

Avropada fərdi məlumatların mühafizəsi

Gregory THUAN Dit DIEUDONNE

Təqdimat

Bu mövzu rəqəmsal inqilab baş verdikdən və rəqəmsal məlumat yayımı həyata keçirilməyə başladıqdan sonra əhəmiyyət kəsb etməyə başlamış, hal-hazırda isə Milli Təhlükəsizlik Agentliyinin (NSA) keçmiş məsləhətçisi Edvard Snouden (Edward Snowden) bir müddət əvvəl açıqlamalar etdiyindən sonra bir çox debatların ana xəttini təşkil etməyə başlamışdır. Qeyd etdiyimiz bu açıqlamalar kəşfiyyat qurumları tərəfindən aparılan kütləvi nəzarət (izləmə) fəaliyyəti və qərbi ölkələrində müntəzəm şəkildə baş verən terrorist hücumları ilə bağlı idi ki, sonuncu da hal-hazırda ictimaiyyətin həm şübhəli olmasına, həm də kütləvi nəzarət prinsiplərini qəbul etməsinə gətirib çıxarmışdır.

O baxımdan bu mövzu sadəcə fərdi məlumatlarla bağlı olan məsələlər dairəsində qalmaqdan çıxır və daha geniş məcrada bu anlama gəlir ki, Birləşmiş Ştatlar və Avropa İstitutları özlərinin oturmuş qanunvericilikləri və digər dövlətlərdə qəbul edilmiş qanunvericilik aktlarına baxışlarından asılı olaraq beynəlxalq aləmdə, yəni beynəlxalq ictimaiyyət qarşısında öz mövqelərini müdafiə etməlidirlər.

Fərdi məlumatların mühafizəsi sahəsində Avropa Şurası və Avropa İttifaqında mövcud olan qanunvericilik bazasının təsvirinə keçməzdən əvvəl fərdi məlumatlar terminini müəyyən etmək vacibdir.

A/ Fərdi məlumatların mühafizəsi ilə bağlı terminologiya

Fərdi məlumatlar termininin başa düşülməsi üçün bir sıra izahatların verilməsi tələb olunur.

Avropa İttifaqı qanunvericiliyində, eləcə də **Avropa Şurasının hüquqi sənədlərində** « fərdi məlumatlar » termininin tərfi aşağıdakı şəkildə müəyyən edilmişdir: “kimliyi müəyyən edilən və ya müəyyən edilə bilən fiziki şəxs barəsində məlumat, yəni, kimliyi bariz şəkildə aşkar olan və ya əlavə məlumatların əldə edilməsi vasitəsilə müəyyən edilə bilən şəxsə dair məlumatlar” (Məlumatların Mühafizəsinə dair Direktiv, Mad. 2(a)).

Ümumilikdə, məlumatların mühafizəsinə dair Avropa qanunvericiliyi hüquqi şəxslərin məlumatlarının işlənməsinin mühafizəsini əhatə etmir (Avropa İttifaqı Ədalət Məhkəməsi (CJEU), birləşdirilmiş işlər C-92/09 və C-93/09, (Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen), 9 Noyabr, 2010, para. 52 və 53). Lakin, milli qanunvericilik orqanları bu məsələni tənzimləməkdə sərbəstdirlər və milli qanunvericilikdə məlumatların mühafizəsi ilə bağlı nəzərdə tutulmuş aktları biznes şirkətləri və assosiasiyalar kimi hüquqi şəxslərə də şamil edə bilirlər (Məlumatların Mühafizəsinə dair Direktiv, 108 sayılı Konvensiyanın 24-cü deklarativ hissələri və 3-cü Maddəsi).

Başqa sözlə, şəxsə aid olan istənilən məlumat fərdi məlumat kimi təfsir edilə bilər. Yəni, fərdi məlumatlar şəxsin şəxsi həyatına və ya peşə və ictimai həyatına aid olan məlumatları əhatə edir (AİHM, Amann İsveçrəyə qarşı (Amann v. Switzerland, n° 27798/95), 16 fevral 2000-ci il; Avropa İttifaqı Ədalət Məhkəməsi (CJEU), Volker və Markus Şeke Hamburq və Hartmunt Eyfer (Volker und Markus Schecke GbR and Hartmut Eifer), yuxarıda qeyd olunub).

Fərdi məlumatların hansı şəkildə saxlanması və ya istifadə edilməsinin məlumatların mühafizəsinə dair qanunvericiliyin tətbiq edilməsi ilə heç bir əlaqəsi yoxdur. Yazılı və ya şifahi ifadələr, eləcə də şəkillər (AİHM, Fon Hannover Almaniya qarşı, 24 iyun 2004-cü il (Von Hannover v. Germany, n° 59320/00, June 24th, 2004); AİHM Skiakka İtaliya qarşı, 11 yanvar 2005-ci il (Sciacca v. Italy, n° 50774/99, January 11th, 2005), eləcə də video görüntüləri (AİHM, Pek Birləşmiş Krallığa qarşı, 28 yanvar 2003-cü il (Peck v. United Kingdom n° 44647/98, January 28th, 2003) ; AİHM, Köpke Almaniya qarşı, 5 oktyabr 2010-cu il (Köpke v. Germany, n° 420/07), 5 oktyabr 2010-cu il) və ya Qapalı Halqa Televiziya (CCTV) tərəfindən yazılmış səs (Fərdi Məlumatlara dair Direktiv, 16 və 17-ci təsviri hissə ; AİHM, P.Q. Birləşmiş Krallığa qarşı, 25 dekabr 2005-ci il (P.G. et J.H. v. United Kingdom, n° 44787/98), 25 dekabr 2001-ci il, 59 və 60-cı maddələr) ; AİHM, Uisse Fransaya qarşı, 20 dekabr 2005-ci il (Wisse v. France, n° 71611/01, 20 dekabr 2005-ci il) fərdi məlumatlar daşıya bilər. Şəxsin DNT məlumatlarını daşdığına görə insan toxumalarının hüceyrə nümunələri də fərdi məlumat hesab edilə bilər.

Nəhayət, həm Avropa İttifaqı qanunvericiliyində, həm də Avropa Şurasının qanunvericiliyində xüsusi kateqoriyaya daxil olan spesifik məlumatlar nəzərdə tutulmuşdur ki, həmin məlumatlar işləndikləri zaman öz təbiətlərinə görə aidiyyəti olan şəxslər üçün risk törədə bilərlər, buna görə də, onların geniş şəkildə mühafizə olunmasına ehtiyac vardır. Xüsusi kateqoriyaya daxil edilən bu spesifik məlumatların (həssas məlumatlar adlandırılır) işlənməsi yalnız səlahiyyətli qurumlar tərəfindən xüsusi təminatlarla əməl edilməklə yerinə yetirilməlidir.

Həssas məlumatların tərifinə gəldikdə, 108 sayılı Konvensiya (6-cı maddə) və Məlumatların Mühafizəsinə dair Direktiv (8-ci Maddə) aşağıdakı kateqoriyalara nəzərdə tutur:

- . İrqi və ya etnik mənşəyi aşkarlayan fərdi məlumatlar;
- . Siyasi, dini və ya digər əqidəni aşkar edən fərdi məlumatlar; və
- . Sağlamlıq və ya cinsi həyata dair fərdi məlumatlar.

Məlumatların Mühafizəsinə dair Direktiv həmkarlar ittifaqına üzvlüyü də həssas məlumatlar siyahısına daxil edir, çünki, bu məlumat şəxsin siyasi dünyagörüşü və mənsubiyyətini aşkar şəkildə bəyan edir. Bundan əlavə, 108 sayılı Konvensiya cinayət işi ilə bağlı məhkumluğa dair fərdi məlumatları da həssas məlumat kimi qiymətləndirir.

Həm Aİ, həm də AŞ məsələ ilə bağlı ümumi sənədlər, eləcə də fərdi məlumatların mühafizəsi ilə bağlı spesifik sənədlər qəbul ediblər.

[B/ Avropada fərdi məlumatların mühafizəsinə dair sənədlər](#)

İlk olaraq Avropa Şurası qanunvericiliyində mövcud olan sənədlərə nəzər salaq.

[1° Avropa İnsan Hüquqları Konvensiyası](#)

Fərdi məlumatların toplanması və istifadəsinə qarşı müdafiə hüququ AİHK-nın 8-ci Maddəsində nəzərdə tutulmuş hüquqların ayrılmaz hissəsini təşkil edir. Həmin Maddə şəxsin şəxsi və ailə həyatına, mənzil və yazışma sirlirinə hörmət bəslənməsini təmin edir və bu hallara məhdudiyət tətbiq edilməsinə icazə verilən halların siyahısını verir.

Avropa İnsan hüquqları Məhkəməsi öz presedent hüququnda dəfələrlə məlumatların mühafizəsi, xüsusilə aşağıdakı məsələlərlə bağlı olan işlərə baxmışdır:

- danışıqların dinlənməsi (bax, misal olaraq, AİHM, Malon Birləşmiş Krallığa qarşı (Malone v. United Kingdom, n° 8691/79, 2 avqust 1984-cü il); AİHM, Kopland Birləşmiş Krallığa qarşı, (Copland v. United Kingdom, n° 62617/00), 3 aprel 20017-ci il),

- müxtəlif izləmə formaları (Bax, misal olaraq, AİHM, Klass və başqaları Almaniyaya qarşı, (Klass and others v. Germany, n° 5029/71, 3 sentyabr 1078-ci il); AİHM, Uzun Almaniyaya qarşı (Uzun v. Germany, n° 35623/05, 2 sentyabr 2010-cu il),

- fərdi məlumatların dövlət qurumları tərəfindən mühafizəsinə qarşı müdafiə (bax, məsələn, AİHM, Leander İsveçə qarşı (Leander v. Sweden, n° 9248/81, 1 iyul 1985-ci il); AİHM, S və Marper Birləşmiş Krallığa qarşı (S. and Marper v. United Kingdom, n° 30562/04, 4 dekabr 2008-ci il).

- tibbi məlumatların mühafizəsi,

- intim və şəxsi həyata dair məlumatların mühafizəsi ifadə azadlığına qarşı.

Məhkəmə izahat verərək aydınlatmışdır ki, AİHK-nın 8-ci Maddəsi dövlətlərdən yalnız bu Konvensiyada nəzərdə tutulmuş hüququn pozuntusuna gətirib çıxara biləcək istənilən hərəkətdən çəkinməyi tələb etmir, eyni zamanda, müəyyən şərtlər daxilində dövlətlər, özlərinin pozitiv öhdəliklərinə müvafiq olaraq şəxsi və ailə həyatı hüququna hörmət bəslənməsini səmərəli şəkildə təmin etmək üçün tədbirlər görməlidirlər (bax, misal olaraq, AİHM, İ Finlandiyaya qarşı (I. v. Finland, n° 20511/03, 17 iyul 2008-ci il; AİHM, K.U. Finlandiyaya qarşı (K.U. v. Finland, n° 2872/02), 2 mart 2009-cu il).

2° Avropa Şurasının 108 sayılı Konvensiyası

1960-cı illərdə informasiya texnologiyalarının meydana gəlməsi ilə şəxslərin fərdi məlumatlarının mühafizəsinin təmin edilməsi məqsədi ilə təfərrüatlı qaydalar işləyib-hazırlamaq ehtiyacı da yaranmışdır və getdikcə artmaqdadır. 1981-ci il 28 yanvar tarixində Fərdi məlumatların avtomatik işlənməsi ilə bağlı fərdlərin mühafizə olunmasına dair Konvensiya (108 sayılı Konvensiya) imzaya açılmışdır. 108 sayılı Konvensiya məlumatların mühafizəsi sahəsində mövcud olan və məcburi hüquqi qüvvəyə malik olan yeganə beynəlxalq sənəd olmuşdur və olmağa davam edir.

108 sayılı Konvensiya fərdi məlumatların dövlət sektorunda və ya özəl sektorda həyata keçirilən istənilən işlənməsini, məsələn məhkəmə və ya hüquq-mühafizə orqanları tərəfindən həyata keçirilən məlumat işlənməsini əhatə edir. Konvensiya fərdi şəxsləri fərdi məlumatların toplanması və işlənməsi zamanı meydana gələ biləcək hər hansı sui-istifadə hallarından müdafiə edir. Buna görə də, Konvensiya məlumatların ədalətli və qanuni şəkildə toplanmasının və

xüsusi legitim məqsədlərlə saxlanılan məlumatların avtomatik surətdə işlənməsinin prinsiplərini müəyyən edir ki, həmin məlumatlardan qeyd edilən legitim məqsədlərə ziddiyyət təşkil edən məramlar naminə istifadə edilməsin və ya onlar zəruri olduğundan artıq müddətə saxlanılmasın.

Fərdi məlumatların toplanması və işlənməsi ilə bağlı təminatlar nəzərdə tutmaqla bərabər 108 sayılı Konvensiya, həmin hüquqi təminatlar olmadıqda həssas məlumatların, məsələn, şəxsin irqi, siyasi fikirləri, sağlamlığı, dini əqidəsi, cinsi həyatı və ya cinayət işi ilə bağlı məhkumluğuna dair məlumatların işlənməsini qadağan edir.

108 sayılı Konvensiyada təsbit edilmiş ümumi prinsipləri və qaydaları inkişaf etdirmək məqsədi ilə AŞ Nazirlər Komitəsi tərəfindən məcburi hüquqi qüvvəyə malik olmayan 15-ə qədər tövsiyə verilmişdir. Bu tövsiyələr xüsusilə hüquq-mühafizə sektorunda, xüsusilə İnternetdə profil məlumatları, avtomatik tibbi məlumatlar və ya özəl həyata aid olan məlumatların qorunmasına aid olmuşdur.

Aİ qanunvericiliyində xüsusilə iki sənəd üstünlük təşkil edir. Birincisi:

3° Məlumatların mühafizəsinə dair 95/46/CE sayılı Direktiv

Aİ-nın məlumatların mühafizəsinə dair əsas sənədi Avropa Parlamentinin və Avropa İttifaqı Şurasının 95/46/EC sayılı 24 oktyabr 1995-ci il tarixli, fiziki şəxslərə aid olan fərdi məlumatların işlənməsi və həmin məlumatların sərbəst dövriyyəsinə dair Direktivdir (Məlumatların mühafizəsinə dair Direktiv).

Bu Direktivin qəbul edilməsində məqsəd məlumatların mühafizə edilməsinə dair milli səviyyədə mövcud olan qanunvericiliyin uyğunlaşdırılması olduğundan, o (direktiv), məlumatların mühafizəsi ilə bağlı milli qanunvericilik aktlarında mövcud olan dəqiqlik ilə müqayisə edilə biləcək bir dəqiqliklə yazılmışdır (Avropa İttifaqı Ədalət Məhkəməsi (CJEU), birləşdirilmiş işlər C-468/10 və C-469/10, Milli Maliyyə və Kredit Məsələləri üzrə Assosiasiyası və Elektron Ticarət və Marketing Federasiyası Dövlət administrasiyasına qarşı (Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v. Administración del Estado, 24 noyabr 2011-ci il). Nəticədə, üzv dövlətlər bu Direktivin icrası ilə bağlı yalnız məhdud sərbəstliyə malikdirlər.

Bundan əlavə, Direktivin maddi hüquq cəhətdən əhatə dairəsi yalnız daxili bazara aid olan məsələlərlə məhdudlaşır. Digər sözlə desək, polis və ədalət mühakiməsi orqanları arasındakı əməkdaşlığa aidiyyəti olan məsələlər onun təsiri altına düşmür.

Bu fərdi şəxslərin, İcmanın orqanları və ya qurumları tərəfindən fərdi məlumatların işlənməsi və onu tamamlayan məlumatların sərbəst hərəkəti ilə bağlı müdafiəsinə dair (EC) n° 45/2001 sayılı Reqlament (Qaydadır).

Fədi məlumatların işlənməsi və elektron rabitə sektorunda məxfiliyin qorunmasına dair 2002/58/EC sayılı Direktiv və ictimaiyyətə və ya ictimai rabitə şəbəkələrinə açıq olan elektron rabitə xidmətləri ilə bağlı yaradılan və ya işlənən məlumatların saxlanmasına dair 2006/24/EC sayılı Direktiv belə misallardandır.

Qeyd olunan bu sənədlərin hamısı Məlumatların Mühafizəsinə dair Direktivə uyğun olmalıdır.

4° Avropa İttifaqının Əsas Hüquqlar Xartiyası

Xartiya yalnız şəxsi və ailə həyatına hörmət hüququnu təmin etmir (7-ci Maddə), eyni zamanda məlumatların mühafizəsi hüququnu da özündə ehtiva edir və bununla da, həmin hüququn müdafiə olunma səviyyəsini Aİ qanunvericiliyində mövcud olan əsas hüquqlar səviyyəsinə qaldırmışdır. Avropa İnstitutları, eləcə də Üzv Dövlətlər bu hüquqa hörmət etməli və onu təmin etməlidirlər; bu eyni zamanda Üzv Dövlətlər tərəfindən İttifaq qanunvericiliyinin icra edilməsinə də şamil edilir (Xartiyanın 51-ci Maddəsi). Xartiya 8-ci Maddəsində sadəcə məlumatların mühafizəsi hüququnu aşkar şəkildə təsbit etmir, həm də 8-ci Maddənin 2-ci bəndində məlumatların mühafizəsi ilə bağlı əsas prinsiplərə istinad edir. Nəhayət, Xartiyanın 8-ci Maddəsinin 3-cü bəndi bu prinsiplərin yerinə yetirilməsi üzərində müstəqil qurum tərəfindən nəzarət olmasını nəzərdə tutur.

Avropada fərdi məlumatların mühafizəsi ilə bağlı ümumi hüquqi çərçivəni artıq müəyyən etdiyimizə görə, indi gəlin həmin mühafizənin əsas prinsiplərinə keçək.

I. Avropanın məlumatların mühafizəsinə dair qanunvericiliyinin əsas prinsipləri

Prinsiplər Avropanın məlumatların mühafizəsinə dair qanunvericiliyinin məğzini təşkil edən 108 sayılı Konvensiyanın 5-ci Maddəsində təsbit olunub. Həmin prinsiplər həmçinin Məlumatların Mühafizəsinə dair Direktivin 6-cı Maddəsində də başlanğıc olaraq qeyd olunub və sonrakı maddələrdə daha təfərrüatlı şəkildə əks etdirilib. Məlumatların mühafizəsinə dair AŞ və Aİ-nin bütün qanunvericilik aktlarında bu prinsiplərə hörmət ifadə olunmalı və bu qanunvericilik şərh edilərkən həmin prinsiplərə istinad edilməlidir.

Bu əsas prinsiplərdən geri çəkilmələr və ya onlara qoyulan bütün məhdudiyyətlər milli səviyyədə nəzərdə tutulmalıdır (108 sayılı Konvensiya, 9-cu Maddə, 2-ci bənd; Məlumatların Mühafizəsinə dair Direktiv, 13-cü Maddə, 2-ci bənd); onlar qanunla nəzərdə tutulmalı, legitim məqsəddə xidmət etməli və demokratik cəmiyyətdə zəruri olmalıdırlar. Bu üç şərtin hər üçünə əməl edilməlidir.

Fərdi məlumatların mühafizəsi ilk növbədə məlumatların işlənilməsi üçün qanunauyğun şərtlərin mövcud olmasını nəzərdə tutur.

A/ Qanunauyğun işlənilmə prinsipi

Aİ və AŞ-nin məlumatların işlənilməsinə dair qanunvericiliyinə müvafiq olaraq istinad edilməli olan ilk prinsip məlumatların qanuni şəkildə işlənilməsi prinsipidir. Bu prinsip 108 sayılı Konvensiyanın 5-ci Maddəsində və Məlumatların Mühafizəsinə dair Direktivin 6-cı Maddəsində demək olar ki, eyni ifadələrlə təsbit edilib.

Bu maddələrin heç birində məlumatların qanunauyğun işlənilməsinin tərifini verilməyib. Bu hüquqi termini başa düşmək üçün AİHK-da və onun AİHM tərəfindən edilən interpretasiyasında əsaslandırılmış müdaxilə adlanan məfhumla, eləcə də Əsas Hüquqlar Xartiyasının 52-ci Maddəsində nəzərdə tutulmuş qanuni məhdudiyyət şərtlərinə müraciət etmək zəruridir.

❖ AİHK –da əsaslandırılmış müdaxilə ilə bağlı nəzərdə tutulan tələblər

Fərdi məlumatların işlənməsi məlumat subyektinin şəxsi həyat hüququna müdaxilə təşkil edə bilər. Lakin, şəxsi həyat hüququ mütləq hüquq deyildir və buna görə də, onun digər şəxslərin və ya bütövlükdə cəmiyyətin (ictimai maraqlar) digər legitim maraqları ilə tarazlaşdırılması və uzlaşdırılması tələb olunur.

Dövlətin, xüsusilə şəxsi həyat hüququna müdaxiləsini əsaslandıran bu şərtlər, aşağıdakılardan ibarətdir:

- **Qanunla nəzərdə tutulmuş müdaxilə**

AİHM-in presedent hüququna əsasən, müdaxilə o zaman qanuni hesab edilir ki, o (müdaxilə) müəyyən səciyyəvi cəhətlərə malik olan milli qanunvericilik aktının müddəalarına əsaslanmış olsun. Qanunvericilik aktı “sözgedən şəxslər üçün əlçatan və onun nəticələri əvvəlcədən görülə bilən” olmalıdır (AİHM, Amann İsveçrəyə qarşı (Amann v. Switzerland [GC]), yuxarıda qeyd olunub, Maddə 50 ; AİHM, Kopp İsveçrəyə qarşı, 25 mart 1998-ci il (Kopp v. Switzerland, n° 23224/94, 25 mart 1998-ci il, mad. 55) və AİHM, İordaçi və digərləri Moldovaya qarşı, (Iordachi and others v. Moldova, n° 25198/02), 10 fevral 2009-cu il, mad. 50). Qayda o halda əvvəlcədən görülə bilən olur ki, “o, istənilən fərdi şəxsin – ehtiyac olduqda müvafiq məsləhət almaqla – öz davranışını tənzimləməsinə şərait yaratsın”. (AİHM, Amann İsveçrəyə qarşı (Amann v. Switzerland [GC]), yuxarıda qeyd olunub, mad. 56 ; AİHM, Malon Birləşmiş Krallığa qarşı (Malone v. United Kingdom), yuxarıda qeyd olunub, mad. 66 ; AİHM, Ailver və digərləri Birləşmiş Krallığa qarşı (Silver and others v. United Kingdom, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75), 25 mart 1983-cü il, mad. 88).

Buna görə də, müdaxilə həyata keçirilməzdən əvvəl milli qanunvericilikdə müəyyən növ müdaxiləyə icazə verilməsi ilə bağlı müddəanın olması zəruridir (AİHM, Teylor-Sabori Birləşmiş Krallığa qarşı (Taylor-Sabori v. United Kingdom, n° 47114/99), 22 oktyabr 2002-ci il).

Məsələn: Rotaru Ruminiyaya qarşı işində (Rotaru v. Romania (ECtHR, Rotaru v. Romania [GC], n° 28341/95, 4 aprel 2000-ci il, mad. 57); həmçinin bax, AİHM, Avropaya inteqrasiya və insan hüquqları Assosiasiyası və Ekimciyev Bolqarıstana qarşı (Association for European integration and human rights and Ekimdzhiyev v. Bulgaria, n° 62540/00), 28 iyun 2007-ci il); AİHM, Şimovolos Rusiyaya qarşı (Shimovolos v. Russia, n° 30194/09), 21 iyun 2011-ci il); və AİHM, Vetter Fransaya qarşı (Vetter v. France, n° 59842/00), 31 may 2005-ci il) müşahidə edilmişdir ki, Ruminiya qanunvericiliyinə əsasən milli təhlükəsizliklə bağlı olan məlumatların toplanması, yazılması və məxfi şəkildə arxivləşdirilməsinə həmin səlahiyyətlərin icrasına məhdudiyət tətbiq etmədən icazə verilirdi və bununla bağlı qərarlar hakimiyyət orqanlarının diskresion hüququna əsasən həll edilirdi. Məsələn, yerli qanunvericilikdə işlənilə bilən məlumatların növü, izləmə tədbirlərinin hansı kateqoriyadan olan insanlara tətbiq edilə biləcəyi və hansı şəraitdə tətbiq edilə biləcəyi, eləcə də həmin tədbirlər tətbiq edilərkən hansı prosedurlara əməl edilməli olduğu nəzərdə tutulmayıb.

Bu nöqsanları nəzərə alaraq AİHM belə nəticəyə gəlmişdir ki, milli qanunvericilik AİHK-nın 8-ci Maddəsində nəzərdə tutulmuş qanunun əvvəlcədən görülə bilən olması tələbinə cavab vermir və bununla da, həmin Maddənin pozuntusu baş vermişdir.

- Legitim məqsədin güdülməsi

Legitim məqsəd ictimai marağ (bütövlükdə cəmiyyətin maraqları) və ya digərlərinin hüquq və azadlıqlarının qorunması ola bilər.

Məsələn: Pek Birləşmiş Krallığa qarşı işində (AİHM, Peck v. United Kingdom, n° 44647/98, 28 yanvar 2003-cü il, xüsusilə mad. 85), ərizəçi küçədə biləklərini kəsməklə intihar etməyə cəhd göstərmiş və müşahidə kameraları tərəfindən bütövlükdə bu cəhdin videoyazıya alındığından xəbərdar olmamışdı. Müşahidə kameralarını izləyən polis ərizəçini xilas etdikdən sonra həmin video yazılarını media orqanına vermiş, onlar da video yazını ərizəçinin üzünü gizlətmədən yayımlamışdılar. AİHM aşkar etmişdir ki, dövlət orqanlarının əlində ərizəçinin razılığı olmadan və ya onun üzünü gizlətmədən videonu yayımlamaq üçün yetərli və müvafiq səbəb yox idi. Bununla da AİHM Konvensiyanın 8-ci Maddəsinin pozulduğunu aşkar etmişdir.

- Demokratik cəmiyyətdə zəruri olan müdaxilə

AİHM bəyan etmişdir ki, “zəruriyyət məfhumunun anlamı ö deməkdir ki, müdaxilə təcili sosial ehtiyaca cavab olaraq həyata keçirilməli və xüsusilə də, qarşıya qoyulmuş legitim məqsədə mütənasib olmalıdır” (AİHM, Leander İsveçə qarşı (Leander v. Sweden), yuxarıda qeyd edilib, Maddə 58).

Misal: Xelili İsveçrəyə qarşı işində (AİHM, Khelili v. Switzerland, n° 16188/07, 18 oktyabr 2011-ci il.), polis apardığı yoxlama zamanı aşkar etmişdi ki, ərizəçi üstündə aşağıdakı sözlər yazılmış vizit-kartlara malikdir: “30 yaşlarında gözəl və cazibədar xanım birlikdə içki içmək və ya vaxtaşırı birlikdə vaxt keçirmək məqsədilə kişi ilə tanış olmaq istəyir Tel. nömrəsi: [...]”. Ərizəçinin dediyinə görə polis bunu aşkar etdikdən sonra onu fahişə kimi qeydiyyatla götürür, ərizəçi isə bu peşənin sahibi olduğunu hər zaman inkar etmişdi. Ərizəçi fahişə sözünün polis tərəfindən tərtib olunan sənədlərdən silinməsinə tələb edir. AİHM qəbul edib ki, müəyyən fərdi şəxslərin şəxsi məlumatlarının şəxsin digər pozuntu törədə biləcəyi ehtimalı ilə saxlanması müəyyən şərtlər daxilində qarşıya qoyulan legitim məqsədlərə mütənasib ola bilər. Lakin, ərizəçinin işində qeyri-qanuni fahişəliklə bağlı iddialar olduqca ümumi xarakterli və qeyri-müəyyən görünürdü və konkret faktlarla təsdiqlənmirdi, belə ki, o, heç bir vaxt qeyri-qanuni fahişəliyə görə məhkum edilməmişdi və buna görə də, burada AİHK-nın 8-ci Maddəsində nəzərdə tutulan təcili sosial ehtiyacın olduğunu iddia etmək mümkün deyildi.

Ərizəçi ilə bağlı saxlanılan məlumatların dəqiqliyini hakimiyyət orqanlarının sübuta yetirməli olduğu faktını və ərizəçinin hüquqlarına müdaxilə edilməsinin ciddiyyətini nəzərə alaraq AİHM belə nəticəyə gəlmişdir ki, polis tərəfindən tərtib edilmiş sənədlərdə fahişə, sözünün saxlanması AİHK-nın 8-ci Maddəsinin pozuntusuna səbəb olmuşdur.

Misal: Leander İsveçə qarşı işində (Leander v. Sweden) (yuxarıda adı şəkilib) AİHM müəyyən etmişdir ki, milli təhlükəsizlik nöqtəyi-nəzərindən əhəmiyyət kəsb edən vəzifələrdə işləmək üçün müraciət edən şəxslərin gizli şəkildə yoxlanması özü-özlüyündə demokratik cəmiyyətdə zərurət tələbinə zidd deyil. Belə insanların maraqlarını qorumaq məqsədilə milli qanunvericilikdə nəzərdə tutulmuş xüsusi təminatları (məsələn, parlament və ya ədliyyə naziri tərəfindən həyata keçirilən nəzarət) nəzərdən keçirən AİHM belə nəticəyə gəlmişdir ki, İsveçdə mövcud olan

əməkdaşlar üzərində nəzarət sistemi AİHK-nın 8-ci Maddəsinin 2-ci bəndinin tələblərinə uyğundur.

Cavabdeh dövlətin malik olduğu geniş mülahizə sərbəstliyini nəzərə alaraq ərizəçinin işində o, belə qərara gəlmişdi ki, milli təhlükəsizlik ilə bağlı olan maraqlar ərizəçinin fərdi maraqları ilə münasibətdə üstünlük təşkil edir.

❖ Aİ Xartiyasına müvafiq olaraq qanuni məhdudiyət tətbiq etmənin şərtləri

Xartiyanın strukturu və ifadə tərzini AİHK-dan fərqlənir. Xartiya təmin edilən hüquqlara müdaxilədən bəhs etmir, bunun əvəzinə, Xartiya tərəfindən tanınan hüquq və azadlıqların məhdudlaşdırılması ilə bağlı bir Maddəyə malikdir.

52-ci Maddənin 1-ci bəndinə əsasən Xartiya tərəfindən tanınmış bütün hüquq və azadlıqların və müvafiq olaraq, fərdi məlumatların işlənilməsi kimi proseslərlə bağlı fərdi məlumatların mühafizəsi hüququnun məhdudlaşdırılmasına aşağıdakı hallarda yol verilir:

- 1) Qanunla nəzərdə tutulan hallarda;
- 2) Məlumatların mühafizəsi hüququnun məğzində hörmət bəsləndikdə
- 3) Zəruri olduqda və mütənasiblik prinsipinə əməl edildikdə; və
- 4) İttifaq tərəfindən tanınan ümumi marağın məqsədlərinə və ya digərlərinin hüquq və azadlıqlarının müdafiəsinə səmərəli şəkildə cavab verdikdə.

İstifadə edilən ifadələrin fərqli olmasına baxmayaraq Xartiyanın 52-ci Maddəsinin 1-ci bəndində nəzərdə tutulan şərtlər AİHK-nın 8-ci Maddəsinin 2-ci bəndində nəzərdə tutulan şərtlərə bənzərdir. Əlbəttə ki, Xartiyanın 52-ci Maddəsinin 1-ci bəndində təsbit edilmiş şərtlər AİHK-ın 8-ci Maddəsinin 2-ci bəndində təsbit edilmiş şərtlərə uyğun olaraq başa düşülməlidir, belə ki, 52-ci Maddənin 3-cü bəndinin birinci cümləsində qeyd edilir ki, “ Xartiyada Avropa İnsan Hüquqları və Əsas Azadlıqları Konvensiyasına əsasən təmin edilən hüquqlar nəzərdə tutulduğuna görə, həmin hüquqların mənası və əhatə dairəsi də Konvensiyada nəzərdə tutulmuş hüquqlarla eyni olmalıdır.”

Buna baxmayaraq, 52-ci Maddənin 3-cü bəndinin son cümləsində deyilir ki, “bu müddəə İttifaq qanunvericiliyində daha geniş mühafizə təmin olunmasının qarşısını almamalıdır.”

Məlumatların mühafizə edilməsi ilə bağlı digər prinsip qarşıya qoyulan məqsədin müəyyən edilməsi və məhdudiyət prinsipidir.

B/ Qarşıya qoyulan məqsədin müəyyən edilməsi və məhdudiyət prinsipi

Məqsədin müəyyən edilməsi və məhdudiyət prinsipi əsasən müəyyən edir ki, fərdi məlumatların işlənilməsi ilə bağlı legitimlik həmin işlənilmənin qarşısına qoyulan məqsəddən asılıdır. Nəzarətçi məlumatların işlənilməsinə başlamazdan əvvəl həmin işlənilmə ilə bağlı qarşıya qoyduğu məqsədin nədən ibarət olduğunu aşkar şəkildə bəyan etməlidir. Aİ qanunvericiliyinə müvafiq olaraq, bunu ya bəyanat verməklə, digər şəkildə ifadə etsək, müvafiq rəhbərə bildiriş göndərməklə etmək mümkündür, ya da ən azından, nəzarətçi barəsində fərdi məlumatların işlənilməsi həyata keçirilən şəxsin daxili sənədləşmə ilə tanış olmasını təmin edə bilər.

Fərdi məlumatların qeyri-müəyyən və ya qeyri-məhdud məqsədlərlə işlənməsi qanunsuz hesab edilir.

Misal: Hava şirkəti uçuşu düzgün şəkildə təşkil edə bilmək üçün sərnəşinlərin fərdi məlumatlarını toplayır. Hava şirkətinə aşağıdakı məlumatları əldə etmək tələb olunur: sərnəşinin oturacaq nömrəsi; əlilliyi olan şəxslərin ehtiyacı olan vasitələr, məsələn, əlil arabası ilə bağlı məlumat; xüsusi yemək növlərinə, məsələn Koşer və ya halal yeməyə olan tələbat. Hava şirkətindən Sərnəşin Ad Qeydiyyatı (PNR) sənədləşməsində olan bu məlumatları təyyarənin enəcəyi hava limanındakı miqrasiya xidmətinə ötürmək tələb olunarsa, bu zaman həmin məlumatlardan immiqrasiyaya nəzarət məqsədi ilə istifadə ediləcəkdir ki, bu da məlumatın toplanmasının ilkin məqsədindən fərqlidir. Buna görə də, məlumatın ötürülməsi üçün yeni hüquqi əsas tələb olunacaqdır (bax aşağıda).

Məlumatların keyfiyyəti ilə bağlı prinsiplər də fərdi məlumatlar subyektinin hüquqlarını qorumaq məqsədi daşıyır.

C/ Məlumatların keyfiyyəti ilə bağlı prinsiplər

❖ Məlumatların aktuallığı ilə bağlı prinsiplər

Yalnız “adekvat, münasib və onların toplanması və daha sonra işlənməsinin məqsədlərindən kənara çıxmayan məlumatlar” işlənilə bilər (108 sayılı Konvensiya, Maddə.5(C); və Məlumatların mühafizəsinə dair Direktiv, Maddə. 6, (1) (C)). Məlumatların işlənməsi üçün seçilmiş bu kateqoriyalara daxil olan məlumatlar mütləq işlənmənin elan edilmiş ümumi məqsədləri çərçivəsində emal edilməli və işlənmənin nəzarətçisi məhz həmin məqsədə müvafiq olan məlumatların toplandığına ciddi nəzarət etməlidir.

❖ Məlumatların dəqiqliyi prinsipi

Fərdi məlumatların işlənməsini həyata keçirən nəzarətçi həmin məlumatdan istifadə etməzdən əvvəl onun (məlumatın) dəqiq və son məlumat olduğundan əğlabatan dərəcədə əmin olmaq üçün tədbirlər görməlidir.

❖ Məlumatın məhdud şəkildə saxlanması prinsipi

Məlumatların Mühafizəsinə dair Direktivin 6 (1)(e) Maddəsində və buna bənzər olaraq 108 sayılı Konvensiyanın 5 (e) Maddəsində Üzv Dövlətlərdən tələb olunur ki, onlar fərdi məlumatları “elə formada saxlasınlar ki, bu onlara həmin məlumatların subyektlərinin identifikasiyasını müəyyən etmək, həmin məlumatların işlənməsinin məqsədi üçün tələb olunan müddətdən artıq bir müddətdə mümkün olmasın”. Məlumatların saxlanması qarşıya qoyulmuş məqsədə mütənasib olmalıdır (AİHM, S. və Harper Birləşmiş Krallığa qarşı (S. et Marper v. United Kingdom), yuxarıda qeyd olunub ; Həmçinin bax, məsələn, AİHM, M.M. Birləşmiş Krallığa qarşı (M.M. v. United Kingdom, n° 24029/07), 13 noyabr 2012-ci il) və bu xüsusilə, polis sektoru üçün keçərlidir. Məlumatın toplanması zamanı qarşıya qoyulan məqsədə çatdıqdan sonra məlumatlar silinməlidir.

Misal: S. və Marper işində (S. et Marper) AİHM belə nəticəyə gəlmişdir ki, Avropa Şurasının

müvafiq sənədlərində nəzərdə tutulmuş prinsiplər, eləcə də Müqaviləyə qoşulan dövlətlərin qanunvericiliyi və təcrübəsi məlumatların saxlanılmasının onların toplandıqlarına səbəb olmuş məqsədə müvafiq olmasını və (xüsusilə polis sektorunda) məhdud müddətdə saxlanılmasını təmin etməlidirlər

Misal: AIHM-in Brunet Fransaya qarşı işində (Brunet v. France, n°21010/10), 18 sentyabr 2014-cü il) ərizəçinin məlumatları istintaqla bağlı məlumatların qeydiyyatının aparıldığı və şübhəli bilinən şəxslərin və zərərçəkmişlərin siyasının daxil edildiyi polis qeydiyyat sistemində (STIC – cinayət əməlləri ilə bağlı məlumatların işlənilməsi sistemi) aşkar edilmişdi, baxmayaraq ki, ona qarşı cinayət işinə xitam verilmişdi. Məhkəmə belə nəticəyə gəldi ki, Konvensiyanın 8-ci Maddəsinin (şəxsi həyat hüququ) pozuntusu baş vermişdi, belə ki, qeydiyyata alınmış məlumatların saxlanılması ərizəçinin şəxsi həyat hüququna mütənasib deyildi və demokratik cəmiyyətdə zəruri tədbir kimi qiymətləndirilə bilməzdi. Məhkəmə spesifik olaraq hesab etmişdi ki, ərizəçinin STIC-də saxlanılan məlumatların silinməsi ilə bağlı müraciət etmək imkanı yox idi və məlumatların saxlanılması üçün nəzərdə tutulmuş iyirmi illik müddət məlumatların qeyri-məhdud müddətdə saxlanılmasına bərabər olan bir təcrübə idi və ya müddətlə bağlı bir ləngimə kimi deyil, daha çox bir norma kimi başa düşülürdü.

Lakin, fərdi məlumatların saxlanılmasına müddət məhdudiyətinin tətbiq edilməsi yalnız elə hallarda mümkündür ki, bu zaman məlumatın saxlanılma şəkli məlumat subyektinin kimliyini müəyyən etməyə imkan versin. Buna görə də, artıq zəruri olmayan məlumatların saxlanılması onların adsızlaşdırılması və ya təxəllüsləşdirilməsi vasitəsilə mümkündür.

Fərdi məlumatların mühafizəsi sahəsində mövcud olan əsas prinsiplərin sonuncusu məlumatların ədalətli işlənilməsi prinsipidir.

D/ Məlumatların ədalətli işlənilməsi prinsipi

Bu prinsip məlumatların işlənilməsini həyata keçirən nəzarətçilərin üzərinə məlumatın daşıyıcısı və bütövlükdə ictimaiyyətə, bu məlumatı işləməyə hazırladıqları barədə qanuni və şəffaf şəkildə məlumat versin. Məlumatların işlənilməsi heç bir halda gizli aparıla bilməz və əvvəlcədən görülə bilinməyən mənfi nəticələrə gətirib çıxarmamalıdır. Nəzarətçilər istehlakçıların, müştərilərin və vətəndaşların onlara aid olan məlumatlardan istifadə edildiyinə dair məlumatlandırılmasını təmin etməlidirlər.

Məlumatların işlənilməsi məlumat subyektlərinə sadə və onlara anlaşılan dildə izah edilməlidir ki, onlar özlərinə aid məlumatların əqibətinin nə olacağını başa düşə bilsinlər. Məlumat subyektinin həmçinin hüququ vardır ki, nəzarətçiyə müraciət etdiyi təqdirdə məlumatlarının işlənilib-islənilməməsi və hansı növ işlənilməyə məruz qalması barədə məlumat əldə etmiş olsun.

Başqa sözlə desək, nəzarətçilər imkan daxilində, məlumat subyektlərinin arzularına müvafiq olaraq hərəkət etməlidirlər. Bu xüsusilə elə hallara şamil edilir ki, bu zaman məlumat subyektlərinin razılığı məlumatın işlənilməsi üçün hüquqi əsası təşkil etsin.

Misal : Haralambi Rumıniyaya qarşı işində (AIHM, Haralambie v. Romania, n° 21737/03, 27 oktyabr 2009-cu il) ərizəçi onun barəsində gizli xidmətin əlində olan məlumatları əldə etməklə bağlı müraciət etmişdi, lakin onun müraciətinə yalnız 5 ildən sonra əməl edilmişdi. AIHM təkrarən vurğulamışdır ki, dövlət qurumlarında saxlanılan fərdi məlumatların subyekti olan

insanların həmin məlumatlara çıxış əldə etməklə bağlı həyati maraqları vardır. Dövlət qurumları onların həmin məlumatlara maneəsiz çıxışını təmin etmək üçün tədbirlər görməlidirlər. AİHM hesab etmişdir ki, nə ötürülən sənədlərin sayı, nə də arxiv sistemində olan nasazlıqlar ərizəçinin öz məlumatlarına çıxış əldə etməklə bağlı müraciətinə cavab verilməsinin 5 il müddətinə gecikdirilməsinə bəraət qazandıra bilməz. Dövlət qurumları ərizəçini effektiv prosedurla təmin etməyiblər ki, həmin prosedurdan istifadə etməklə əqlabatan müddət ərzində fərdi məlumatlara çıxış əldə etmək mümkün olsun. Bununla da, AİHM AİHK-ın 8-ci Maddəsinin pozuntusunu aşkar etmişdir.

Misal: K.H. və başqaları Slovakiyaya qarşı işində (AİHM, K.H. and others v. Slovakia, n° 32881/04, 6 noyabr 2009-cu il), ərizəçilər roma (qaraçı) etnik mənşəyinə malik olan səkkiz qadın idi. Onlar hamilə olduqları zaman Slovakiyanın şərqində yerləşən iki xəstəxanada müalicə almışdılar və daha sonra doğuşu da orada həyata keçirmişdilər. Daha sonra, dafələrlə cəhd göstərmələrinə baxmayaraq, onlardan heç biri yenidən hamilə qala bilməmişdi. Milli məhkəmələr xəstəxanalara göstəriş vermişdilər ki, ərizəçilərə və onların nümayəndələrinə məsləhətlər versinlər və bəzi çıxarışların əl ilə köçürülməsinə icazə versinlər, lakin dediklərinə görə, sui-istifadənin qarşısını almaq məqsədilə onların sənədlərin fotosurətini almaqla bağlı müraciətlərini rədd etmişdilər. AİHK-ın 8-ci Maddəsinə əsasən, Dövlətlər məlumatın subyektləri ilə bağlı əllərində olan sənədlərin surətini həmin subyektə təqdim etməlidirlər. Dövlətlər fərdi məlumatla bağlı materialların surətinin çıxarılması üçün tədbirlər görməli və ya, ehtiyac olarsa, imtinaya səbəb olan səbəbləri açıqlamalıdır. Ərizəçilərin işində milli məhkəmələr tibbi sənədlərin surətini çıxarmağa qoyulan qadağanı sui-istifadənin qarşısının alınması ilə izah etmişdilər. Lakin, AİHM ərizəçilərin özləri barədə məlumatdan necə sui-istifadə edə biləcəklərini başa düşmədiyini bildirmişdi. Bundan əlavə, belə sui-istifadənin baş verməsi riskindən qurtarmaq üçün, məsələn, həmin materiallara çıxışı olan şəxslərin sayını məhdudlaşdırmaq mümkün idi. AİHM belə nəticəyə gəlmişdir ki, 8-ci Maddənin pozuntusu baş vermişdir, çünki, Dövləti ərizəçilərə onların sağlamlıqlarına dair məlumatları verməkdən imtina etməyə məcbur edən səbəblər mövcud deyildi.

Məlumatların mühafizəsi ilə bağlı bu dörd prinsipin ümumi asayış nöqtəyi-nəzərindən əhəmiyyəti böyükdür. Onların konkret situasiyalara tətbiqi müəyyən mənada mülahizə sərbəstliyi və vasitələrin müəyyən seçiminə şərait yaradır.

II. Fərdi məlumatların mühafizəsi prinsiplərinin tətbiqi ilə bağlı qaydalar

AŞ qanunvericiliyi bu interpretasiya sərbəstliyini aydınlaşdırmağı 108 sayılı Konvensiyanın Tərəflərinə həvalə edir.

Bu qaydaların üç növünü müəyyən edə bilərik. Bu qaydalardan birincisi məlumatların işlənilməsinin qanunauyğun olmasını təmin etmək məqsədi daşıyır.

A/ Qanunauyğun işlənilmə ilə bağlı qaydalar

❖ Qeyri-həssas məlumatların qanunauyğun şəkildə işlənilməsi

Aİ qanunvericiliyinə görə, fərdi məlumatlar aşağıdakı hallarda qanunauyğun şəkildə işlənir (Məlumatların mühafizəsinə dair Direktivin 7-ci Maddəsi):

1) Məlumatın işlənməsi məlumat subyektinin razılığı ilə həyata keçirilsin; və ya

Aİ qanunvericiliyinə əsasən, məlumatların qanunauyğun şəkildə işlənməsinin əsasını təşkil edən razılıq Məlumatların Mühafizəsinə dair Direktivin 7 (a) Maddəsində təsirli şəkildə təsbit edilmiş və Xartiyanın 8-ci Maddəsində bariz şəkildə göstərilmişdir.

Aİ qanunvericiliyi etibarlı razılığın üç elementinin mövcudluğunu müəyyən edir ki, həmin elementlər əsasında məlumat subyektlərinin onlara aid olan məlumatlardan istifadə edilməsini həqiqətən qəbul etmək arzusunda olub-olmadıqlarını müəyyən etmək mümkündür:

- Razılıq verdikləri zaman məlumat subyektləri təzyiq altında olmamalıdırlar;
- Məlumat subyektlərinə nəyə razılıq verəcəkləri və bu razılığın hansı nəticələrə gətirib çıxara biləcəyi ilə bağlı məlumat verilməlidir; və
- Razılığın təsirləri ağılabatan və konkret olmalıdır.

108 sayılı Konvensiya razılığın şərtini müəyyən etmir, bunu etmək yerli qanunvericiliyə həvalə edilir. Buna baxmayaraq, Avropa Şurasının qanunvericiliyinə əsasən azad və sərbəst şəkildə verilmiş razılığın elementləri yuxarıda qeyd etdiyimiz Aİ qanunvericiliyində və 108 sayılı Konvensiyaya müvafiq verilmiş və toplanılan və işlənən fərdi məlumatların mühafizəsi ilə bağlı olan Tövsiyədə (Bax n° R (97 sayılı Tövsiyə) göstərilən elementlərdir. Tövsiyə Nazirlər Komitəsi tərəfindən 30 sentyabr 1997-ci ildə təsdiq edilmişdir).

Azad və sərbəst razılığın mövcudluğu yalnız o halda etibarlı ola bilər ki, sözügedən şəxsin həqiqətdə seçim etmək imkanı olsun və razılıq vermədiyi təqdirdə həmin şəxs aldatma, hədə-qorxu gəlmə, məcbur etmə və ya digər mənfi nəticələrlə üzləşmək riski altında olmasın.

Misal: Bir sıra hava limanlarında sənişinlər minik zonasına daxil olmaq üçün bütöv bədənin skan aparatından keçməlidirlər. Əgər sənişinlərə aid olan məlumatlar aşkar edildikləri zaman işlənirsə, bu, Məlumatların mühafizəsinə dair Direktivin 7-ci Maddəsində nəzərdə tutulmuş hüquqi əsaslara uyğun həyata keçirilməlidir. Bədənin skaner aparatından keçirilməsi sənişinlərə bəzi hallarda seçim kimi təklif edilir və bununla da nəzərdə tutulur ki, onların razılaşması işlənməni həyata keçirmək üçün əsas ola bilər. Lakin, sənişinlər qorxa bilərlər ki, onların imtina etməsi müəyyən şübhələr yarada və ya, əlavə təhlükəsizlik tədbirlərinin, məsələn, onların üzərində axtarış aparılmasının həyata keçirilməsinə səbəb ola bilər. Bir çox sənişinlər bədən skanerindən keçməyə ona görə razılıq verirlər ki, bu onlara hansısa potensial problemlərdən və ya gecikmələrdən yaxa qurtarmağa imkan verir. Bu razılığın kifayət qədər azad və sərbəst olmadığına inanmaq üçün kifayət qədər əsas var.

Misal: Sənişinə aid olan məlumatların, yəni, onların kimliyi, yemək vərdişləri və sağlamlığı ilə bağlı məlumatların xarici ölkədəki immiqrasiya qurumlarına ötürülməsi məlumatların mühafizəsinə dair qanunvericiliyə əsasən azad və sərbəst razılıq kimi qiymətləndirilə bilməz, belə ki, səyahət edən sənişinlər ölkəyə daxil olub-olmadıqlarına dair seçim etmək imkanına malik deyillər. Belə məlumatların qanunauyğun şəkildə ötürülə bilməsi üçün razılıqdan fərqli bir hüquqi

əsas, böyük ehtimalla, xüsusi qanun tələb olunur.

Bununla bağlı, 11 sentyabr 2001-ci ildə baş verən terrorist hücumlarından sonra Amerika Birləşmiş Ştatları ayrıca qanun qəbul edərək bəyan etmişdi ki, hava şirkətləri gömrük xidmətinə və Amerikanın təhlükəsizlik xidmətinə öz sərnişinlərinə dair məlumat verməlidirlər. Buna əməl edilmədikdə onlar, daha geniş təhlükəsizlik tədbirlərinə və cərimələrə məruz qala, eləcə də onların təyyarəsinin hava limanına enməsinə icazə verilməyə bilər. Sərnişinlərin ad qeydiyyatı (PNR) kimi toplanılan bu məlumatların məzmununu hava şirkətinin təklif etdiklərindən və sərnişinlərin istəklərindən asılı olaraq dəyişir. Buraya rezervasiyanı həyata keçirən səyahət agentliyi, uçuş planı, uçuş nömrəsi, tarixi və s. ilə bağlı məlumat, hətta sərnişinlərin əlaqə məlumatları (telefon nömrəsi və s.) daxil ola bilər. Bundan əlavə, burada həmçinin qiymət, ödəmə metodu və ya mümkün olduqda, kredit kartının nömrəsi, mehmanxana rezervasiyası, gəlişdə təmin olunan avtomobil, uçuş zamanı göstərilməsi istənilən xidmətlər (əvvəlcədən rezervasiya edilmiş oturmaq nömrəsi, yemək növü – vegetarian, Koşer yeməyi və s.) və sərnişinin sağlamlıq vəziyyəti ilə bağlı məlumatı (diabet xəstəsi olması, görmə və ya eşitmə problemi olması və s.) görmək mümkündür. Bu müddəalar fərdi məlumatların mühafizəsinə dair İcma (Aİ) qanunvericiliyində nəzərdə tutulmasa da, 2004-cü ilin mayında ABŞ və Aİ arasında Sərnişin ad qeydiyyatı (PNR) razılaşması sazişi imzalanmışdır. Belə saziş Kanada ilə də bağlanmışdır və hal-hazırda PNR sazişi Aİ-na üzv olan dövlətlər arasında da müzakirə edilir.

Bundan əlavə, məlumatın işlənilməsinə həyata keçirən nəzarətçi ilə məlumatın subyekti arasında tabeçilik və ya iqtisadi bərabərsizlik elementləri olan hallarda razılığın verilməsinin sərbəstliyi məsələsini mübahisələndirmək mümkündür.

Misal: İri miqyaslı şirkət əməkdaşları arasında ünsiyyəti genişləndirmək məqsədi ilə bütün işçilərinin adları, şirkət daxilindəki vəzifəsi və peşə ünvanı ilə bağlı məlumatların daxil ediləcəyi məlumat kitabçası hazırlayır. Kadrlar şöbəsinin rəhbəri təklif edir ki, işçilərin iclaslar zamanı bir-birini tanıya bilməsi üçün onların şəkilləri də həmin məlumat kitabına daxil edilsin. İşçilərin nümayəndələri tələb edirlər ki, fotosəkillər hər bir əməkdaşın razılığı olmadan əlavə edilməsin. Belə vəziyyətdə, hər bir əməkdaşın, onun şəklinin məlumat kitabına daxil edilməsi ilə bağlı razılığı hüquqi əsas hesab edilə bilər, çünki, aydındır ki, şəklın məlumat kitabına daxil edilməsi özü-özlüyündə mənfi nəticələrə gətirib çıxara bilməz. Bundan əlavə, əgər əməkdaş şəklini məlumat kitabına daxil etməkdən imtina etsə, böyük ehtimalla, bu onunla işəgötürən arasında xoşagəlməz münasibətlərin yaranmasına gətirib çıxarmayacaqdır.

2) Məlumatın işlənilməsi məlumat subyektinin tərəf olduğu müqavilənin icrası üçün zəruri olsun; və ya

3) Məlumatın işlənilməsi məlumat subyektinin üzərində olan hüquqi öhdəlik nöqtəyi-nəzərindən zəruri olsun; və ya

Misal: həkimlər və xəstəxanalar bir neçə il ərzində müayinə və müalicə etdikləri xəstələrlə bağlı məlumatın qeydiyyatını aparmaqla bağlı hüquqi öhdəlik daşıyırlar; işəgötürənlər sosial təminat və vergi məsələləri ilə bağlı öz işçiləri ilə bağlı məlumatları, şirkətlər isə vergi məqsədləri üçün öz müştərilərinin məlumatlarını emal etməlidirlər.

AŞ – nın qanunvericiliyinə əsasən, nəzarətçinin hüquqi öhdəlikləri də, xüsusilə, AİHK-nın 8-ci

Maddəsinin 2-ci bəndində göstərildiyi kimi, digərlərinin legitim maraqları mövcud olan hallarda məlumatların legitim şəkildə işlənməsi üçün əsas ola bilər.

4) Məlumat subyektinin həyatı əhəmiyyət kəsb edən maraqları; və ya

AŞ – nın qanunvericiliyində məlumat subyektinin həyatı əhəmiyyət kəsb edən maraqları AİHK-in 8-ci Maddəsində məlumatların mühafizəsinə legitim şəkildə müdaxilə etmək üçün əsas kimi göstərilməmişdir. Lakin, AŞ-nin 108 sayılı Konvensiyaya əlavə olaraq verdiyi bəzi tövsiyələrdə məlumat subyektlərinin həyatı maraq kəsb edən maraqları məlumatların legitim şəkildə işlənməsi üçün hüquqi əsas olaraq aydın şəkildə nəzərdə tutulmuşdur (Profil Tövsiyəsi, mad. 34 (b)).

Məlumat subyektlərinin həyatı maraq kəsb edən maraqlarının məlumatın işlənməsi üçün əsas gətirilən səbəblərin əksəriyyətində nəzərə alınması aşkardır: əsas hüquqların müdafiəsi heç bir halda müdafiə olunan şəxsin həyatı əhəmiyyət kəsb edən maraqlarına xələl gətirməməlidir.

5) məlumatın işlənməsi ictimai əhəmiyyət kəsb edən vəzifənin icrası üçün və ya məlumatın ötürüldüyü nəzarətçiyə və ya üçüncü tərəfə həvalə edilən səlahiyyətlərin həyata keçirilməsi üçün zəruri olsun; və ya

Fərdi məlumatların ictimai sahədə fəaliyyət göstərən dövlət orqanları tərəfindən istifadəsi AİHK-nin 8-ci Maddəsinin təsiri altına düşür.

6) məlumatın işlənməsi, məlumatın ötürüldüyü nəzarətçi və ya üçüncü tərəfin qarşısında duran legitim maraqların məqsədi baxımından, bu məqsədlər məlumat subyektinin insan hüquqları və əsas azadlıqlarından üstünlük təşkil etdiyi hallar istisna olmaqla, zəruridir.

Bənzər ifadələrə AŞ-nin tövsiyələrində də rast gəlmək olar. Beləliklə, Profilləmə Tövsiyəsi profil yaratmaq məqsədi ilə fərdi məlumatların işlənməsini o halda legitim olaraq tanıyır ki, bu işlənmə üçüncü tərəfin legitim maraqlarına əsasən həyata keçirilmiş olsun; burada həmin hallar istisna təşkil edir ki, “həmin hallarda bu məqsədlər məlumat subyektinin insan hüquqları və əsas azadlıqlarından üstünlük təşkil etsin (Profilləmə Tövsiyəsi, mad. 3.4 (b))”.

❖ Həssas məlumatların qanunauyğun işlənməsi qaydaları

Fərdi məlumatların qanunauyğun işlənməsi xüsusi ciddi rejimə tabedir.

AŞ qanunvericiliyi həssas məlumatların müvafiq surətdə istifadəsi ilə bağlı müdafiəni təmin etmə öhdəliyini milli qanunvericiliyə həvalə edir, Aİ qanunvericiliyi isə Məlumatların Mühafizəsinə dair Direktivin 8-ci Maddəsində aşağıdakı kateqoriyalara daxil edilən məlumatların işlənməsi ilə bağlı təfərrüatlı sistem nəzərdə tutur: irqi və ya milli mənşə, ictimai rəy, dini və ya fəlsəfi əqidə, həmkarlar ittifaqına üzvlük, sağlamlıq vəziyyəti və ya cinsi həyat ilə bağlı məlumatlar.

Həssas məlumatların işlənməsi prinsip etibarlı ilə qadağan olunur (Məlumatların Mühafizəsinə dair Direktiv, mad. 8 (1)). Lakin, Direktivin 8-ci Maddəsinin 2-ci və 3-cü bəndində bu qadağadan

azadolmaların məhdud siyahısı verilmişdir. Bu azadolmalara məlumat subyektinin aşkar razılığı, məlumat subyektinin həyati əhəmiyyət kəsb edən maraqları, üçüncü tərəflərin müəyyən legitim maraqları və ya mühüm ictimai maraqlar (məlumat subyektinin maraqlarının müdafiəsi ilə bağlı təminatlar tətbiq etməklə) daxildir.

Buna əsas misallardan biri olaraq tezliklə bir sıra Üzv Dövlətlərdə tətbiq olunması gözlənilən elektron tibbi tarixçələri (qeydiyyat sənədlərini) göstərmək olar. Bu sənədlər xəstənin müalicəsi ilə məşğul olan səhiyyə qurumları tərəfindən toplanılan məlumatlardan ölkə ərazisində fəaliyyət göstərən və xəstəyə səhiyyə xidmətləri göstərən digər səhiyyə qurumları tərəfindən istifadə edilməsini mümkün edir.

Fərdi məlumatların müdafiəsinin ümumilikdə təmin edilməsi, eyni zamanda, işlənən məlumatların təhlükəsizliyinin təmin edilməsini nəzərdə tutur. Məlumatların işlənməsinin təhlükəsizliyini təmin etmək üçün bir neçə qayda var.

B/ Məlumatların işlənməsinin təhlükəsizliyi

❖ Məlumatların təhlükəsizliyi

AŞ-nin məlumatların mühafizəsinə dair qanunvericiliyi, eləcə də **Aİ-nin qanunvericiliyi** təsbit edir ki, məlumatı emal edən nəzarətçilər və digərləri məlumatların təhlükəsizliyini təmin etmək üçün lazımı tədbirlər görmək öhdəliyi daşıyırlar.

AŞ qanunvericiliyində nəzərdə tutulub: *“Avtomatlaşdırılmış məlumat materiallarında saxlanan fərdi məlumatların qəza nəticəsində və ya icazəsiz şəkildə məhv edilməsi, dəyişdirilməsi və yayılmasına qarşı mühafizəsi məqsədilə müvafiq təhlükəsizlik tədbirləri görülməlidir (108 sayılı Konvensiya, mad. 7)”*.

❖ Məxfilik

Aİ qanunvericiliyində məlumatların təhlükəsiz şəkildə işlənməsi həmçinin nəzarətçilərin məlumatların məxfiliyini təmin etmək və üçüncü tərəflərə açıqlamamaqla bağlı ümumi öhdəliyi ilə təmin edilir (Direktivin 7 və 8-ci Maddələri).

AŞ qanunvericiliyində məlumatları məxfi saxlamaq öhdəliyi 108 sayılı Konvensiyanın 7-ci Maddəsində nəzərdə tutulan məlumatların təhlükəsizliyi ifadəsində də ehtiva edilir.

Məlumatların məxfi saxlanması ilə bağlı peşə vəzifələrinin pozulması Aİ-nin bir sıra Üzv Dövlətlərində və 108 sayılı Konvensiyaya Tərəf olan ölkələrdə cinayət məsuliyyəti yaradır.

Qaydaların son kateqoriyasının məqsədi fərdi məlumatların işlənməsinin şəffaflığını təmin etməkdən ibarətdir.

C/ Məlumatların işlənməsinin şəffaflığı ilə bağlı qaydalar

Həm AŞ, həm də Aİ qanunvericiliyinə əsasən nəzarətçilər məlumatın subyektini xəbərdar etməlidirlər (108 sayılı Konvensiya, mad. 8 (a); və Məlumatların Mühafizəsinə dair Direktiv mad. 10 və 11). Bu öhdəlik məlumat subyektinin bununla bağlı müraciət edib-etməməsindən və ya

həmin məlumata marağ göstərib-göstərməməsindən asılı olmayaraq nəzarətçi tərəfindən yerinə yetirilməlidir.

Subyektə verilən məlumata işlənilmənin məqsədi, nəzarətçinin kimliyi və əlaqə məlumatları daxil edilməlidir (8 sayılı Konvensiyanın 8 (a) maddəsi; və Məlumatların Mühafizəsinə Dair Direktivin 10 (a) (b) maddələri.).

Məlumatların ədalətli şəkildə işlənilməsi prinsipi məlumat subyektlərinə xəbərdarlıq etmək məqsədilə təqdim edilən məlumatın asanlıqla başa düşülən olmasını tələb edir. Burada istifadə edilən linqvistik ifadə tərzində məlumat subyektinə uyğun olaraq seçilməlidir.

AŞ qanunvericiliyində 108 sayılı Konvensiyanın 9-cu Maddəsi 8-ci Maddədən azadolmanı nəzərdə tutur: buraya milli qanunvericilikdə nəzərdə tutulan, Dövlətin təhlükəsizliyini, ictimai asayışı, Dövlətin maliyyə maraqlarını təmin etmək, cinayət əməllərinin qarşısını almaq, məlumatın subyektini qorumaq və digərlərinin hüquq və azadlıqlarını qorumaq məqsədi ilə demokratik cəmiyyətdə zəruri olan azadolmalar daxildir.

Fərdi məlumatların mühafizəsi və onların işlənilməsinin təhlükəsizliyini təmin etməyə yönləndirilmiş qaydaların fonunda məlumat subyektlərinin özlərinə aid məlumatla bağlı malik olduqları hüquqlarını nəzərdən keçirmək vacibdir.

III. Məlumat subyektlərinin hüquqları

Birinci və ən vacib olan məsələ ondan ibarətdir ki, məlumat subyektləri onlara aid olan məlumatlara çıxış əldə etmək hüququna malikdirlər.

A/ Şəxsin özünə aid olan məlumatlara çıxış əldə etməsi hüququ

Aİ qanunvericiliyinə əsasən şəxsin özünə aid olan məlumatlara çıxışa malik olma hüququ Məlumatların Mühafizəsinə dair Direktivin 12-ci Maddəsində və Xartiyanın 8 (2) Maddəsində fundamental hüquq kimi nəzərdə tutulmuşdur. Direktiv bu çıxış hüququnun keçmişə aid olub-olmadığını və aiddirsə, keçmişdə hansı müddəti əhatə etdiyini aydın şəkildə müəyyən etmir. Bununla bağlı Aİ-nin Cinayət Məhkəməsi tərəfindən vurğulanmışdır ki, şəxsin özünə aid olan məlumatlara çıxış hüququna müddətlərlə bağlı lüzumsuz məhdudiyət qoymaq olmaz. Məlumat subyektləri həmçinin keçmişdə aparılmış məlumat işlənilməsi əməliyyatları ilə bağlı məlumatları əldə etmək üçün də əgəlabatan imkanlarla təmin edilməlidirlər.

AŞ qanunvericiliyinə əsasən, şəxsin özünə aid olan məlumatlara çıxışa malik olması hüququ aşkar şəkildə 108 sayılı Konvensiyanın 8-ci Maddəsində təsbit edilmişdir. AİHM dəfələrlə müəyyən etmişdir ki, şəxsin özünə aid olan və başqaları tərəfindən saxlanılan və ya emal edilən məlumatlara çıxış əldə etmək hüququ vardır və bu hüquq şəxsi həyata hörmət hüququndan irəli gəlir (AİHM, Qaskin Birləşmiş Krallığa qarşı (Gaskin v. United Kingdom, n° 10454/83), 7 iyul 1989-cu il ; AİHM, Odièvre Fransaya qarşı (Odièvre v. France [GC], n° 42326/98), 13 fevral 2003-cü il ; AİHM, K.H. və başqaları Slovakiyaya qarşı (K.H. and Others v. Slovakia), yuxarıda qeyd olunub ; AİHM, Godelli İtaliyaya qarşı (***Godelli v. Italy***, n° 33783/09), 25 sentyabr 2012-ci il). Çıxışa dair bu hüquq milli qanunvericilikdə təsbit edilməlidir.

108 sayılı Konvensiyanın 9-cu Maddəsi və Məlumatların Mühafizəsinə dair Direktivin 13-cü Maddəsinə əsasən, nəzarətçilərin məlumat subyektinin çıxış ilə bağlı müraciətinə cavab verməsi yalnız digərlərinin legitim maraqları səbəbindən müvəqqəti olaraq məhdudlaşdırıla bilər (AİHM, Leander İsveçə qarşı (Leander v. Sweden), yuxarıda qeyd olunub). Belə maraqlara məlumatların mühafizəsi ilə, maraqlardan üstün olan milli təhlükəsizlik, ictimai asayiş, cinayət əməllərinin təqibi və s. ilə bağlı olan maraqlar, eləcə də bəzi şəxsi maraqlar (məsələn, tibbi göstərişlər üzündən) daxil edilə bilər. Bütün azadolmalar və məhdudlaşdırma tədbirləri demokratik cəmiyyətdə zəruri və qarşısına qoyduğu məqsədə mütənasib olmalıdır.

İkincisi, məlumat subyektlərinin öz fərdi məlumatlarına düzəliş etmə, onları silmə və gizləmə hüququ vardır.

B/ Fərdi məlumatlara düzəliş etmə, onları silmə və gizləmə hüququ

AİHM bir sıra işlərdə, ərizəçi gizli qeydiyyat sənədlərində saxlanılan məlumatların dəqiqliyini mübahisələndirmək məqsədi ilə onlara çıxış əldə edə bilmədiyi hallarda AİHK-nin 8-ci Maddəsinin pozuntusunu aşkar etmişdir (AİHM, Rotaru Rumıniyaya qarşı (Rotaru v. Romania), yuxarıda sitat gətirilib)

Misal: Siubotaru Moldovaya qarşı işində (AİHM, (Ciubotaru v. Moldavia, n° 27138/04, 27 aprel 2010-cu il, (51) (59)), ərizəçi rəsmi sənədlərdə etnik mənşəyini dəyişərək moldovalı deyil, rumıniyalı olaraq göstərmək istəmiş, lakin buna nail ola bilməmişdi. İddia edildiyinə görə, buna səbəb onun öz müraciətini əsaslandırma bilməməsi olmuşdu. AİHM dövlətlərin etnik mənşə ilə bağlı məlumatları qeydiyyatda aldıkları zaman şəxsin etnik kimliyi ilə bağlı obyektiv sübutlar tələb etməsini qəbul edilən hesab etmişdi. Belə bir müraciət, sırf subyektiv və əsaslandırılmamış səbəblərə söykəndikdə, dövlət orqanları bundan imtina edə bilərlər. Lakin, ərizəçinin müraciəti onun öz etnik mənşəyi ilə bağlı malik olduğu subyektiv baxışlarla bağlı sadə bir səbəb deyildi; o, rumın etnik mənşəyi ilə obyektiv və yoxlanıla bilən əsaslarla məsələn, dil, ad, rəğbət və s. ilə bağlı olduğunu iddia edirdi. Buna baxmayaraq, milli qanunvericiliyə əsasən ərizəçidən onun valideynlərinin rumin etnik mənşəyinə malik olduqlarına dair sübut gətirməsi tələb olunurdu. Moldovada mövcud olan tarixi reallıqları nəzərə alıqda, belə bir tələb aşılması mümkün olmayan maneə təşkil edirdi və onun etnik mənşəyinin, sovet dövlət orqanları tərəfindən onun valideynlərinin etnik mənşəyi ilə bağlı aparılmış qeydiyyatda göstərilən etnik mənşədən fərqli olmasını mümkün edirdi. Ərizəçinin təqdim etdiyi yoxlanıla bilən obyektiv sübutların yoxlanılmasını təmin etməməklə Dövlət ərizəçinin şəxsi həyatına hörmətlə bağlı pozitiv öhdəliyini yerinə yetirməmişdi. Bununla da, AİHM Avropa İnsan Hüquqları Konvensiyasının 8-ci Maddəsinin pozuntusunu aşkar etmişdi.

Məlumat subyektləri həmçinin nəzarətçilər tərəfindən üçüncü tərəflərə məlumatın istənilən gizlənməsi, düzəldilməsi və ya silinməsi ilə bağlı göndərilən bildirişləri də əldə etmək hüququna (əgər onlar bu əməliyyatları ilə bağlı əvvəlcədən məlumat alıblarsa) da malikdirlər.

Bu yaxınlarda Aİ Cinayət Məhkəməsi Məlumatların Mühafizəsinə dair Direktivin ərazi üzrə tətbiqinin interpretasiyasının əhatə dairəsini genişləndirərək, onu artıq unudulmuş bir hüquqa da şamil edib (Google İspaniya işi (CJEU [GC], Google Spain SI and Google Inv. V. Agencia Española de Protección de Datos and Mario Costeja González, aff. C-131/12, 13 may 2014-cü il). İnternet axtarış motorları, istifadəçilərin müraciəti əsasında, onların adı ilə bağlı axtarışdan sonra

çıxan nəticələri siyahıdan silməlidirlər. Aİ Cinayət Məhkəməsi unudulmuş bu hüquqdan istifadə edilməsini bir sıra təminatlarla çərçivələndirir ki, həmin təminatlar da bu yeni “hüququ” digər fundamental hüquqlarla uzlaşdırır.

Hər şeydən əvvəl, Məhkəmə məlumatın dəqiq olmaması, köhnəməsi və ya zəruri olan müddətdən çox saxlanması ilə bağlı olaraq onun silinməsinə icazə verən qanunu nəzərdən keçirir (Aİ CM, Google İspaniya, yuxarıda sitat gətirilib, 92-ci bənd). İkincisi, AİCM xüsusi hallar, məsələn, şəxsin ictimai sahədə xüsusi rol oynaması, onun əsas hüquqlarına müdaxilənin ictimaiyyətin həmin məlumatlara çıxış əldə edilməsi ilə bağlı malik olduğu yüksək maraqlarla əsaslandırılması kimi hallarda, məlumat subyektinin həmin məlumatları silmə hüququna malik olub-olmamasını nəzərdən keçirir (AİCM, Google İspaniya, yuxarıda sitat gətirilib, maddə 97).

C/ Etiraz etmə hüququ

❖ Məlumat subyektinin xüsusi vəziyyətinə görə etiraz etmə hüququ

Məlumat subyektlərinin onlara aid məlumatların işlənilməsinə qarşı etiraz etməsi üçün ümumi hüquq nəzərdə tutulmayıb (AİHM, M.S. İsveçə qarşı (M.S. v. Sweden, n° 20837/92), 27 avqust 1997-ci il, həmin işdə tibbi məlumatlar razılıq və ya etiraz etmə imkanı olmadan ötürülmüşdü (kommunikasiya edilmişdi); AİHM, Leander İsveçə qarşı (Leander v. Sweden), yuxarıda qeyd olunub; və ya AİHM, Mosley Birləşmiş Krallığa qarşı (Mosley v. United Kingdom, n° 48009/08, 10 may 2011-ci il).

Məlumatların mühafizəsinə dair bu prinsiplərin və qaydaların hamısı, eləcə də, məlumat subyektlərinin hüquqları, kontekstdən kənar nəzərdən keçirilməməlidir: bəzi hallarda fərdi məlumatların mühafizəsi hüququ və digər fundamental hüquqlar arasında tarazlaşdırma testinin aparılması zəruridir.

IV. Hüquqların tarazlaşdırılması

AİHM sistemində məlumatların mühafizəsi 8-ci Maddəyə əsasən (şəxsi və ailə həyatına hörmət hüququ) təmin edilir, **Xartiya sistemində** isə bu hüquq, rəqabət təşkil edən digər hüquqların əhatə dairəsinə hörmət bəsləməklə tətbiq edilməlidir. AİHK-in 8 (2) Maddəsinə əsasən “[...] ya digər şəxslərin hüquq və azadlıqlarını müdafiə etmək üçün qanunla nəzərdə tutulmuş və demokratik cəmiyyətdə zəruri olan hallar istisna olmaqla, dövlət hakimiyyəti orqanları tərəfindən bu hüququn həyata keçirilməsinə mane olmağa yol verilmir”.

Həm AİHM, həm də AİCM müvafiq olaraq dəfələrlə müəyyən etmişdirlər ki, AİHK-nin 8-ci Maddəsinə və Xartiyanın 8-ci Maddəsinə şərh və tətbiq edərəkən hüquqlar arasında tarazlıq yaradılması zəruridir (AİHM, fon Hannover Almaniya qarşı (Von Hannover v. Germany (n° 2) [GC], n° 40660/08 et 60641/08), 7 fevral 2012-ci il ; AİCM, birləşdirilmiş işlər Milli Kredit Qurumlarının Birliyi (ASNEF) və Ticarət və Marketing Federasiyası Dövlət İdarəetməsinə qarşı (Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) və Federación de Comercio Electrónico y Marketing Directo (FECEDM) v. Administración del Estado), yuxarıda qeyd olunub, Maddə 48 ; CJEU, C-275/06, İspaniya Musiqi İstehsalçıları İspaniya Telefonikaya qarşı (Productores de Música de España (Promusicae) v. Telefónica de España SAU), 29 yanvar 2008-ci il, Maddə 68.).

Tarazlığı nümayiş etdirmək üçün aşkar edilə bilən bir neçə simvolik nümunə vardır. Birinci nümunə məlumatların mühafizəsi hüququ ilə ifadə azadlığı arasında tarazlıq yaradılması ilə bağlıdır.

A/ İfadə azadlığı

Məlumatın mühafizəsi hüququ ilə tarazlaşdırılmalı olan hüquqlardan biri ifadə azadlığı hüququdur. Hər iki hüququn əhəmiyyətini nəzərə alaraq AİHM bir neçə istiqamətləndirici qərar qəbul etmişdir.

Misal: Aksel Stringer Almaniyaya qarşı işində (AİHM, Axel Springer AG v. Germany [GC], n° 39954/08), 7 fevral 2012-ci il, 90 və 91-ci Maddələr), AİHM müəyyən etmişdir ki, milli məhkəmə tərəfindən məşhur aktyorun həbs və məhkum edilməsi ilə bağlı məlumat dərc etmək istəyən qəzetin sahibinə tətbiq edilən qadağa, AİHK-nin 10-cu Maddəsinin pozuntusuna səbəb olmuşdur. AİHM onun presedent hüququnda ifadə azadlığı və ailə və şəxsi həyata hörmət hüququ arasında tarazlıq yaradılması ilə bağlı müəyyən edilmiş meyarları təkrarən vurğulamışdır. Aşağıdakı suallar verilmişdir:

- . Birincisi, məqalədə bəhs edilən hadisə ümumi ictimai maraq kəsb edirdimi? Şəxsin həbs və məhkum edilməsi ictimai marağa səbəb olan məhkəmə faktı idi və buna görə də, ictimai maraq kəsb edirdi;
- . İkincisi, sözügedən şəxs ictimai xadim idimi? Sözügedən şəxs ictimai xadim kimi qiymətləndirilə bilmək üçün kifayət qədər məşhur olan aktyor idi; və
- . Üçüncüsü, məlumat necə əldə edilmişdi və etibarlı idimi? Məlumat prokurorluqdan alınmışdı və tərəflərdən heç biri hər iki məqalədə qeyd olunan məlumatların səhihliyi ilə bağlı mübahisə qaldırmamışdı.

Buna müvafiq olaraq, AİHM belə qərara gəlmişdi ki, şirkətin üzərinə nəşr ilə bağlı qoyulan məhdudiyətlər aktyorun şəxsi həyatını qorumaqla bağlı legitim məqsədə mütənəsib olmamışdır və beləliklə də, AİHK-nin 10-cu Maddəsinin pozuntusunu aşkar etmişdi.

Misal: Fon Hannover Almaniyaya qarşı işində (n° 2) (yuxarıda sitat gətirilib, 118 və 124-cü Maddələr), AİHM Monako Şəhzadəsi Karolina və onun həyat yoldaşının xizək tətili zamanı çəkilmiş şəkillərinin dərc edilməsi ilə bağlı AİHK-nin 8-ci Maddəsinə əsasən şəxsi ailə həyatı hüququnun pozulduğunu aşkar etməmişdi. Fotoşəkil məqalə ilə müşayiət olunmuşdu ki, orada da digər məsələlərlə yanaşı, şəhzadə Reynerin pisləşməkdə olan səhhətindən bəhs edilirdi. AİHM belə nəticəyə gəlmişdir ki, milli məhkəmələr nəşriyyat şirkətinin söz azadlığı hüququ və və ərizəçilərin şəxsi həyat hüququ arasında tarazlıq testi tətbiq ediblər. Milli məhkəmələr tərəfindən Şəhzadə Reynerin xəstəliyinin “müasir cəmiyyətdə baş verən hadisə” kimi qiymətləndirilməsi əqlabatan hesab etmək olar və buna görə də, AİHM belə nəticəyə gəlmişdi ki, dərc edilən fotoşəkil onu müşayiət edən məqalə ilə birlikdə ümumi maraq kəsb edən məsələ ilə bağlı debatlarla müəyyən mənada töhfə vermişdi. AİHM bununla da, AİHK-nin 8-ci Maddəsinin pozuntusunu aşkar etməmişdi.

Avropa İnsan Hüquqları Məhkəməsinin presedent hüququnda maraqlar arasında tarazlıq yaradılması məqsədi ilə istifadə edilən meyarlardan biri də ifadə azadlığından istifadə edilməsinin ümumi maraq kəsb edən debata töhfə verib-vermədiyini müəyyən etməkdən ibarətdir (Fon Hannover Almaniyaya qarşı (n° 2) (yuxarıda sitat gətirilib, 118 və 124-cü Maddələr.).

Misal: Mosey Birləşmiş Krallığa qarşı işində (yuxarıda qeyd olunub, 129 və 130-cu Maddələr) ölkə miqyasında dərc edilən həftəlik jurnal, ərizəçinin intim fotosəkillərini dərc etmişdi. Ərizəçi AİHK-nin 8-ci Maddəsinin pozuntusu baş verdiyini iddia etmişdi, belə ki, həmin qəzetin dərc etdiyi materialın hər hansı bir şəxsin şəxsi həyat hüququnu poza biləcəyi ehtimalı olduğu zaman həmin şəxsə bildiriş göndərmək öhdəliyi olmadığına görə o (ərizəçi), məlumatların dərc edilməsinə qadağa qoyulmasını tələb edə bilməmişdi. Hətta bu səpgidən olan məlumatın maarifləndirmə deyil, əyləndirmə məqsədi ilə yayılması baş verdikdə belə, yenə də şübhəsiz ki, o, AİHK-nin 10-cu Maddəsindən bəhrələnmə bilər, bu şərtlə ki, şəxsi və intim xarakterli məlumatların yayılması heç bir ictimai maraq kəsb etmədiyi hallarda AİHK-nin 8-ci Maddəsinin tələbləri ilə tarazlaşdırılmış olsun. Lakin, nəşrdən əvvəl tətbiq edilən və senzura formasında istifadə edilən bilən məhdudiyətlərə xüsusi diqqətlə yanaşmaq lazımdır. Əvvəlcədən bildiriş göndərmənin malik ola biləcəyi çəkindirici təsiri, belə təsirin effektivliyi ilə bağlı şübhələri və bu sahədə mövcud olan geniş mülahizə sərbəstliyini nəzərə alaraq AİHM belə qərar gəlmişdi ki, 8-ci Maddə əvvəlcədən bildiriş göndərməklə bağlı hüquqi öhdəlik yaratmır. Nəticədə, AİHM 8-ci Maddənin pozuntusunu aşkar etməmişdi.

Misal: Biriuk Litvaya qarşı işində (AİHM, (Biriuk v. Lithuania, n° 23373/03), 25 noyabr 2008-ci il.) ərizəçi onun HIV xəstəsi olduğuna dair məqalə nəşr edən gündəlik qəzetin onun hüquqlarını pozduğunu iddia etmişdi. Bu məlumat aşkar şəkildə yerli xəstəxananın səhiyyə işçiləri tərəfindən verilmişdi. AİHM belə qənaətə gəlmişdi ki, sözügedən məqalə ümumi maraq kəsb edən debata heç bir töhfə verməmişdi və təkrarən vurğulanmışdı ki, yalnız tibbi məlumatların deyil, bütövlükdə şəxsi məlumatların mühafizəsi AİHK-nin 8-ci Maddəsində təsbit edilmiş şəxsi və ailə həyatına hörmət hüququnun zəruri elementini təşkil edir. AİHM belə bir fakta xüsusi əhəmiyyət vermişdir ki, qəzetə görə yerli xəstəxananın əməkdaşları tibbi məlumatların məxfi saxlanması ilə bağlı peşə öhdəliklərini pozaraq ərizəçinin HIV virusuna yoluxması ilə bağlı məlumatı açıqlamışdılar. Nəticədə, Dövlət ərizəçinin şəxsi və ailə həyatına hörmət hüququnu təmin etməklə bağlı öhdəliyini yerinə yetirməmişdir. AİHM bununla da 8-ci Maddənin pozuntusunu aşkar etmişdi.

Tarazlıq həmçinin məlumat subyektlərinin müdafiəsi və üçüncü tərəflərin məlumat əldə etmək hüququ arasında yaradılmalıdır.

B/ Sənədlərə çıxış əldə etmək hüququ

Xartianın 11-ci Maddəsində və AİHK-nin 10-cu Maddəsində nəzərdə tutulan informasiya azadlığı hüququ yalnız məlumatı ötürmək hüququnu deyil, məlumatı almaq hüququnu da müdafiə edir. Demokratik cəmiyyətin mövcud olması üçün hökumətin şəffaf olmasının nə dərəcədə zəruri olduğunun başa düşülməsi getdikcə artır. Dövlət qurumlarının əlində olan məlumatlara çıxış hüququ, bütün Avropa vətəndaşlarının və Üzv Dövlətlərdə yaşayan və ya qeydiyyatda olan bütün fiziki və hüquqi şəxslərin mühüm hüququ kimi qəbul edilmişdir.

AŞ qanunvericilində biz, Nazirlər Komitəsinin dövlət sənədlərinə çıxış ilə bağlı (2002) 2 sayılı 21 fevral 2002-ci il tarixli Tövsiyəsində təsbit edilmiş prinsiplərə istinad edə bilərik.

Misal: Tarsasaq a Szabadsaqyoqokert Macarıstana qarşı işində (AİHM, Társaság a Szabadságjogokért v. Hungary, n° 37374/05), 14 aprel 2009-cu il, bax 27, 36, 37 və 38-ci Maddələr) ərizəçi - insan hüquqlarının müdafiəsi ilə məşğul olan QHT Konstitusiya

Məhkəməsinə müraciət edərək onların icraatında olan bir işlə bağlı məlumata çıxış əldə etmək istəmişdi. Konstitusiyaya Məhkəməsi həmin işi qaldırmış parlament üzvü ilə məsləhətləşmədən bundan imtina etmişdi və cavabını bununla əsaslandırılmışdı ki, Konstitusiyaya Məhkəməsinin icraatında olan işlərə dair məlumat şikayətçinin razılığı olmadan üçüncü tərəflərə ötürülə bilməz. Milli məhkəmələr imtina ilə bağlı bu qərarı qüvvədə saxlayaraq onu əsas gətirmişdilər ki, belə fərdi məlumatın mühafizəsi başqalarının ictimai (dövlət) məlumatlara çıxış əldə etmək hüququ tərəfindən inkar edilə bilməz (başqalarının dövlətin əlində olan məlumatlara çıxış əldə etmək hüququ bu hüquqdan üstün sayıla bilməz). Ərizəçi ictimai nəzarətçi rolunu oynayır və buna görə də onun hüquqları mətbuata verilən hüquqlara bərabər idi. AİHM mətbuatın azadlığı ilə bağlı olan məsələlərdə ardıcıl olaraq belə mövqə sərgiləmişdir ki, ictimaiyyətin ümumi maraq kəsb edən məsələlərlə bağlı məlumat əldə etmək hüququ vardır. Ərizəçinin əldə etmək istədiyi məlumat hazır və mövcud idi və məlumat toplanmasını heç bir şəkildə tələb etmədi. Belə olan şəraitdə, Dövlətin ərizəçiyə lazım olan məlumatın axışını təmin etmək öhdəliyi var idi. Bütövlükdə Məhkəmə hesab etmişdi ki, ictimai maraq kəsb edən məlumatlara çıxışa maneə törədilməsi mətbuatda və ya bənzər sahələrdə işləyənləri ictimai nəzarətçi olmaq kimi zəruri funksiyaları yerinə yetirməkdən çəkindirə və ya həvəsdən sala bilər. Bununla da AİHM 10-cu Maddənin pozuntusunu aşkar etmişdi.

Simvol xarakteri daşıyan son misal xüsusilə əhəmiyyətlidir və bu yaxınlarda baş vermiş hadisələrin fonunda, xüsusilə əhəmiyyət kəsb edən mövzuya çevrilmişdir. Bu fərdi məlumatların mühafizəsi ilə milli təhlükəsizlik məsələləri arasında tarazlığın yaradılmasıdır.

C/ Milli Təhlükəsizlik

Milli təhlükəsizlik zərurəti və şəxsi həyatın gizliliyi və fərdi məlumatların mühafizəsi arasında tarazlığın müəyyən edilməsi hal-hazırda, xüsusilə Edvard Snoudenin açıqlamalarından sonra bir çox debatların ana xəttini təşkil etməyə başlamışdır.

Buna cavab olaraq Avropa, Amerika şirkətlərinin avropalı istehlakçılarla aid olan fərdi məlumatların ötürülməsi ilə bağlı məhkəmə qərarlarına əməl etməzdən əvvəl İttifaqın dövlət qurumlarına məlumat verməyi tələb etmək arzusunda olduğunu ifadə edir (ABŞ Milli Təhlükəsizlik Agentliyinin (NSA) müxtəlif Üzv Dövlətlərdə müşahidə proqramı, müşahidə aparıcı qurumlar, onların Aİ vətəndaşlarının fundamental hüquqlarına təsiri və Ədliyyə və Daxili İşlər sahəsində transatlantik əməkdaşlıqla bağlı hesabat (2013/2188(INI)).

Parlament Assambleyasının Hüquqi Məsələlər və İnsan Hüquqları Komitəsi tərəfindən 21 aprel 2015-ci ildə qəbul edilmiş “Kütləvi Nəzarət” (AS/Jur (2015) 01) hesabatı kütləvi müşahidə aparılmasının nöqsanlarını qeyd edir. Burada müəyyən kəşfiyyat xidmətləri tərəfindən heç bir terrorist fəaliyyətində iştirak etməyən və milli təhlükəsizlik üçün heç bir təhdid törətməyən insanlara qarşı kibernetik hücumlar həyata keçirildiyi barədə məlumat verilir. Həmin hücumlar zamanı, əsasən, həmin şəxslərin Anonymous fəalları tərəfindən aparılan forum müzakirələrində iştiraka çıxışı kəsilmişdi. Bundan əlavə, bəzi insanların izlənməsinə səbəb, yalnız həmin agentliklərin öz məktublaşmalarını (kommunikasiyalarını) gizli tutmaq məqsədilə təhlükəsiz server proqramından istifadə etmək istəməsi, digərlərinin casusluq fəaliyyətinə məruz qalmasına səbəb isə onların siyasətçi, diplomat, jurnalist, hüquqşünas və ya insan hüquqları sahəsində fəal kimi fəaliyyət göstərməsi olmuşdur (AŞPA hesabatı § 43, 47, 53 və 60). Son olaraq, müəyyən Avropa Dövlətləri, digər kəşfiyyat qurumları ilə əməkdaşlıq şəraitində özlərinin, əslində

yurisdiksiyalarında olan insanları qorumaq məqsədi daşıyan qanunlarından və məhdudiyyətlərindən yan keçirlər (AŞPA hesabatının 30-37-ci maddələri).

Terrorizmə qarşı mübarizə nə qədər çox əhəmiyyət kəsb etsə də, şəxsi həyatın gizliliyinə hörmətlə bağlı təminatlara əməl edilməlidir. Terrorist təhdidi ilə üzləşsələr belə, “Dövlətlərin öz yurisdiksiyalarında olan şəxsləri gizli izləməyə məruz qoymaqla bağlı qeyri-məhdud diskresion hüququ yoxdur” (AİHM, Klass və başqaları Almaniyaya qarşı, n°5029/71, 6 sentyabr 1979-cu il, 48-49-cu bəndlər).

Nəticədə AŞ qanunvericiliyində 108 saylı Konvensiyanın təsir dairəsi fərdi məlumatların mühafizəsindən kənara çıxaraq metadata adlanan, şəxsin hərəkətləri və birləşmə fəaliyyəti ilə bağlı şəxsi və olduqca dəqiq olan və xüsusilə, smartfonlarda aşkar edilən məlumatları da əhatə etməyə başlamışdır (108 saylı Konvensiyanın 2-ci Maddəsi).

AİHM terrorizm və mütəşəkkil cinayət kimi təhdidlərə qarşı mübarizədə izləmə aparılmasına ehtiyac olduğunu qəbul etsə də, hakimiyyətdən (səlahiyyətdən) sui-istifadə hallarına yol verməmək üçün qanunvericilikdə nəzərdə tutulmuş minimal təminatlara əməl etmək zəruri olduğunu qeyd edir. Belə ki, “...[...]icraedici orqan öz səlahiyyətlərini gizli surətdə icra etdikdə, özbaşınalıq baş verməsi riski artır” (AİHM, Segerstedt-Viberq və başqaları İsveçə qarşı (Segerstedt-Wiberg and others v. Sweden, n° 62332/00), 6 sentyabr 2006-cı il, 76-cı maddə).

Beləliklə, qanunda görülməsi ehtimal edilən tədbirlərin xarakteri, əhatə dairəsi və müddəti kifayət qədər nəzərdə tutulmalı, onları əmr etmək üçün mövcud olması tələb olunan əsaslar, onlara icazə verməli, icrasını yerinə yetirməli və icrası üzərində nəzarəti həyata keçirməli olan qurumlar və milli qanunvericilikdə nəzərdə tutulmuş müdafiə vasitələri aydın şəkildə müəyyən edilməlidir (AİHM, Şimovolos Rusiyaya qarşı (Shimovolos v. Russia, n°30194/09), 28 noyabr 2011-ci il, 68-ci Maddə; icraatda olan iş Biq Brozer Uotç və başqaları Birləşmiş Krallığa qarşı (Big Brother Watch and others v. United Kingdom), n°58170/13 sayılı müraciət).

Öz qiymətləndirməsi zamanı AİHM nəzarət orqanlarının fəaliyyətini, onların izləmənin aparılması ilə bağlı məsuliyyət daşıyan orqanlardan həqiqətən asılı olmadığını və onların effektiv və davamlı nəzarət aparmaqla bağlı yetərli səlahiyyətə malik olduğunu müəyyən etmək məqsədi ilə müşahidə etmişdir (AİHM, Şimovolos Rusiyaya qarşı (Shimovolos v. Russia), yuxarıda qeyd edilib ; AİHM, Klass və başqaları Almaniyaya qarşı (Klass and others v. Germany, 48-49-cu maddələr).

Beləliklə, Avropa Şurası Parlament Assambleyasına görə, qanunvericilik bazasının effektiv icrasına nail olmaq və şəxsi həyatın gizliliyi hüququnu müdafiə etməyin yeganə yolu kəşfiyyat xidmətlərini adekvat məhkəmə nəzarətinə, inzibati nəzarətə və ya parlament nəzarətinə tabe etməkdən ibarətdir. Bu o deməkdir ki, nəzarət qurumlarının müvafiq məlumatlara çıxışı olması üçün izləmə sistemlərinin şəffaflığı təmin edilməlidir (AŞPA hesabatının 96 və 114-cü maddələri).

Hal-hazırda Fransa kütləvi izləmə (müşahidə) ilə bağlı qanunvericilik bazası qəbul etmək ərəfəsindədir. Kəşfiyyat (gizli xidmətlər) ilə bağlı bu qanunvericilik layihəsinin məqsədi prosedur müəyyən etməkdən ibarətdir ki, həmin prosedura əsasən kəşfiyyat qurumları rəsmi şəkildə geniş miqyaslı müşahidə tədbirləri keçirə, danışıqları dinləyə və ya məlumatları saxlaya bilsinlər. Bu qanun layihəsi bu səbəbdən mübahisələndirilir ki, ona əsasən müəyyən edilən

prosedurların hakimin deyil, Baş Nazirin qərarından asılı olması planlaşdırılır. Bundan əlavə, müşahidəni aparmaq üçün məqsədlər siyahısı sadəcə terrorizmlə bağlı məsələlərdən ibarət olmayacaq və Fransanın müdafiə və elmi maraqlarının müdafiəsi, ictimai asayişin pozulmasına səbəb ola biləcək kütləvi zorakılıq halları və ya mütəşəkkil cinayətkarlıqla bağlı məsələlər də buraya daxil ediləcəkdir.

Lakin, fərdi məlumatların toplanmasına yalnız sözügedən şəxsin icazəsi olduğu hallarda və ya müstəsna olaraq, hədəfin cinayət əməlinə iştirakı ilə bağlı şübhələr mövcud olduqda məhkəmə tərəfindən verilmiş əmr əsasında icazə verilməlidir.

Parlament Assambleyasının hesabatı həmçinin Üzv Dövlətlərin təcili surətdə öz qanunvericiliklərinə dəyişiklik edərək onların Konvensiyaya uyğun olmasını təmin etməsinin zəruri olduğunu təkrarən vurğulayır. Bundan əlavə, Parlament Assambleyası “kəşfiyyat məəcəlləsinin” yaradılmasını dəstəkləyir ki, onun da məqsədi bütün Dövlətlərin razılışma əsasında əməl edəcəyi ümumi standartları yaratmaqdan ibarətdir (Tövsiyə Layihəsi, § 2.2). Nəticədə, Avropanın kəşfiyyat qurumları arasında terrorizm və mütəşəkkil cinayətkarlığa qarşı mübarizə və fərdi məlumatların mübadiləsi sahəsində mövcud olan əməkdaşlıq ümumi hüquqi çərçivə əsasında həyata keçirilər. Bununla da, izləmədən siyasi və ya iqtisadi məqsədlər üçün istifadə edilməsinin qarşısı alınmış olar.

Bu təqdimatın yekun hissəsinə keçməzdən əvvəl məlumat subyektlərinin ixtiyarında olan hüquqi vasitələri qeyd etmək vacibdir.

V. Fərdi məlumatlardan istifadə üzərində nəzarət və tətbiq edilən sanksiyalar

Ümumilikdə, hüquqda nəzərdə tutulmuş qaydaların effektivliyi və xüsusilə də, sözügedən şəxslərin hüquqlarının qorunması, geniş mənada, onların tətbiqi ilə bağlı mexanizmlərin mövcudluğundan asılıdır. Məlumatların mühafizəsinə dair Avropa qanunvericiliyinə əsasən, milli qanunvericilik, məlumat subyektlərinin, onlara məxsus olan məlumatları qoruya bilməsi üçün vasitələr təmin etməlidir.

Buna müvafiq olaraq, milli qanunvericiliyə əsasən məlumat subyektlərinə öz hüquqlarından istifadə etmək və məlumatların işlənməsinə nəzarət etmək ilə bağlı köməklik göstərmək məqsədi ilə müstəqil nəzarət qurumları yaradılmalıdır.

A/ Müstəqil nəzarət

AŞ qanunvericiliyində, 108 sayılı Konvensiyaya edilən Əlavə Protokol nəzarət qurumlarının yaradılmasının məcburi olduğunu nəzərdə tutmuşdur. Bu sənədin 1-ci Maddəsində müstəqil nəzarət qurumlarının yaradılması ilə bağlı hüquqi çərçivə təsbit edilmişdir ki, Müqaviləyə Qoşulan Tərəflər onu milli qanunvericiliklərinə daxil etməlidirlər.

Əlavə protokol həmin qurumların vəzifə və səlahiyyətlərini təsvir etmək üçün Məlumatların Mühafizəsinə dair Direktivdə istifadə edilən ifadələrə bənzər ifadələrdən istifadə edir. Buna

müvafiq olaraq, prinsip etibarı ilə nəzarət qurumları Aİ və AŞ qanunvericiliyinə əsasən eyni tərzdə fəaliyyət göstərməlidirlər.

Aİ qanunvericiliyinə əsasən, məlumatların mühafizəsini həyata keçirən qurumların müstəqilliyi Avropa İttifaqının Fəaliyyətinə dair Sazişin (TFEU) 16 (2) Maddəsi və Xartiyanın 8 (3) Maddəsi ilə təmin edilir. Xüsusilə bu sonuncu müddəə, müstəqil qurum tərəfindən həyata keçirilən nəzarəti məlumatın mühafizəsi ilə bağlı fundamental hüququn zəruri elementi kimi şərh edir.

Avropa Komissiyası Macarıstana qarşı işində (CJEU, C-288/12, European Commission v. Hungary, 8 aprel 2014-cü il, 50 və 67-ci Maddələr), Aİ Cinayət Məhkəməsi (CJEU) qeyd etmişdir ki, “hər bir nəzarət qurumunun ona həvalə edilən vəzifələri tam müstəqil şəkildə icra etmək imkanına malik olmasını təmin etmək öhdəliyi Üzv Dövlətlərin, həmin qurumun fəaliyyətini həyata keçirmək üçün şərait yaradılması ilə bağlı öhdəlik daşımalarını nəzərdə tutur”.

Fərdi məlumatların işlənilməsi üzərində nəzarəti həyata keçirmək məqsədi ilə müstəqil nəzarət qurumlarının yaradılmasının ən yüksək mərtəbəsində dayanan və AİHK və Xartiya tərəfindən təmin edilən səmərəli hüquqi vasitələrdən istifadə hüququ milli qanunvericilikdə hər kəsin istifadə edə biləcəyi səmərəli hüquqi vasitələrin nəzərdə tutulmasını tələb edir.

B/ Hüquqi vasitələr və sanksiyalar

❖ Nəzarətçiyə müraciətlər

Sənədləri əldə etmək hüququ və etiraz etmək hüququ nəzarətçi ilə qarşı-qarşıya həyata keçirilməlidir. Milli nəzarət qurumu və ya məhkəməyə edilən müraciət qəbul edilməz hesab olunacaqdır.

Müraciətə cavab verməzdən əvvəl nəzarətçi qismində müraciət edilmiş qurum, müraciət edənin kimliyini müəyyən etməlidir ki, həmin şəxsin doğrudan da iddia etdiyi şəxs olduğundan əmin olsun və bununla da, məxfilik prinsipinin pozulmasına yol verilməsin.

Əgər bir şəxsə, müəssisəyə və quruma nəzarətçi qismində müraciət edilibsə və həmin qurum nəzarətçi olduğunu inkar etmirsə, bu zaman o (qurum), milli qanunvericilikdə nəzərdə tutulmuş çərçivəyə əsasən aşağıdakıları etməlidir:

- Müraciəti qəbul etməli və müraciət göndərən şəxsə müraciətinin qəbul edildiyinə dair bildiriş göndərməlidir; və ya
- Müraciətin hansı səbəblərdən qəbul edilmədiyini müraciət göndərən şəxsə bildirməlidir.

❖ Nəzarət qurumlarına göndərilən iddialar

Nəzarətçiyə müraciət göndərən, müraciətinə mənfi cavab verilən və ya vaxtlı-vaxtında qənaətbəxş cavab ala bilməyən hər bir şəxs, kömək əldə etmək məqsədilə məlumatların mühafizəsi üzrə milli nəzarət qurumuna tələb ilə müraciət edə bilər.

Milli nəzarət qurumlarında qaldırılmış işlərin nəticələrinin hüquqi səmərəsi milli qanunvericilikdən asılı olacaqdır: qurumun qərarı hüquqi cəhətdən icra edilə bilərmi, yəni, onların icrası rəsmi qurum tərəfindən həyata keçirilməlidirmi yoxsa nəzarətçi, nəzarətçi qurum

tərəfindən çıxarılan qərarın (rəyin, tövsiyənin) icrasını təmin etmədikdə məhkəməyə müraciət etmək lazımdır?

Milli nəzarət qurumları tərəfindən çıxarılan qərarlardan məhkəməyə şikayət vermək imkanı mövcud olmalıdır. Bu həm məlumat subyektlərinə, həm də nəzarətçilərə şamil edilir, belə ki, nəzarət qurumları qarşısında qaldırılan işlərdə onlar tərəflərdən birini təşkil edirlər.

❖ Məhkəməyə verilmiş şikayətlər

AŞ qanunvericiliyində, AİHK-a Qoşulmuş Dövlətdə milli səviyyədə baş verdiyi iddia edilən və eyni zamanda AİHK-in 8-ci maddəsinin pozuntusunu təşkil edən məlumatların mühafizəsi hüququnun pozuntuları ilə bağlı əlavə olaraq və ölkədaxili hüquqi vasitələri tükətmək və digər qəbuledilənlik meyarlarına əməl etmək şərti ilə, Avropa İnsan Hüquqları Məhkəməsinə də şikayət etmək mümkündür (AİHK-in 34 – 37-ci Maddələri).

Baxmayaraq ki, AİHM-ə verilən şikayətlər AİHK-a Qoşulmuş Dövlətlərdən birinə qarşı olmalıdır, onlar dolayısıyla özəl şəxslərin hərəkətləri və ya yol verdikləri nöqsanlarla bağlı da ola bilər, bu şərtlə ki, Üzv Dövlət AİHK-a müvafiq olaraq üzərinə götürdüyü pozitiv öhdəliyə əməl etməyərək öz milli qanunvericiliyində məlumatların mühafizəsinə yetərli hüquqi əsaslar yaratmamış olsun.

Misal: K.U. Finlandiyaya qarşı işində (ECtHR, K.U. v. Finland, yuxarıda qeyd olunub), azyaşlı şəxs olan ərizəçi şikayət etmişdi ki, internet tanışlıq səhifəsində onun seksual xarakterli şəkilləri yerləşdirilib. Xidmət provayderi Finlandiya qanunvericiliyində məxfiliklə bağlı nəzərdə tutulmuş müddəaları əsas gətirərək, həmin məlumatı yerləşdirən şəxsin kimliyini açıqlamaqdan imtina etmişdi. Ərizəçi iddia edirdi ki, Finlandiya qanunvericiliyində ərizəçi ilə bağlı ittihamedic materialları internetə yerləşdirən şəxs kimlərinə qarşı tətbiq ediləcək yetərli müdafiə nəzərdə tutulmamışdı. AİHM müəyyən etdi ki, dövlətlərdən yalnız fərdlərin şəxsi həyatına özbaşına müdaxilə etməkdən çəkinmək tələb olunmur; onlar həmçinin, pozitiv öhdəlik daşıya bilərlər ki, “hətta fərdi şəxslər arasında olan münasibətlər sahəsində belə, şəxsi həyat hüququna hörmət bəslənməsini təmin etmək məqsədi ilə tədbirlər görsünlər”. Ərizəçinin işində onun praktiki və effektiv müdafiəsi əməli törədən şəxsiyyətinin müəyyən edilməsini və onun ittiham edilməsini tələb edirdi. Buna baxmayaraq, dövlət belə müdafiəni təmin etməmişdi və bununla da, AİHM Avropa İnsan hüquqları Konvensiyasının 8-ci Maddəsinin pozuntusunu aşkar etmişdi.

Misal: Köpke Almaniyaya qarşı işində (AİHM, Köpke v. Germany (dec.), yuxarıda qeyd olunub), ərizəçi iş yerində oğurluq hadisəsi törətməkdə ittiham edilirdi və buna görə də gizli kamera müşahidəsinə məruz qalmışdı. AİHM müəyyən etdi ki, bu işdə heç nə dövlət orqanları öz mülahizə sərbəstlikləri çərçivəsində ərizəçinin 8-ci Maddə altında qorunan şəxsi həyata hörmət hüququ və onun işəgötürəninin öz mülkiyyət maraqlarını müdafiə etmək hüququ və ictimaiyyətin ədalət mühakiməsinin düzgün idarə olunmasına olan marağı arasında ədalətli balans yarada bilmədiyinə dəlalət etmir. Buna görə də ərizə qəbuledilməz elan olundu.

AİHM Avropa İnsan Hüquqları Konvensiyasında təsbit olunan hər hansı bir hüququn Tərəf Dövlət tərəfindən pozulduğunu aşkar etdikdə, həmin Tərəf Dövlət AİHM tərəfindən qəbul edilmiş qərarı icra etməlidir. İcra tədbirləri, hər şeydən əvvəl, pozuntuya son qoymalı və mümkün olan dərəcədə, ərizəçi üçün meydana gəmiş mənfi nəticələri aradan qaldırmalıdır. İcra ilə bağlı qərarlar, həmçinin, Məhkəmə tərəfindən aşkar edilmiş pozuntulara bənzər pozuntuların qarşısını

almaq məqsədi ilə ümumi tədbirlərin görülməsini, yəni qanunvericiliyə və ya praktikaya dəyişikliklər edilməsini və ya digər tədbirlər görülməsini tələb edə bilər.

AİHM Avropa İnsan Hüquqları Konvensiyasının pozulduğunu aşkar etdikdə, o (Məhkəmə) AİHK-nın 41-ci Maddəsinə müvafiq olaraq, ərizəçiyə Tərəf Dövlətin hesabına ədalətli əvəz ödənilməsinə təyin edə bilər.

❖ Sanksiyalar

AŞ qanunvericiliyinə əsasən, 108 sayılı Konvensiyanın 10-cu Maddəsi nəzərdə tutur ki, 108 sayılı Konvensiyada nəzərdə tutulmuş məlumatın mühafizəsi prinsiplərinin effektiv təminatını təmin etmək məqsədilə hər bir Tərəf özünün yerli qanunvericiliyinin müddələrinin pozulmasına görə müvafiq sanksiyalar və hüquqi vasitələr nəzərdə tutmalıdır (AİHM, İ Finlandiyaya qarşı işi (I. v. Finland), yuxarıda qeyd olunub; AİHM, K.U. Finlandiyaya qarşı (K.U. v. Finland), yuxarıda qeyd edilib).

Aİ qanunvericiliyinə əsasən, Məlumatların Mühafizəsinə dair Direktivin 24-cü Maddəsində Üzv Dövlətlərin “bu Direktivin müddələrinin icrasını təmin etmək məqsədi ilə müvafiq tədbirlər görməli olduğu və xüsusilə, həmin müddələrin pozulması halında tətbiq edilməsi üçün cəza tədbirləri nəzərdə tutmalı olduqları [...]” qeyd edilib.

Hər iki sənəd Üzv Dövlətlərə müvafiq sanksiyalar və hüquqi vasitələrin müəyyən edilməsində geniş mülahizə sərbəstliyi verir.

Buna baxmayaraq, “*Aİ Üzv Dövlətləri fərdi şəxslərin Aİ qanunvericiliyində nəzərdə tutulmuş hüquqlarının pozulmasına görə hansı tədbirlərin görülməsinin ən məqsədəuyğun olduğunu müəyyən etməkdə mülahizə sərbəstliyinə malik olsalar da, Avropa İttifaqına dair Sazişin 4 (3) Maddəsində təsbit edilən sadıq əməkdaşlıq prinsiplərinə uyğun olaraq effektivlik, ekvivalentlik, mütənasiblik və çəkindiricilik ilə bağlı minimal tələblərə əməl etməlidirlər*”(Avropa İttifaqı Fundamental Hüquqlar üzrə Agentliyinin məlumatların mühafizəsi ilə bağlı islahat paketinə dair 2/2012 sayılı rəyi, Vyana, 1 oktyabr 2012-ci il, səh. 27). AİCM (CJEU) dəfələrlə bildirmişdir ki, milli qanunvericilik sanksiyaların müəyyən edilməsində tam sərbəst deyil.