaktır.[393]

(f) Suçun Nitelikli Unsurları

Türk Ceza Kanunu'nun 137 nci maddesinde, "(1) Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi halinde, verilecek ceza yarı oranında artırılır" denilmek suretiyle, m.132 ile m.136 arasında tanımlanmış olan suçlar açısından nitelikli haller düzenlenmiştir. Dolayısıyla bu madde, "özel hayata ve hayatın gizli alanına suçlar" başlığı altındaki tüm suçlar açısından uygulanamayacaktır. 137. madde, ancak; "haberleşmenin gizliliğini ihlal" (TCK m.132), "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" (TCK m.133), "özel hayatın gizliliğini ihlal" (TCK m.134), "kişisel verilerin kaydedilmesi" (TCK m.135) ve "verileri hukuka aykırı olarak verme veya ele geçirme" (TCK m.136) suçları açısından uygulanabilecektir. Aynı başlık altında yer alan "verileri yok etmeme" (TCK m.138) suçu açısından bu nitelikli hallerin uygulanması mümkün olmayacaktır.

TCK m. 137'de iki farklı nitelikli hal öngörülmüştür. Bunlar; m.132 ila m.136 arasındaki suçların; kamu görevlisi tarafından ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir. Her ne kadar bu başlık altında açıklandığı üzere, TCK m.137'de öngörülmüş olan nitelikli haller TCK'nın 132 ila 136 ncı maddeleri bakımından geçerli olsalar da, konumuz kişisel veriler olduğundan, bu nitelikli haller aşağıdaki başlıklarda yalnızca 135 ve 136 ncı maddeler açısından incelenecektir.

---

[391] **Dönmezer**, s. 105, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 275, **Centel-Zafer-Çakmut**, s .254, **Koca-Üzülmez**, s. 113, **Demirbaş**, s. 222 - 223, **Zafer**, Ceza Hukuku Genel Hükümler, s. 175 - 176, **Öztürk- Erdem**, s. 181 - 182.

[392] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 275, **Demirbaş**, s. 222.

[393] Aynı yönde; **Yaşar-Gökcan-Artuç** s. 4121.

aa. Suçun Kamu Görevlisi Tarafından ve Görevinin Verdiği Yetki Kötüye Kullanılmak Suretiyle İşlenmesi

Suçun bu nitelikli halini değerlendirilirken, suçun kamu görevlisi tarafından ve görevinin verdiği yetkiyi kötüye kullanarak işlenmesi söz konusu olduğundan, öncelikle "kamu görevlisi" ifadesinin ceza hukuku açısından ne anlama geldiğinin incelenmesi gerekecektir. Kamu görevlisi, Türk Ceza Kanunu'nun 6 ncı maddesinde "Kamu görevlisi deyiminden; kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi" olarak tanımlanmıştır. Bu itibarla kanun koyucu suçların nitelikli hali bakımından kamu görevlisi sıfatını haiz olma şartını aramış, özel hayatın gizliliğine karşı işlenen ve yukarıda sayılan suçların nitelikli hallerini görünüşte özgü suç olarak düzenlemiştir[394].

137 nci maddenin ilk fıkrasına göre, 135 veya 136 ncı maddedeki suçları işleyen kişinin kamu görevlisi olması ve bu işlemi görevinin verdiği yetkiyi kötüye kullanmak suretiyle yapması halinde failin cezası yarı oranında artırılacaktır. Maddenin tanımından da açıkça anlaşıldığı üzere, failin yalnızca kamu görevlisi olması bu nitelikli halin uygulanması için yeterli olmayacak; ayrıca kamu görevlisinin bu fiili görevinin verdiği yetkiyi kötüye kullanarak ve göreviyle bağlantılı olarak işlemiş olması aranacaktır[395]. Buradan da kamu görevlisinin aynı zamanda bu hususta bir yetkisi olması gerektiği de anlaşılmaktadır[396].

Bir polis memurunun, yetkisi kapsamında kalan parmak izi alma veya kişilerin fotoğraflarını kaydetme işlemlerini hukuka aykırı olarak yapması durumunda, bu nitelikli halin uygulanacağı söylenebilir. Aynı şekilde, kişisel verinin kaydedilmesi işlemi hukuka uygun olarak gerçekleşmiş olsa dahi, polis memurunun bu verileri

---

[394] **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 609.
[395] **Şen**, **Ersan**, Yeni Türk Ceza Kanunu Yorumu, s. 608, **Malkoç**, s. 914.
[396] Türkiye Milli DNA Veri Bankası Kanunu Tasarısı'nın yasalaşması halinde, veri bankasının başkan, başkan yardımcısı, Yürütme Kurulu üyeleri ve diğer personelinin, DNA verilerini hukuka aykırı olarak kaydetmesi (m.135) veya hukuka aykırı olarak vermesi veya ele geçirmesi (m.136) durumunda, failin cezası için önce ilgili madde uyarınca cezası belirlenecek, ardından TCK'nın 137 nci maddesi uyarınca kamu görevlisi oldukları için bu cezada yarı oranında artırım yapılacak, son olarak da tasarının 43 üncü maddesinin son fıkrası gereğince toplam ceza yarı oranında artırılacaktır. Ayrıntılı bilgi için "Türkiye Milli DNA Veri Bankası Kanunu Tasarısı" başlığı altındaki açıklamalara bakınız.

daha sonra hukuka aykırı olarak vermesi durumunda, TCK'nın 136 ncı maddesindeki suç oluşacak ve yine bu nitelikli hal uygulanacaktır.

Her ne kadar bir kamu görevlisinin yetkisini kötüye kullanarak TCK m.135 veya m.136'da tanımlanmış olan suçları işlemesi TCK'nın 257 nci maddesindeki kamu görevlisinin görevini kötüye kullanması suçunu oluştursa da, görevi kötüye kullanma suçunun genel nitelikte bir suç olması ve ancak başka bir suç oluşturmayan fiillerin bu madde kapsamında cezalandırılacak olması sebebiyle, TCK m.135 ve m.136'daki suçlar kamu görevlisi tarafından işlendikleri zaman m.257 değil, m.135 veya m.136 ve m.137 uygulanacaktır[397].

ab. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi

137 nci maddede düzenlenmiş olan diğer nitelikli hal de, failin TCK m.135 ve m.136'da düzenlenmiş olan suçları belli bir meslek ve sanatın sağladığı kolaylıktan faydalanarak işlemesine ilişkindir.

Doktrindeki bir görüşe göre, bu madde 765 Sayılı TCK'nın 198 inci maddesinde düzenlenmiş olan "açıklanmasından zarar doğacak bir sırrı sıfatı veya mesleği gereği öğrenip kanuna aykırı olarak açıklama" ve 200 üncü maddede düzenlenen "Posta ve telgraf memurlarından bir kimsenin memuriyet sıfatını suiistimal suretiyle bir mektup, bir zarf, bir telgraf veya sair açık bir muhabere evrakını zapt etmesi veya kapalı evrakı açması veya telefon, telgraf mükalemat ve muhaberatı mahremiyetini ihlal etmesi" suçlarına karşılık olarak düzenlenmiştir[398].

Maddenin düzenlenişinde her ne kadar "meslek ve sanatın" sağladığı kolaylıktan yararlanmaktan bahsedilmiş olsa da, doktrinde "veya" yerine "ve" kelimesinin kullanılmış olmasını eleştiren görüşe[399] katılmaktayız; zira gerçekten de maddenin mevcut düzenleniş biçiminden ortaya sanki bu nitelikli halin uygulanabilmesi için failin hem mesleğinden hem de sanatından yararlanması

[397] **Yaşar-Gökcan-Artuç**, s. 4122.
[398] **Meran**, **Necati**, Gerekçeli-Karşılaştırmalı 5237 Sayılı Türk Ceza Kanunu, Seçkin Yayınevi, Ankara 2004, s. 657, **Polater**, s. 84 - 85.
[399] **Özbek**, TCK İzmir Şerhi, s. 953.

gerektiği gibi bir anlam çıkmaktadır. Oysa ki faile ceza verilirken bu nitelikli halin uygulanması için failin hem mesleğinden hem icra ettiği bir sanattan yararlanmış olmasına gerek olmayıp; bunlardan yalnızca birinin sağladığı kolaylığı kullanmış olması yeterlidir; yeter ki söz konusu meslek veya sanat suçu işlemeye elverişli ve bunun icrası ile suçun işlenmesi arasında bir sebep sonuç ilişkisi olsun[400].

Doktrindeki bir görüşe göre, belli bir meslek ve sanat ifadesinden "bilişim sektörüyle ve bu sektörün teknik kısmıyla ilgili bir iş kolu" anlaşılacaktır[401]. Kanaatimizce, maddenin ifade edilişinden böyle bir sonuca varmak mümkün değildir; zira özellikle kişisel verilerin kaydedilmesi ve kişisel verileri verme veya ele geçirme suçları açısından, bu suçların işlenmesini kolaylaştıracak tek meslek ve sanatın bilişim sektörüyle ilgili olduğunu söylemek, 137 nci maddenin kapsamını anlamsız bir şekilde daraltmak olacaktır. Madde gerekçesinde de açıkça belirtilmiş olduğu üzere, kişisel verilerin kaydedilmesi suçu yalnızca bilişim sistemi aracılığıyla değil, kağıt üzerine kaydetmek şeklinde de olabilecektir. Dolayısıyla, örneğin bir hemşirenin veya doktorun hastaların bilgilerine ulaşmadaki kolaylıkları da icra ettikleri mesleğin getirdiği bir kolaylık kapsamında değerlendirilebilecek, failin cezası 137 nci madde uyarınca artırılacaktır[402].

Şunu ifade etmek gerekir ki; maddenin ikinci fıkrasında "Kişilerin … cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır." denmesi suretiyle bu verilerin özel olarak sayılmaları gereksiz olmuştur; zira bunların kaydedilmesi açısından faile verilecek ceza açısından ilk fıkraya yollama yapılmaktadır. Şayet ikinci fıkrada bu veriler sayıldıktan sonra, bunların hukuka aykırı olarak kaydedilmeleri nitelikli hal olarak düzenlenmiş olup, suçun cezası ağırlaştırılmış olsaydı, bu durumda bu verilerin ismen sayılmalarının bir anlam ifade ettiği söylenebilecekti. Ancak bu durumda ikinci fıkrada sayılan bu veriler bakımından yapılan düzenlemenin ilk fıkradakinden hiçbir farkı kalmamış, bunların sayılması anlamsız olmuştur; zira hem ilk fıkradaki genel düzenlemeye konu olan verilerin hem de ikinci fıkrada sayılmış olan verilerin hukuka aykırı olarak

---

[400] **Özbek**, TCK İzmir Şerhi, s. 954.
[401] **Dülger**, s. 275.
[402] Aynı yönde; **Yaşar-Gökcan-Artuç**, s. 4122, **Özbek**, TCK İzmir Şerhi, s. 954, **Parlar-Hatipoğlu**, s. 2097.

kaydedilmeleri gerekmekte ve iki durum için de aynı ceza öngörülmektedir[403]. Nitekim Türk Ceza Kanununun Meclis Alt Komisyonu tarafından kabul edilen tasarısında söz konusu kişisel verilerin kaydedilmesi suçun nitelikli bir hali olarak öngörülmüş; cezanın daha ağır olmasını gerektirecek bir düzenleme yapılmıştı. Buna rağmen Adalet Komisyonu'ndan genel kurula gönderilen ve sonuçta kanunlaşan metinden bu ifade çıkarılmış, bugünkü haline dönüştürülmüştür[404]. Kanaatimizce, kanun tasarısının bu husus ile ilgili olan kısmı değiştirilmemiş ve 135 inci maddede teker teker sayılan bu nitelikli kişisel verileri kaydetmek cezanın ağırlaştırılması sonucunu doğuracak şekilde kalmış olsaydı, çok daha isabetli olacaktı. Ancak bizim de katıldığımız görüşe göre, bu tür kişisel verilerin kaydedilmesinin haksızlık içeriği daha ağır olduğundan, bu verilerin kaydı gerçekleştiğinde, hakim TCK m.61 gereği ceza tayininde alt sınırdan uzaklaşabilecektir[405].

(2) Manevi Unsur

Bu suçun genel kastla işlenebileceğini söylemek doğru olacaktır. Kanun koyucu bu suçun işlenmesi açısından özel bir kast aramamış, suçun unsuru haline gelecek bir saik belirtmemiştir. Buna ek olarak, kanunda suçun taksirle işlenebileceğine ilişkin herhangi bir düzenleme yapılmamıştır. Suçların taksirle işlenebilmeleri için, mutlaka kanunda taksirle işlenebileceklerine ilişkin özel bir düzenleme bulunmalıdır[406]. Zira Türk Ceza Kanunu açısından suçların kastla işlenmesi genel kural olup; suçların taksirle işlenmeleri istisnai bir durumdur. Dolayısıyla, TCK m.22 gereği, bu suç açısından taksirle işlenmesi hususunda özel bir düzenleme yapılmadığından, suçun taksirle işlenemeyeceği açıktır[407].

Suçun düzenlemesi açısından, ilk fıkrada ve ikinci fıkrada belirli veriler açısından "hukuka aykırı" olarak kişisel verileri kaydetmeden bahsedilmektedir. Dolayısıyla kanun bu suç açısından özel bir hukuka aykırılık bilinci aramaktadır. Her ne kadar bu husus hukuka aykırılık başlığı altında incelenecek olsa da, 1. fıkradaki

---

[403] Aynı yönde bkz. **Malkoç**, s. 912; "*Madde 135/2 nitelikli kişisel sebepleri saymıştır ancak ağırlaştırıcı sebep haline getirmemiştir. Bunların ağırlaştırıcı sebep olarak belirlenmesi gerekirdi*."
[404] **Dülger** s. 275 - 276.
[405] **Malkoç**, s. 912, **Şener**, s. 75.
[406] **Erem, Faruk**, Ümanist Doktrin Açısından: Türk Ceza Hukuku Genel Hükümler, Cilt I, 7. Baskı, Ankara 1966, s.506.
[407] Nitekim bu husus TCK'nın 22 nci maddesinde "*Taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır*" şeklinde belirtilmiştir.

kişisel verileri "hukuka aykırı olarak" kaydetme açısından ve 2. fıkradaki "hukuka aykırı olarak" "kişilerin ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veriler" açısından, bu suç ancak doğrudan kastla işlenebilecek; olası kastla işlenmesi söz konusu olamayacaktır. Ancak kanaatimizce, 2. fıkranın ilk kısmında yer alan "Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenleri" hakkındaki kişisel veriler açısından "hukuka aykırı olarak" kaydetme özel olarak aranmadığından, bu verileri kaydetme açısından suçu doğrudan kastla işlemek mümkün olacağı gibi olası kastla işlemek de mümkün olabilecektir.

Doğrudan kastta, fail, bilinen bir sonucun ortaya çıkmasını isteyerek hareket edecek, yani gerçekleştirmekte olduğu fiilin neticesini bilecek ve meydana gelmesini isteyecektir[408]. Bu durumda kişisel verileri hukuka aykırı olarak kaydeden kimselerin, kişisel verileri hukuka aykırı olarak kaydettiklerini bilmeleri ve istemeleri gerekecektir.

Olası kastta[409], failde kastın bilme unsuru bulunmakta olup isteme unsuru net bir şekilde bulunmamaktadır, ancak failde ayrıca netice açısından bir kabullenme veya umursamama hali söz konusudur[410]. Dolayısıyla suçun faili kanunda geçen "Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenleri" hakkındaki kişisel verileri kaydettiğini bilecek, bunları kaydetmeye ilişkin doğrudan açık bir isteği bulunmayacak; ancak bunları kaydetmeyi umursamayacak veya kabullenecektir. Yalnızca başka bir amacına ulaşabilmek için bu verileri de kaydetme olasılığının yüksek olduğunu bilecek ve kaydetmeyi umursamayacak, ortaya çıkabilecek olan "söz konusu verileri kaydetme" neticesini kabullenecektir.

Bu konuda şöyle bir örnek vermek mümkündür; (B) internet kullanıcıları arasında girilen sitelerle bu sitelere girenlerin yaşları açısından bir araştırma yapmakta, rastgele seçtiği internet kullanıcılarının yaşlarını ve isimlerini kaydederek

---

[408] Doğrudan Kast, Türk Ceza Kanunu'nun 21 inci maddesinin ilk fıkrasında "*Suçun oluşması kastın varlığına bağlıdır. Kast, suçun kanunî tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir.*" Şeklinde tanımlanmıştır.

[409] Olası Kast, Türk Ceza Kanunu'nun 21 inci maddesinin ikinci fıkrasında "*Kişinin, suçun kanunî tanımındaki unsurların gerçekleşebileceğini öngörmesine rağmen, fiili işlemesi halinde olası kast vardır*" şeklinde düzenlenmiştir.

[410] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 331, **Centel-Zafer-Çakmut**, s. 391, **Koca-Üzülmez**, s. 151, **Demirbaş**, s. 356, **Zafer**, Ceza Hukuku Genel Hükümler, s. 216, **Öztürk-Erdem**, s. 252.

sonunda bir istatistik yapma ve bunun sonucunda bir grafik çıkarma amacındadır. (B), bu amaçla (A)'nın kişisel verilerini kendi bilgisayarına kaydetmiştir. Burada (B) açısından manevi unsur incelendiğinde, (B)'nin kaydettiği (A)'ya ait kişisel veriler açısından, (A)'nın adı, soyadı ve yaşı m.135/f.1 kapsamında kaldığından, bu verileri hukuka aykırı olarak kaydettiğini bilmesi aranacaktır ve (B)'nin doğrudan kastının bulunması gerekecektir. Zira aşağıda hukuka aykırılık başlığı altında ayrıntılı olarak açıklanacağı üzere hukuka aykırılık bilinci kastın bilme unsuru kapsamında değerlendirilmekte olup, kişinin hukuka aykırılığı bilmemesi durumunda suçun oluştuğundan söz edilemeyecektir[411].

Aynı örnekte, (B), (A)'nın siyasi ve dini görüşleri açısından, olası kastla hareket etmiş olsa dahi, ayrıca hukuka aykırı olarak hareket ettiğini bilip bilmediğine bakılmaksızın, suç olası kastla işlenmiş sayılacaktır, zira 135 inci maddenin ikinci fıkrasında özel hukuka aykırılık bilinci aranmamıştır. Bu durum için şöyle bir ayrıntıdan bahsedilebilir: (B)'nin, (A)'nın kişisel verilerini başka bir yerden kopyaladığı ve bunlardan yalnızca (A)'nın adını, yaşını ve telefon numarasını kaydetmek istemiş olduğunu, ancak bunları ayrı ayrı kopyalamak için ayıklamak kendisine zor geldiği için, başka kişisel verileri (A'nın siyasi ve dini görüşleri) de içeren dokümanın tamamını kopyalayıp kaydetmiş olduğunu düşünelim. Bu durumda (B), (A)'nın siyasi ve dini görüşlerini kaydettiğini bilecek, bunları kaydetmeyi istememiş olacak, ancak bunların kaydedilmesini umursamayacak ve kabullenmiş olacaktır. (A)'nın adı, yaşı ve telefon numarası olan kişisel verilerini kaydetme hedefine ulaşmak için, (A)'nın dini ve siyasi görüşünün de kaydedilip kaydedilmediğini umursamamış, olası bir kaydı kabullenmiş olacaktır. Bu durumda (A)'nın adı, yaşı ve telefon numarası açısından (B)'nin bu kaydı hukuka aykırı olarak kaydettiğini bilip bilmediği ve doğrudan kastı aranacak, (A)'nın dini ve siyasi görüşleri açısından ise olası kastla hareket etmiş olması suçun oluşması için yeterli olacaktır.

(3) Hukuka Aykırılık

Bu suçtaki hukuka aykırılık unsuru, 135 inci maddenin 1. ve 2. fıkraları açısından, hatta 2. fıkrada özel olarak belirtilmiş olan kişisel veriler arasında da bir

[411] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 402.

ayrıma tabi tutularak incelenmelidir. Maddenin ilk fıkrasında "Hukuka aykırı olarak kişisel verileri kaydeden kimse" den bahsedilirken, ikinci fıkrada "Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse" den bahsedilmektedir. Genel olarak "kişisel veriler" açısından ve "kişilerin ahlakî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel veriler" açısından kanun koyucu tarafından "hukuka aykırı olarak" denilmek suretiyle özel bir hukuka aykırılık bilinci aranmış olmasına rağmen, "siyasî, felsefî veya dinî görüşler, ırkî kökenler" açısından kanun koyucu "hukuka aykırı olarak" ifadesini kullanmamış, dolayısıyla bu kişisel veriler için özel hukuka aykırılık bilinci aranmamıştır.

Kanun koyucunun bazı maddeler açısından özel olarak "hukuka aykırılık" unsurunu vurgulamış olmasına ilişkin doktrinde farklı görüşler mevcuttur[412]. Ancak bizim de katıldığımız görüşe göre, "hukuka aykırılık" unsurunun bazı maddelerde özel olarak belirtilmesi, belirtilmeyen maddeler açısından failde yaptığı fiilin hukuka aykırı olduğu bilincinin aranmayacağı, hukuka aykırılığın özellikle belirtildiği maddeler açısından ise aranacağı anlamına gelmektedir. Dolayısıyla bu durumda maddelerde özellikle belirtilmiş olan hukuka aykırılık artık suçun işlenmesi bakımından, failde özel hukuka aykırılık bilincinin aranacağını göstermekte, bu da tipikliğin içerisinde değerlendirilmektedir[413]. Yani failin kastının bilme unsurunun bu özel hukuka aykırılığı da kapsaması gerekecek ve suç yalnızca doğrudan kastla işlenebilecektir.

---

[412] Bazı suçlar açısından kanunda özel olarak hukuka aykırılık unsurunun vurgulanmasına ilişkin doktrindeki farklı görüşlerle ilgili ayrıntılı bilgi için bkz., **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 402, **Dönmezer**, **Sulhi-Erman**, **Sahir**, Nazari ve Tatbiki Ceza Hukuku Genel Kısım 2, İstanbul 1994, s. 19. Örneğin Dönmezer-Erman'a göre, tipiklikte hukuka aykırılığın özel olarak zikredilmesi halinde, artık failde hukuka aykırı olarak hareket ettiğini bilmesi ve istemesi aranacak, dolayısıyla hakim failin kastını değerlendirirken bu hususu da değerlendirecektir. Nitekim Önder'e göre de, "*Bu biçim suç tiplerinin ihlal edilmiş olması karşısında hakim, bu ihlalin hukuka aykırılığı da ihtiva ettiği ve hukuka aykırılığın karinesini teşkil ettiği esasından hareket edemeyecektir. Öyle ise, hakim bu suçlarda hukuka aykırılığın varlığını ayrıca tesbit etmek zorunda bulunmakta, maddede özellikle gösterilen hukuka aykırılık deyiminin kapsamını ve içeriğini aramak zorunda kalmaktadır.*"; **Önder, Ayhan**, s. 141-142.

[413] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 402; "*Hukuka aykırılık, tipikliğin bir unsuru değil, suçun genel bir unsurudur. Ancak suç tipinde, hukuka aykırılık unsuruna işaret eden, 'hukuka aykırı olarak', 'hukuka aykırı bir başka davranışla', 'hukuka aykırı yolla', 'haklı bir neden olmaksızın' gibi bir ifadeye yer verilmişse, hukuka aykırılık tipikliğe ait bir unsur özelliği kazanır. Çünkü ilgili suç tipinde fiilin hukuka aykırılığına özellikle işaret edilmiştir. Hukuka aykırılığın tipikliğe ait bir unsur özelliği kazandığı bu gibi hallerde, failin işlediği fiilin hukuka aykırı olduğunu bilmesi, yani doğrudan kastla hareket etmesi aranır.*"

Maddede "siyasî, felsefî veya dinî görüşler, ırkî kökenler" açısından hukuka aykırılığın özel olarak belirtilmemiş olması, doktrinde bu verilerin hukuka uygun kaydedilmesinin dahi suça sebep olacağına yönelik fikirlerin doğmasına sebep olmuştur[414].

Bu görüşe göre, siyasi, felsefi veya dini görüşler ve ırki kökenlerle ilgili kişilere ait verilerin kaydedilmesi, fiilin özelliği gereği hukuka aykırıdır ve hukuka uygunluğu söz konusu olamaz; dolayısıyla bu verilerle ilgili olarak yapılacak her türlü kayıt hukuka aykırıdır ve suçtur. Kanaatimizce bu görüş isabetli değildir; zira maddede bu verilerle ilgili olarak "hukuka aykırı olarak" kaydedilmelerinin özel olarak aranmamış olması, bu verilerin hukuka uygun olarak kaydedilseler dahi bunun suç teşkil edeceğini değil, bu verileri kaydeden kimselerde özel bir hukuka aykırılık bilinci aranmayacağına işaret etmektedir. Dolayısıyla bu veriler açısından yapılacak kaydın da hukuka aykırı olması gerekecek, ancak failde hukuka aykırılık bilinci özel olarak aranmayacaktır. Ayrıca hukuka uygunluk sebeplerinin mevcut olması durumunda, artık bunların kaydedilmesinin suç teşkil edeceğini ifade etmek de mümkün olmayacaktır. Kaldı ki, Türk hukukunun bu alandaki düzenlemelerine kaynak teşkil ettiği söylenebilecek "95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi" ile Avrupa Konseyi tarafından hazırlanan "108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmede", ırk, etnik köken, siyasi görüş, dini inanç, sendika üyeliği, sağlık ve cinsel yaşam gibi

---

[414] Bkz. **Parlar-Hatipoğlu**, s. 2089; "*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi, vatandaşlar arasında bu sayılan etmenlere dayanan grup mensubiyeti nedeniyle ayrımlar yapılması, yürürlükteki kanun ve nizamların, uluslararası düzenlemelerin izin vermediği bir durum olduğundan, bu tür bilgilerin kişisel veri olarak kaydedilmesi başlı başına hukuka aykırılık içeriği taşımaktadır. Yasa koyucu bu düzenleme ile aslında millet bireyleri arasında bölücülük yapılmasını önlemek ve özel hayatın gizliliği ve korunması hakkında müdahale içeriği taşıyan bu fiilleri yaptırım altına almak suretiyle bu hakka güvence sağlamak amacını gütmektedir.*"
Bkz. **Ketizmen**, s. 235; "*Madde gerekçesinden, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin veriler yönünden* ***mutlak bir yasak getirilmek istendiği*** *anlaşılmaktadır.*"
Bkz. **Değirmenci**, s. 202; "*135. maddenin 2. fıkrasında ise, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerin* ***hiçbir şekilde kaydedilemeyeceğini*** *belirtmiştir. Ancak madde gerekçesinden de anlaşıldığı üzere siyasi, felsefi veya dini görüşleri ile ırki kökenlerine ait verilerin hiçbir şekilde tutulmamasına karşın, kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerin kaydına, suçlulukla mücadele, suç ve suçluların ortaya çıkarılması amacıyla kanunlarda izin verilebilecektir.*"
Bkz. **Özbek**, TCK İzmir Şerhi, s. 949; "*Yine TCK m.135/2 fıkrada sayılan veriler arasında da bir ayrım yapmış, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgileri mutlak dokunulmaz veriler olarak kabul ederken; ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri nisbi dokunulmaz veriler olarak kabul etmiştir. Diğer bir deyişle ilk grupta yer alan veriler hiçbir şekilde kaydedilemez (işlenemez) ve bunu mümkün kılan bir hukuk kuralı yaratılamaz. Buna karşılık ikinci grup verilerin kaydedilmesi mümkündür.*"

hassas kişisel verilerin temelde işlem yasağına tabi tutulduğu, ancak istisnalar ve iç hukukta yeterli güvencelerin getirilmesi durumunda bunların da kaydedilebileceği öngörülmüştür[415]. Bahsedilen bu düzenlemelere uyum amacı da taşıyan Türk Ceza Kanunu'nun bu maddesinin söz konusu kişisel verilerin kaydedilmesini tamamıyla yasakladığı ve hukuka uygun kayıt yapılsa dahi bunun suç teşkil edeceğini düşünmek, kanaatimizce doğru olmayacaktır.

Hukuka aykırılık tüm suçlar açısından aranan bir unsurdur; zira hukuka uygun yapılan bir eylemin suç teşkil etmesi düşünülemez. Bu sebeple hukuka aykırılığın bazı suçlarda özel olarak belirtilmesi hukuka uygun olarak yapılan kayıtların suç teşkil edeceğini değil; yalnızca artık failde özel hukuka aykırılık bilincinin de aranacağı anlamına gelmektedir[416].

Bu hususta bizim görüşümüzü destekleyen en iyi örnek, 5490 Sayılı Nüfus Hizmetleri Kanunu'nun "Aile kütüklerinde bulunması gereken kişisel bilgileri" düzenleyen 7 nci maddesinin "e" bendinde, bu bilgilerden birinin kişinin "dini" olacağı şeklinde bir düzenleme getirilmiş olmasıdır. Her ne kadar aile kütüklerinde veya nüfus cüzdanında kişilerin hangi dine mensup olduklarına ilişkin bir kaydın tutulması din ve vicdan hürriyeti kapsamında tartışmalı bir husus olsa da, kişisel verilerin kaydedilmesi suçu açısından artık bu kanun maddesinin bir hukuka uygunluk sebebi teşkil ettiği hususunda hiçbir şüphe yoktur. Yukarıda ifade ettiğimiz aksi görüşü savunanlara göre ise, hukuka uygun olarak siyasi, felsefi veya dini görüşlere, ırki kökenlere ilişkin kişisel verilerin kaydedilmesi hiçbir koşulda hukuka

---

[415] **Başalp**, Bağımsız Veri Koruması Kurumlarının Yapısı, s. 18-19.

[416] Aynı yönde bkz. **Yaşar-Gökcan-Artuç**, s. 4120; "*…kişilerin siyasi, felsefi ve dini görüşlerine, ırki kökenlerine ilişkin bilgileri kişisel veri olarak kaydeden kimsenin cezalandırılacağı vurgulanmış, bunun için eylemin hukuka uygun veya aykırı olması arasında bir fark yokmuş gibi düzenleme yapılmıştır. Böylece bu kişisel verileri kaydetmenin bile, YTCK'nın 135. maddesinde düzenlenen suçu oluşturacağı yönünde görüşler oluşmasına sebep olunmuştur. Kanaatimizce, bu şekilde bir yorum kabul edilemez.*"

Aynı yönde bkz. **Dülger**, s. 273; "*Kişisel verilerin kaydedilmesi suçunun düzenlendiği 135. maddenin 2. fıkrasında nitelikli kişisel veriler ayrıca düzenlenirken 'kişilerin siyasi, felsefi ve dini görüşlerine, ırki kökenlerine' ilişkin verilerin kaydedilmesi eylemleri açısından failin yaptığı eylemin hukuka aykırı olduğunu bilmesi hali ayrıca aranmamıştır. Buna göre fail eylemini gerçekleştirirken bunun ister hukuka uygun olduğunu bilsin ister bilmesin hareketinin neticelenmesiyle suç gerçekleşmiş olacak ve artık yargılama esnasında failin hukuka aykırı bir eylem yaptığının bilincinde olarak hareket ettiğinin ispat edilmesi gerekmeyecektir.*"

Şen, Ersan, Yeni Türk Ceza Kanunu Yorumu, s. 605; "*…Türk Ceza Kanunu hükümleri anayasal hüküm niteliği taşımamaktadır. Bu sebeple Yeni Türk Ceza Kanunu'nun 135/II. maddesi, kişilerin siyasi, felsefi veya dini görüşlerine ya da ırki kökenlerine ilişkin veri tespitlerinin yapılmasını uygun sayacak bir özel yasa düzenlemenin önüne geçemeyeceği gibi, yasak da getiremez. Bu konuda, Yeni Türk Ceza Kanunu'nun 5. maddesi de sorunu çözemeyecektir.*"

uygun sayılamayacağına ve suç teşkil edeceğine göre[417]; bu görüş kapsamında aile kütüklerine kişilerin dini görüşlerinin kaydedilmesi 135 inci maddedeki suçu oluşturacaktır ki, buna katılmak kanaatimizce mümkün değildir.

Hukuka uygunluk sebepleri, fiili hukuken meşru hale getirirler ve bu madde açısından hem ilk fıkrada, hem de ikinci fıkradaki tüm kişisel veriler açısından hukuka uygunluk sebeplerinden birinin veya birkaçının bulunması durumunda, kişilerin fiili suç olmaktan çıkacaktır. Türk Ceza Kanunu'nda sayılmış olan hukuka uygunluk sebepleri, kanun hükmünü yerine getirme (TCK m.24/1), meşru savunma (TCK m.25), hakkın kullanılması (TCK m.26/1) ve ilgilinin rızası (TCK m.26/2)'dır.

Kanun hükmünün yerine getirilmesine bu suç açısından örnek vermek gerekirse, 5352 Sayılı "Adli Sicil Kanunu" tarafından, adli sicil kayıtlarının ve mahkumiyetlerin kaydedilebileceği öngörülmektedir. Bu durumda kişilerin adli sicil kayıtlarının ve mahkumiyetlerinin kaydedilmesi kanundaki bir hüküm tarafından öngörülmüş olduğundan, bu tür bir kaydın yapılması, kişisel verinin kaydedilmesini hukuka uygun hale getirecek; suç olmaktan çıkaracaktır.

Kanun hükmünün yerine getirilmesine bir diğer örnek olarak ise, 2559 Sayılı "Polis Vazife ve Selahiyet Kanunu"ndaki[418] düzenlemedir. Bu kanunun 5 inci maddesine göre[419], kişilerin parmak izlerinin ve fotoğraflarının polis tarafından

---

[417] **Özbek**, TCK İzmir Şerhi, s. 949, **Değirmenci**, s. 202, **Ketizmen**, s. 235.

[418] Polis Vazife Ve Selahiyet Kanunu, K.n. 2559; RG.t. 14.07.1934, S. 2751.

[419] PVSK'nın 5 inci maddesine göre, "*Polis;*

a) Gönüllü,

b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan,

c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen,

ç) Türk vatandaşlığına başvuruda bulunan,

d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı,

e) Gözaltına alınan,

kişilerin parmak izini alır.

Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.

Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir.

5271 Sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 Sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir.

(a) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkrada belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir.

arşivlenmesi mümkündür; dolayısıyla bu kapsamda polis tarafından yapılacak olan bir kişisel veri kaydı hukuka uygun sayılacak, 135 inci madde kapsamında suç sayılmayacaktır[420]. Bazı yazarlara göre, kişisel verilere ilişkin olarak bu kanunlar kapsamında gerçekleştirilecek olan kayıtların hukuka uygun sayılmaları ve suç teşkil etmemeleri için, "bu konuda yetkili makama kanun tarafından verilmiş açık bir yetkinin" bulunması gerekmektedir[421].

CMK'nın 135 inci maddesinde de, "Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir" denilerek kişisel verilerin kaydedilmesini hukuka uygun kılan bir hüküm ihdas edilmiştir. Bu madde kapsamında iletişimin dinlenmesi sonucu elde edilen konuşmalara ait kayıtlar da kişisel veri olarak değerlendirilmelerine rağmen; CMK hükmünün yerine getirilmesi söz konusu olduğu için TCK'nın 135 inci maddesi uyarınca suç sayılmamaktadır. Dolayısıyla, CMK m.135'te öngörülmüş olan usul ve esaslara uygun olarak yapılan bir iletişim tespiti, kişisel verilerin kaydedilmesi suçunu oluşturmayacak; bir hukuka uygunluk sebebi teşkil edecektir. Yalnız CMK'nın 135 inci maddesinin 6 ncı fıkrasında şüpheli veya sanığın telefon numaralarını gösterir kayıtlarının hangi suçlar bakımından tutulabileceği belirtilmiş olup, buna aykırı olarak yapılacak bir kaydın, artık hukuka uygunluk sebebi sayılmayacağını ve 135 inci maddedeki suçu oluşturacağını belirtmek gerekir[422].

Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hakim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir.

Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir.

Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkan tanıyan bir güvenlik sistemi kurulur.

Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz.

Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir."

[420] **Yaşar-Gökcan-Artuç**, s. 4119.

[421] **Yaşar-Gökcan-Artuç**, s. 4119.

[422] **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 602.

Kişisel verilerin kaydedilmesi suçu açısından hukuka uygunluk sebebi teşkil edecek benzer Ceza Muhakemesi Kanunu hükümleri ise; 75 inci, 76 ncı, 78 inci ve 81 inci maddelerdir. 75 inci maddeye göre, "Bir suça ilişkin delil elde etmek için şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesine ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine; Cumhuriyet savcısı veya mağdurun istemiyle ya da re'sen hakim veya mahkeme, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verilebilir." 76 ncı madde uyarınca da 75 inci maddede belirtilmiş olan örneklerin, 75 inci maddeden farklı olarak mağdurdan alınmasına Mahkeme tarafından veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısınca karar verilebilir. 78 inci maddede, "75 ve 76 ncı maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler" yapılabileceği ifade edilmiştir. Nitekim CMK madde 80'de " 75, 76 ve 78 inci Madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup..." denmek suretiyle, söz konusu maddeler sonucunda elde edilecek olan sonuçların kişisel veri olduklarına ilişkin açık bir tanımlama yapılmış ve bunların ancak kanunda belirtilen amaçlarla kullanılabilecekleri belirtilmiştir. Dolayısıyla yapılacak bu kayıtlar Ceza Muhakemesi Kanunu uyarınca kanuna uygun bir şekilde yapıldıkları müddetçe, TCK m.135 açısından bir hukuka uygunluk sebebi teşkil edeceklerdir.

Ceza Muhakemesi Kanunu'nun kişisel verilerin kaydedilmesi suçu için hukuka uygunluk sebebi teşkil edecek bir diğer hükmü ise 81 inci maddedir. Bu maddeye göre, "Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur." Böylece, kişiler hakkında kişisel veri niteliği taşıyan bilgilerin kaydedilmesine ilişkin yine açık bir hüküm sevk edilmiştir ve bu da TCK m.135 açısından bir hukuka uygunluk sebebidir.

Bir diğer örnek Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğinin Tespiti Hakkında Yönetmeliğin 15 inci maddesidir[423]. Bu maddede,"Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle, fotoğrafı, iris görüntüsü, beden ölçüleri, diş izi, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak eşkal bilgileri, kulak, dudak gibi organların bıraktığı kimlik tespitine yarayabilecek vücut izleri ile sesi ve görüntüleri, fizik kimliğin tespitinde kullanılan diğer teknik yöntemler ile kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur." denilmek suretiyle şüpheli veya sanığın kişisel verilerinin alınmasına ilişkin bir kural getirilmiştir. Ancak aynı yönetmelik ile, alınan bu kişisel verilerin akıbeti de düzenlenmiştir. 16 ncı maddeye göre, "Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde bu Yönetmeliğin 15 inci maddesi hükümleri uyarınca elde edilen veriler, Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle derhal yok edilir ve bu husus tutanağa geçirilir." Ancak yönetmeliğin 17 nci maddesinde şiddetle eleştirilebilecek bir hüküm getirilmiş ve mahkumiyet kararı verilmesi halinde Yönetmeliğin 15 inci maddesinin birinci ve ikinci fıkraları uyarınca elde edilen verilerin kolluk tarafından, üçüncü fıkrasında belirtilen diş izlerinin ise bu işlemi yapan sağlık kuruluşu tarafından arşivleneceği belirtilmiştir. Bu noktada, bu denli önemli kişisel verilerin kişilerin mahkumiyeti halinde arşivlenmelerinin önü açılmış ancak buna hiçbir sınırlama getirilmemiştir. Bu itibarla bu arşivlemenin ne zaman sona ereceği belirtilmemiş, sanki hakkında mahkumiyet kararı verilmiş sanığın kişisel verilerinin sonsuz bir süre arşivde tutulabileceği şeklinde bir anlam çıkmasına sebep olacak bir düzenleme yapılmıştır. Kaldı ki, Yönetmeliğin 15 inci maddesindeki düzenlemede, üst sınırı iki yıl veya daha fazla olan suçlardan bahsedilmektedir. Bu durumda örneğin 3 ya da 4 yıl hapis cezasına mahkum edilen bir kişinin kişisel verileri bu mahkumiyet sebebiyle arşivlenecek, daha sonra bu verilerle ne yapılacağı sorusu ise yanıtsız kalacaktır. Düşüncemize göre, yönetmeliğin bu maddesinin en kısa sürede düzeltilmesi, arşivlenmiş olan bilgilerin tutulacakları süreye ilişkin açık bir düzenleme getirilmelidir, zira mevcut haliyle bu hüküm mahkumiyet kararı almış olup kişisel verileri arşivlenmiş olan kişilerin özel hayatının gizliliğini ihlal eder mahiyettedir.

[423] **Şener**, s. 79.

Son olarak kanun hükmünün yerine getirilmesine örnek olarak, 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun[424] 4 üncü maddesine değinilebilir. Bu madde kapsamında sayılmış olan görevler çerçevesinde Milli İstihbarat Teşkilatı'nın kişisel verileri kaydetmesinin hukuka aykırı sayılamayacağı ve bu kayıtların TCK m.135 kapsamında suç teşkil etmeyeceği söylenebilir.

Bir diğer hukuka uygunluk sebebi olarak TCK'nın 26 ncı maddesinin ilk fıkrasında düzenlenmiş olan hakkın kullanılması da bu başlık altında incelenmelidir. Örnek olarak hekimlerin, avukatların veya gazetecilerin mesleki gereklerden kaynaklanan mecburiyetle kişisel verileri kayda almaları durumunda, 135 inci maddede düzenlenen kişisel verilerin kaydedilmesi suçu oluşmayacaktır[425].

Son olarak yine bir diğer hukuka uygunluk sebebi olan ve TCK'nın 26 ncı maddesinin ikinci fıkrasında düzenlenen ilgilinin rızasının da kişisel verilerin kaydedilmesi açısından hukuka uygunluk sebebi teşkil edeceği açıktır[426]. Nitekim; madde gerekçesinde "Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır" denmektedir. Yukarıda CMK'nın 76 ncı maddesi uyarınca 75 inci maddede belirtilmiş olan örneklerin mağdurdan alınmasına Mahkeme tarafından veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısınca karar verilebileceğine değinilmişti. 76 ncı maddenin ikinci fıkrasında "Mağdurun rızasının varlığı halinde, bu işlemlerin yapılabilmesi için birinci fıkra hükmüne göre karar alınmasına gerek yoktur" denilmek suretiyle mağdurun rızasının bu örneklerin alınması için yeterli olduğu ve bu rızanın varlığı halinde birinci fıkrada

---

[424] Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, K.n. 2937; R.G.t. 03.11.1983, S. 18210.

[425] **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 603, **Malkoç**, s. 912.

[426] Aksi görüş için; **Özbek**, TCK İzmir Şerhi, s. 957 – 958; "… *Ancak bilindiği üzere mağdurun üzerinde serbestçe tasarrufta bulunabileceği bir hakkın var olup olmadığı konusunda yararlanılabilecek bir başka kriter fiilin şikayete tabi olup olmadığıdır. Kural olarak soruşturulması ve kovuşturulması şikayete tabi suçlar bakımından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu kabul edilebilir. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında düzenlenmiş bulunan suçlardan kişisel verilerin kaydedilmesi suçu şikayete tabi değildir. Bu durumda yasa koyucunun bu bölüm altında yer alan suçlar bakımından kişisel veriler bakımından bireyin değil, kamunun menfaatinin daha ağır bastığını kabul ettiği söylenebilir. O halde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından ilgilinin rızası hukuka uygunluk sebebi uygulanabilir değildir.*"

sayılmış olan koşullar aranmaksızın söz konusu örneklerin alınmasının hukuka uygun olacağı vurgulanmıştır.

Günümüzde bankalarda doldurulan formlarda, internet üzerinden herhangi bir siteye üye olunurken, alışveriş için kullanılacak indirim kartlarının formlarında ve benzeri yerlerde kişiler kendi rızalarıyla kişisel bilgilerini vermektedirler. Burada üzerinde durulması gereken temel husus, kişinin verilerini paylaşırken güttüğü amaçtır. Çoğunlukla, kişilerin paylaştıkları kişisel veriler, kişilerin rızası bulunduğundan hukuka uygun olarak kaydedilmekte; ancak daha sonra bu verileri alan kurum ve kuruluşlar tarafından kişilerin bu verileri verme amacı kullanılmaktadırlar. Bu kullanım bu verileri kişinin rıza gösterdiği amacın dışında kaydetmek olabileceği gibi, bu verileri başka kurum ve kuruluşlara verme veya satma şeklinde tezahür edebilmektedir. Hukuka uygun olarak kaydedilmiş olan verilerin başkalarına verilmesi 136 ncı madde kapsamında inceleneceğinden bu husus üzerinde durulmayacaktır; ancak hukuka uygun olarak yapılan bir kaydın amacı dışında kullanılması hususu üzerinde durmak gerekecektir.

Bu tür durumlarda temel sorun, hukuka uygun olarak kaydedilmiş olan kişisel verilerin hukuka aykırı bir amaç için kullanılmasının 135 inci maddedeki suç kapsamında değerlendirilip değerlendirilmeyeceğine ilişkindir. Düşüncemize göre, ilgili kişinin rıza gösterdiği amaç dışında kişisel verilerinin toplanmasının ya da kanun tarafından gösterilmiş olan amaç dışında kaydedilmesinin madde 135 kapsamında suç olarak kabul edilebileceği muhakkaktır[427].

Hukuka uygun olarak alenileşmiş kişisel verilerin kaydedilmelerinin de artık suç sayılmayacağını kabul etmek gerekecektir. Zira kişisel verilerin hukuka aykırı olarak kaydedilmelerinin kişilerin özel hayatını korumak maksadı taşıdığı dikkate alındığında, artık bu tür bir kişisel verinin kaydedilmesinin kişilerin özel hayatına müdahale olduğunun kabul edilmesi mümkün olmayacaktır ve dolayısıyla kişisel verilerin kaydedilmesi suçu oluşmayacaktır[428].

[427] Aynı yönde; **Ketizmen**, s. 237, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 603.
[428] **Ketizmen** s. 239.

d. Suçun Özel Görünüş Şekilleri

(1) Teşebbüs

Kişisel verilerin kaydedilmesi suçu sırf hareket suçu olduğundan; bu suçun teşebbüs aşamasında kalması ancak icra hareketlerinin bölünebilir olması durumunda söz konusudur[429]. Örneğin; (A), (B)'nin Facebook sayfasında yalnızca arkadaşlarıyla paylaşmış olduğu kişisel verileri, (B)'nin arkadaşı olmaması halinde göremez. Ancak (A), o verileri görmesini sağlayan bir program kullanarak verileri kaydetmek üzere kopyalar, fakat kaydedecek herhangi bir word sayfası açamadan bilgisayarı kapanırsa ve kaydetmek istediği verileri kaydedemezse, kişisel verilerin kaydedilmesi suçu teşebbüs aşamasında kalmış olacaktır. Zira bu durumda kişisel veriyi kopyalayarak icra hareketlerine başlamış olacak, ancak word dosyasına yapıştırıp dosyayı kaydetmediği için icra hareketleri (A)'nın iradesi dışındaki sebeplerden dolayı tamamlanamadığından suç oluşmuş olmayacaktır.

Yukarıda manevi unsurlar başlığı altında da değerlendirildiği gibi, kişilerin "siyasî, felsefî veya dinî görüşler, ırkî kökenlerine" ilişkin kişisel verilerin açısından hukuka özel aykırılık aranmadığı için bu veriler olası kastla da kaydedilebileceklerinden, böyle bir durumda suçun teşebbüs aşamasında kalması söz konusu olamayacaktır. Olası kastla işlenen suçlara teşebbüs mümkün olmadığından, bu verilerin olası kastla kaydedilmeleri açısından da teşebbüsten bahsedilemeyecektir.

Türk Ceza Kanunu'nun 36 ncı maddesinde gönüllü vazgeçme hususu düzenlenmiştir. Buna göre, "Fail, suçun icra hareketlerinden gönüllü vazgeçer veya kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlerse, teşebbüsten dolayı cezalandırılmaz; fakat tamam olan kısım esasen bir suç oluşturduğu takdirde, sadece o suça ait ceza ile cezalandırılır." Gönüllü vazgeçmeden bahsedebilmek için, failin vazgeçme aşamasında hür iradesinin bulunması gerekmekte[430], harici maddi veya manevi sebeplerle iradesinin etkilenmemiş olması

---

[429] **Toroslu**, s. 294.

[430] **Demirbaş**, s. 440. Nitekim Yargıtay Ceza Genel Kurulu, 25.04.2983 T., 6/98 E. ve 194 K. Sayılı kararında, gönüllü vazgeçmeyi "*Fail icra hareketlerini yarıda bıraktığı zaman bunları sonuna kadar götürebileceği kanaatinde ise ve bu kanaate rağmen icraya devam etmemişse, ihtiyariyle vazgeçme vardır*" şeklinde tanımlamıştır.

aranmaktadır[431]. Buna ek olarak, gönüllü vazgeçme hükümlerinin uygulanabilmesi için, suçun teşebbüs aşamasına gelmiş olması, yani failin suçun icrasına doğrudan doğruya başlamış olması gereklidir[432]. Sırf hareket suçlarında, hareket yapıldığı anda netice de ortaya çıkmakta olup, kişisel verilerin kaydedilmesi suçunun sırf hareket suçlarından olduğundan, bu suç açısından gönüllü vazgeçmenin mümkün olabilmesi ancak icra hareketlerinin bölünebilir olmaları durumunda söz konusu olacaktır. Yukarıda verilen örneğe bakıldığında, (A)'nın kaydetme işleminden kendi hür iradesiyle vazgeçerek bilgisayarı kapatması veya kopyalama işlemini tamamlamaması halinde gönüllü vazgeçmeden bahsedilecek ve (A)'ya bu kişisel verilerin kaydedilmesi suçuna teşebbüsten ceza verilmeyecektir. Ancak bilgisayarın kapanması veya elektriklerin kesilmesi gibi kendi iradesi dışındaki etkenler sebebiyle (A)'nın eylemini tamamlayamaması halinde, (A) bu suça teşebbüsten cezalandırılacaktır.

(2) İştirak

Bu suç açısından iştirakin her halinden bahsetmek mümkün olabilecektir. Suçun birden fazla kişi tarafından müştereken ve fiil üzerinde ortak hakimiyet kurma suretiyle işlenmesi halinde, bu kişilerin her biri müşterek fail olarak (TCK m.37/f.1) sorumlu tutulacaktır. Yaptığı fiilin hukuki anlam ve sonuçlarını veya suç olduğunu anlamayan bir kişinin, örneğin bir çocuğun veya bir akıl hastasının, araç olarak kullanılarak bu suçun işlenmesi halinde ise, diğer kişileri araç olarak kullanan kişi suçun işlenmesinden fail olarak sorumlu tutulacaktır (TCK m.37/f.2). Türk Ceza Hukukunda dolaylı fail olarak adlandırılan bu kimseler, suç teşkil eden fiili kendileri bizzat işlemeseler de, fiili suç işlediğinin farkında olmayan birine işletmekte olduklarından cezai sorumluluk açısından fail gibi cezalandırılırlar[433]. Hukuka aykırı olarak kişisel verilerin kaydedilmesi için aklında bu suçu işleme fikri olmayan bir kişiyi suç işlemeye ikna ederek azmettiren kişi azmettiren olarak (TCK m.38), bu suçu işlemek isteyen bir kişinin suçu işlemesini kolaylaştıran, kendisine yardım eden kişi de yardım eden olarak (TCK m.39) sorumlu tutulabilecektir.

---

[431] **Dönmezer**, s. 127, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 610, **Centel-Zafer-Çakmut**, s. 462, **Zafer**, Ceza Hukuku Genel Hükümler, s. 378, **Öztürk-Erdem**, s. 302, **Toroslu**, s. 290.

[432] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 610, **Öztürk-Erdem**, s. 301.

[433] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 635, **Centel-Zafer-Çakmut**, s. 487, **Zafer**, Ceza Hukuku Genel Hükümler, s. 394.

Bu suçun nitelikli hali kapsamında, iştirak edenlerin kamu görevlisi olmaları veya belli bir sanat veya meslek sahibi olmaları halinde, bu kişilere verilecek ceza daha ağır olacaktır. Suçun nitelikli hallerinden biri suçu işleyenin kamu görevlisi olması olduğundan, çalışmamızın üst kısmında belirtildiği üzere, görünüşte özgü suçtan bahsedilecektir. Özgü suçlara iştirakte uygulanan kurala göre, suçun faili olabilmek için gerekli özelliği haiz olmayan kişi, müşterek fail olarak değil, azmettiren veya yardım eden olarak sorumlu tutulur[434]. Ancak, "şerikliğe nazaran failliğin asliliği" prensibi gereğince[435], kamu görevlisi olmayan bir kişi ile kamu görevlisi olan bir kimsenin bu suçu birlikte işlemeleri halinde, kamu görevlisi olmayan fail 135 inci maddedeye göre, kamu görevlisi olan fail ise 137 nci maddedeki nitelikli hale göre cezalandırılacaktır. Bu itibarla, 137 nci maddede düzenlenen suçun nitelikli halinin işlenebilmesi için, failin kamu görevlisi olması şart olup, kamu görevlisi olmayan bir kişinin kamu görevlisini azmettirmesi veya yardım etmesi halinde, bu kişi azmettiren veya yardım eden olarak sorumlu tutulacak, ancak kamu görevlisi olmayan bir kişinin suçun işlenmesine bizzat katılması halinde, bu kişi azmettiren veya yardım eden olarak değil, şerikliğe nazaran failliğin asliliği prensibi uyarınca 135 inci maddeye göre fail olarak cezalandırılacaktır[436].

(3) İçtima

İçtima açısından ilk olarak 135 inci maddedeki suçu zincirleme suç hükümleri kapsamında değerlendirmek gerekir. Kişisel verilerin kaydedilmesi suçunun, aynı kişiye değişik zamanlarda birden fazla kez işlenmesi halinde TCK m.43'ün birinci fıkrasında düzenlenmiş olan zincirleme suç hükümleri bu noktada uygulama bulacaktır. Bu hükme göre "Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır."

---

[434] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 635, **Centel-Zafer-Çakmut**, s. 497, **Koca-Üzülmez**, s. 383, **Zafer**, Ceza Hukuku Genel Hükümler, s. 404.

[435] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s.658.

[436] Nitekim, Resmi Belgede Sahtecilik suçunu düzenleyen TCK'nın 204 üncü maddesinde de, ilk fıkrada sivil bir kimsenin bu suçu işlemesi düzenlenmiş, ikinci fıkrada ise suçu işleyenin kamu görevlisi olması durumunu düzenleyen nitelikli bir hal öngörülmüştür. Bu suçta da, sivil bir kişi ile kamu görevlisinin suçu birlikte gerçekleştirmeleri halinde, sivil olan fail 204 üncü maddenin ilk fıkrasına göre fail olarak, kamu görevlisi olan fail ise aynı maddenin ikinci fıkrasına göre fail olarak cezalandırılır. **Artuk**, **Mehmet Emin-Gökcen**,**Ahmet-Yenidünya**, **A. Caner**, Ceza Hukuku Özel Hükümler, 11. Baskı, Ankara 2011, s. 518.

Tek bir hareketle birden fazla kişinin kişisel verilerinin kaydedilmesi durumu için ise, doktrinde iki farklı görüş vardır. Bunlardan birine göre[437], bu durumda da zincirleme suç hükümleri uygulanacak; ancak diğer görüşe göre[438] verilerin ait olduğu kişi sayısınca suç oluşacaktır. Tek bir fiille birden fazla kişiye karşı suç işlenmesi hali, TCK'nın 43 üncü maddesinin ikinci fıkrasında düzenlenmiştir ve doktrinde buna bazı yazarlarca aynı neviden fikri içtima denilmektedir[439]. Buna göre, "Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da, birinci fıkra hükmü uygulanır", yani bir cezaya hükmedilir ancak bu ceza dörtte birinden dörtte üçüne kadar artırılır. Maddenin üçüncü fıkrasında ise, kasten öldürme, kasten yaralama, yağma ve işkence suçları açısından bu hükmün uygulanmayacağı ve her bir suç için ayrı ceza verileceği belirtilmiştir. Bu itibarla, bizim düşüncemize göre, kişisel verilerin kaydedilmesi suçu TCK'nın 43 üncü maddesinin üçüncü fıkrasında yer alan suçlardan olmadığından, doktrindeki ilk görüş isabetli olup, tek bir hareketle birden fazla kişinin kişisel verileri hukuka aykırı olarak kaydedilirse aynı neviden fikri içtima hükümleri uygulanarak bir cezaya hükmedilecek, ancak failin cezası artırılacaktır.

TCK'nın "Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında yer alan diğer suçlar, 132 nci maddede düzenlenen "Haberleşmenin gizliliğini ihlal"[440], 133 üncü maddede düzenlenen "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması"[441] ve 134 üncü maddede yer alan "Özel hayatın gizliliğini ihlal"

---

[437] **Yaşar-Gökcan-Artuç**, s.4122.
[438] **Malkoç**, s. 912.
[439] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 693, **Koca-Üzülmez**, s. 422.
[440] TCK'nın 132 nci maddesine göre, *"(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.*
(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.
(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.
(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır."
[441] TCK'nın 133 üncü maddesine göre, *"(1) Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.*
(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adlî para cezası ile cezalandırılır.
(3) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı

suçlarıdır. Bu bölümde, 135 inci maddede düzenlenmiş olan "Kişisel verilerin kaydedilmesi" suçunun bu maddelerle olan ilişkisine değinmek gerekir.

132 inci maddenin birinci fıkrasının ilk cümlesinde, kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi suç olarak düzenlenmiş, ikinci cümlede ise bu gizlilik ihlalinin haberleşme içeriklerinin kaydı suretiyle gerçekleşmesi halinde cezanın artırılacağı öngörülmüştür. Bu maddede düzenlenmiş olan suçu işleyen bir kimsenin, haberleşme içeriklerini kaydetmek suretiyle gerçekleştirdiği fiil kapsamında, yaptığı kayıtların içerisinde kişisel verilerin de bulunması halinde, hem 132 nci maddenin ilk fıkrasında düzenlenmiş olan suçu, hem de 135 inci maddede düzenlenmiş olan kişisel verilerin kaydedilmesi suçunu işlemiş olacaktır. Böyle bir durumda, kanaatimizce fail işlediği her iki suçtan ayrı ayrı cezalandırılmayacak, bu suçlar arasında farklı neviden fikri içtima hükümleri uygulanarak, tek bir hareketiyle kanunun birden fazla suçun oluşmasına sebebiyet veren fail, TCK'nın 44 üncü[442] maddesine göre en ağır cezayı gerektiren suçun cezasıyla cezalandırılacaktır.

TCK'nın 133 üncü maddesinin birinci fıkrasında, kişiler arasında aleni olmayan konuşmaların bir aletle dinlenmesi veya bunların bir ses cihazı ile kaydedilmesi suç olarak düzenlenmiştir. Maddede suç olarak düzenlenmiş olan kişiler arasındaki aleni olmayan konuşmaları bir ses cihazı ile kaydeden kişinin, aynı zamanda birtakım kişisel veriler de kaydetmiş olması durumunda kişisel verilerin kaydedilmesi suçu da oluşmuş olacaktır. Örneğin kişiler arasında aleni olmayan siyasi içerikli bir tartışmadaki konuşmaları kaydeden bir kişi, hem kişiler arasındaki aleni olmayan konuşmaları kaydederek 133 üncü maddede düzenlenmiş olan suçu, hem de kişilerin siyasi görüşlerini ifade etmiş olmaları durumunda kişisel verilerin kaydedilmesi suçunu işlemiş olacaktır. Bu durumda da, 132 nci madde ile ilgili olarak söylediğimiz gibi, 133 üncü ve 135 inci maddelerde düzenlenen suçlar arasında farklı neviden fikri içtima hükümlerinin (TCK m.44) uygulanması gerekeceği ve failin en ağır cezayı gerektiren suçtan cezalandırılması gerektiği kanaatindeyiz. Böyle bir durumda 135 inci maddede düzenlenen kişisel verilerin kaydedilmesi suçunun cezası daha ağır olduğundan bu maddeye göre hüküm tesis

---

aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de, aynı cezaya hükmolunur."

[442] Türk Ceza Kanunu'nun 'Fikri İçtima' başlıklı 44 üncü maddesi, "*İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.*" şeklinde düzenlenmiştir.

edilecek, ancak yapılan kayıt esnasında birden fazla kişinin kişisel verileri kaydedilmişse, zincirleme suç hükümleri de uygulanarak, tek fiille birden fazla kişiye karşı kişisel verilerin kaydedilmesi suçu işlendiğinden, aynı neviden fikri içtima hükmü (TCK m.43/2) gereği failin cezası artırılacaktır.

133 üncü maddenin ikinci fıkrasında, aleni olmayan bir söyleşinin ses alma cihazı ile diğer konuşanların rızası olmadan kaydedilmesi suç olarak düzenlenmiştir. 133 üncü maddenin ilk fıkrası ile ilgili olarak yukarıdaki paragrafta yaptığımız açıklamaya benzer olarak, bir kişinin söyleyişinin kaydedilmesi esnasında sesini kaydettiği kişilere veya başkalarına ait kişisel verileri de kaydetmesi durumunda, 135 inci madde düzenlenen kişisel verilerin kaydedilmesi suçu da oluşmuş olacaktır. Örneğin, yapılan söyleşinin kişilerin siyasi görüşlerini, dini görüşlerini veya aileleri ile ilgili hususi durumlarını paylaştıkları bir söyleşi olması halinde, yapılacak kayıt 133 üncü maddedeki suçu meydana getirdiği gibi, 135 inci maddedeki suç da oluşmuş olacaktır. Böyle bir durumda, düşüncemize göre, oluşan bu iki suç arasında fikri içtima hükümleri uygulanarak, fail en ağır cezayı gerektiren suçtan dolayı cezalandırılacaktır. Kişisel verilerin kaydedilmesi suçunun, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçundan daha ağır bir ceza gerektirdiği göz önüne alındığında, böyle bir durumda fail, kişisel verilerin kaydedilmesi suçundan yargılanacak, birden fazla kişinin kişisel verilerini yaptığı tek hareket olan "kaydetme" ile kayıt altına alması durumunda, aynı neviden fikri içtima hükmü (TCK m.43/2) dolayısıyla cezası artırılacaktır.

İçtima açısından 135 inci maddenin 134 üncü madde ile ilişkisi üzerinde de durulmalıdır. 134 üncü maddenin ilk fıkrasında "Kişilerin özel hayatının gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, cezanın alt sınırı bir yıldan az olamaz." şeklinde bir düzenleme yer almaktadır. Doktrindeki bir görüşe göre[443], kişisel verilerin özel hayatın gizliliğinin ihlal edilerek kaydedilmesi durumunda 134 üncü maddenin ilk fıkrasında tanımlanmış olan suç oluşacaktır. Kanaatimizce bu görüş kısmen doğrudur; zira 134 üncü maddenin ilk fıkrasının ikinci cümlesinde gizliliğin "görüntü veya seslerin"

[443] **Parlar-Hatipoğlu**, s. 2089 - 2090.

kayda alınması suretiyle ihlalinden bahsedilmektedir[444]. Bu koşullarda, kişilerle ilgili görüntü veya seslerin dışındaki kişisel verilerin kaydedilmesi açısından, bir anlamda özel hayatın gizliliği ihlal edilmiş olsa da, 134 üncü maddede tanımlanmış olan suçun değil, 135 inci maddedeki kişisel verilerin kaydedilmesi suçunun oluşacağı kabul edilmelidir. Şayet kişisel veri olan "görüntü veya seslerin" kaydedilmesi söz konusu ise, bu durumda 134 üncü madde ile 135 inci madde arasında farklı neviden fikri içtima hükümleri uygulanacaktır.

135 inci maddede düzenlenmiş olan kişisel verilerin kaydedilmesi suçu ile 136 ncı maddede düzenlenmiş olan kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun içtima açısından birlikte değerlendirilmeleri 136 ncı maddedeki içtima başlığı altında incelenecektir; zira bu iki suç açısından içtima durumunun değerlendirilebilmesi için öncelikle 136 ncı maddenin de incelenmesi gerektiği görüşündeyiz.

TCK'nın 'Bilişim Sistemine Girme' başlıklı 243 üncü maddesinde düzenlenen suç ile 135 inci maddedeki suçların bir arada işlenmeleri de mümkündür. Bu durumda, kişisel verileri kaydedecek olan kimselerin, bu suçu bilişim sistemlerine girme suretiyle işleyebilecekleri de malumdur. TCK'nın 243 üncü maddesinde, "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimsenin" cezalandırılacağı öngörülmüştür. Dolayısıyla başkasının kişisel verilerini kaydetmek isteyen bir kimse, bu kişisel verilerin bir bilişim sisteminde kayıtlı olması durumunda, önce bu bilişim sistemine girecek, ardından oradaki verileri alıp kendi istediği bir yere kaydedecektir. Failin kişisel verilere ulaşmak ve onları kaydetmek için bir bilişim sistemine girmesi gereken durumlar açısından, doktrinde[445] bizim de katıldığımız bir görüşe göre, 243 üncü maddedeki bilişim sistemine girme suçu, 135 inci maddedeki kişisel verilerin kaydedilmesi suçu açısından geçitli bir suç olacaktır[446]. Böylece tek suç oluşacak, fail yalnızca kişisel verilerin kaydedilmesi suçu bakımından öngörülmüş olan cezaya

---

[444] Aynı yönde, **Soyaslan**, s. 344; "*Veri olarak kaydedilen şey kişiye ait ses veya görüntü ise, … 134/2. maddeyi ihlal suçunu oluşturacaktır.*"

[445] **Dülger**, s. 275.

[446] **Dönmezer**, geçitli suçu, "*… aynı bir failin, aynı mağdura karşı hafiften ağıra doğru giden bir süreç izleyerek ve fakat bütün hareketleriyle de aynı bir hukuki yararı ihlal etmek suretiyle ve işlediği suça ait neticelerin aynı harekete tek bir nedensellik bağlantısı ile bağlandığı ve cürmi kastın da hafiften ağıra doğru değişik neticeleri içerdiği suçtur… fail daha ağır suçu işlemek için, daha hafif suçtan geçmek durumunda kalmaktadır.*" şeklinde tanımlamıştır, s. 117.

çarptırılacaktır. Ancak fail bir bilişim sistemine girmiş ve orada belli bir süre kalmış, sistemde tesadüfen gördüğü kişisel verileri de kaydetmişse, artık bu iki suç arasında gerçek içtima hükümlerinin uygulanarak faile her iki suçtan da ceza verilmesi gerektiğini kabul etmek gerekecektir.

135 inci maddenin uygulanması açısından, bu başlık altında üzerinde durulacak bir diğer husus, TCK'nın 244 üncü maddesi ile ilişkisidir. 244 üncü maddenin 2 nci fıkrasında "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" denilmiştir. 244 üncü maddede bahsedilen verilerin sisteme yerleştirilmesi her ne kadar 135 inci maddedeki suça benzese de, 135 inci maddede düzenlenen suç yalnızca kişisel verileri kapsarken, 244 üncü maddedeki suç genel olarak tüm verileri kapsar. Buna ek olarak 135 inci maddede kişisel verilerin kaydedilmesi bilişim sistemiyle yapılabileceği gibi, başka yollardan da yapılabilir. Halbuki 244 üncü maddede verilerin sisteme yerleştirilmesi ancak bilişim sistemi içerisinde yapılabilecektir. Kanaatimizce kişisel verilerin bilişim sistemleri kullanılarak bir bilişim sistemine yerleştirilmek suretiyle kaydedilmeleri durumunda, failin tek hareketiyle hem 135 inci maddede düzenlenmiş olan kişisel verilerin kaydedilmesi suçu, hem de 244 üncü maddenin ikinci fıkrasında düzenlenmiş olan sisteme veri yerleştirme suçu oluşmuş olacaktır. Bu durumda da, oluşan bu suçlar arasında fikri içtima hükümleri uygulanarak fail cezası en ağır olan suçun cezasıyla cezalandırılacaktır.

TCK'nın 286 ncı maddesinde düzenlenen 'Ses veya Görüntülerin Kayda Alınması' suçu, soruşturma ve kovuşturma işlemleri sırasındaki ses veya görüntüleri yetkisiz olarak kayda alan veya nakleden kişinin, altı aya kadar hapis cezası ile cezalandırılacağını öngörmüştür. Yapılan kaydın, soruşturma işlemlerine dahil olmuş kişilerin veya başkalarının kişisel verilerini içermesi halinde, hem 286 ncı maddede düzenlenen suç, hem de 135 inci maddede düzenlenmiş olan kişisel verilerin kaydedilmesi suçu işlenmiş olacak, böylece fail tek bir fiil ile kanunu birden fazla hükmünü ihlal etmiş olacaktır. Failin bu iki suçu tek bir fiille işlemesi halinde, fail her iki suçtan ayrı ayrı cezalandırılmayacak, fikri içtima hükümleri uygulanarak faile en ağır cezayı öngören suçun cezası verilecektir. Bu iki madde değerlendirildiğinde, 135 inci maddede daha ağır bir cezanın öngörüldüğü ve dolayısıyla faile 135 inci

maddenin uygulanacağını söylemek mümkün olacaktır. Yapılan kayıtta birden fazla kimsenin kişisel verilerinin bulunması halinde ise, aynı neviden fikri içtima hükümleri uygulanarak failin cezası artırılacaktır.

e. Yaptırım

Kişisel verilerin kaydedilmesi suçunu işleyen kimseye, 6 aydan 3 yıla kadar hapis cezası verilir. Ancak kanunda bu suçun nitelikli hali olarak düzenlenmiş olan 137 nci madde uyarınca, bu suçun kamu görevlisi tarafından veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında artırılır.

Ceza Muhakemesi Kanunu'nun 231 inci maddesinin beşinci fıkrasına göre, "sanığa yüklenen suçtan dolayı yapılan yargılama sonunda hükmolunan ceza, iki yıl veya daha az süreli hapis veya adlî para cezası ise; mahkemece, hükmün açıklanmasının geri bırakılmasına karar verilebilir." Aynı maddenin altıncı fıkrasında ise bunun koşulları sayılmış, bu kararın verilebilmesi için, "sanığın daha önce kasıtlı bir suçtan mahkum olmamış bulunması, Mahkemece, sanığın kişilik özellikleri ile duruşmadaki tutum ve davranışları göz önünde bulundurularak yeniden suç işlemeyeceği hususunda kanaate varılması, Suçun işlenmesiyle mağdurun veya kamunun uğradığı zararın, aynen iade, suçtan önceki hale getirme veya tazmin suretiyle tamamen giderilmesi" gerektiği belirtilmiştir. Kişisel verilerin kaydedilmesi suçu açısından öngörülen hapis cezası 6 aydan 3 yıla kadar olarak belirlendiği için, hakimin takdir edeceği cezanın iki yıl veya daha az süreli hapis cezası olması mümkündür. Bu itibarla CMK'nın 231 inci maddesinde sayılan koşulların gerçekleşmesi halinde hükmün açıklanmasının geri bırakılması söz konusu olabilecektir.

Bu suçu işleyen fail hapis cezasına çarptırıldığı takdirde, TCK m.53/1 uyarınca bu maddede yer alan hak yoksunlukları fail hakkında uygulanacaktır[447]. Suçun

[447] Hak yoksunlukları TCK'nın 53 üncü maddesinin ilk fıkrasında "*(1) Kişi, kasten işlemiş olduğu suçtan dolayı hapis cezasına mahkumiyetin kanuni sonucu olarak;*
a) Sürekli, süreli veya geçici bir kamu görevinin üstlenilmesinden; bu kapsamda, Türkiye Büyük Millet Meclisi üyeliğinden veya Devlet, il, belediye, köy veya bunların denetim ve gözetimi altında bulunan kurum ve kuruluşlarca verilen, atamaya veya seçime tabi bütün memuriyet ve hizmetlerde istihdam edilmekten,

nitelikli hallerinden biri olan kamu görevlisinin bu suçu işlemesi durumunda ise, verilmiş olan cezanın hapis cezası olup olmadığına ve ertelenmiş olup olmadığına bakılmaksızın TCK m.53/5 uyarınca fail hakkında verilen cezanın yarısından bir katına kadar failin kamu görevinden yoksun bırakılmasına da karar verilir[448].

TCK'nın 140 ıncı maddesinde, "Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenmiş olan suçlar bakımından, bu suçların işlenmesi sebebiyle tüzel kişilerin cezai sorumluluğu "(1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur" şeklinde düzenlenmiştir. 140 ıncı madde açısından böyle bir düzenleme getirilmesinin sebebi, doktrinde aksine görüş[449] olsa da, tüzel kişilerin TCK kapsamında fail olabileceklerinin kabul edilmemiş olmasıdır[450]. Nitekim TCK'nın 20 nci maddesinin ikinci fırkasında "tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır" şeklinde bir ifade kullanılmış, böylece tüzel kişilerin suç faili olamayacaklarına işaret edilmiş ve bunların cezalandırılmalarının mümkün olmadığı vurgulanmıştır[451]. Bu itibarla tüzel kişilerin bu suçun işlenmesinden kaynaklı olarak hukuka aykırı yarar sağlamaları halinde, bunlara TCK'nın 60 ıncı maddesinde[452] öngörülmüş olan güvenlik tedbirleri uygulanacaktır[453].

---

b) Seçme ve seçilme ehliyetinden ve diğer siyasî hakları kullanmaktan,
c) Velayet hakkından; vesayet veya kayyımlığa ait bir hizmette bulunmaktan,
d) Vakıf, dernek, sendika, şirket, kooperatif ve siyasî parti tüzel kişiliklerinin yöneticisi veya denetçisi olmaktan,
e) Bir kamu kurumunun veya kamu kurumu niteliğindeki meslek kuruluşunun iznine tabi bir meslek veya sanatı, kendi sorumluluğu altında serbest meslek erbabı veya tacir olarak icra etmekten,
Yoksun bırakılır." şeklinde düzenlenmiştir.

[448] **Yaşar-Gökcan-Artuç**, s. 4123.

[449] **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 612; "*Tüzel kişilerin suç faili olabileceği ve temsilcileriyle birlikte ceza sorumluluğunun bulunduğunu kabul etmemiz sebebiyle, tüzel kişilere ceza yaptırımı uygulanamayacağını öngören düzenlemeyi benimsemediğimizi ifade etmek isteriz.*"

[450] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 304 - 309, **Koca-Üzülmez**, s. 100 - 101.

[451] Aksi görüş için bkz. **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 612; "*5237 Sayılı kanunun 20. maddesinde, 'tüzel kişilerin fiillerinden dolayı gerçek kişi temsilcilerinin cezai açıdan sorumlu sayılacağına veya tüzel kişinin değil, onun adına fiili icra eden gerçek kişinin sorumlu tutulacağına' dair açık hüküm olmadığından, gerçek kişi temsilcilerin ceza sorumlusu sayılmaları mümkün değildir.*"

[452] Tüzel kişilere özgü güvenlik tedbirleri, TCK'nın 60 ıncı maddesinde; "*(1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkumiyet halinde, iznin iptaline karar verilir.*
(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.

f. Soruşturma Usulü, Görevli ve Yetkili Mahkeme, Dava Zamanaşımı

139 uncu maddede, soruşturulması ve kovuşturulması için şikayet şartı aranan maddeler "(1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır" şeklinde düzenlenmiştir. Bu maddeye göre, TCK'nın "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde yer alan haberleşmenin gizliliğini ihlal (m.132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (m.133) ve özel hayatın gizliliğini ihlal (m.134) suçlarının soruşturulması ve kovuşturulması şikayet şartına bağlanmıştır. Bu paragrafta sayılan suçlar bu çalışma kapsamına girmediğinden bu hususta ayrıntılı bir inceleme yapılmayacak olsa da, şikayet şartının niteliğine kısaca değinilecektir. Şikayet şartı bir ceza muhakemesi şartı olup[454], bu şartın gerçekleşmemesi söz konusu suçun oluşmaması anlamına gelmemekle beraber[455], failin tipiklikte öngörülen fiili işlemesiyle suç meydana gelmekte, ancak şikayet şartına bağlı suçlarda şikayetin bulunmaması bu suçların soruşturulup kovuşturulmasına engel teşkil etmektedir. Dolayısıyla şikayet, bir ceza muhakemesi şartı olması sebebiyle, bu şartın bulunmaması suçun oluşmasında değil, soruşturulup kovuşturulmasında önem arz etmektedir. Bu itibarla TCK m.139'da düzenlenmiş şikayete bağlı suçlar arasında 135 inci maddedeki kişisel verilerin kaydedilmesi suçu bulunmadığından, bu suçun soruşturulması ve kovuşturulması şikayete bağlı olmayıp, Cumhuriyet Savcılığınca resen yapılacaktır. Bu suçun kamu görevlisi tarafından görevi sebebiyle işlenmesi halinde, 4483 Sayılı kanuna göre, soruşturma ancak yetkili merciden soruşturma izni alındıktan sonra yapılabilecektir[456].

---

(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir
(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır" şeklinde düzenlenmiştir.

[453] **Dülger**, s. 286.

[454] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 571, **Koca-Üzülmez**, s. 301.

[455] **Malkoç**, s. 916.

[456] **Yaşar-Gökcan-Artuç** s. 4123.

135 inci maddedeki suçu işleyen kişiler, 5235 Sayılı kanunun[457] 11 inci maddesi uyarınca Asliye Ceza Mahkemesi'nde yargılanacaklardır. Aynı kanunun 14 üncü maddesi gereğince ağırlaştırıcı ve hafifleştirici nedenler görevli mahkemenin belirlenmesine etki etmediğinden, madde 137'de öngörülmüş olan nitelikli hallerin oluşması durumunda dahi görevli mahkeme yine Asliye Ceza Mahkemesi olacaktır.

Yetkili mahkemenin belirlenmesi açısından ise, ceza ve ceza muhakemesi hukukundaki temel kurallar uygulanacak, buna göre CMK'nın 12 nci maddesine göre temelde suçun işlendiği yer mahkemesi yetkili olacaktır. Suçun işlendiği yerden kasıt ise, suçun hareketinin yapıldığı yer veya neticesinin ortaya çıktığı yerdir[458]. Ancak, kişisel verilerin kaydedilmesine ilişkin suçların büyük bir kısmının bilişim sistemleri vasıtasıyla işlendiği düşünüldüğünde, hareketin icra hareketlerinin bir kısmının Türkiye'de, diğer kısmının başka bir ülkede yapılması veya Türkiye'nin farklı şehirlerinde gerçekleşmesi ihtimali yüksektir. Bu durumda mesafe suçlarından bahsedilir ve ülkeler arası gerçekleşen mesafe suçlarında, TCK'nın 8 inci maddesinin birinci fıkrası gereğince "fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır."[459] Suçun Türkiye'nin farklı yerlerinde işlenmesi halinde ise, doktrinde ülke içinde gerçekleşen mesafe suçlarından bahsedilir ve suç hareketle neticenin meydana geldiği her yerde işlenmiş sayılabileceği belirtilmiştir[460]. Şayet suçun işlendiği yer tespit edilemiyorsa, yedek yetki kuralları uygulanarak, TCK'nın 13 üncü maddesinde belirtilen kurallar uygulanır.[461] Buna göre, "suçun işlendiği yer belli değilse, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi yetkilidir. Şüpheli veya sanığın Türkiye'de yerleşim yeri yoksa Türkiye'de en son adresinin bulunduğu yer mahkemesi yetkilidir. Mahkemenin bu suretle de belirlenmesi olanağı yoksa, ilk usul işleminin yapıldığı yer mahkemesi yetkilidir."

Ceza Muhakemesi Kanunu'nun 253 üncü maddesinde uzlaşma kurumu düzenlenmiş olup bu maddeye göre, soruşturulması veya kovuşturulması şikayete bağlı olan suçlar ile, şikayete bağlı olup olmadığına bakılmaksızın Türk Ceza

---

[457] Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev Ve Yetkileri Hakkında Kanun, K.n. 5235; R.G.t. 07.10.2004, S. 25606.
[458] **Kunter, Nurullah-Yenisey, Feridun-Nuhoğlu, Ayşe**, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Baskı, İstanbul 2010, s. 581, **Öztürk- Erdem**, s. 285.
[459] **Centel-Zafer-Çakmut**, s. 523.
[460] **Centel-Zafer-Çakmut**, s. 523, **Öztürk-Erdem**, s. 285.
[461] **Yurtcan**, **Erdener**, Ceza Yargılaması Hukuku, 12. Baskı, İstanbul 2007, s. 111.

Kanununda yer alan; Kasten yaralama (üçüncü fıkra hariç, madde 86; madde 88), Taksirle yaralama (madde 89), Konut dokunulmazlığının ihlali (madde 116), Çocuğun kaçırılması ve alıkonulması (madde 234), Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması (dördüncü fıkra hariç, madde 239) suçları uzlaşmaya tabidir. Uzlaşma kurumu, temel olarak, ceza muhakemesinin ilerlemesini durdurup faille mağdurun uzlaştırılmasını ve üçüncü bir kişi önünde iradeleri çerçevesinde bir anlaşma yaparak ceza uyuşmazlığına son vermeleridir[462]. Bu itibarla, kişisel verilerin kaydedilmesi suçu, TCK'nın 139 uncu maddesi gereği şikayete tabi olmaması ve CMK'nın 253 üncü maddesinde sayılan suçlar arasında yer almaması itibariyle uzlaşmaya tabi suçlardan değildir.

TCK m.66/1'e göre ise, bu suçun dava zamanaşımı süresi sekiz senedir ve nitelikli haller uygulansa dahi cezanın üst sınırı beş senenin altında kalacağından, dava zamanaşımı süresi değişmeyecektir[463].

2. TCK m. 136: Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme

a. Genel Bilgiler

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, TCK'nın 136 ncı maddesinde "*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır*[464]" şeklinde düzenlenmiştir.

Gelişen teknoloji ve bireylerin bilişim sistemlerini gittikçe daha sık kullanır hale gelmeleri, bazı fiillerin daha sık işlenmesine ve dolayısıyla bazı suçların meydana gelmesine sebep olmuştur. Yukarıda da değinildiği üzere, günümüzde artık hemen hemen herkes kişisel verilerini belli başlı sebeplerle birtakım kurum ve kuruluşlara vermekte, ancak bazen bu kurum ve kuruluşlar bu kişisel verileri başkalarına verebilmekte veya satabilmektedirler. Yapılan alışverişlerde kullanılacak indirim kartlarını alabilmek için, bankalarda işlem yaptırabilmek için, yeni telefon

[462] **Centel-Zafer-Çakmut**, s. 476.
[463] **Parlar-Hatipoğlu**, s. 2091.
[464] 136 ncı maddenin gerekçesi, "*Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır.*" şeklinde düzenlenmiştir.

hatları satın alabilmek için ve daha sayılabilecek pek çok işlemi yapmak için artık bireylerin kişisel verilerini paylaşmaları olağan bir durum haline gelmiş; günlük hayatta farkında olmadan sürekli bir kişisel veri akışı ortaya çıkmıştır.

Kişisel verilerin hukuka uygun paylaşımı nasıl artmışsa, buna paralel olarak, bunların hukuka aykırı olarak paylaşılmaları ve ele geçirilmeleri de artmıştır. İşte bu sebeple Türk Ceza Kanunu'nda, bu tür fiilleri cezalandırmak için bir madde öngörülmüştür. Bu madde, kişisel verilerin hukuka aykırı olarak verilmesini, yayılmasını ve ele geçirilmesini cezalandırmaktadır. Dolayısıyla aynı zamanda, kimlik hırsızlığı olarak tanımlanabilen eylemlere karşı da uygulanabilecektir.[465]

b. Suçla Korunan Hukuki Değer

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, kişisel verilerin kaydedilmesi suçunda olduğu gibi, özel hayatın gizliliğini korumaktadır. Bu husus 135 inci maddede kişisel verilerin kaydedilmesi suçunda suçla korunan hukuki değer başlığı altında incelendiğinden, bu başlık altında tekrar ayrıntılı olarak incelenmeyecektir.

c. Suçun Unsurları

(1) Maddi Unsurlar

(a) Fiil

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, seçimlik hareketli bir suçtur[466]. Seçimlik hareketli suçlarda, suç tipinde birden fazla bağımsız hareket öngörülmüştür ve failin bunlardan herhangi birini işlemesi suçun tamamlanması için yeterlidir[467]. Dolayısıyla suçun tamamlanması için, tipiklikte tanımlanan tüm hareketlerin gerçekleştirilmesine gerek bulunmamaktadır. Maddede öngörülmüş olan seçimlik hareketlerin hepsinin birden veya iki tanesinin birden yapılması birden fazla

[465] **Dülger**, s. 276.
[466] Aynı yönde; **Yaşar-Gökcan-Artuç**, s. 4126, **Özbek**, TCK İzmir Şerhi, s. 960, **Arslan-Azizağaoğlu**, s. 611, **Dülger**, s. 278, **Soyaslan**, s. 347, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 608.
[467] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 257, **Centel-Zafer-Çakmut**, s. 252, **Koca-Üzülmez**, s. 109, **Demirbaş**, s. 210, **Zafer**, Ceza Hukuku Genel Hükümler, s. 174.

suç oluşturmayacak, yine tek suç olduğu kabul edilecektir. Ancak bu husus madde 61 gereği cezanın tayininde göz önünde bulundurulabilecektir[468]. 136 ncı maddede suçun oluşabilmesi için, verme, yayma ve ele geçirme olmak üzere toplam üç fiil öngörülmüştür ve bunlardan herhangi birinin işlenmesi ile bu suç oluşacaktır.

Şayet daha önce kaydedilmiş olan bir kişisel verinin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi söz konusu ise, bu kaydın hukuka uygun veya aykırı olduğuna bakılmaksızın bu suç oluşacaktır. Zira gerekçesinden de anlaşıldığı üzere, 136 ncı maddede düzenlenmiş olan suç 135 inci maddede düzenlenen kişisel verilerin kaydedilmesi suçundan bağımsız bir suç olarak tanımlanmıştır. Bu durumda örneğin, (A)'nın kişisel verilerini kaydetmiş olan (B)'nin, bu kişisel verileri hukuka aykırı olarak vermesi veya yayması, kişisel verilerin daha önce hukuka aykırı olarak kaydedilip kaydedilmediklerine bakılmaksızın suç sayılacaktır. Aynı şekilde, (B)'nin, (A)'nın kişisel verilerini bir şekilde bulup ele geçirmesi durumunda da, ele geçirilen kişisel verilerin hukuka uygun olarak kaydedilip kaydedilmediklerine bakılmayacaktır. Bu madde açısından önemli olan husus kişisel verinin hukuka aykırı olarak kaydedilmiş olup olmadığı değil; nasıl kaydedilmiş olursa olsun; verme, yayma veya ele geçirme eylemlerinin hukuka aykırı olarak yapılmış olmasıdır.

135 inci maddenin gerekçesinde belirtildiği üzere, kaydedilmiş olan kişisel verinin yalnızca bilişim sisteminde kayıtlı olması aranmayacak, el yazısıyla düzenlenmiş bir kayıt da 135 inci madde kapsamında kişisel verinin kaydedilmiş olması olarak anlaşılacaktır. Kanaatimizce bu husus 136 ncı madde açısından da geçerli olup; yaymanın, ele geçirmenin veya vermenin bilişim sistemleri vasıtasıyla yapılması aranmayacak; bu fiillerin el yazısıyla veya daktilo gibi araçlarla, kağıt veya benzeri yüzeylerde kaydedilmiş olan kişisel veriler açısından işlenmeleri durumunda da bu suç meydana gelecektir. Böylece, failin bilişim sisteminde kayıtlı başkasına ait kişisel veriyi bilgisayar aracılığıyla ele geçirmesi, yayması veya vermesi ile kağıt üzerine kaydedilmiş olan başkasına ait kişisel veriyi ele geçirmesi, yayması veya vermesi arasında herhangi bir fark yoktur. Ayrıca, ele geçirme, yayma veya verme eylemlerinin bilişim sistemi aracılığıyla yapılmasıyla manüel şekilde

[468] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 258.

yapılması arasında da suçun oluşması bakımından kanaatimizce bir fark bulunmamaktadır.

Verme, yayma ve ele geçirme için doktrinde birden fazla tanım bulunmaktadır ve bunların birkaçına değinmek gerekmektedir. Yaşar-Gökcan-Artuç'a göre, verme, "bir kimsenin elindeki bir şeyi bir diğerine sunması"; yayma, "bir kimsenin elindeki bir şeyi birden fazla kimsenin bilgisine sunması, birden fazla kimseye vermesi, ulaştırması"; ele geçirme ise "bir kimsenin bir başkasının elinde olan bir materyali onun rızası dışında veya rızasıyla elde etmesi" dir[469]. Yazarlara göre, verme ile yayma arasındaki temel fark vermede tek bir kişiye ulaştırma söz konusu iken, yaymada kişisel verinin birden fazla kişiye ulaştırılmasıdır[470]. Soyaslan ise kavramların tanımlanmasında daha çok örnekleme yoluna gitmiş, vermenin "elden ya da posta, cd-rom üzerine kaydedilerek ya da internet üzerinden elektronik posta yoluyla"; ele geçirmenin "kişisel verilerin üzerinde kayıtlı olduğu belgelerin bulunduğu yerden alınması, verilerin kayıtlı olduğu bilişim sistemine girilerek verilerin bir diskete kaydedilmesi ve disketin alınması yoluyla"; yaymanın ise "verilerin yazılı olarak mektup şeklinde birden fazla kişiye gönderilmesiyle gerçekleştirilebileceği gibi, internet üzerinde bir web sitesinde kişisel verileri başkaları için erişilebilir kılmak ya da bir forum odasında açıklama yapmak yoluyla" gerçekleştirilebileceğini belirtmiştir[471]. Özbek, vermek ve yaymanın temel amacının "aktarmak" olduğunu belirtmiş, ikisinin arasındaki farkın ise, vermenin iki kişi arasındaki bir eylemi tanımlarken, yaymanın daha çok aktarmak amacıyla bir araç kullanmayı ve birden fazla kişiyi hedeflemesinden kaynaklandığını belirtmiştir[472]. Yine Özbek'e göre, ele geçirme fiili kaydetme şeklinde de yapılabilecektir ancak kaydetme 135. maddede ayrıca cezalandırıldığından ele geçirmenin kaydetmek dışında kalan eylemleri ifade ettiği düşünülmelidir[473].

Maddede öngörülmüş olan seçimlik hareketlere bakıldığında, suçun icrai suçlardan olduğu görülmektedir. Zira, kanun koyucu kişisel verilerin hukuka aykırı olarak verilmesini, ele geçirilmesini veya yayılmasını yasaklamış, bu yasağa uymayarak icrai bir hareketle bu fiilleri gerçekleştirenlerin cezalandırılmalarını

[469] **Yaşar-Gökcan-Artuç**, s. 4126.
[470] **Yaşar-Gökcan-Artuç**, s. 4126.
[471] **Soyaslan**, s. 346, **Dülger**, s. 277-278.
[472] **Özbek**, TCK İzmir Şerhi, s. 960.
[473] **Özbek**, TCK İzmir Şerhi, s. 961.

öngörmüştür. Bu noktada, yayma fiili açısından, rızanın baştan verilip sonradan geri alınması durumunda, başlangıçta hukuka uygun olan fiilin yaymanın sona erdirilmemesi halinde hukuka aykırılık teşkil edeceğini ve suçun ihmali hareketle oluşacağını belirtmek gerekir. Gerçekten de, örneğin bir kişinin resminin bir sosyal paylaşım sitesinde paylaşılmasına rıza göstermesi halinde resim paylaşılabilecek ve bu fiil suç oluşturmayacaktır. Ancak kişinin rızasının kalktığı andan itibaren, resmin paylaşıldığı siteden geri çekilmemesi, yani hareketsiz kalınması, suç teşkil edecektir. Bu itibarla yayma fiili açısından, suçun konusunu teşkil eden verinin hukuka aykırı olarak yayılması halinde suç icrai hareketle, ancak başlangıçta hukuka uygun olarak yayılmış olan bir kişisel verinin, hukuka uygunluk ortadan kalktıktan sonra, hukuka aykırı olarak yayılmaya devam edilmesi halinde suç ihmali hareketle gerçekleşmiş olacaktır.

136 ncı maddede düzenlenen suçun, verme veya ele geçirme seçimlik hareketleri açısından, hareketin yapılmasıyla suç oluşacağından ani suç söz konusudur. Ancak "yayma" hareketi açısından değerlendirildiğinde, suçun hem ani suç hem de mütemadi suç olarak değerlendirilebileceği kanaatindeyiz. Örneğin, bir kimsenin kişisel verilerinin hukuka aykırı olarak bir internet sitesinde yayımlanması durumunda, suç tamamlanmış olacak, ancak bu veriler o sitede kaldıkları müddetçe farklı zamanlarda farklı kişilerin bilgisine sunulmaya devam edeceklerinden suç bitmemiş olacaktır. Ancak kişisel verilerin posta yoluyla birden fazla kimseye gönderilmeleri durumunda, posta bu kişilere ulaştığı anda yayma fiili işlenerek suç oluşmuş olacağından, ani suç olarak değerlendirilecektir.

(b) Fail

Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçunu düzenleyen 136 ncı maddede, suçu işleyebilecek kişi için "kişi" sözü kullanılmıştır. Kanun fail açısından herhangi bir özellik aramamış, herkesin bu suçu işleyebileceğini, dolayısıyla herkesin bu suçun faili olabileceğini düzenlemiştir. Ancak TCK'nın 137 nci maddesi ile özel bir düzenleme getirilerek, failin kamu görevlisi olması nitelikli bir hal olarak düzenlenmiştir. Bu itibarla 135 inci maddede olduğu gibi, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, temel

şekli herkes tarafından işlenebilen, ancak belli kişiler tarafından işlendiğinde suçun nitelikli halinin oluştuğu, fail açısından bir görünüşte özgü suçtur[474].

(c) Mağdur

Bu suçun mağduru açısından maddede herhangi bir özellik gösterilmemiş olduğundan, bu suçun mağduru herhangi bir birey olabilecektir. Kanaatimizce mağdur yalnızca gerçek kişiler olabileceğinden, bu suç açısından ancak konunun sahibi olan gerçek kişi mağdur olabilecektir. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu bakımından, konu kişisel veriler olduğundan, suçun mağduru da, kişisel verilerin sahibi olan gerçek kişi olabilecektir. Tüzel kişiler ise ancak suçtan zarar gören olabileceklerdir.

(d) Konu

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun konusu "kişisel verilerdir." Türk Ceza Kanunu'nun kişisel verilerle ilgili olarak düzenlenmiş suçları açısından yukarıda "1. Genel Bilgiler" başlığı altında ayrıntılı açıklama yapıldığından, burada bu husus üzerinde tekrar durulmayacaktır.

Bu suçta, kişisel verilerin verilmesi, yayılması veya ele geçirilmesi sebebiyle herhangi bir zararın ortaya çıkması aranmamaktadır. Dolayısıyla bu suç bir zarar suçu değil; bir tehlike suçudur. Zira suçta tanımlanmış fiillerin işlenmesiyle suç oluşmakta, kişisel verileri verilen, yayılan veya ele geçirilen kişinin bundan dolayı herhangi bir zarara uğrayıp uğramadığına bakılmaksızın, kişinin zarara uğrama tehlikesinin doğması suçun oluşması için yeterli sayılmaktadır. Kanun koyucu, 136 ncı maddeyi düzenlerken, hakimin, suçun konusu üzerinde tehlikenin meydana gelip gelmediğini araştırmasını öngörmemiştir. Bu itibarla, suçun konusu bakımından tehlikenin doğup doğmadığına bakılmayacağından kişisel verilerin verilmesi, yayılması veya ele geçirilmesi soyut tehlike suçudur.

---

[474] **Koca-Üzülmez**, s. 101; "… *herkes tarafından işlenebilen özel verileri hukuka aykırı olarak verme veya ele geçirme (m.136) suçunun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi hali ise görünüşte özgü suçu oluşturmaktadır.*"

(e) Netice

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu sırf hareket suçudur. Sırf hareket suçlarında hareketin yapılmasıyla suç gerçekleşir ve tamamlanır. Dolayısıyla bu tür suçlarda suçun tamamlanması için neticenin ortaya çıkmasına gerek yoktur; hareketin yapılmasıyla tipiklikte belirtilmiş olan ihlal tamamlanır. Kişisel verileri verme veya ele geçirme suçu açısından da, herhangi bir neticenin ortaya çıkmasına gerek olmayıp, kişisel verilerin hukuka aykırı olarak verilmeleri, yayılmaları veya ele geçirilmeleri gerçekleştiği an bu suç oluşmuş olacaktır. Dolayısıyla, sadece bu fiillerin işlenmesi suçun oluşması için yeterli olacak, ayrıca failin bundan bir fayda sağlaması veya mağdurun bir zarar görmesi aranmayacaktır.

(f) Suçun Nitelikli Unsurları

TCK'nın 137 nci maddesine göre, suçun kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında artırılacaktır. Bu hususta ayrıntılı bilgi için, çalışmamızda TCK'nın 135 inci maddesinde suçun nitelikli unsurları başlığı altındaki açıklamalara bakılmalıdır.

(2) Manevi Unsur

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun genel kastla işlenebileceğini söylemek doğru olacaktır. Kanun koyucu bu suçun işlenmesi açısından özel bir kast aramamış, suçun unsuru haline gelecek bir saik belirtmemiştir. Buna ek olarak, kanunda suçun taksirle işlenebileceğine ilişkin herhangi bir düzenleme yapılmamıştır. Dolayısıyla, bu suç açısından da taksirle işlenmesi hususunda özel bir düzenleme yapılmadığından, suçun taksirle işlenemeyeceği açıktır.

Suçun düzenlemesi açısından, kişisel verileri "hukuka aykırı" olarak verme veya ele geçirmeden bahsedilmektedir. Dolayısıyla kanun bu suç açısından özel bir

hukuka aykırılık bilinci aramaktadır. Kişisel verileri "hukuka aykırı olarak" verme veya ele geçirme açısından bu suç ancak doğrudan kastla işlenebilecek; olası kastla işlenmesi söz konusu olamayacaktır; zira bu suç açısından failde aranacak olan özel hukuka aykırılık bilinci artık suçun bir unsuru olarak tipiklik kapsamında değerlendirilecektir.

(3) Hukuka Aykırılık

135 inci maddenin ilk fıkrasında ve ikinci fıkrasının bir kısmında olduğu gibi, 136. maddede de, hükümde tanımlanmış olan suçun oluşması için, verme, yayma veya ele geçirme fiilleri "hukuka aykırı olarak" işleneceklerdir. Dolayısıyla başkasının kişisel verilerini hukuka uygun olarak vermek, yaymak veya ele geçirmek artık 136 ncı maddedeki suçu oluşturmayacaktır.

Kanun koyucunun bazı maddeler açısından özel olarak "hukuka aykırılık" unsurunu vurgulamış olmasına ilişkin doktrinde farklı görüşler mevcuttur ve bu görüşlere 135 inci madde incelenirken değinilmiştir. Bizim de katıldığımız görüşe göre, "hukuka aykırılık" ın bazı maddelerde özel olarak belirtilmesi, diğer maddeler açısından failde yaptığı fiilin hukuka aykırı olduğu bilincinin aranmayacağı, hukuka aykırılığın özellikle belirtildiği maddeler açısından ise aranacağı anlamına gelmektedir. Yani failin kastının bu özel hukuka aykırılığı da kapsaması gerekecek ve suç yalnızca doğrudan kastla işlenebilecektir. Dolayısıyla failde bu hukuka aykırılık bilincinin bulunmaması ve failin işlediği fiilin hukuka aykırı olduğunu bilmemesi durumunda bu suç oluşmayacaktır.

Suçun oluşması için fiilin hukuka aykırı olarak işlenmesi gerektiğine göre, hukuka uygun olarak işlendiğinde suçun oluşmayacağı açıktır. Hukuka uygunluk sebepleri, fiili hukuken meşru hale getirirler ve bu madde açısından hem ilk fıkrada, hem de ikinci fıkradaki tüm kişisel veriler açısından hukuka uygunluk sebeplerinden birinin veya birkaçının bulunması durumunda, kişilerin fiili suç olmaktan çıkacaktır. Bu madde açısından inceleyeceğimiz hukuka uygunluk sebepleri ilgilinin rızası ile kanun hükmünü yerine getirmedir.

Doktrinde aksine görüş[475] olsa da, kanaatimizce bir kişinin kişisel verilerinin verilmesi, yayılması veya ele geçirilmesi hususlarında rızasının bulunabileceği açıktır, zira kişisel verileri üzerinde kişilerin mutlak tasarruf hakları bulunmaktadır. Bu sebeple bir kişinin kişisel verileri verildiğinde, yayıldığında veya ele geçirildiğinde, veri öznesinin rızası varsa, artık bu fiilin suç teşkil etmeyeceği ve fiilleri işleyen açısından bir hukuka uygunluk sebebi meydana getireceği açıktır. Böylece fiil suç olmaktan çıkacak, hukuk düzenince meşru olarak kabul edilecektir.

Kanun hükmünün yerine getirilmesine verilebilecek bir örnek 5352 Sayılı Adli Sicil Kanunu'nun 7 ve 8 inci maddelerine[476] ilişkindir[477]. Bu maddelerde adli sicil bilgilerinin kimlere ve hangi kuruluşlara verilebileceği belirtilmiştir. Bir kimsenin kişisel verilerinin bu madde uyarınca ve yine bu maddede belirtilen kişilere veya kurum ve kuruluşlara verilmesi durumunda, artık TCK'nın 136 ncı maddesinde tanımlanmış olan suç oluşmayacak; bu hüküm bir hukuka uygunluk sebebi olacaktır. Ancak, adli sicil bilgilerinin bu kanundaki hükümlerde sayılmış kişilerden başka kişilere verilmesi durumunda, artık bir hukuka uygunluk sebebi olduğundan bahsedilemeyecek, fiil hukuka aykırı olduğundan, 136 ncı maddedeki suçu oluşturacaktır. Nitekim bu husus aynı kanunun 11 inci maddesinde "Adlî sicil ve arşiv bilgileri gizlidir. Bu bilgiler, görevlilerce açıklanamaz ve bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamaz" denilmek suretiyle vurgulanmıştır[478].

Kanun hükmünün yerine getirilmesi açısından, 135 inci madde incelenirken de değinilmiş olan CMK m.80'de, "75, 76 ve 78 inci Madde hükümlerine göre alınan

---

[475] Bkz. **Özbek**, TCK İzmir Şerhi, s. 962; "*Kural olarak soruşturulması ve kovuşturulması şikayete tabi suçlar bakımından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu kabul edilebilir… m.136'da yer alan 'verileri hukuka aykırı olarak verme veya ele geçirme' suçu şikayete bağlı değildir. Bu suç bakımından bireyin değil, kamunun menfaatinin daha ağır bastığı kabul edilmiştir. O halde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından ilgilinin rızası hukuka uygunluk sebebi olarak uygulanabilir değildir.*"

[476] 7 nci madde şu şekilde düzenlenmiştir: "*(1) Adlî sicil bilgileri, kullanılış amacı belirtilmek suretiyle;*
a) İlgili kişiye veya vekaletnamede açıkça belirtilmek koşuluyla vekiline,
b) Kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına,
Verilebilir.
(2) Yabancı devletler tarafından istenilen adlî sicil bilgileri mütekabiliyet esasına göre verilir."

8 nci madde şu şekilde düzenlenmiştir: "*(1) Adlî sicil bilgileri; mahalli adlî sicillerde Cumhuriyet başsavcılıklarınca, asliye mahkemelerinin bulunmadığı ilçelerde kaymakamlıklarca, yurt dışında elçilik ve konsolosluklarca, merkezî adlî sicilde ise Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğünce verilir.*"

[477] **Yaşar-Gökcan-Artuç**, s. 4126.

[478] **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 608.

örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez" denmek suretiyle kişilerin vücudundan örnek alınması ve bu örnekler üzerinde moleküler gentik inceleme yapılması durumlarına ilişkin bir kural getirilmiştir. CMK 80'deki emredici hükme uyulmayıp elde edilen bu kişisel verilerin dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından başkasına verilmesi veya yayılması TCK m. 136'daki suçu oluşturacaktır[479].

d. Suçun Özel Görünüş Şekilleri

(1) Teşebbüs

136 ncı maddede düzenlenmiş olan kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu sırf hareket suçu olduğundan; bu suçun teşebbüs aşamasında kalması ancak icra hareketlerinin bölünebilir olması durumunda söz konusudur ki suçun niteliği göz önüne alındığından bu suç bakımından teşebbüsün gerçekleşmesi mümkün görünmektedir[480].

İcra hareketlerinin bölünebilir olması halinde, bu suç açısından gönüllü vazgeçemeden de bahsedilebilecektir. Failin kendi hür iradesiyle, icra hareketleri tamamlanmadan, kişisel verileri vermekten, yaymaktan veya ele geçirmekten vazgeçmesi halinde, fail bu suça teşebbüsten cezalandırılmayacak, ancak o ana kadarki fiilleri başka bir suç oluşturuyorsa o suçtan cezalandırılacaktır. Örneğin, (A), elinde (B)'nin kişisel verilerini hukuka uygun olarak bulundurur ancak bunları hukuka aykırı olarak gazeteci arkadaşı (G)'ye göndermeye karar verir. (A), bu verileri internetten mail yoluyla gönderirken, maile (B)'nin kişisel verilerini yazar, adres kısmına da (G)'nin mail adresini ekler, ancak sonra yaptığının yanlış olabileceğini düşünerek bu maili taslak olarak kendi mailleri arasında saklayarak (G)'ye göndermez. Yapılan hukuka uygun bir arama neticesinde de, (A)'nın bilgisayarındaki bu taslak mail ortaya çıkar. İşte bu durumda, (A)'nın, (B)'nin kişisel verilerini hukuka aykırı olarak vermeye karar vererek suçun icra hareketlerine başladığı, ancak kendi iradesiyle suçu işlemekten vazgeçerek suçtan gönüllü olarak vazgeçtiği söylenecek ve ceza almayacaktır. Buna karşın (A), kişisel verileri kendi

[479] **Parlar-Hatipoğlu**, s. 2092 - 2093.
[480] **Malkoç**, s. 913.

mail adresinden değil de, şifresini kırmak suretiyle girdiği kardeşi (K)'nın mail adresinden göndermeye karar vererek, vazgeçmiş ve söz konusu maili taslak halinde bırakmış olsaydı, gönüllü vazgeçme bulunduğundan, 136 ncı maddede düzenlenen suça teşebbüsten cezalandırılmayacak, ancak kardeşinin şifresini kırmak suretiyle mail adresine girmiş olması, TCK m. 243'te düzenlenen bilişim sistemine girme suçunu oluşturduğundan ve bu suç kişisel verileri verme suçundan vazgeçme anına kadar oluşmuş başka bir suç olduğundan, (A), 243 üncü maddedeki suçtan cezalandırılacaktır.

(2) İştirak

Bu suç açısından iştirakin her halinden bahsetmek mümkün olabilecektir. İştirak şekilleri ile ilgili ayrıntılı bilgi için çalışmamızda TCK'nın 135 inci maddesinin incelendiği kısımda iştirak başlığı altındaki açıklamalara bakılmalıdır.

(3) İçtima

İçtima açısından ilk olarak 136. maddedeki suçu zincirleme suç hükümleri kapsamında değerlendirmek gerekir. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun, aynı kişiye birden fazla defa işlenmesi halinde TCK m.43'te düzenlenmiş olan zincirleme suç hükümleri bu noktada uygulama bulacaktır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunda, kanun koyucu birden fazla bağımsız hareketle bu suçun işlenebileceğini öngörmüş; seçimlik hareketli bir suç ihdas etmiştir. Seçimlik hareketli suçlarda, kanun koyucu her ne kadar suçun işlenmesi için birden fazla hareket öngörmüşse de, bu hareketlerden hepsinin birden yapılması veya birkaç tanesinin birden yapılması birden fazla suç oluşturmayıp bu husus hakim tarafından 61 inci maddedeki hususların değerlendirilmesiyle ceza tayin edilirken dikkate alınır[481]. Bu itibarla 136 ncı maddede düzenlenen suç açısından öngörülmüş olan verme, yayma veya ele geçirme hareketlerinden tek birinin yapılması suçun oluşması için yeterli olup, bunlardan iki tanesinin veya üçünün de yapılması birden fazla suç oluştuğuna işaret etmez ve hakim tarafından ceza tayin edilirken TCK 61 inci madde kapsamında cezanın alt

[481] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 258, **Koca-Üzülmez**, s. 109.

sınırından uzaklaşılmasını gerektirebilir[482]. Ancak, failin farklı zamanlarda aynı kişiye karşı bu seçimlik hareketlerden birini veya ikisini veyahut üçünü işlemesi halinde, m. 43/1 uygulama alanı bulacak, zincirleme suç hükümleri uygulanacaktır. Bu hususu bir örnekle açıklamak gerekirse, (A)'nın (B)'nin fotoğrafını hukuka aykırı olarak ele geçirip, (B)'nin rızası bulunmaksızın bir sosyal paylaşım sitesinde yayması halinde, aynı zaman diliminde gerçekleşen bu seçimlik hareketlerin ikisinin birden yapılması zincirleme suç hükümlerinin uygulanmasını gerektirmeyecek, tek suç oluştuğu kabul edilecektir. Ancak (A)'nın, önce (B)'nin fotoğrafını hukuka aykırı olarak ele geçirmesi, belli bir süre geçtikten sonra ise, (B)'nin bir sözüne öfkelendiği için daha önce ele geçirdiği resmi bir sosyal paylaşım sitesinde yayması halinde, artık farklı zamanlarda oluşan suçlardan söz edilecek ve TCK'nın 43 üncü maddesinin birinci fıkrası uyarınca zincirleme suç hükümleri uygulanarak (A)'nın cezası dörtte birinden dörtte üçüne kadar artırılacaktır[483].

135 inci madde ile ilgili olarak içtima başlığı altında yaptığımız açıklamalarda, 132 nci, 133 üncü ve 134 üncü maddelerin de özel hayata ve hayatın gizli alanına karşı işlenen suçlarda olduğunu belirtmiştir. Bu başlık altında da, bu maddelerin 136 ncı madde ile olabilecek içtima durumu incelenecektir.

132 inci maddenin ikinci fıkrasında, kişilerin arasındaki haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi, üçüncü fıkrasında ise kişinin kendisiyle yapılan haberleşmelerin içeriğinin diğer tarafın rızası olmaksızın alenen ifşa edilmesi suç olarak düzenlenmiştir. Buna göre bir kişinin bu fiillerden birini gerçekleştirerek 132 nci maddenin ikinci ya da üçüncü fıkrasında düzenlenen suçu işlemesi halinde, ifşa edilen haberleşme içeriklerinin içerisinde, başkalarının veya haberleşmenin taraflarının kişisel verilerinin de bulunması halinde, 132 nci maddenin yanı sıra, 136 ncı madde de ihlal edilmiş olacaktır. Örneğin 132 nci maddenin ilk fıkrasına örnek oluşturacak şekilde, arkadaşları arasındaki ve arkadaşlarına ilişkin

---

[482] **Malkoç**, s. 913.

[483] "Sanığın işyerinde haciz yapıldığı sırada katılan avukatın yokluğunda 'İrfan'ın anasını eşekler… etsin' şeklinde sövmesi biçimindeki eyleminin ihtilat öğesinin varlığı araştırılarak ikiden fazla kişiye ihtilat ettiğinin belirlenmesi durumunda 765 Sayılı Yasanın 482/1, 273. maddelerinde yazılı suçun oluşacağı, bu fiilden bir süre sonra telefon ettiği katılana sinkaflı sözlerle sövmesi şeklinde kabul edilen ikinci eyleminin de, 765 Sayılı TCY'nın 268/3. madde ve fıkrası yollamasıyla 266/3 üncü maddesine uyan suçu oluşturduğu gözetilmeden, eylemler arasında kısa bir sürenin bulunduğu ve aynı olaya dayandığı için tek suç oluşacağı yolundaki yasaya aykırı kabul ve gerekçelerle aynı yasanın 266/3. maddesiyle ceza verilmesi." 07.03.2007 T., 2007/13420 E., 2007/2232 K. Sayılı Yargıtay 4. Ceza Dairesi kararı, aktaran; **Artuk**, **Mehmet Emin-Gökcen**, **Ahmet-Yenidünya**, **A. Caner**, TCK. Şerhi, Özel Hükümler, Cilt 3, Ankara 2009, s. 3130.

kişisel verileri ihtiva eden haberleşme içeriklerini ifşa eden bir kişi, hem 132 nci maddenin ikinci fıkrasında düzenlenmiş olan suçu, hem de 136 ncı maddede düzenlenmiş olan suçu işlemiş olacaktır. Aynı husus hem 132 nci maddenin üçüncü fıkrasında düzenlenen kendisiyle yapılan haberleşmenin içeriğini diğer tarafın rızası olmaksızın alenen ifşa edilmesi, hem de ifşa edilen haberleşme içeriğinde başkalarının veya haberleşmenin diğer muhatabının kişisel verilerinin bulunması durumunda da söz konusu olacaktır. Fail, tek hareketiyle kanunda düzenlenmiş olan birden fazla suçu ihlal ettiği için, farklı neviden fikri içtima hükümleri uygulanarak, hangi suçun cezası ağırsa, o suçun cezası ile cezalandırılacaktır. Bu durumda 136 ncı maddenin cezası daha ağır olduğundan bu madde uygulanacak, ifşa edilen haberleşme içerikleri ile, birden fazla kişinin kişisel verilerinin hukuka aykırı olarak yayılması halinde ise, zincirleme suç hükümlerini düzenleyen 43 üncü maddenin ikinci fıkrasına göre, tek bir fiil ile aynı suç birden fazla kişiye karşı işlendiği için aynı neviden fikri içtima hükümleri uygulanarak failin cezası artırılacaktır.

133 üncü maddenin üçüncü fıkrasında ise, maddenin ilk iki fıkrasına göre "kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir … ses alma cihazı ile kaydeden" veya "katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan" kişinin bunları başkalarına vermesi veya diğer kişilerin bilgi edinmeleri suç olarak düzenlenmiştir. 133 üncü maddenin ilk iki fıkrasına göre kaydedilmiş olan haberleşme içeriklerinin, aleni olmayan söyleşinin veya aleni olmayan konuşmanın taraflarının veya başkalarının kişisel verilerini de ihtiva etmesi durumunda, failin bu haberleşme içeriklerini başkasına vermesi veya diğer kişilerin bilgi edinmelerini sağlaması halinde, hem 133 üncü maddenin üçüncü fıkrasında düzenlenmiş olan, hem de 136 ncı maddede düzenlenmiş olan suç oluşmuş olacaktır. Düşüncemize göre, böyle bir durumda da, fail tek bir hareketiyle birden fazla suçun oluşmasına sebebiyet vermiş olacağından, fail hakkında fikri içtima hükümleri uygulanacak, fail en ağır cezayı gerektiren suçun cezası ile cezalandırılacaktır. Ancak böyle bir durumda, başkasına verilen haberleşme içeriklerinde birden fazla kişinin kişisel verilerinin yer alması durumunda veya birden fazla kişinin kişisel verileri ile ilgili başkasının bilgi edinmesi sağlandığında, zincirleme suç hükümlerini düzenleyen 43 üncü maddenin aynı neviden fikri içtimaı düzenleyen ikinci fıkrası gereğince, failin cezasında artırıma gidilecektir.

Özel hayatın gizliliğini ihlal suçunu düzenleyen 134 üncü maddenin ikinci fıkrasında, kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimsenin, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı belirtilmiştir. Failin, kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa etmesi halinde, bu ses veya görüntülerin ait oldukları kişilerin veya başkalarının kişisel verilerini ihtiva etmeleri halinde, aynı zamanda kişisel verileri hukuka aykırı olarak yayma fiili oluşarak 136 ncı maddede düzenlenen suç meydana gelecektir. Bu durumda, fail tek bir fiili ile birden fazla suçun ihlal edilmesine sebebiyet vermiş olacak, ancak her iki suçtan ayrı ayrı cezalandırılmayıp fikri içtima kuralları gereğince cezası en ağır olan suçun cezasıyla cezalandırılacaktır. Cezası en ağır olan suç TCK'nın 136 ncı maddesinde düzenlenen suçtur ve dolayısıyla fail bu maddeye göre cezalandırılacaktır. İfşa ettiği ses ve görüntülerde birden fazla kimsenin kişisel verisinin bulunması halinde ise, aynı neviden fikri içtima hükmü gereğince cezasında artırıma gidilecektir.

135 inci maddedeki kişisel verilerin kaydedilmesi suçu ile 136 ncı maddede tanımlanmış olan kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçlarının bir arada bulunması durumundaki içtima kuralları açısından doktrinde farklı görüşler mevcuttur. Bir görüşe göre, 135 inci maddedeki kişisel verinin kaydedilmesi suçu, 136 ncı maddedeki kişisel verilerin hukuka aykırı olarak verme veya ele geçirme suçu açısından bir geçit suç oluşturacak, fail yalnızca 136 ncı maddedeki suçtan cezalandırılacaktır[484]. Bir diğer görüşe göre ise, failin 135 inci maddede düzenlenmiş olan kişisel verilerin kaydedilmesi suçunu işledikten sonra 136 ncı maddedeki seçimlik hareketlerden birini, ikisini veya hepsini birden işlemesi durumunda, burada geçitli suçtan söz edilemeyecek, fail iki ayrı suç işlemiş olduğundan gerçek içtima hükümleri uygulanarak iki suçtan ayrı ayrı ceza verilecektir[485]. Kanaatimizce, şayet 136 ncı maddede düzenlenen suçu işleme kastıyla hareket eden bir kimse için, ele geçirme, yayma veya verme fiillerini işleyebilmesi için, kişisel veriyi kaydetmesinin zorunlu olması halinde artık burada geçitli suçtan bahsedilebilecektir. Zira failin kastı 136 ncı maddedeki suçu işlemeye yönelmişse ve bu esnada yapılan "kayıt" 136 ncı maddede yer alan fiilleri

[484] Bkz. **Soyaslan**, s. 348, **Dülger**, s. 280, **Özbek**, TCK İzmir Şerhi, s. 962 - 963.
[485] Bkz. **Yaşar-Gökcan-Artuç**, s. 4128, **Malkoç**, s. 913, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 607, **Doğan**, **Yusuf Hakkı**, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", s. 9, www.ceza-bb.adalet.gov.tr/makale/146.doc, 14.03.2012.

işleyebilmek için gerçekleştiriliyorsa, tek suç oluştuğu kabul edilerek faile 136 ncı maddede düzenlenen suçtan ceza verilecektir. Ancak, failin farklı zamanlarda ve birbirinden bağımsız olarak önce bir kayıt işlemi gerçekleştirmesi, ardından kaydettiği kişisel veriyi hukuka aykırı olarak vermesi, ele geçirmesi veya yayması halinde artık iki ayrı suçun oluştuğu kabul edilmeli, fail hem 135 inci maddedeki hem de 136 ncı maddedeki suçtan ayrı ayrı cezalandırılmalıdır. Kişinin tek hareketle bir kişisel veriyi hem kaydetmesi hem de ele geçirmesi veya yayması veya vermesi durumlarında artık fikri içtimadan bahsetmek gerekecektir. Buna örnek olarak bir kişinin, başkasına ait kişisel veriyi bir foruma kaydetmesi gösterilebilir. Burada kaydetme işleminin yapılmasıyla birlikte artık bu veriler herkese açık hale gelmiş olacağından aynı zamanda yayılmış sayılacaklardır[486]. Böylece failin tek hareketiyle kişisel veriler hem hukuka aykırı olarak kaydedilmiş, hem de hukuka aykırı olarak yayılmış olacaklardır. İşte böyle bir durumda artık farklı neviden fikri içtimadan bahsedilecek ve fail en ağır cezayı öngören 136 ncı maddeden cezalandırılacaktır[487].

TCK'nın 239 uncu maddesinde, "Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması" suçu düzenlenmiştir[488]. Bu maddenin ilk fıkrasında, sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişinin şikayet üzerine cezalandırılacağı öngörülmüştür. Burada bahsi geçen sır kavramının kişisel veri kavramından farklı olduğu muhakkaktır. Kişisel veri, kimliği belirli veya kimliği belirlenebilir kişilere ait tüm verileri kapsamakta iken[489], müşteri sırrı Bankacılık Kanunu'nun 4 üncü maddesinde yer alan faaliyetlerin ve bu kapsamda sunulan her türlü hizmet sonucunda bankanın öğrendiği müşteriye ait ve aldığı hizmete dair bilgiler, sır kavramı ise; sınırlı sayıda kimsenin ulaşabildiği, alenen bilinmemesinde bir kimsenin çıkarının bulunduğu ve

---

[486] **Özbek**, TCK İzmir Şerhi, s. 958, **Şener**, s. 80.
[487] Aynı yönde; **Şener**, s. 80.
[488] Kanunun 239 uncu maddesine göre, "*(1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkraya göre cezaya hükmolunur.*
(2) Birinci fıkra hükümleri, fennî keşif ve buluşları veya sınaî uygulamaya ilişkin bilgiler hakkında da uygulanır.
(3) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu halde şikayet koşulu aranmaz.
(4) Cebir veya tehdit kullanarak bir kimseyi bu madde kapsamına giren bilgi veya belgeleri açıklamaya mecbur kılan kişi, üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır."
[489] **Doğan**, s. 5.

bu kişinin açıklanmasını istemediği bilgilerdir[490]. Dolayısıyla, bir kimsenin meslek veya sanatı, sıfatı veya görevi kapsamında vakıf olduğu bir sırrı yetkisiz kişilere vermesi veya ifşa etmesi halinde, yalnızca 239 uncu maddedeki suçun değil, 136 ncı maddede düzenlenmiş olan suçun da oluşması mümkündür. Fail, tek hareketle birden fazla hükmü ihlal ettiği için, her ikisinden ayrı ayrı cezalandırılmayacak, bu suçlar arasında fikri içtima hükmü uygulanarak, fail cezası en ağır olan suçun cezasıyla cezalandırılacaktır. 136 ncı maddede öngörülen ceza daha ağır olduğundan, fail bu suçun cezasıyla cezalandırılacak, ifşa edilen veya yetkisiz bir kişiye verilen belgelerde birden fazla kişinin kişisel verilerinin yer alması durumunda ise aynı neviden fikri içtima hükümleri uygulanarak failin cezası artırılacaktır. Örneğin bir kişinin bankadan kredi çekmesine ilişkin belgeler ve bunların içeriği müşteri sırrı kapsamındadır. Ancak bu belgelerde aynı zamanda müşterinin vatandaşlık numarası ve adı ile soyadı da yer alacaktır. Bu belgelerin ifşa edilmesi veya yetkisiz kişilere verilmesi halinde, hem müşteri sırrı ifşa edilerek 239 uncu maddedeki suç, hem de kişisel veri olan vatandaşlık numarası ile ismin ifşası sebebiyle 136 ncı maddede düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşacak, bu suçların cezalandırılmasında farklı neviden fikri içtima kuralları uygulanacaktır. Buna ek olarak, müşterinin bankadan kredi çekebilmesi için kefil de aranmışsa ve kredi alınmasına ilişkin belgeler kefil olan kişinin adı ve soyadı ile T.C. kimlik numarası gibi kişisel verileri de ihtiva ediyorsa, hem müşterinin hem de kefil olan kişinin kişisel verileri ifşa edilmiş olacağından aynı neviden fikri içtima hükmü uygulanarak failin cezası artırılacaktır.

TCK'nın 243 üncü maddesinde düzenlenen bilişim sistemine girme suçu ile 136 ncı maddede düzenlenen suçun bir arada bulunması da olasıdır. Bu durumda, failin kişisel verileri verme, yayma veya ele geçirme fiillerini, bilişim sistemlerine girme suretiyle çok daha kolay işleyebileceği bilinmektedir. TCK'nın 243 üncü maddesinde, "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimsenin" cezalandırılacağı öngörülmüştür. Dolayısıyla başkasının kişisel verilerini vermek, yaymak veya ele geçirmek isteyen bir kimse, bu kişisel verilerin bir bilişim sisteminde kayıtlı olmaları durumunda, önce bu bilişim sistemine girecek, ardından oradaki verileri hukuka aykırı olarak ele geçirebilecektir. Benzer şekilde, kişisel verileri başkasına vermek isteyen failin

[490] **Ekici**, **Akın**, "Bankacılık Mevzuatı Kapsamında Banka ve Müşteri Sırrı, Bankacılar Dergisi", Sayı 63, 2007, s. 53.

elektronik posta yöntemi ile bu fiili çok daha kolaylıkla işleyebileceği, yayma açısından ise aynı anda birden fazla e-posta göndermek suretiyle veya birden fazla kişinin erişim sağlayabildiği forum ortamlarda bu verileri paylaşmak suretiyle bu fiili işleyebileceği açıktır. Failin kişisel verilere ulaşmak ve onları ele geçirmek, vermek veya yaymak için bir bilişim sistemine girmesi gereken durumlar açısından, doktrinde[491] bizim de katıldığımız bir görüşe göre, 243 üncü maddedeki bilişim sistemine girme suçu, 136 ncı maddede tanımlanmış olan suç açısından geçitli bir suç olacaktır. Böylece fail yalnızca kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu bakımından öngörülmüş olan cezaya çarptırılacaktır. Ancak failin 136 ncı maddedeki suçu işlemesi için mutlaka bir bilişim sistemine girmesini gerektiren bir durum söz konusu olmadığında, örneğin fail bir kişinin şifresini kırarak mail adresine girdikten sonra orada gördüğü kişisel verileri almaya karar verip ele geçirdiyse bu durumda iki suç arasında gerçek içtima hükümleri uygulanacak, fail iki ayrı suçtan cezalandırılacaktır.

136 ncı maddenin uygulanması açısından, bu başlık altında üzerinde durulacak bir diğer husus, TCK'nın 244 üncü maddesi ile oluşabilecek hukuki tartışmadır. 244 üncü maddenin 2 nci fıkrasında "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" denmek suretiyle, 136 ncı maddeye benzer bir hüküm sevk edilmiştir. Ancak 244 üncü maddede bahsedilen verilerin başka yere gönderilmesi her ne kadar 136 ncı maddedeki suça benzer görünse de, 136 ncı maddede düzenlenen suç yalnızca kişisel verileri kapsarken, 244 üncü maddedeki suç genel olarak tüm veriler içindir. Buna ek olarak 136 ncı maddede kişisel verilerin verilmesi, yayılması veya ele geçirilmesi bilişim sistemiyle olabileceği gibi, başka yollardan da olabilir. Halbuki 244 üncü maddede var olan verilerin başka bir yere gönderilmesi veya sisteme veri yerleştirilmesi ancak bilişim sistemi içerisinde yapılabilecektir. Düşüncemize göre, kişisel verilerin bilişim sistemleri kullanılarak oldukları yerden başka bir yere gönderilmeleri veya sisteme veri yerleştirilmesi durumunda, bu verilerin kişisel veri olmaları ve bu fiille aynı anda hukuka aykırı olarak verme veya yayma da söz konusu ise, hem 136 ncı maddede tanımlanmış olan suç, hem de 244 üncü maddede düzenlenmiş olan suç oluşacaktır. Tek bir fille birden fazla suç işleyen fail ise, bu

[491] **Dülger**, s. 280.

durumda farklı neviden fikri içtima hükümleri uyarınca, en ağır olan suçun cezasıyla cezalandırılacaktır. Ancak, kişisel verilerin, hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi söz konusu olmaksızın, bu nitelikteki verilerin 244 üncü maddede sayılmış olan fiillerle bozulmaları, yok edilmeleri, değiştirilmeleri veya erişilmez kılınmaları halinde 244 üncü madde tek başına uygulama alanı bulacaktır.

TCK'nın 258 inci maddesinde düzenlenen bir diğer suç "Göreve ilişkin sırrın açıklanması" na göre, "Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir." Maddede düzenlenen suç özgü bir suç olup, yalnızca kamu görevlileri tarafından işlenebilmekte ve yine yalnızca görevleri sebebiyle vakıf oldukları belgeler ve bilgiler açısından uygulama alanı bulmaktadır. Buna göre, bir kamu görevlisinin görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği bir belgeyi açıklaması, yayınlaması veya başkasının bu konuda bilgi edinmesini kolaylaştırması halinde, bu belgede ayrıca başkalarına ait kişisel verilerin bulunması durumunda, 258 inci maddede düzenlenen suçun yanı sıra, 136 ncı maddedeki kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu da işlenmiş olacaktır. Suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılarak işlenmiş olması halinde, 137 nci maddede öngörülen nitelikli hal uygulanarak verilecek ceza yarı oranında artırılmalıdır. Böyle bir durum ortaya çıktığı zaman, kamu görevlisi olan fail, tek bir hareketiyle hem kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunu, hem de göreve ilişkin sırrın açıklanması suçunu işlemiş olacağından, 44 üncü maddede düzenlenen fikri içtima hükmü uygulanacak, böylece faile en ağır cezayı öngören suçun cezası verilecektir. Yalnız bu durumda, 136 ncı maddede de, 258 inci maddede de öngörülen ceza aynı olup, bu ceza bir yıldan dört yıla kadar hapis cezasıdır. Ancak, failin kamu görevlisi olması nedeniyle, 136 ncı madde uygulanırken, nitelikli halleri düzenleyen 137 nci madde devreye girerek verilecek cezayı yarı oranında artıracağından, kanaatimizce burada uygulanması gereken madde 136 ncı madde olacak, 137 nci madde gereği de failin cezası artırılacaktır.

TCK'nın 285 inci maddesinde, "Gizliliğin ihlali" suçu düzenlenerek, ilk fıkrada soruşturmanın gizliliğini alenen ihlal eden kişinin, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacağı, ikinci fıkrada ise kanuna göre kapalı yapılması gereken veya kapalı yapılmasına karar verilen duruşmadaki açıklama veya görüntülerin gizliliğini alenen ihlal eden kişinin birinci fıkraya göre cezalandırılacağı belirtilmiştir. Soruşturmanın gizliliğinin ihlal edilmesi kapsamında, soruşturma kapsamında, soruşturmaya şüpheli, şikayetçi veya tanık olarak dahil olan kişilerin kişisel verilerinin paylaşılması da değerlendirilmedir. Soruşturma kapsamında kalan ve soruşturma sürecine dahil olmuş kişi veya kişilerin kişisel verilerini ihtiva eden bir bilginin veya belgenin ifşa edilmesi halinde, hem 285 inci madde ile düzenlenen gizliliğin ihlali suçu, hem de verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşmuş olacaktır. Böyle bir durumda, fail tek bir fiili ile kanundaki birden fazla suçu ihlal etmiş olacağından, bu suçlar arasında farklı neviden fikri içtima kuralları uygulanacak, fail cezası en ağır olan suçun cezası ile cezalandırılacaktır.

285 inci maddeye benzer olarak 286 ncı maddede de, soruşturma aşamasındaki gizliliğin korunması açısından bir hüküm sevk edilmiş, soruşturma ve kovuşturma işlemleri sırasındaki ses veya görüntüleri yetkisiz olarak kayda alan veya nakleden kişinin, altı aya kadar hapis cezası ile cezalandırılacağı öngörülmüştür. Bu tür ses ve görüntülerin kaydedilmesi hususu 135 inci maddenin içtima kısmında incelenmiş olup, bu başlık altında nakletme fiili incelenecektir. Nakletmek, "nakil işini yapmak, bir yerden başka bir yere geçirmek, iletmek" veya "anlatmak, aktarmak" anlamına gelmektedir[492]. Dolayısıyla, kişisel veriler içeren ses veya görüntülerin nakledilmeleri ile, nakledildikleri yer gizliliği ihlal edecek nitelikte ise, nakleden açısından 136 ncı maddede düzenlenmiş olan kişisel verilerin hukuka aykırı olarak verme veya yayma fiilleri, belirli bir kişiye nakledildiyorsa ise hukuka aykırı olarak ele geçirme fiilleri gerçekleşmiş olacaktır. Bu itibarla, fail tek bir hareketi ile hem 286 ncı maddede düzenlenen, hem de 136 ncı maddede düzenlenen suçların her ikisini de ihlal etmiş olacak, ancak fail her iki suçtan cezalandırılmak yerine, fikri içtima kuralları uygulanarak en ağır cezayı öngören fiilin cezasıyla cezalandırılacaktır.

[492] Türk Dil Kurumu, Büyük Türkçe Sözlük, http://tdkterim.gov.tr/bts/, 09.02.2012.

e. Yaptırım

TCK madde 136'da tanımlanmış olan suçu işleyen kimseye, 1 yıldan 4 yıla kadar hapis cezası verilir. Ancak kanunda bu suçun nitelikli hali olarak düzenlenmiş olan 137 nci madde uyarınca, bu suçun kamu görevlisi tarafından veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında artırılır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçu açısından öngörülen hapis cezası 1 yıldan 4 yıla kadar olarak belirlendiği için, hakimin takdir edeceği cezanın iki yıl veya daha az süreli hapis cezası olması mümkündür. Bu itibarla CMK'nın 231 inci maddesinde sayılan koşulların gerçekleşmesi halinde hükmün açıklanmasının geri bırakılması uygulanabilecektir.

Bu suçu işleyen fail hapis cezasına çarptırıldığı takdirde, TCK m.53/1 uyarınca bu maddede yer alan hak yoksunlukları fail hakkında uygulanacaktır. Suçun nitelikli hallerinden biri olan kamu görevlisinin bu suçu işlemesi durumunda ise, verilmiş olan cezanın hapis cezası olup olmadığına ve ertelenmiş olup olmadığına bakılmaksızın TCK m.53/5 uyarınca fail hakkında verilen cezanın yarısından bir katına kadar failin kamu görevinden yoksun bırakılmasına da karar verilir[493].

TCK'nın 140 ıncı maddesi gereği, tüzel kişilerin bu suçun işlenmesinden kaynaklı olarak hukuka aykırı yarar sağlamaları halinde, bunlara TCK'nın 60 ıncı maddesinde öngörülmüş olan güvenlik tedbirleri uygulanacaktır.

f. Soruşturma Usulü, **Görevli ve Yetkili Mahkeme**, **Dava Zamanaşımı**

TCK m.139'un ihtiva ettiği şikayete bağlı suçlar arasında 136 ncı maddedeki kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu bulunmadığından, bu suçun soruşturulması ve kovuşturulması şikayete bağlı olmayıp, Cumhuriyet Savcılığınca resen yapılacaktır. Bu suçun kamu görevlisi tarafından görevi sebebiyle

[493] **Yaşar-Gökcan-Artuç**, s. 4128.

işlenmesi halinde, 4483 Sayılı kanuna göre, soruşturma ancak yetkili merciden soruşturma izni alındıktan sonra yapılabilecektir[494].

136 ncı maddedeki suçu işleyen kişiler, 5235 Sayılı kanunun 11 inci maddesi uyarınca Asliye Ceza Mahkemesi'nde yargılanacaklardır. Aynı kanunun 14 üncü maddesi gereğince ağırlaştırıcı ve hafifleştirici nedenler görevli mahkemenin belirlenmesine etki etmediğinden, madde 137'de öngörülmüş olan nitelikli hallerin oluşması durumunda dahi görevli mahkeme yine Asliye Ceza Mahkemesi olacaktır.

Yetkili mahkemenin tespiti için, ceza ve ceza muhakemesi hukukunun temel esasları uygulanacak olup, bu hususta ayrıntılı açıklamalar 135 inci madde incelenirken yapıldığından, bu konu üzerinde tekrar durulmayacaktır.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, TCK'nın 139 uncu maddesi gereği şikayete tabi olmaması ve CMK'nın 253 üncü maddesinde sayılan suçlar arasında yer almaması itibariyle, bu suç uzlaşmaya tabi suçlardan değildir.

TCK m.66/1'e göre ise, bu suçun dava zamanaşımı süresi sekiz senedir ve nitelikli hallerin (TCK m.137) uygulanacağı durumlarda ise m.66/3'te "Dava zamanaşımı süresinin belirlenmesinde … suçun daha ağır cezayı gerektiren nitelikli halleri de göz önünde bulundurulur" şeklinde bir hüküm bulunduğundan, m.66/1-d bendi uyarınca bu süre 15 senedir[495].

3. TCK m. 138: Verileri Yok Etmeme

a. Genel Bilgiler

Verileri yok etmeme suçu, TCK'nın 138 inci maddesinde "Kanunların belirlediği süreler geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir" şeklinde düzenlenmiştir. Kişisel verilerin korunması başlığı altında incelemiş olduğumuz diğer suçlar gibi, 765 Sayılı Türk Ceza Kanunu'nda bu suçun

[494] **Yaşar-Gökcan-Artuç**, s. 4129.
[495] **Parlar-Hatipoğlu**, s. 2095.

karşılığı bulunmamaktadır. Bu sebeple bu düzenleme de yeni bir düzenleme olup, temelde kişisel verilerin keyfiliğe bağlı olarak tutulmalarının önüne geçilmek istenmiştir ve bu kişisel verilerin, onları yok etmekle yükümlü olanlar tarafından kanun tarafından öngörülen hukuki sürelerde yok edilmemesi hali yaptırıma bağlanmıştır.

Doktrinde, kişisel verileri yok etmeme suçu açısından aşağıda kapsamlı bir şekilde değinilecek olan temel bir görüş ayrılığı bulunmaktadır. Bir kısım yazarlar bu suç açısından korunan hukuki değeri "özel hayatın gizliliği" ve "kamu idaresinin güvenilirliği ve işleyişi" olarak kabul etmekte olup buna bağlı olarak mağdurun toplum, kişisel verileri silinmeyen kişinin ise suçtan zarar gören olduğunu belirtmektedirler[496]. Aksi görüşte olan diğer yazarlar ise bu suç ile korunan hukuki değerin özel hayatın gizliliği olduğunu ve mağdurun kişisel verileri silinmeyen veri sahibi olduğunu savunmaktadırlar[497].

Bu görüş ayrılığının bir sonucu olarak, suçta korunan hukuki değerin "özel hayatın gizliliği" ve "kamu idaresinin güvenilirliği ve işleyişi" olduğunu ifade eden yazarlar, 138 inci maddede düzenlenmiş olan bu suçu, TCK'nın 257 inci[498] maddesinde düzenlenmiş olan görevi kötüye kullanma suçunun özel bir hali olarak görmektedirler[499]. Bu yazarlara göre, 257 nci maddede görevi kötüye kullanma halinde uygulanacak genel bir hüküm getirilmiş olup, bu husus maddede "kanunda ayrıca suç olarak tanımlanan haller dışında" denilmek suretiyle vurgulanmıştır. İşte bu yazarlara[500] göre, 138 inci maddedeki kişisel verileri yok etmeme suçu 257 nci

---

[496] **Dülger**, s. 282 - 286, **Soyaslan**, s. 350 - 351.

[497] **Yaşar-Gökcan-Artuç**, s. 4132 - 4133, **Özbek**, TCK İzmir Şerhi, s. 964 - 965, **Arslan-Azizağaoğlu**, s. 614 - 615, **Parlar-Hatipoğlu**, s. 2098 - 2100.

[498] Kanunun "Görevi Kötüye Kullanma" başlıklı 257 nci maddesi şu şekilde düzenlenmiştir:
"*(1) Kanunda ayrıca suç olarak tanımlanan haller dışında, görevinin gereklerine aykırı hareket etmek suretiyle, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*
(2) Kanunda ayrıca suç olarak tanımlanan haller dışında, görevinin gereklerini yapmakta ihmal veya gecikme göstererek, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.
(3) İrtikap suçunu oluşturmadığı takdirde, görevinin gereklerine uygun davranması için veya bu nedenle kişilerden kendisine veya bir başkasına çıkar sağlayan kamu görevlisi, birinci fıkra hükmüne göre cezalandırılır."

[499] **Dülger**, s. 282, **Soyaslan**, s. 350, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 610, **Malkoç**, s. 915.

[500] Yaşar-Gökcan-Artuç, her ne kadar 138. maddede düzenlenmiş olan suçun, 257 nci maddedeki görevi ihmal suçunun özel hali olduğu görüşünde olsalar da, bu görüşte olan diğer yazarlardan korunan hukuki menfaat ve mağdur hususunda ayrılmaktadırlar. Suçun 257 nci maddenin özel bir halini teşkil ettiğini savunan diğer yazarlar korunan hukuki menfaatin özel hayatın gizliliği ve kamu idaresinin güvenilirliği ve işleyişi, mağdurun ise kamu olduğunu kabul etmekte iken, aksi görüşte olan

maddede anılan "ayrıca suç olarak tanımlanan haller" den biridir[501]. Dolayısıyla verileri yok etmeme suçu özel bir görevi yerine getirmeme ve görevi ihmal suçu olarak uygulanacaktır.

Verileri yok etmeme suçunun, kanunda; Özel Hükümler kitabının Kişilere Karşı Suçlar kısmında ve Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar bölümünde düzenlendiği görülmektedir. Buna bağlı olarak kanun koyucunun maddeyi ihdas etme amacı da göz önüne alındığında, kanaatimizce, kanun metninde "… yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde" şeklinde bahsedilen kişilerin kamu görevlisi olmaları gerektiğine ve bu suçun 257 nci maddede düzenlenmiş olan görevi kötüye kullanma suçunun özel bir hali olduğuna katılmak mümkün değildir. Günümüzde kişilerin verileri her tür ortamda tutulmakta, saklanmakta ve kullanılmaktadır. Dolayısıyla bu tür verilerin yok edilmesi gerektiğinde bunu yapmakla yükümlü olan ancak kamu görevlisi olmayan pek çok kişi vardır. Bu itibarla verileri yok etmeme suçu açısından, madde metninde değinilen "görev" kavramını kamu görevi ile sınırlamak maddenin düzenleniş amacına da aykırı olacak, kamu görevlisi olmayıp kişisel verileri yok etme görevini yerine getirmeyen kişilere karşı bu yaptırımın uygulanamamasına sebep olacaktır. Dolayısıyla bu suçun, kişisel verileri yok etmekle yükümlü olup, yok etmeyen tüm kişileri kapsayacağı ve kanunda düzenlendiği yer de dikkate alındığında suçun veri öznesine karşı işlenmiş olacağını kabul etmek yerinde olacaktır. Bu itibarla, maddede geçen "yok etmekle görevli" ifadesinin mutlaka kamu görevlisi anlamına gelmeyeceği görüşünde olduğumuzdan, düşüncemize göre bu suçu görevi kötüye kullanma suçunun özel hali olarak kabul etmek de mümkün değildir.

---

yazarlara göre bu suçla korunan hukuki menfaat özel hayatın gizliliği olup mağdur da kişisel verileri kaydedilen ancak kanuni süreler geçmesine rağmen silinmeyen kişidir. Yaşar-Gökcan-Artuç ise, kişisel verileri yok etmeme suçunun 257. maddedeki görevi ihmalin özel bir hali olduğunu kabul etmekle beraber, korunan hukuki değerin özel hayatın gizliliği, mağdurun ise kişisel verileri kaydedilmiş olup silinmeyen kişi olduğunu savunmaktadırlar, **Yaşar-Gökcan-Artuç**, s. 4132-4133.

[501] Dülger'e göre, "*Bu suç tipleri düzenlenirken 'kanunda ayrıca suç olarak tanımlanan haller dışında' ifadesi kullanılarak 257. maddenin 1. ve 2. fıkralarındaki suç tiplerinin genel nitelikte olduğu, bunun dışında görevi yerine getirmeme ve görevi ihmal suçlarının başka maddelerde özel eylemler açısından düzenlenebileceği belirtilmiştir. İşte inceleme konusu olan verilerin yok edilmemesi suçu da böyle bir özel görevi yerine getirmeme ve görevi ihmal suçudur. Çünkü yasayla 'verileri yok etmekle görevlendirilen kişi' bunu kamu görevi olarak yapmaktadır.*", **Dülger**, s. 282.
Şen'e göre, "*Elbette bu suç kasten işlenebilen bir suç olup, görevi ihmal suçunun özel bir tipini oluşturmaktadır.*", **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 610.

b. Suçla Korunan Hukuki Değer

Verileri yok etmeme suçunda korunan hukuki değer hususunda, bu suçun görevi kötüye kullanma suçunun özel bir halini oluşturup oluşturmadığı düşüncesine bağlı olarak; doktrinde iki temel görüş vardır. Birinci görüşe göre, bu suç açısından korunan yegane hukuki değer özel hayatın gizliliği olmayıp; bunun yanında "kamu idaresinin güvenilirliği ve işleyişi" de korunmaktadır[502]. İlk görüşü savunan yazarlara göre, kamu idaresinde bulunan ve silinmesi gerektiği halde silinmeyen kayıtların bulunması durumunda, bunun idareye olan güveni zedeleyeceği ve bu suçun ihdas edilmesiyle bu güvenin korunmak istendiği ifade edilmektedir. Bizim de katıldığımız ikinci görüş, kişisel verileri yok etmeme suçunun özel hayatın gizliliğini koruduğu ve bu itibarla korunan hukuki değerin özel hayatın gizliliği olduğunu savunmaktadır[503].

Verileri yok etmeme suçunun kanunda düzenlendiği yer dikkate alındığında, suçun kişilere karşı suçlar kısmında, özel hayata ve hayatın gizli alanına karşı suçlar bölümü altında bulunması sebebiyle suçun veri öznesinin özel hayatının gizliliğini korumayı amaçladığı hususunda her iki görüş açısından da bir tereddüt bulunmamaktadır. Burada görüş ayrılığına neden olan temel husus bu suçun aynı zamanda kamu idaresinin güvenilirliğini ve işleyişini de koruyup korumadığıdır. Düşüncemize göre, Türk Ceza Kanunu'nda düzenlenen tüm suçlar açısından kamu düzeninin ve kamu idaresinin güvenirliğinin bir parça korunmaya çalışıldığı savunulabilir. Dolayısıyla bu suç bakımından da, suçun düzenlenmesiyle kamu idaresinin güvenirliğinin genel anlamda korunmaya çalışıldığı düşünülebilir. Ancak, suçun Kişilere Karşı Suçlar kısmında ve Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar bölümünde düzenlendiği dikkate alındığında, suçun ihdas edilmesiyle korunmaya çalışılan temel değerin kişisel verileri yok edilmeyen veri öznelerinin özel hayatlarının gizliliği olduğu anlaşılmaktadır.

---

[502] **Dülger**, s. 282, **Soyaslan**, s. 350.
[503] **Yaşar-Gökcan-Artuç**, s. 4132, **Özbek**, TCK İzmir Şerhi, s. 964, **Arslan-Azizağaoğlu**, s. 614, **Parlar-Hatipoğlu**, s. 2008.

c. Suçun Unsurları

(1) Maddi Unsurlar

(a) Fiil

Suçu oluşturan hareket kanuni dayanaklarla hukuka uygun olarak kaydedilmiş kişisel verilerin, kanunun yükümlü kıldığı kişilerce, kanunun öngördüğü süreler içerisinde yok edilmemesidir. Doktrinde yazarlardan bir kısmı, kanunun lafzından yola çıkarak, hareketin "sistem içinde yok etmek" olduğunu savunmaktadır[504]. Ancak bu suçun konu başlığı altında ayrıntılı olarak değinildiği üzere, kanaatimizce 135 inci ve 136 ncı maddelerdeki suçlarda kişisel verilerin kaydedilmesi ile ilgili sisteme kayıt şartı aranmadığından, 138 inci maddeyi bu şekilde dar yorumlamak kanun koyucunun amacına ters düşecektir. Bu itibarla her ne kadar kanun metninde sistem içinde yok etme ifadesi geçiyor olsa da, sistem dışında bir yere kaydedilmiş olan kişisel verilerin de bu suçun konusunu oluşturacağını ve bunları yok etmemenin de bu suçu oluşturan hareketlerden biri olduğunu kabul etmek gerekecektir[505].

Kaydedilen kişisel veriler bir bilişim sistemine kaydedilmişse buradan silinmeleri, belli bir belge üzerine kaydedilmemişlerse belgenin imha edilmesi şeklinde gerçekleşebilir. Yalnız burada dikkat edilmesi gereken husus, suçun oluşmaması için, kaydedilmiş olan kişisel verinin yeniden elde edilemeyecek şekilde yok edilmesi gerektiğidir. Bilgisayarlarda tutulan kayıtlarda bir bilgiyi yalnızca silmek onu yok etmek anlamına gelmemektedir, zira birtakım yöntemlerle bu bilgiler yeniden ortaya çıkarılabilmektedir. Bu nedenle kanaatimizce, kaydedilmiş olan kişisel verinin yeniden ortaya çıkarılmasını imkansız kılacak şekilde yok edilmesi gerekmektedir. Nitekim Türkçede, yok etmek; "ortadan kaldırmak, ifna etmek, izale

---

[504] **Arslan-Azizağaoğlu**, s. 615, **Parlar-Hatipoğlu**, s. 2100.

[505] **Dülger**, s. 285; "*… verilerin sistemden yok edilmemesi çok çeşitli şekillerde olabilecektir. Örneğin veriler yazılı halde bulunuyorsa yakmak suretiyle ya da veriler bir bilişim sisteminde sanal veri olarak bulunuyorsa bunların silinmesi ya da verilerin üzerinde bulunduğu cd-rom ya da sabit diskin kırılması suretiyle verilerin yok edilmesi görevi yerine getirilebilecektir.*"

Soyaslan, s. 351; "*Yakmak veya sanal sistemden silinmek suretiyle, cd-rom ya da sabit diskin kırılması suretiyle olabilir.*"

Yaşar-Gökcan-Artuç, s. 4135; "*Yok etme eylemi, bilgisayardaki bilgiler için; tüm kopyaların silinmesi, herhangi bir örneğinin kalmaması, fiziki belgeler için ise; geri dönüşü olmayacak şekilde ortadan kaldırılmasını belirtir.*"

etmek, varlığına son vermek" anlamına gelmektedir[506]. Doktrinde, kişisel verilerin yok edilmesinin "verinin içerdiği bilgi ya da enformasyon ile ilgili kişinin arasındaki bağlantının ortadan kaldırılması şeklinde de gerçekleştirilebileceği"[507] fikrine ise katılmanın mümkün olmadığı düşüncesindeyiz; zira 138 inci maddenin metninde açık bir şekilde kişisel verileri "yok etmeme" den bahsedilmekte olup, kaydedilmiş olan kişisel verilerin ortadan kaldırılmamasını kastetmektedir. Veri öznesinin bu verilerle bağlantısının kesilmesi ve veriler ile veri öznesi arasında bağlantı kurulamamasını sağlama yok etme anlamına değil, verinin anonimleştirilmesi anlamına geldiğinden, bu yöntem verileri yok etme olarak değerlendirilemeyecektir.

Doktrinde; bizim de katıldığımız görüşe göre, verileri yok etmeme suçunda bahsedilen kanuni sürelerdeki "kanun" ifadesinin hem maddi hem de şekli kanun olarak anlaşılması gerekmektedir[508]. Bunun doğal sonucu olarak da yalnızca bir kanunla değil idarenin herhangi bir düzenleyici işlemiyle de kişisel verilerin belirli bir süre sonra yok edilmeleri öngörülebilir ve bu da kanunun doğuracağı bir yükümlülükle eşdeğerdir. Dolayısıyla verileri yok etmeme suçunun dayanağını oluşturan yükümlülük bir kanundan kaynaklanabileceği gibi, bir yönetmelikten de kaynaklanabilecektir.

Kanunlar genel olarak Ceza Muhakemesi Kanunu'nda olduğu gibi, kaydedilmiş olan kişisel verilerin hangi sürede yok edilmesi gerektiğini belirtmektedirler ve bu sürenin açıkça gösterildiği durumlarda verileri yok etmekle yükümlü kişi bu süre dolmadan verileri yok etmek zorundadır[509]. Ancak verilerin kaydedilmesini öngörmüş olan kanun yok edilmeleri ile ilgili olarak net bir süre belirlemek yerine "hemen silinir", "derhal yok edilir" gibi kavramlara yer vermiş olabilir. Doktrinde bizim de katıldığımız bir görüşe göre, kanunda kesin sürelerin olmadığı ifadeler de emredici niteliktedir ve somut olaya göre makul sürede yok etme işleminin yapılması gerekmektedir[510].

---

[506] http://tdkterim.gov.tr/bts/ 30.11.2011.
[507] **Ketizmen**, s. 241.
[508] **Özbek**, TCK İzmir Şerhi, s. 965, **Dülger**, s. 285.
[509] Örneğin, çalışmamızın aşağıdaki konu kısmında ayrıntılı olarak değinileceği üzere, CMK'nın 137 nci maddesinde, CMK'nın 135 inci maddesine göre toplanmış olan verilerin belirli hallerde en geç on gün içinde yok edilmeleri gerektiği öngörülmüştür.
[510] **Yaşar-Gökcan-Artuç**, s. 4134 - 4135.

Doktrindeki bir görüşe göre verileri yok etmeme suçu ile ilgili önemli bir diğer husus, maddede kişisel verilerin kaydedilme amacının ortadan kalktıktan sonra ne olacağına değinilmemiş olmasıdır[511]. Yazar, maddedeki kanuni süreler geçtikten sonra yok etmeme ifadesinin yetersiz ve eksik olduğunu ileri sürmekte, hukuka uygun olarak kaydedilmiş olan kişisel verilerin kaydedilme amaçları ortadan kalktığında veya gerçekleşmediğinde de yok edilmeleri gerektiğini belirtmektedir. Ancak yazara göre, böyle bir düzenleme yapılacak olsa dahi, amacın hangi durumlarda gerçekleşmediği veya ortadan kalktığının kanunla belirlenmesi hususunun 138 inci maddede yer almış olması gerekir; aksi halde amacın neye göre ortadan kalkmış olacağı hususu soyut bir ifade olarak kalacak, bu da kanunilik ilkesine aykırılık teşkil edecektir.

Verileri yok etmeme suçu yapılması gereken icrai bir davranışın yapılmaması anlamına geldiğinden, bu suç ihmali hareketlerle işlenebilen suçlardandır. İhmali suçların, hukuk kurallarının belirli bir emredici davranış öngörmüş olması, ancak bu hareketin yapılmayarak olumsuz bir davranışla suçun işlenmesi şeklinde oluştuklarına yukarıda değinmiştik. Bu noktada önemlilik arz eden husus, suç tipinde yapılması emredilmiş olan hareketin kasten yapılmamasıdır[512]. Bu açıklamalardan da anlaşıldığı üzere, TCK'nın 138 inci maddesinde düzenlenmiş olan verileri yok etmeme suçu değerlendirildiğinde, kanun, verileri yok etmekle yükümlü olan kişilerin bu verileri yok etmelerini emredici kural olarak öngörmüştür. Bu kuralı olumsuz bir davranışla yerine getirmeyenler ise cezalandırılmış, dolayısıyla bu suç ihmali bir suç olarak düzenlenmiştir.

(b) Fail

Verileri yok etmeme suçunu, ancak verileri yok etmekle yükümlü olan kişi işleyebilecektir. Bu açıdan bu suçun bir özgü suç olduğu ve herkes tarafından işlenebilecek bir suç olmadığı kabul edilmelidir[513]. Bir kişinin kişisel verilerin yok

---

[511] **Ketizmen**, s. 241.

[512] **Önder, Ayhan**, s. 51, **Koca-Üzülmez**, s. 312, **Toroslu**, s. 111, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 259 - 260; "*Ancak belirtelim ki, ihmali suçlarda failin sadece hareketsiz kalması yeterli değildir, önemli olan suç tipinde belirlenmiş olan hareketin yapılmamış bulunmasıdır. Bu suçlarda kanun koyucunun suç tipinde yapılmasını emrettiği hareketi gerçekleştirmekle yükümlü kimse, sadece hareketsiz kalabileceği gibi, kendisinden beklenen davranışı yapmayıp bunun yerine başka bir icrai harekette bulunmuş da olabilir*."

[513] **Yaşar-Gökcan-Artuç**, s. 4133, **Özbek**, TCK İzmir Şerhi, s. 964.

edilmemesi suçunu işleyebilmesi için kanunda gösterilmiş olan sürelerde yok etmesi gereken kişisel verileri yok etmemesi ve bu verileri yok etmekle yükümlü kılınmış olması yeterlidir[514]. Ayrıca failin kamu görevlisi olması da şart olmayıp, fail kişisel verileri yok etmekle yükümlü herhangi bir kişi olabilmektedir[515]; ancak doktrindeki genel görüşe göre bu suç genellikle kamu görevlisi sıfatı taşıyan kişilerce işlenmektedir.

(c) Mağdur

Suçun koruduğu hukuki değer ve bu suçun TCK'nın 257 nci maddesinin özel bir halini oluşturup oluşturmadığı hususundaki görüş farklılıklarının bir neticesi olarak, mağdurun kim olacağı konusu da yazarlar arasında görüş ayrılığına neden olmuştur. Verileri yok etmeme suçunun koruduğu hukuki değerin özel hayatın gizliliği ve "kamu idaresinin güvenilirliği ve işleyişi" olduğunu savunan yazarlara göre, bu suçun mağduru kamu idaresi olup, kişisel verileri silinmeyen kişi suçtan zarar görendir[516]. Korunan hukuki değerin özel hayatın gizliliği olduğu görüşünü benimseyen yazarlara göre ise; bu suçun mağduru kişisel verileri kaydedilmiş olup kanunda öngörülen süreler geçmiş olmasına rağmen kişisel verileri silinmeyen kişidir[517]. Biz de korunan temel hukuki değerin özel hayatın gizliliği olduğu düşüncesine iştirak ettiğimizden, bu suçun mağdurunun kişisel verileri silinmeyen kişiler olduğunu kabul etmek gerektiği düşüncesindeyiz.

(d) Konu

Suçun konusu hukuka uygun olarak kaydedilmiş olan kişisel verilerdir. Bu maddedeki suçun oluşabilmesi için, kişisel verilerin hukuka uygun olarak kaydedilmiş olmaları gerekmektedir ki; kanun tarafından belirli sürelerde silinmeleri gereksin. Bu nedenle ancak hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanuni süreler dolduğu zaman silinmeleri gerektiğinden bahsedilebilir. Kişisel veriler

---

[514] **Yaşar-Gökcan-Artuç**, s. 4133, **Dülger**, s. 283, **Parlar-Hatipoğlu**, s. 2099, **Özbek**, TCK İzmir Şerhi, s. 965, **Şen**, **Ersan**; "5237 Sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İstanbul Barosu Dergisi, Cilt:79, Sayı:3, 2005, s. 719, **Değirmenci**, s. 203.

[515] **Özbek**, TCK İzmir Şerhi, s. 965, **Parlar-Hatipoğlu**, s. 2099, **Dülger**, s. 283, **Soyaslan**, s. 350, **Yaşar-Gökcan-Artuç**, s. 4133, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 611, **Malkoç**, s. 915.

[516] **Dülger**, s. 283, **Soyaslan**, s. 350.

[517] **Özbek**, TCK İzmir Şerhi, s. 965, **Parlar-Hatipoğlu**, s. 2100, **Arslan-Azizağaoğlu**, s. 615, **Yaşar-Gökcan-Artuç**, s .4133.

hukuka aykırı olarak kaydedilmişlerse zaten yukarıda incelenmiş olan ve TCK'nın 135 inci maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu oluşacaktır[518].

Verileri yok etmeme suçunun oluşması için herhangi bir zararın meydana gelmiş olması aranmamakta olup, verilerin kanuni süreler geçmiş olmasına rağmen yok edilmemeleri ile suç tamamlanmış olacaktır. Tehlike suçlarında suçun oluşması için bir zararın meydana gelmesi aranmayıp hareketin yöneldiği konunun objektif olarak zarar uğrama tehlikesi ile karşı karşıya kalmış olması yeterli olduğundan verileri yok etmeme suçu bir tehlike suçudur. Kanun koyucunun hareket ile tehlike arasında bir nedensellik bağının bulunup bulunmadığının araştırılmasını öngörmemiş olması sebebiyle de bu suç bir soyut tehlike suçudur[519]; buna göre hareketin yapılması ile beraber konu üzerinde bir tehlikenin ortaya çıktığı varsayılacak; bu tehlikenin ayrıca mevcut olup olmadığı araştırılmayacaktır.

Ceza Muhakemesi Kanunu'nun yetkililere verdiği yetki ile toplanan kişisel veriler yine bu kanunun belirlediği sürelerin dolması veya kanunda belirtilen koşulların gerçekleşmesi ile yok edilmelidirler[520]. CMK'nın "Şüpheli Veya Sanığın Beden Muayenesi Ve Vücudundan Örnek Alınması" başlıklı 75 inci ve "Diğer Kişilerin Beden Muayenesi Ve Vücuttan Örnek Alınması" başlıklı 76 ncı maddelerinde bir suça ilişkin delil elde etmek için şüpheli veya sanığın vücudundan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesinden bahsedilmektedir. "Genetik İnceleme Sonuçlarının Gizliliği" başlıklı 80 inci maddede ise, alınan bu örnekler üzerinde yapılan inceleme sonuçlarının, kişisel veri niteliğinde olduğu, başka bir amaçla kullanılamayacağı; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyeceği düzenlenmiştir. 80 inci maddenin ikinci fıkrasında bu bilgilerin, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet savcısının huzurunda derhal yok edilecekleri ve bu hususun dosyasında muhafaza edilmek üzere tutanağa geçirileceği belirtilmiştir.

---

[518] **Yaşar-Gökcan-Artuç**, s. 4133.
[519] **Özbek**, TCK İzmir Şerhi, s. 966.
[520] **Yaşar Gökcan Artuç**, s. 4133, **Parlar-Hatipoğlu**, s. 2098 - 2099, **Özbek**, TCK İzmir Şerhi, s. 965.

CMK'nın "Fizik Kimliğin Tespiti" başlıklı 81 inci maddesine göre de, üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulacağı, ikinci fıkrasında ise kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde söz konusu kayıtların Cumhuriyet savcısının huzurunda derhal yok edilecekleri ve bu hususun tutanağa geçirileceği öngörülmüştür.

CMK'nın "İletişimin Tespiti, Dinlenmesi Ve Kayda Alınması" başlıklı 135 inci maddesi ile "Kararların Yerine Getirilmesi, İletişim İçeriklerinin Yok Edilmesi" başlıklı 137 nci maddesinde de benzer örnekler vardır. Zira 135 inci maddeye göre bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimin tespit edilebilmesi, dinlenebilmesi, kayda alınabilmesi mümkün kılınmıştır. Ancak 137 nci maddedeki düzenleme ile 135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hakim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhal son verileceği, bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilecekleri öngörülmüştür.

Ceza Muhakemesi Kanunu'nun bu konuya temas eden bir diğer maddesi de "Teknik Araçlarla İzleme" başlıklı 140 ıncı maddesidir. Bu maddede öngörülmüş olan suçların işlendiği hususunda kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabileceği, ancak elde edilen delillerin, maddede sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamayacakları; ceza kovuşturması bakımından gerekli

olmadığı takdirde Cumhuriyet savcısının gözetiminde derhal yok edileceği düzenlenmiştir.

Kişisel verilerin yok edilmesine ilişkin birtakım kurallar getirmiş olan bir diğer kanun da 5352 Sayılı Adli Sicil Kanunu'dur[521]. Bu kanunun "Adli Sicil Bilgilerinin Silinmesi" başlıklı 9 uncu maddesine göre adlî sicildeki bilgilerin; cezanın veya güvenlik tedbirinin infazının tamamlanması, ceza mahkumiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık, ceza zamanaşımının dolması ve genel af halinde Adlî Sicil ve İstatistik Genel Müdürlüğünce silinerek, arşiv kaydına alınacağı öngörülmüş olup, aynı kanunun "Adli Sicil ve Arşiv Bilgilerinin Silinmesi" başlıklı 12 nci maddesinin ikinci fıkrasında, fiilin kanunla suç olmaktan çıkarılması halinde, bu suçtan mahkumiyete ilişkin adlî sicil ve arşiv kayıtlarının, talep aranmaksızın tamamen silineceği, üçüncü fıkrasında ise kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi halinde, önceki mahkumiyet kararına ilişkin adlî sicil ve arşiv kaydının tamamen silineceği belirtilmiştir[522].

Ceza Muhakemesi Kanunu'nun ve Adli Sicil Kanunu'nun bu maddelerine göre toplanmış olan kişisel verilerin, yine aynı kanunda belirtilmiş olan şartların gerçekleşmesine rağmen yok edilmemelerinin TCK'nın 138 inci maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçunu oluşturacağı şüphesizdir.

"Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti Dinlenmesi Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş Görev ve Yetkileri Hakkında Yönetmelik" in[523] 11 ve 12 nci maddelerinin ihlal edilmesi halinde de 138 inci maddedeki suçun işlenmesi söz konusu olacaktır. "Kayıtların yok edilmesi" başlığı

---

[521] **Yaşar-Gökcan-Artuç**, s. 4134, **Soyaslan**, s. 350, **Özbek**, TCK İzmir Şerhi, s. 966, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 610.

[522] Adli Sicil Kanunu'nun 12. maddesinin ilk fıkrası "*(1) Arşiv bilgileri, ilgilinin ölümü üzerine ve her halde kaydın girildiği tarihten itibaren seksen yılın geçmesiyle tamamen silinir*." şeklinde düzenlenmişti. Ancak maddenin bu fıkrası Anayasa Mahkemesi'nin 20.1.2011 T., 2008/44 E., 2011/21 K. Sayılı Kararı ile iptal edilmiş olup, Kararın Resmi Gazete'de yayımlandığı 14.4.2011 tarihinden bir yıl sonra yürürlüğe girmesi hüküm altına alınmıştır.
http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.5352&sourceXmlSearch=&MevzuatIliski=0 27.11.2011.

[523] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti Dinlenmesi Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş Görev ve Yetkileri Hakkında Yönetmelik, R.G.t. 10.11.2005, S. 25989.

altında düzenlenmiş olan 11 inci maddenin son fıkrasında, dinlemenin içeriğine ilişkin kayıtların yok edilmelerine ilişkin bir düzenleme yer almakta, maddede belirtilen koşullar oluştuğunda, kayıtların 10 gün içinde yok edilmesi gerektiği ifade edilmektedir[524]. 12 nci maddede ise, telekomünikasyon yoluyla iletişimin hangi hallerde tespit edilebileceği, dinlenip kayda alınabileceği belirtilmiştir[525]. Maddede, şüpheli veya sanığın tanıklıktan çekinilebilecek kişilerle arasındaki iletişimin kayda alınamayacağı genel bir kural olarak öngörülmüş; böyle bir durumun kayda alma işlemi gerçekleştikten sonra anlaşılması üzerine, alınan kayıtların derhal yok edileceği ifade edilmiştir. Buna göre, bu Yönetmelik'in 11 ve 12 nci maddelerinde öngörülen koşulların oluşmasına rağmen söz konusu kayıtları silmekle yükümlü kişilerin bu görevlerini yerine getirmemeleri durumunda, 138 inci maddede düzenlenen suç oluşacaktır. 12 nci maddede kaydedilmemiş olması gereken iletişimin kaydedilmiş olması durumunda yapılacak yok etme işlemi için kesin bir süre verilmemiş olsa da, yukarıda "fiil" başlığı altında ifade ettiğimiz üzere, "derhal" gibi ifadeler de emredici nitelikte olup somut olayın koşullarına göre, bu tür kayıtların en kısa sürede yok edilmeleri gerekecektir.

---

[524] Madde 11'in tam metni şu şekildedir: "*Hakim kararları ile yazılı emirler hakkındaki gelişmeler ilgili kurum tarafından derhal Başkanlığa bildirilir.*

Uygulanan tedbirin sona ermesi, gecikmesinde sakınca bulunan hallerde verilen yazılı emir hakkında hakim tarafından aksine karar verilmesi ya da yazılı emir hakkında yirmi dört saat içinde hakim onayının alınamaması hallerinde, kararın veya yazılı emrin uygulanmasına Başkanlık tarafından derhal son verilir.

Dinlemenin içeriğine ilişkin kayıtlar ilgili kurumların en üst amirinin ve bu kayıtların Başkanlıkta da tutulması halinde Başkanın denetimi altında en geç on gün içinde yok edilir. Durum bir tutanakla tespit olunur ve bu tutanak denetimlerde ibraz edilmek üzere muhafaza edilir."

[525] Yönetmeliğin 12 nci maddesinin tam metni şu şekildedir: "*Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı, kararını derhal hakimin onayına sunar ve hakim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hakim tarafından aksine karar verilmesi halinde tedbir Cumhuriyet savcısı tarafından derhal kaldırılır.*

Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştikten sonra bu durumun anlaşılması halinde, alınan kayıtlar derhal yok edilir.

Birinci fıkra hükmüne göre verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkan veren kodu, tedbirin türü, kapsamı ve süresi belirtilir.

Tedbir kararı en çok üç ay için verilebilir; bu süre, bir defa daha uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hakim bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

Şüpheli veya sanığın yakalanabilmesi için, mobil telefonun yeri, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebilir. Bu hususa ilişkin olarak verilen kararda, mobil telefon numarası ve tespit işleminin süresi belirtilir. Tespit işlemi en çok üç ay için yapılabilir; bu süre, bir defa daha uzatılabilir.

Bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur."

Suçun konusu hususunda değinilmesi gereken bir diğer önemli nokta da kanun metninde yok edilmemesi suç sayılan kişisel verilerin "sistem içinde" kişisel veriler şeklinde düzenlenmiş olmasıdır. Kanun metninin kendisinden veya gerekçesinden "sistem içindeki" verilerden ne anlaşılması gerektiğine ilişkin açık bir düzenleme bulunmamaktadır. Bu itibarla, bu suç değerlendirildiğinde, suçun konusunu teşkil eden kişisel verilerin kapsamına yalnızca bir bilişim sisteminde yer alan verilerin mi dahil olacağı sorunu gündeme gelebilir[526]. Kanaatimizce maddede kullanılan bu ifade yerinde olmamıştır; zira yukarıdaki başlıklarda açıklandığı üzere, kişisel verilerin kaydedilmesinin yalnızca bilişim sistemleri aracılığı ile değil, örneğin yazı ile yazılmak suretiyle de yapılabileceğini ifade etmiştik. Bu sebeple, Ceza Muhakemesi Kanunu, Adli Sicil Kanunu veya benzer düzenlemeler ihtiva eden kanunlar uyarınca kaydedilmiş olan kişisel verilerin, kağıt üzerine yazmak suretiyle hukuka uygun olarak kaydedilip, kanunun öngördüğü süreler sona erdikten sonra yok edilmemeleri durumunda, kişisel verileri yok etmeme suçunun oluşmayacağını söylemek mümkün değildir. Bu itibarla, 138 inci maddenin lafzı her ne kadar "sistem içindeki" verilerin yok edilmemesi şeklinde düzenlenmiş olsa da, kanaatimizce TCK'nın 135 inci maddesindeki kişisel verilerin hukuka aykırı olarak kaydedilmeleri suçunun gerekçesinde kişisel verilerin yalnızca bilişim sistemleri aracılığıyla değil, elle yazmak gibi başka yöntemlerle de kaydedilebilecekleri belirtildiğinden, kanun koyucunun amacı da dikkate alınarak, bu madde için de, bir sistem içinde bulunmayıp başka bir yöntemle kaydedilmiş olan kişisel verinin kanuni süreler geçtikten sonra yok edilmemesi halinde suçun oluşacağını kabul etmek gerekecektir.

(e) Netice

Verileri yok etmeme suçu açısından, suçun sırf hareket suçu olduğunu söylemek mümkün olup, sırf hareket suçlarında hareketin yapılmasıyla suç gerçekleşip tamamlandığından, suçun tamamlanması için neticenin ortaya çıkmasına gerek bulunmamaktadır. Bu itibarla hareketin yapılmasıyla tipiklikte belirtilmiş olan ihlal tamamlanmaktadır.

Verileri yok etmeme suçu açısından da, herhangi bir neticenin ortaya çıkmasına gerek olmayıp, daha önce kaydedilmiş olan kişisel veriler, kanunda

[526] **Ketizmen**, s. 242.

belirtilen sürelerin geçmiş olmasına rağmen silinmedikleri an bu suç gerçekleşmiş olacaktır[527]. Dolayısıyla, salt verilerin süreler geçmiş olmasına rağmen silinmemesi suçun oluşması için yeterli olacak, ayrıca failin bu verileri kullanması veya bunlardan bir fayda sağlaması aranmayacaktır.

(f) Suçun Nitelikli Unsurları

138 inci maddenin madde metninde suç için herhangi bir nitelikli hal öngörülmediği gibi[528], TCK'nın 137 nci maddesinde "Yukarıdaki maddelerde tanımlanan suçların" ifadesinin yer alması sebebiyle, bu maddede öngörülmüş olan nitelikli haller verileri yok etmeme suçunu kapsamamaktır. Bu nedenle TCK'nın 138 inci maddesinde düzenlenmiş olan bu suç açısından cezanın ağırlaştırılmasını ya da hafifletilmesini gerektiren bir nitelikli hal öngörülmemiştir. Halbuki, düşüncemize göre, 138 inci maddede bahsedilmiş olan yok etmekle yükümlü olan kişiler kapsamına yalnızca kamu görevlileri girmediği ve özel sektörde çalışan kişiler de bu suçun faili olabilecekleri için, bu madde açısından fiilin kamu görevlisi tarafından işlenmesi bir nitelikli hal olarak öngörülebilirdi. Maddede, görevi gereği yükümlü olmaktan bahsedildiğine göre, fail her durumda bu suçu işlerken mesleğinin veya sanatının sağladığı kolaylıktan faydalanacaktır. Dolayısıyla 137 nci maddenin ikinci fıkrasında öngörülmüş olan nitelikli halin bu suç açısından öngörülmesi gerekmediği düşüncesindeyiz. Ancak failin kamu görevlisi olmasının daha ağır neticelere yol açabileceği ve kamu düzeni ile kamunun işleyişine zarar vereceği düşünüldüğünde, suçu kamu görevlisinin işlemesi halinin cezanın artırılmasını gerektiren bir nitelikli hal olarak düzenlenmesi gerektiği kanaatindeyiz.

(2) Manevi Unsur

TCK'nın 138 inci maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçu genel kastla işlenebilir. Suçun işlenebilmesi için herhangi bir saik aranmıştır. Bu sebeple, failin, kanuni süreler geçmiş olmasına ve kaydedilmiş olan kişisel verileri yok etmekle yükümlü olmasına rağmen bu görevini kasten yerine getirmemesi yeterlidir. TCK'da bu suçun taksirli haline ilişkin herhangi bir

[527] **Soyaslan**, s. 351, **Yaşar-Gökcan-Artuç**, s. 4137, **Parlar-Hatipoğlu**, s. 2101.
[528] **Yaşar-Gökcan-Artuç**, s. 4136, **Özbek**, TCK İzmir Şerhi, s. 966, **Parlar-Hatipoğlu** s. 2101.

düzenleme bulunmadığından, suçun taksirle işlenmesi mümkün olmayacak, failin mutlaka kasten hareket etmesi gerekecektir.

(3) Hukuka Aykırılık

Verileri yok etmeme suçu açısından öngörülmüş olan özel bir hukuka uygunluk nedeni düzenlememiş olduğundan, hukuka uygunluk nedenleri Türk Ceza Kanunu'nun genel hükümlerine göre belirlenecektir.

Hukuka uygunluk nedenlerinden biri olan kanun hükmünün yerine getirilmesinin (görevin ifası) bu suç açısından bir hukuka uygunluk sebebi oluşturabileceği düşünülebilir. Her ne kadar doktrinde aksi görüşler bulunsa da[529], ilgilinin rızasının bulunması durumunda, kanaatimizce suç oluşmaz[530]. Ancak kişisel verilerin kanunda öngörülmüş olan süreler geçmiş olmasına rağmen meşru müdafaa kapsamında silinmemelerinin hukuka uygunluk sebebi teşkil etmesi uygulamada mümkün gözükmemektedir. Hakkın icrasına bakıldığında ise, doktorların hastalarının kayıtlarını tutmaları düşünülebilecek olsa da, hasta bilgilerinin belirli bir süre geçtikten sonra silinmesi ile ilgili kanunda hüküm bulunması halinde, silmeme işleminin hakkın icrası kapsamında değerlendirilmesi kanaatimizce mümkün olmayacaktır.

d. Suçun Özel Görünüş Şekilleri

(1) Teşebbüs

Verileri yok etmeme suçu ihmali suçlardan olduğundan[531], kanunda belirtilen sürenin dolduğu an, kişisel veri silinmemişse suç meydana gelmiş olacaktır. Bu

---

[529] Bkz. **Özbek**, TCK İzmir Şerhi, s. 966; "*Bu suç bakımından ilgilinin rızası hukuka uygunluk sebebi olarak düşünülebilir ise de kural olarak soruşturulması ve kovuşturulması şikayete tabi suçlar bakımından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu kabul edilebileceğinden ve m.138'de yer alan bu suç şikayete bağlı bulunmadığından bu suç bakımından ilgilinin rızası hukuka uygunluk sebebi uygulanabilir değildir*."

Bkz. **Dülger**, s. 285; "*Bu suç tipinin mağduru kamu düzeni olduğu için, yok edilmeyen verilerin ilgilisi de olsa suçtan zarar gören kişinin rızası eylemi hukuka uygun hale getiremeyecektir. Bunun dışında bu suç tipi açısından yasadan kaynaklanan bir hukuka uygunluk sebebi de bulunmamaktadır*."

[530] **Yaşar-Gökcan-Artuç**, s. 4136.

[531] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 261; "*İhmal halinin cezalandırılabilmesi için bir zarar neticesinin ortaya çıkıp çıkmadığına bakılmaz, salt ihmalin yapılmasıyla suç tamamlanır*."

suçun ihmali bir suç olması sebebiyle[532] ve verilerin süre dolmasına rağmen silinmemeleri halinde suç meydana gelmiş olacağından, suçun teşebbüse elverişli olmadığını kabul etmek yerinde olacaktır[533].

(2) İştirak

Bu suça iştirak açısından her ne kadar bazı yazarlar[534] iştirak açısından her tür iştirakin gerçekleşebileceğini ve iştirak açısından bir özellik bulunmadığını savunmakta iseler de; kanaatimizce bu suç özgü suç olduğundan ve yalnızca kişisel verileri belirli sürelerde yok etmekle görevlendirilmiş kişiler bu suçu işleyebileceklerinden, verileri yok etmeme suçunda özgü suçlara iştirak kuralları uygulanacaktır. Buna göre, kişisel verileri yok etmeme suçu açısından ancak bu verileri yok etmekle kanun tarafından yükümlü kılınmış olan kişi suçun faili olabileceğinden, bu suçu o kişi ile birlikte işleyenler ancak TCK'nın 40 ıncı maddesinin 2. fıkrası uyarınca azmettiren ya da yardım eden olarak sorumlu olabileceklerdir[535].

(3) İçtima

Hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerde silinmemeleri durumunda, bu suç aynı kişiye karşı birden fazla defa değişik zamanlarda işlenirse zincirleme hükümleri uygulanacak, ancak aynı kişinin aynı kişisel verilerinin çok uzun bir süre silinmemesi durumunda bu artık tek suç sayılacak ve zincirleme suç hükümleri uygulanmayacaktır. Benzer şekilde, yapılan kişisel veri kaydındaki kişisel veriler birden fazla kimseye aitse ve bunların kanuni süreler geçmiş olmasına rağmen silinmemesi durumunda birden fazla kimsenin kişisel verisi silinmemiş olacak, suç aynı hareketle birden fazla kişiye karşı işlenmiş

---

[532] **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 261; "*İcrai suçlar teşebbüse elverişliyken, saf (gerçek) ihmali suçlarda teşebbüs hali gerçekleşmez.*", **Dönmezer**, s. 130, **Centel-Zafer-Çakmut**, s. 458, **Zafer**, Ceza Hukuku Genel Hükümler, s. 193, **Koca-Üzülmez**, s. 346 - 347, **Demirbaş**, s. 217.

[533] **Arslan-Azizağaoğlu**, s. 615, **Parlar-Hatipoğlu**, s. 2101, **Yaşar-Gökcan-Artuç**, s. 4136, **Özbek**, TCK İzmir Şerhi, s. 967, **Dülger**, s. 286, **Soyaslan**, s. 351, **Şen**, Yeni Türk Ceza Kanunu Yorumu, s. 611, **Malkoç**, s. 915.

[534] **Dülger**, s. 286, **Özbek**, TCK İzmir Şerhi, s. 967, **Arslan-Azizağaoğlu**, s. 615.

[535] **Parlar-Hatipoğlu**, s. 2101, **Yaşar-Gökcan-Artuç**, s. 4137, **Artuk-Gökcen-Yenidünya**, Ceza Hukuku Genel Hükümler, s. 297.

olacaktır. Bu durumda da aynı neviden fikri içtima hükümleri uygulanacak cezası artırılacaktır[536].

Verileri yok etmeme suçunun oluşabilmesi için, verilerin hukuka uygun olarak kaydedilmiş olmaları gerektiğini yukarıda ifade etmiştik. Kanunun, belirli süreler geçtiği zaman silinmesini öngördüğü kişisel verilerin mevcut olabilmesi için, kanaatimizce o kişisel verilerin zaten kanundan alınmış olan yetkiyle toplanmış ve kaydedilmiş olması gerekmektedir. Bu nedenle, hukuka aykırı olarak kaydedilmiş olan kişisel veriler bakımından kişisel verileri yok etmeme suçu oluşamayacağından, doktrinde aksini savunan bir görüş bulunsa da[537], kanaatimizce TCK'nın 135 inci maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi ile 138. maddede düzenlenen kişisel verileri yok etmeme suçları arasında herhangi bir içtima durumunun oluşması söz konusu olamayacaktır.

Öte yandan, TCK'nın 136 ncı maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun bu madde ile olabilecek içtima ilişkisi üzerinde durmak gerekir. Hukuka uygun olarak kaydedilmiş olan kişisel verileri kanuni süreler dolmuş olmasına rağmen, bunları silmekle yükümlü olan kişinin verileri silmemesi durumunda, fail aynı zamanda bu verileri hukuka aykırı olarak başkalarına verebilir. Kanaatimizce bu durumda, failin, TCK'nın 136 ncı maddesi ile 138 inci maddesi arasında gerçek içtima hükümlerine göre cezalandırılması gerekecektir[538].

e. Yaptırım

Kişisel verileri yok etmeme suçunun yaptırımı olarak kanunda yalnızca hürriyeti bağlayıcı ceza öngörülmüş olup, ceza altı aydan bir yıla kadar hapis cezası olarak belirlenmiştir.

Verileri yok etmeme suçu açısından öngörülen hapis cezası 6 aydan 1 yıla kadar olarak belirlendiği ve 137 nci maddede belirlenen nitelikli haller bu maddede

---

[536] **Yaşar-Gökcan-Artuç**, s. 4137, **Parlar-Hatipoğlu**, s. 2101, **Özbek**, TCK İzmir Şerhi, s. 967, **Dülger**, s. 286.
[537] **Özbek**, TCK İzmir Şerhi, s. 966; "*Kişisel veriler hukuka aykırı olarak kaydedilmiş ve sonra da yok edilmemişse iki ayrı suç bulunur.*"
[538] **Yaşar-Gökcan-Artuç**, s. 4137, **Parlar-Hatipoğlu**, s. 2101.

düzenlenen suça uygulanmadığı için, hakimin takdir edeceği ceza iki yıl veya daha az süreli hapis cezası olacaktır. Bu itibarla CMK'nın 231 inci maddesinde sayılan koşulların gerçekleşmesi halinde hükmün açıklanmasının geri bırakılması uygulanabilecektir.

Tüzel kişilerin bu suçun işlenmesinden kaynaklı olarak hukuka aykırı yarar sağlamaları halinde ise, TCK'nın 140 ıncı maddesinde öngörüldüğü üzere, bunlara TCK'nın 60 ıncı maddesinde öngörülmüş olan güvenlik tedbirleri uygulanacaktır[539].

f. Soruşturma Usulü, **Görevli ve Yetkili Mahkeme**, **Dava Zamanaşımı**

138 inci maddede düzenlenmiş olan suçun soruşturulması ve kovuşturulması şikayete bağlı değildir, zira 139 uncu maddede hangi suçların şikayete bağlı olduğu düzenlenirken, 138 inci maddedeki verileri yok etmeme suçu buraya dahil edilmemiştir ve bu itibarla suçun soruşturulması ve kovuşturulması Cumhuriyet Başsavcılığınca re'sen yapılacaktır.

5235 Sayılı kanunun onuncu maddesi uyarınca, bu suç için öngörülmüş olan hapis cezasının üst sınırı iki yıldan az olduğundan, açılan davaya bakmakla görevli mahkeme sulh ceza mahkemesidir.

Yetkili mahkemenin tespiti için, ceza ve ceza muhakemesi hukukunun temel esasları uygulanacak olup, bu hususta ayrıntılı açıklamalar 135 inci madde incelenirken yapıldığından, bu konu üzerinde tekrar durulmayacaktır.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, TCK'nın 139 uncu maddesi gereği şikayete tabi olmaması ve CMK'nın 253 üncü maddesinde sayılan suçlar arasında yer almaması itibariyle, bu suç uzlaşmaya tabi suçlardan değildir.

Suçun zamanaşımı süresi ise, TCK'nın 66/1-e maddesi gereğince sekiz yıldır.

---

[539] **Dülger**, s. 286.

SONUÇ

Gelişen teknoloji ve hızla artan küreselleşme neticesinde, kişisel verilerin tutulması, paylaşılması, transfer edilmesi ve işlenmesi ivme kazanmış, bunun doğal sonucu olarak bu kişisel verilerin korunması hususunda düzenlemeler yapılmasını gerektiren gelişmeler yaşanmıştır. Kişisel verilerin korunması, bireylerin kendilerini serbestçe geliştirebilmeleri, kendi kişisel verilerinin akıbetini belirleyebilmeleri ve buna bağlı olarak özgürleşebilmeleri için son derece önemli bir yere sahiptir. Nitekim, kişisel verilerin korunması, uluslararası/ulusal kaynaklarda, temel hak ve özgürlükler bağlamında ele alınmış, bireylerin özel hayatının korunmasının bir parçası olarak, insanların bilgi akışı çağı içerisinde kendi şahsi verilerinin kontrolünü ellerinde tutabilmelerinin son derece önem arz ettiği ifade edilmiştir.

Kişisel verilerin korunması, Türkiye'de her ne kadar gerektiği kadar önem atfedilmeyen bir konu olsa da, bu alandaki hukuki düzenlemeler Avrupa ve Amerika'da yaklaşık 40 sene önce başlamıştır. Zamanla bu alanda özellikle Avrupa ülkeleri ve Avrupa Birliği son derece önemli düzenlemeler yapmış, ancak dünyanın diğer ülkelerinde de bu hususa ilişkin çalışmalar yapılmıştır. Avrupa ülkelerinin neredeyse tamamında kişisel verilerin korunmasına ilişkin özel bir kanun bulunmakta, bunun yanı sıra bu koruma anayasalar, ceza kanunları veya başka kanunlarla desteklenmektedir. Kişilerin temel hak ve özgürlüklerinin en önemli garantörlerinden biri olarak kabul edilen Avrupa İnsan Hakları Sözleşmesi'nde, kişisel verilerin korunması hususu açık bir düzenleme olarak yer almamakta ise de, Avrupa İnsan Hakları Mahkemesi, bu hususu Sözleşme'nin 8 inci maddesi ile düzenlenen özel hayatın ve aile hayatının korunması kapsamında kabul ederek yarattığı içtihat hukukuyla koruma altına almıştır. Bunun haricinde OECD Sözleşmesi, AB Temel Haklar Şartı, 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, 95/46 Sayılı Avrupa Topluluğu Kişisel Verilerin Korunması Yönergesi ve 2002/58/AT Sayılı Özel

Yaşamın ve Elektronik İletişimin Korunması Yönerge gibi uluslararası kaynaklar da kişisel verilerin korunmasında büyük rol oynamaktadır.

Türkiye ise, 108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'yi yaklaşık 30 sene evvel imzalamış olmasına rağmen, Sözleşme'nin şart koştuğu ve kişisel verilerin korunması alanını düzenleyen özel bir kanun çıkarmaması sebebiyle, Sözleşme'yi hala onaylamamıştır. Düşüncemize göre, Türkiye'nin dünyadaki diğer ülkelere nazaran bu alanda ne kadar geri kaldığının en önemli göstergelerinden biri budur. Bu Sözleşme'yi 46 ülke imzalamış, bunlardan 43 tanesi de onaylayarak ulusal mevzuatlarında bu alanı özel olarak düzenleyen bir kanun çıkarmışlardır. Türkiye'de ise, yaklaşık olarak 10 senedir kişisel verilerin korunması hakkında bir kanun tasarısı mevcut olmasına rağmen bu alanda hiçbir adım atılmamaktadır. Bunun yanı sıra DNA verilerinin tutulması ile ilgili olarak, günümüzde bu alanın yalnızca Ceza Muhakemesi Kanunu ve bazı yönetmeliklere göre düzenlenmiş olması daha şimdiden uygulamada birtakım sıkıntılar yaratmaktadır. Son yıllarda hızla gelişen DNA verilerinin incelenmesine ilişkin alan, özellikle organize suçla mücadele hususunda dünyadaki ülkeleri ellerindeki kişisel veriler hususunda işbirliği yapmaya yöneltmektedir. Ancak Türkiye'nin, iç hukukunda ne DNA verileri veya olası bir DNA bankası ile ilgili ne de kişisel verilerin korunması ile ilgili özel bir kanuna sahip olmaması, diğer ülkelerde bulunan koruma standartlarının yakalanamamasına sebep olmaktadır. Özellikle Avrupa ülkelerinin 95/46/AT Sayılı Yönerge uyarınca eşdeğer düzeyde koruma bulunmaksızın ellerindeki kişisel verileri AB üyesi olmayan diğer ülkelere aktarmamaları ileride Türkiye için ciddi sıkıntılar doğurmaya açık bir alan oluşturmaktadır.

Türkiye Cumhuriyeti Anayasası'nda, kişisel veriler, yıllardır 20 inci maddede düzenlenen özel hayatın gizliliği hakkı kapsamında değerlendirilmekte ve korunmakta iken, 2010 yılında yapılan referandumla, bu maddeye bir fıkra eklenerek bireylerin kişisel verilerinin korunması açık bir şekilde Anayasal güvence altına alınmıştır. Bunun yanı sıra Borçlar Kanunu ve Medeni Kanun, İş Kanunu, Bankacılık Kanunu ve Adli Sicil Kanunu gibi başka kanunlarda da bu hususla ilgili düzenlemeler bulunmaktadır. Çalışmamızın ikinci bölümünün konusunu, mevcut tasarılar ve bunlarda yer alan cezai hükümler ile Türk Ceza Kanunu'ndaki kişisel

verilerin korunması amacıyla düzenlenen suçlar teşkil etmiştir. Bu kapsamda, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı incelenmiştir. Düşüncemize göre, bu iki tasarıda da, kanunlaşmaları halinde uygulamada ciddi sorunlara yol açabilecek ifadeler yer almaktadır. Çalışmamızda, tasarıların kanunlaşması halinde bizce ortaya çıkabilecek sorunlar ortaya konmuş ve bu ifadeler tartışılmıştır. Her ne kadar mevcut durumda bu tasarılar henüz kanunlaşmamış olsalar da, Türkiye de eninde sonunda diğer tüm ülkelerde olduğu gibi, kişisel verilerin korunması hususunu düzenleyen özel bir kanun çıkarmak durumunda kalacaktır. Bu anlamda bir diğer sorun ise, mevcut tasarıların bu haliyle kanunlaşması durumunda, bize göre uygulamada önemli sorunların baş gösterecek olmasıdır. Tasarıların incelendiği başlık altında ayrıntılı olarak incelenen bazı maddeler, adeta tasarıların veri öznelerini koruma amacıyla değil; bu verileri işleyecek olan kişileri koruma amacıyla hazırlandığı izlenimini doğurmaktadır. Zira özellikle Kişisel Verilerin Korunması Hakkında Kanun Tasarısı kişisel verilerin korunması hveri öznelerini koruyan ve bu kapsamda onlara bazı haklar tanıyan hemen hemen her maddenin ilerleyen fıkralarında, verilen bu hakları neredeyse kullanılamaz ve işlevsiz hale getirecek derecede geniş sınırlamalar bulunmaktadır.

5237 Sayılı Türk Ceza Kanunu'nda ise, kişisel verilerin korunması alanında ortaya çıkan sorunları azaltmak ve engelleyebilmek, bu tür eylemlerde bulunanları cezalandırmak ve yine bu tür eylemlerde bulunacakları caydırabilmek adına, kişisel verilerle ilgili düzenlemelere gidilmiş, bu alanda yeni suçlar ve cezalar ihdas edilmiştir. Kanun'un "Kişilere Karşı Suçlar" başlıklı İkinci Kısmın "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde, 135 inci maddede "Kişisel verilerin kaydedilmesi", 136 ncı maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" ve 138 inci maddede "Verileri yok etmeme" suçları düzenlenmiş, 137 nci maddede ise cezanın artırılmasını gerektiren nitelikli haller sayılmıştır. Bu suçlara göre, kişisel verileri hukuka aykırı olarak kaydeden (m.135), kişisel verileri hukuka aykırı olarak veren, ele geçiren veya yayan (m.136) ve yok etmekle yükümlü olduğu kişisel verileri yok etmeyen (m.138) kişiler ilgili kanun maddelerinde öngörülen cezai yaptırımlar uygulanacaktır. Kanun incelenirken, maddelerin düzenlenişinin genel anlamda Fransız Ceza Kanunu'nda bu alanı düzenleyen maddelerle büyük oranda benzerlik taşıdığı görülmüştür. Hatta, Fransız Ceza Kanunu'nda olduğu gibi, düşüncemize göre isabetsiz bir şekilde, hassas kişisel

verileri işleyen kişiler ile diğer kişisel verileri işleyen kişilere uygulanacak cezai yaptırımda herhangi bir fark öngörülmemiştir. Halbuki hassas nitelikteki kişisel veriler, yapıları ve içerdikleri bilgiler itibariyle hukuka aykırı olarak işlenmeleri halinde ilgili kişiselere çok daha ciddi zararlar verebileceklerdir. Bu anlamda, Türk Ceza Kanunu'nda öngörülmüş olan ve bu alanı düzenleyen suçlar açısından (m.135, m.136,m.138) bu hususun cezanın artırılmasını gerektiren bir nitelikli hal olarak düzenlenmesi gerektiği düşüncesindeyiz.

Netice olarak, Türkiye'de kişisel verilerin doğrudan Anayasal güvenceye kavuşturulması önemli bir adım olsa da, uygulamada bu alanı düzenleyecek ve toplumun ihtiyaç duyduğu kuralları getirecek çerçeve niteliğinde özel bir düzenleme bulunmadığı sürece, kişisel verilerin korunması hususunda gerçekleştirilen ihlallerin önüne etkili bir şekilde geçilmesi mümkün olmayacaktır. Bu itibarla Türkiye'nin bir an önce, diğer ülkelerde olduğu gibi, kişisel verilerin korunmasını özel olarak düzenleyen bir çerçeve kanun çıkarması ve bu kanunun uygulanmasını sağlaması şarttır. Zira mevcut durumda, uygulama ihlalleri önlemeye yönelik olmaktan ziyade, yapılan ihlalleri cezalandırmaya yöneliktir. Halbuki kişisel veriler toplanması, işlenmesi, yayılması ve aktarılması son derece kolay ve bir defa bu işlemler gerçekleştikten sonra geri dönüşü neredeyse imkansız olan sonuçlara yol açan bir konudur. Bu niteliği itibariyle, Türkiye'de yapılan ihlalleri cezalandırmaya ne kadar önem atfedilmişse, yapılabilecek ihlalleri önlemeye çok daha fazla önem verilmesi ve bir an önce Avrupa Birliği ülkelerinin yakalamış oldukları koruma standardının yakalanması gerekmektedir.

KAYNAKÇA

I. KİTAPLAR

Aksoy, **Hüseyin Can**, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Baskı, Ankara, Mart 2010.

Arslan, **Çetin-Azizağaoğlu**, **Bahattin**, Yeni Türk Ceza Kanunu Şerhi, 1. Baskı, Kasım 2004.

Artuk, **Mehmet Emin-Gökcen**, **Ahmet-Yenidünya**, **A. Caner**, Ceza Hukuku Genel Hükümler, 5. Baskı, Ankara 2011.

Artuk, **Mehmet Emin-Gökcen**, **Ahmet-Yenidünya**, **A. Caner**, Ceza Hukuku Özel Hükümler, 11. Baskı, Ankara 2011.

Artuk, **Mehmet Emin-Gökcen**, **Ahmet-Yenidünya**, **A. Caner**, TCK. Şerhi, Özel Hükümler, Cilt 3, Ankara 2009.

Başalp, **Nilgün**, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.

Centel, **Nur-Zafer**, **Hamide**, Ceza Muhakemesi Hukuku, 8. Baskı, İstanbul, Ekim 2011.

Centel, **Nur-Zafer**, **Hamide-Çakmut**, **Özlem**, Türk Ceza Hukukuna Giriş, 7. Baskı, İstanbul, Kasım 2011.

Demirbaş, **Timur**, Ceza Hukuku Genel Hükümler, 7. Baskı, Ankara 2011.

Dönmezer, **Sulhi**, Genel Ceza Hukuku Dersleri, İstanbul 2003.

Dönmezer, **Sulhi-Erman**, **Sahir**, Nazari ve Tatbiki Ceza Hukuku Genel Kısım 2, İstanbul 1994.

Dülger, **Murat Volkan**, Bilişim Suçları, 1. Baskı, Kasım 2004.

Erem, Faruk, Ümanist Doktrin Açısından: Türk Ceza Hukuku Genel Hükümler, Cilt I, 7. Baskı, Ankara 1966.

Erem, **Faruk-Danışman**, **Ahmet-Artuk**, **Mehmet Emin**, Ceza Hukuku Genel Hükümler, Ankara 1997.

Forest, **David**, Droit des Données Personnelles, Paris 2011.

Gözübüyük, Abdullah Pulat, Alman, Fransız, İsviçre ve İtalyan Ceza Kanunlariyle Muhakeyeseli Türk Ceza Kanunu Gözübüyük Şerhi, Cilt I, 5. Baskı, İstanbul 1988.

Hakeri, **Hakan**, Ceza Hukuku Genel Hükümler, 12. Tıpkıbasım, Ankara 2011.

Helvacı, Serap, Gerçek Kişiler, 4. Baskı, İstanbul 2012.

Ketizmen, **Muammer**, Türk Ceza Hukukunda Bilişim Suçları, 1. Baskı, Ankara 2008.

Koca, **Mahmut-Üzülmez**, **İlhan**, Türk Ceza Hukuku Genel Hükümler, 4. Baskı, Eylül 2011.

Kunter, Nurullah-Yenisey, Feridun-Nuhoğlu, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Baskı, İstanbul 2010.

Küzeci, **Elif**, Kişisel Verilerin Korunması, Ankara 2010.

Malkoç, **İsmail**, Açıklamalı – İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu, 1. Cilt, Ankara 2007.

Meran, **Necati**, Gerekçeli-Karşılaştırmalı 5237 Sayılı Türk Ceza Kanunu, Seçkin Yayınevi, Ankara 2004.

Oğuzman, Kemal-Seliçi, Özer-Oktay Özdemir, Saibe, Kişiler Hukuku, 10. Baskı, İstanbul 2010.

Önder, Ayhan, Ceza Hukuku Genel Hükümler, Cilt II-III, 2. Baskı, İstanbul 1992.

Özbek, **Veli Özer**, TCK İzmir Şerhi – Yeni Türk Ceza Kanununun Anlamı, Cilt 2 Özel Hükümler, Ankara, Şubat 2008.

Özgenç, **İzzet**, Türk Ceza Hukuku Genel Hükümler, 6. Baskı, Ankara 2011.

Öztürk, **Bahri-Erdem**, **Mustafa Ruhan**, Uygulamalı Ceza Muhakemesi Hukuku, 12. Baskı, Ankara, Kasım 2008.

Öztürk, **Bahri-Erdem**, **Mustafa Ruhan-Sırma**, **Özge-Saygılar**, **Yasemin F.-Alan**, **Esra**, Ana Hatlarıyla Ceza Muhakemesi Hukuku, 1. Baskı, Ankara 2010.

Parlar, **Ali-Hatipoğlu**, **Muzaffer**, Açıklamalı – Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, 2. Cilt, 3. Baskı, Ankara 2010.

Polater, **Yusuf Ziya**, Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması, 1. Baskı, Ankara 2010.

Soyaslan, **Doğan**, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010.

Şen, **Ersan**, Yeni Türk Ceza Kanunu Yorumu, Cilt 1, İstanbul, Nisan 2006.

Şimşek, **Oğuz**, Anayasa Hukukunda Kişisel Verilerin Korunması, 1. Baskı, Şubat 2008.

Tezcan, **Durmuş-Erdem**, **Mustafa Ruhan-Sancakdar**, **Oğuz-Önok**, **Rıfat Murat**, İnsan Hakları El Kitabı, 4. Baskı, Ankara 2011.

Toroslu, **Nevzat**, Ceza Hukuku Genel Kısım, 16. Baskı, Ankara, Eylül 2011.

Yaşar, **Osman-Gökcan**, **Hasan Tahsin-Artuç**, **Mustafa**, Türk Ceza Kanunu, Cilt 3, 1. Baskı, Ankara, Şubat 2010.

Yurtcan, **Erdener**, Ceza Yargılanası Hukuku, 12. Baskı, İstanbul 2007.

Zafer, **Hamide**, Ceza Hukuku Genel Hükümler, 2. Baskı, İstanbul, Ekim 2011.

Zafer, **Hamide**, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m. 132-134), 1. Baskı, Haziran 2010.

II. DERGİ VE MAKALELER

- **Yerli Kaynaklar**

Akıllıoğlu, **Tekin**, "Kişisel Verilerin Korunması ve İdare", Maltepe Üniversitesi Hukuk Fakültesi Dergisi (1997/1998 – 2007-2008 Üniversitemizin ve Fakültemizin 10. Yıl Kuruluş Armağanı), 2008/Özel Sayı, s. 13 – 29.

Akyürek, **Güçlü**, **"**Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı", Suç ve Ceza Dergisi, Sayı 3, Temmuz-Ağustos-Eylül 2001, s. 43 – 60.

Altaş, **Ebru**, "Bir Koruma Tedbiri Olarak Moleküler Genetik İncelemeler ve DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı", Ceza Hukuku Dergisi, Sayı:1 Nisan 2007, s. 77 – 110.

Arsava, **Füsun A.**, "AB'nin Anayasallaşma Sürecinde Temel Haklar Şartı", Ankara Avrupa Çalışmaları Dergisi, Cilt 3, Sayı 2, Bahar 2004, s.1-9, http://dergiler.ankara.edu.tr/dergiler/16/3/413.pdf, 21.03.2012.

Atak, **Songül**, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", Türkiye Barolar Birliği Dergisi, Sayı 87, 2010, s. 90 – 120.

Atak, **Songül**, "Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri", Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Dergisi, Sayı 59-60, Temmuz Ağustos 2009, s. 200 – 222.

Başalp, **Nilgün**, "Bağımsız Veri Koruması Kurumlarının Yapısı" Bilişim Hukukunun Son 10 Yılı Sempozyumu, www.erzincan.edu.tr/gundem.php?al=86, 14.03.2011.

Beyli, **Ceylin**, "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler", Bilişim Hukuku, Mete Tevetoğlu (der.), İstanbul, Aralık 2006, s. 70 – 79.

Değirmenci, **Olgun**, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", TBB Dergisi, Sayı 58, 2005, s. 195 – 208.

Doğan, **Yusuf Hakkı**, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", www.ceza-bb.adalet.gov.tr/makale/146.doc, 14.03.2012.

Ekici, **Akın**, "Bankacılık Mevzuatı Kapsamında Banka ve Müşteri Sırrı, Bankacılar Dergisi", Sayı 63, 2007, s. 51 – 70.

İlkiz, **Fikret**, "Kişisel Verilerin Korunması ve Kanun Tasarısı", Güncel Hukuk Dergisi, Sayı 67, Temmuz 2009, s. 12 – 23.

Kalaycı, **Emre**, "Haberleşme Özgürlüğü ve Kişisel Bilgilerin Korunması", Elektrik Mühendisleri Odası İzmir Şubesi Aylık Bülteni, Temmuz 2008, s. 33-36, http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/200807_Emre.pdf, 02.01.2012.

Keser Berber, **Leyla**, "Uluslararası Standartlar ve İyi Uygulama Kodları Işığında Kişisel Verilerin Korunması ve Kişisel Bilgi Yönetimi Sistemleri Oluşturulması", http://www.docstoc.com/docs/91480740/ULUSLARARASI-STANDARTLAR-ISIGINDA-KISISEL-VERILERIN-KORUNMASI, 13.05.2012.

Mahmutoğlu, **Fatih Selami**, "Beden Muayenesi Ve Vücuttan Örnek Alınması", https://docs.google.com/viewer?a=v&q=cache:n3ORpGq-MuMJ:cezahukuku.istanbul.edu.tr/ders-gerecleri/cmh/makale/bedenmuayenesi.doc+t%C4%B1bbi+muayene+fatih+selami+mahmuto%C4%9Flu&hl=tr&gl=tr&pid=bl&srcid=ADGEESjMfeKA8ljstyikRAlkKq1sUpT_pkNMKnJo_mOHiAqUYFXF-rAYlSPqTB_3K8Uyrxx55CgTVLYT7AaXkMSFbC6dELe_zgdHl3oSmDYszwqQZHQEr5f-iaNEVAEKLqD3qgJL2kOz&sig=AHIEtbRR10D8T20MWiH3Y4CyWbq2Ic3K3A, 06.05.2012.

Özbek, **Veli Özer**, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Hakkında Görüşlerimiz", Ceza Hukuku Dergisi, Sayı:1 Nisan 2007, s. 47 – 76.

Özdemir, **Hayrunisa**, "İletişim Alanında Kişisel Verilerin Korunması", Bilişim Hukukunun Son 10 Yılı Sempozyumu, www.erzincan.edu.tr/gundem.php?al=86, 09.10.2011.

Özdilek, **Ali Osman**, "DNA'nın Kanıt Olarak Kullanılması", Montreal, Kasım 2002, http://www.hukukcu.com/bilimsel/kitaplar/dna_kanit.htm, 15.12.2011.

Şen, **Ersan**, "5237 Sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar", İstanbul Barosu Dergisi, Cilt:79, Sayı:3, 2005, s. 707 – 720.

Şen, **Ersan**, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, Cilt:83, Sayı:3, 2009, s. 1197 – 1214.

Şener, **Gülnihal Emine**, **"**Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu", Adalet Dergisi (T.C. Adalet Bakanlığı Yayın İşleri Daire Başkanlığı), 39. Sayı, Ocak 2011, s. 72 – 86, http://www.yayin.adalet.gov.tr/dergi/39.say%C4%B1/05%20-%20EM%C4%B0NE%20G%C3%9CLN%C4%B0HAL%20%C5%9EENER.pdf 21.09.2012.

Tahmazoğlu Uzeltürk, Sultan, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, Sayı 93, Eylül 2010, s. 3151 – 3156.

Ünver, **Yener**, "Kişisel Verilerin Korunması", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2008/1, s. 163 – 199.

Wolters, **Gereon**, "Alman Ceza Usul Hukuku'nda Bedensel Muayene ve DNA Analizi", Ar.Gör. Fatih Gündoğdu (çev.), Fasikül Dergisi, Sayı 7, Haziran 2010, s. 37 - 41.

- **Yabancı Kaynaklar**

Bygrave, **Lee A.**, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, Vol. 6, 1998, s. 247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf, 12.03.2012.

Grant, **Hazel**, "Data Protection 1998 - 2008", Computer Law & Security Review, Vol. 25, Issue 1, 2009, s. 44 – 50, http://www.sciencedirect.com/science/article/pii/S0267364908001696, 05.05.2012.

Hook, **Elizabeth I.-Martin**, **Cécile-Ivanova**, **Suzette**, "Transborder Law: Application of the European Union Data Privacy Law to Multinational Corporations", International Law Practicum, Vol. 21, No. 2, Autumn 2008, s. 124 – 131, http://international.westlaw.com/result/default.wl?rp=%2fsearch%2fdefault.wl&rltdb=CLID_DB370529135145&sp=intmar-

000&fn=_top&service=Search&action=Search&query=%22TRANSBORDER+LAW%3a+APPLICATION+OF+THE+EUROPEAN+UNION+DATA+PRIVACY+LAW%22&rs=WLIN12.04&db=INLPRAC&eq=search&srch=TRUE&rlt=CLID_QRYRLT9421036135145&fmqv=s&origin=Search&vr=2.0&method=TNC&cfid=1&mt=314&sv=Split&pbc=BC6E23F9, 04.03.2012.

Keele, **Benjamin J.**, "Privacy By Deletion: The Need For A Global Data Deletion Principle", Indiana Journal of Global Legal Studies, Vol. 16, Issue 1, Winter, 2009, s.363–384, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1508025, 10.03.2012.

Loring, **Tracie B.**, "An Analysis Of The Informational Privacy Protection Afforded By The European Union And The United States", Texas International Law Journal, Vol. 37, Spring 2002, s. 421 – 459, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(LORING)+%26+da(2002)&db=TXILJ&rlt=CLID_QRYRLT2779154574145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB1771456554145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012.

Moshell, **Ryan**, "…And Then There Was One: The Outlook For A Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection", Texas Tech Law Review, Vol. 37, Winter 2005, s. 357-432, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(MOSHELL)&db=TXTLR&rlt=CLID_QRYRLT18876875145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB496725055145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012.

Murray, **Patrick J.**, "The Adequacy Standart Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standart?", Fordham İnternational Law Journal, Vol. 21, Issue 3, 1997, s. 932–1018,

http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1563&context=ilj, 10.03.2012.

Rihm, **Thomas**, "New International Data Transfer Rules for Switzerland: Business Friendly by Respecting Employees' Privacy Rights", Employment & Industrial Relations Law, Vol. 18, No. 2, s. 16–18, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(THOMAS+RIHM)&db=EMPIRL&rlt=CLID_QRYRLT2593415432155&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB2779545422155&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 06.03.2012.

Schwartz, Paul M., "European Data Protection Law and Restrictions on International Data Flows", Iowa Law Review, Vol. 80, Issue 3, May 1995, s. 471 – 496, http://0-heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/ilr80&div=27&collection=journals&set_as_cursor=15&men_tab=srchresults, 07.03.2012.

Sepúlverda, **Magdalena-Banning**, **Theo van-Gudmundsdóttir-Chamon**, **Christine**, **"**Human Rights Protection,Cases and Commentaries", Council of Europe, 2004, s. 130–144, http://www.wcl.american.edu/humright/hracademy/documents/Class2Reading3HRProtectionCasesandCommentaries.pdf?rd=1, 09.03.2012.

Simitis, **Spiros**, "From the Market to the Polis: The EU Directive on the Protection of Personal Data, Iowa Law Review, Vol. 80, Issue 3, May 1995, s. 445–471, http://0-heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/ilr80&div=26&collection=journals&set_as_cursor=6&men_tab=srchresults, 05.03.2012.

Suda, **Yohei**, "Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States", Washington University Global Studies Law Review, Vol. 4, Issue 2, 2005, s. 209 – 262, http://0-

heinonline.org.libunix.ku.edu.tr/HOL/Page?handle=hein.journals/wasglo4&div=16&collection=journals&set_as_cursor=1&men_tab=srchresults&terms=yohei|suda&type=matchall, 10.03.2012.

Sullivan, **James M.**, "IADC International Law Committee Survey of Electronic Discovery and Data Privacy Law, Defense Counsel Journal, Vol. 77, No. 3, July 2010, s. 396-421, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=AU(SULLIVAN)&db=DEFCJ&rlt=CLID_QRYRLT9391719534145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB4617418514145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 12.04.2012.

Vicien-Milburn, **Maria**, "The United Nations And Personal Data Protection", Oktober 2005, http://www.a-datum.ru/downloads/conferences/27th/The%20united%20nations%20and%20personal%20data%20protection.pdf, 28.02.2012.

Walden, **Ian**, "Anonymising Personal Data", International Journal of Law and Information Technology, Summer 2002, s. 224 – 237, Westlaw International Database, http://international.westlaw.com/result/default.wl?cfid=1&mt=314&origin=Search&query=%22ANONYMISING+PERSONAL+DATA%22&db=INTJLIT&rlt=CLID_QRYRLT865515374145&method=TNC&service=Search&eq=search&rp=%2fsearch%2fdefault.wl&sp=intmar-000&srch=TRUE&vr=2.0&action=Search&rltdb=CLID_DB7284547364145&sv=Split&fmqv=s&fn=_top&rs=WLIN12.04, 28.02.2012.

III. BELGE, GÖRÜŞ, ARAŞTIRMA VE RAPORLAR

108 Sayılı Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, http://conventions.coe.int/treaty/en/treaties/html/108.htm, 26.02.2012.

4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTurkey 2010) Sonuç Bildirgesi, http://www.biltekhaber.com/Web/Haber/HaberOku.aspx?haberID=2651, 08.01.2012.

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows CETS No.: 181, (181 Sayılı Ek Protokol), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=ENG, 27.02.2012.

Avrupa Birliği Temel Haklar Bildirgesi, İnsan Hakları Derneği, http://www.ihd.org.tr/index.php?option=com_content&view=article&id=900:avrupa-birligi-temel-haklar-bildirgesi&catid=37:san-haklarylgeleri&Itemid=96, 21.03.2012.

Avrupa Birliği Temel Haklar Şartı (İngilizce metin), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF, 21.03.2102.

Avrupa Birliği Temel Haklar Şartı (Türkçe metin), http://www.ihd.org.tr/index.php?option=com_content&view=article&id=900:avrupa-birligi-temel-haklar-bildirgesi&catid=37:san-haklarylgeleri&Itemid=96, 21.03.2012.

Avrupa İnsan Hakları Sözleşmesi, http://www.echr.coe.int/NR/rdonlyres/3BAA147F-29C9-48CE-AF64-FB85A86B2433/0/CONVENTION_TUR_WEB.pdf, 07.05.2012.

Birleşmiş Milletler Şartı Fransızca Metni, http://www.un.org/fr/documents/charter/pdf/charter.pdf, 07.05.2012.

Birleşmiş Milletler Şartı, http://www.un.org/fr/documents/charter/index.shtml, 27.02.2012

Directive On Privacy And Electronic Communications, (2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişim Korunması Yönergesi), http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, 10.05.2012.

Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 95/46/AT Sayılı Yönerge http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF, 15.05.2012.

Guidelines for the Regulation of Computerized Personal Data Files, http://www.unhcr.org/refworld/pdfid/3ddcafaac.pdf, 28.02.2012.

Kanun Tasarısı Hakkında Türkiye Bilişim Vakfı Görüşü, 2003, http://www.tbv.org.tr/TBV/Documents/BTHukuku/KisiselVerilerinKorunmasiKanunTasarisi-TBVGorus.pdf, 28.12.2011.

OECD Guidelines for the Security of Information Systems and Networks, http://www.oecd.org/dataoecd/16/22/15582260.pdf, 23.02.2012.

OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, http://www.oecd.org/dataoecd/32/45/38921342.pdf, 23.02.2012.

Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data 2005 (108 Sayılı Sözleşme'de düzenlenen ilkelerin biyometrik verilerin toplanmasında ve işlenmesinde uygulanmasına ilişkin gelişme raporu) http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf, 27.02.2012.

Report Of The Oecd Task Force On Spam: Anti-Spam Toolkit Of Recommended Policies And Measures, http://www.oecd.org/dataoecd/63/28/36494147.pdf, 23.02.2012.

The European Union Constitution (Avrupa Birliği Anayasası), http://www.proyectos.cchs.csic.es/euroconstitution/Treaties/Treaty_Const.htm, 15.03.2012.

The Organisation for Economic Co-operation and Development Convention, http://www.oecd.org/pages/0,3417,en_36734052_36761863_1_1_1_1_1,00.html, 20.02.2012.

United Nations Secretariat, Administrative instruction Medical standards and clearances, http://www.fsu.unlb.org/docs/related_documents/AI-2000-7.pdf, 28.02.2012.

- **Yabancı Kanun Metinleri**

Alman Ceza Kanunu, (Strafgesetzbuch, StGB), Federal Law Gazette [Bundesgesetzblatt] Part I p. 945, p. 3322, http://www.iuscomp.org/gla/statutes/StGB.htm, 11.05.2012.

Alman Ceza Muhakemesi Kanunu, (Strafprozeßordnung, StPO), Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, p. 1319), http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, (Almanca Metin) http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html, (İngilizce Metin), 11.05.2012.

Alman Telemedia Kanunu (İngilizce Metin) http://www.cgerli.org/fileadmin/user_upload/interne_Dokumente/Legislation/Telemedia_Act__TMA_.pdf, 11.05.2012.

Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/data.pdf, 13.05.2012.

Federal Act concerning the Protection of Personal Data http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf, 08.01.2012.

Federal Almanya Cumhuriyeti Anayasası (Türkçe Metin) http://www.scribd.com/hsencan/d/51218711-Alman-Anayasas%C4%B1, 12.05.2012.

Federal Data Protection Act (BDSG) http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile, 08.01.2012.

Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz, BDSG), http://www.iuscomp.org/gla/statutes/BDSG.htm, (İngilizce Metin) http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf (Almanca Metin), 12.05.2012.

Fransız Ceza Kanunu, http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006417929&idSectionTA=LEGISCTA000006165309&cidTexte=LEGITEXT000006070719&dateTexte=20120304, 04.03.2012.

İsviçre Ceza Kanunu, http://www.admin.ch/ch/f/rs/311_0/index.html, (İngilizce Metin), 07.07.2012.

İsviçre Federal Anayasası (Constitution fédérale de la Confédération suisse), http://www.admin.ch/ch/f/rs/1/101.fr.pdf (Fransızca Metin), http://www.admin.ch/ch/e/rs/1/101.en.pdf (İngilizce Metin), 06.03.2012.

İsviçre Medeni Kanunu, http://www.admin.ch/ch/e/rs/2/210.en.pdf (İngilizce Metin), http://www.admin.ch/ch/f/rs/2/210.fr.pdf (Fransızca Metin), 07.03.2012.

Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (6 Ocak 1978 tarihli, bilişime, (bilişim) dosyalara ve özgürlüklere ilişkin kanun), http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf, 04.03.2012.

Loi Fédérale sur la Protection des Données - LPD (19 Haziran 1992 tarihli Verilerin Korunmasına İlişkin Federal Kanun),

http://www.admin.ch/ch/e/rs/2/235.1.en.pdf (İngilizce Metin), http://www.admin.ch/ch/f/rs/2/235.1.fr.pdf (Fransızca Metin), 06.03.2012.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Kişisel verilerin işlenmesi hususunda bireylerin korunmasına ilişkin ve 6 Ocak 1978 kanunda değişiklik yapan kanun), http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=, 04.03.2012.

Personal Data Protection Code, http://www.garanteprivacy.it/garante/document?ID=1219452, 08.01.2012.

The Privacy Act of 1974, http://www.justice.gov/opcl/privstat.htm, 03.03.2012.

US Freedom of Information Act (FOIA), http://uspolitics.about.com/library/bl_foia.htm, 03.03.2012.

IV. YARARLANILAN İNTERNET SİTELERİ

Adalet Bakanlığı Mevzuat Bilgi Sistemi, http://mevzuat.basbakanlik.gov.tr/, 14.05.2012.

Adalet Bakanlığı, İnsan Hakları Bilgi Bankası, http://www.inhak-bb.adalet.gov.tr/aihs/aihs.htm, 26.02.2012.

Atasoy, **Sevil**, "DNA Bankasında Karar Zamanı", 19.11.2006, Hürriyet Gazetesi, http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=5464077&yazarid=145, 27.12.2011.

Avrupa Birliği Resmi Web Sitesi, Avrupa Birliği Tarihi, http://europa.eu/about-eu/eu-history/index_en.htm, 15.03.2012.

Avrupa İnsan Hakları Mahkemesi Karar Arama Motoru, http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en, 07.05.2012.

Avrupa Konseyi Türkiye, http://www.avrupakonseyi.org.tr/akih.htm, 06.05.2012.

Birleşmiş Milletler Örgütü Resmi Web Sitesi, http://www.un.org/fr/aboutun/, 27.02.2012.

Cihan Haber Ajansı, "Başbakanlık Milli Dna Veri Bankası Kanunu Tasarısını İade Etti", 04.12.2011, http://www.sondakika.com/haber-basbakanlik-milli-dna-veri-bankasi-kanunu-tasarisi-3167637/, 26.12.2011.

Council of Europe Treaty Office, http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=09/01/2012&CL=ENG, 09.01.2012.

Court de Cassation (Fransız Yargıtayı resmi web sitesi), http://www.courdecassation.fr/, 04.03.2012.

Federal Data Protection and Information Commissioner – FDPIC, (İsviçre Federal Veri Koruma ve Danışma Komiseri) Resmi web sitesi, http://www.edoeb.admin.ch/org/00828/01335/index.html?lang=en, 06.03.2012.

Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&view=gts, 12.05.2012.

http://www.dataprotection.ch/en/news.asp?action=select&newsNO=57298&id=6213, 08.03.2012.

http://www.globallawwatch.com/2011/06/analysis-swiss-federal-court-decisions-raise-threshold-for-justification-of-data-processing/, 08.03.2012.

http://www.truste.com/pdf/EU_Data_Sheet.pdf, 03.03.2012.

La Commission Nationale de l'Informatique et des Libertés - CNIL (Enformatik ve Özgürlükler Milli Komisyonu) Resmi Web Sitesi, http://www.cnil.fr/la-cnil/ 04.03.2012.

Privacy International, Switzerland - Privacy Profile, https://www.privacyinternational.org/article/switzerland-privacy-profile#_ftn1, 09.03.2012.

Türk Dil Kurumu, Büyük Türkçe Sözlük, http://tdkterim.gov.tr/bts/, 09.02.2012.

http://www.anayasa.gen.tr/cumhurbaskani.htm 27.12.2011

- **Mahkeme Kararları**

06.01.1999 T, 1996/68 E., 1991/1 K. Sayılı Anayasa Mahkemesi kararı, http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=1458&content=, 13.05.2012.

06.07.2010 T., 2009/915 E., 2010/803 K. Sayılı Hatay İdare Mahkemesi kararı, http://www.isciler.org/yazi/parmak-iziyle-mesai-takibi-yapilamaz.-mahkeme-karari, 12.05.2012.

15.05.2006 T., 2005/6811 E., 2006/1959 K. Sayılı Danıştay 12. Daire Kararı, kararın tam metni için bkz. http://www.kararevi.com/karars/805368_danistay-e-2005-6811-k-2006-1959, 13.05.2012.

21.06.1995 T., 1995/17 E., 1995/16 K. Sayılı Anayasa Mahkemesi Kararı, http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=1199&content=, 10.05.2012.

31.03.1987 T, 1986/24 E., 1987/8 K. Sayılı Anayasa Mahkemesi Kararı, http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=762&content=, 08.05.2012

A.B.D. Temyiz Mahkemesi'nin 1976 Tarihli "United States v. Miller" kararı, 425 U.S. 435, http://supreme.justia.com/cases/federal/us/425/435/case.html, 03.03.2012.

Fransız Yargıtay'ının 02.10.2001 tarihli kararı, http://www.privacynetwork.info/arresten/27.pdf, 04.03.2012

ÖZGEÇMİŞ

Nil Melek Gültekin 1987 yılında Fransa'da doğdu. Ortaokul öğrenimini Emine Örnek Koleji'nde 2001 yılında tamamlayarak aynı sene Bursa Anadolu Lisesi'ne başladı. 2005 yılında Bursa Anadolu Lisesi'nden mezun oldu. Lisans öğrenimini yarı burslu olarak gördüğü Koç Üniversitesi Hukuk Fakültesi'nden 2009 yılında mezun oldu. Yüksek Lisans eğitimini ise 2009 yılında kabul edildiği Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı'nda tamamlamış, İstanbul Barosu avukatlık stajını bitirerek avukatlık ruhsatını almıştır. Suç ve Ceza Dergisi'nin Nisan Mayıs Haziran 2010 tarihli 2. Sayısında "*AİHS m.5 Kapsamında İngiltere ve Türkiye'de Terör ile İlgili Mevuzatlar ve Bunlara İlişkin AİHM Kararları*" ve Suç ve Ceza Dergisi'nin Temmuz Ağustos Eylül 2010 tarihli 3. Sayısında "*Fransa, İtalya ve Türkiye' de Düşünce, Vicdan ve Din Özgürlüğü Kapsamında Dini Sembollerin Kullanımı*" isimli iki makalesi yayımlanan Nil Melek Gültekin, halen 2011 yılında atandığı Marmara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Anabilim Dalı'nda araştırma görevlisi olarak çalışmaktadır.