• развивать фондовый рынок.

Литература:

1.Асаул, А.Н. Экономика недвижимости: Учебник для вузов. 4-е изд., испр / А.Н. Асаул. — М.: АНО ИПЭВ, 2018. — 432 с

2. Бердникова, В.Н. Экономика недвижимости 2-е изд., испр. и доп. учебник и практикум для академического бакалавриата / В.Н. Бердникова. — Люберцы: Юрайт, 2018. — 190 с.

3. https://hcsbk.kz/ru/affordable-housing/bakytty-otbasy/reports/

4. Официальный сайт ГУ «Управление строительства, архитектуры и градостроительства Карагандинской области»- https://oblstroit-krg.gov.kz/ru/

Нугманов М.Г., Айтмолдин Б.А., Казахский гуманитарно-инновационный университет, г.Семей, Юридический факультет, магистранты по специальности «Деловое администрирование»

(Научный руководитель – магистр экономических наук Байгиреева Ж.З.)

АДМИНИСТРАТИВНО- ПРАВОВЫЕ РЕЖИМЫ КОНФИДЕЦИОНАЛЬНОЙ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ

Становление на Западе основ информационного общества, использование информационных технологий в сфере государственного управления позволило в 60 - е годы прошлого века систематизировать и обрабатывать огромный объем персональных данных. Это способствовало повышению оперативности в деятельности исполнительной власти, принятию выверенных стратегических и оперативных решений в экономической, политической, социальной и иных сферах общественной жизни.

Однако формирование сферы *privacy — персональных данных* - в то же время потребовало жесткой правовой регламентации процессов сбора, обмена, хранения, актуализации и уничтожения соответствующей информации. Значимый объем международных источников правового регулирования privacy объясняется трансграничностью потоков персональных данных и востребованностью единого концептуального начала в установлении стандартов формирования и использования privacy, и в первую очередь - в сфере деятельности исполнительной власти. Инициатива в правом регулировании данной сферы принадлежит следующим международным организациям: Организации по Экономическому Сотрудничеству и Развитию (OECD), Евросоюзу, Организации Американских Государств, Сообществу стран Шенгенского соглашения («Шенгенское информационное пространство»), Международной торговой палате.

Концептуальным источником правового регулирования сферы privacy является Конвенция 108 Совета Европы 1981 года о защите частных лиц по отношению к автоматизированной обработке персональных данных. Подписавшие данную Конвенцию государства обязуются *формировать национальные правовые реэюимов персональных данных на основе следующих принципов:* приобретение и обработка персональных данных должны осуществляться честным и законным образом; их хранение и использование должны определяться конкретными целями и не превышать по объему потребности; персональные данные должны быть полными, точными и актуализированными и храниться в формах, позволяющих идентифицировать субъекта персональных данных.

Персональные данные в Конвенции определяются как любая информация, относящаяся к некоему идентифицированному или доступному для идентификации индивидууму (субъекту данных). Такое исключительно широкое определение данного понятия предоставляет государствам - участникам Конвенции возможность свободы определения данного понятия и его структурирования в национальном законодательстве. Для реализации положений Конвенции создан постоянный Консультативный комитет.

Правовые основы режима персональных данных в международном праве включают следующие его составляющие:

- базовые принципы в сфере privacy,
- порядок трансграничного оборота персональных данных,
- защиту персональных данных,

- статус международных органов, осуществляющих выработку единой правовой политики в сфере privacy и ее реализацию.

Защита персональных данных включает такие составляющие, как принципы качества данных (категории базовых, оценочных персональных данных, данных особо чувствительного свойства и соответственно уровни их защиты) и права субъекта данных.

Рассмотрим некоторые *особенности национальных правовых режимов персональных данных.*

Юридические санкции за нарушение режима персональных данных разнообразны. Так, например, в соответствии с законодательством Австрии лишение свободы на срок до 1 года грозит за нарушение конфиденциальности или несанкционированное вмешательство в обработку данных. Нарушение отдельных положений закона Австрии 1978 г. о персональных данных может повлечь штраф до 24175.000 евро. Штраф или лишение свободы сроком до 1 года предусмотрено в качестве уголовной санкции за нарушение режима персональных данных в процессе профессиональной деятельности в Германии. Законодательством Франции[1] предусмотрены более жесткие санкции - тюремное заключение на срок от 1 года до 5 лет или крупный денежный штраф до 2.216.000 евро за нарушение порядка сбора, хранения, распространения, персональных данных. За автоматизированную обработку персональных данных без официального разрешения - тюремное заключение сроком от 6 месяцев до 3 лет и (или) денежный штраф в размере до 216.000 евро. Данные примеры демонстрируют достаточную жесткость режима персональных данных и намерение государства защищать личные права субъектов персональных данных от посягательств на них.

Следует отметить, что основополагающие принципы международного и национального законодательства в сфере защиты персональных данных распространены во многих странах и на корпоративные субъекты права - группы лиц, ассоциации, учреждения, компании, корпорации независимо от наличия или отсутствия у них статуса юридического лица. Этому не препятствуют соответствующие рекомендации Совета Европы, которые реализованы в законодательстве Австралии, Дании, Исландии, Норвегии, Швейцарии, Люксембурга[24^].

В связи с введением в сфере деятельности исполнительной власти электронного государственного управления (el - government) значимым становится *административно — правовое регулирование оборота персональных данных в сети Интернет.* Оно основано на следующих принципах:

1) контролирующий административный орган осуществляет регистрацию деятельности, связанной с оборотом персональных данных, в том числе и в сфере исполнительной власти, согласно Директиве Евросоюза № 97/66.

2) юрисдикция определенного государства в отношении применения юридических санкций за нарушение правового режима персональных данных определяется исходя из «места причинения вреда» и «доступности сайта»; с территории страны юрисдикции контролирующий административный орган осуществляет регистрацию деятельности, связанной с оборотом персональных данных, в том числе и в сфере исполнительной власти,

3) на сайте, содержащем персональные данные, предоставленные органам государственной власти, должна быть размещена информация о правах субъекта персональных данных и ее правовые источники,

4) сайт с содержащимися персональными данными подлежит сертификации на предмет информационной безопасности, на что указывает логотип сертификата (наиболее распространенными являются логотипы «TRAST», «BBOnline),

5) перехват, отслеживание персональных коммуникаций осуществляется административными органами только в целях обороноспособности, безопасности, расследования преступлений, и т.д.,

6) кеширование (промежуточная фиксация) персональных данных, в том числе идентификационных кодов личности, допускается в ходе электронного обмена между исполнительной властью и гражданами только для избежания повторного запроса информации, но не для сбора и после дующей ее обработки[2].

---

[1] Ст. 41 Закона Франции № 78 - 17. Указ. соч. С. 268.

[2] Калятин В. О. Персональные данные в Интернете // Журнал Российского права. 2002. № 5. С. 77.

Таким образом, *правовой режим персональных данных* в зарубежном законодательстве *основан на общих принципах,* зафиксированных в нормах *международного права*, и реализуется на уровне национального законодательства *посредством детальной регламентации:*

прав субъектов персональных данных,

деятельности органов, осуществляющих контрольно - надзорные функции в сфере privacy,

стандартов сбора, обработки, оборота, актуализации и верификации персональных данных,

их защиты как организационно - техническими средствами, так и возможностью применения юридических санкций.

В правовом регулировании сферы персональных данных используются модельные источники права, которые содержат основополагающие принципы, используемые при формировании законодательства в сфере отдельных видов персональных данных[3].

Следует отметить, что в административной сфере зарубежных государств интенсивно используются *средства биометрической идентификации личности,* которые подпадают под статус персональных данных. Защита их ориентирована на международные стандарты, разработкой которых занимается Международная организация стандартизации и Международная электротехническая комиссия. Жесткие требования этих стандартов и являются условиями защиты прав идентифицируемых субъектов[4].

Правовой режим служебной тайны.

Для ряда государств свойственна единая концепция правового регулирования общественных отношений по поводу информации, функционирующей в режиме тайны, в самом обобщенном значении этого слова. Так, присущая российскому законодательству дифференциация информации ограниченного доступа на сведения, функционирующие в режиме государственной тайны, и конфиденциальную информацию, не свойственны Великобритании, США, Албании, Болгарии, Чехии, ряду других стран.

Вторая - информация, вопрос о предоставлении которой населению решается административными органами по собственному усмотрению. Административным органам делегируется право частичного документа, то есть право изъять из документа часть информации и предоставить документ в «урезанном» виде, а также право на информацию об отсутствии данного документа, если он содержит сведения, не подлежащие разглашению. К таковым относятся: сведения, позволяющие идентифицировать человека по фамилии, имени, дате рождения или путем сопоставления с другой информацией, если может иметь место возможность нанесения ущерба его правам и интересам;

Режим конфиденциальной информации, используемой в сфере деятельности исполнительной власти, следует признать достаточно жестким исходя из требований информационной безопасности, которые аналогичны системам защиты военной информации. Это *стандарты информационной безопасности (Evoluation Criteria for IT Security ICO / IEC 15408 - 1,2,3 1999\E),* которые предполагают такие параметры, как широта, глубина, централизация защиты, контроль за распределением информации, кадровая безопасность.

Межгосударственный обмен конфиденциальной информацией в административной сфере на территории Содружества независимых государств регламентируется Соглашением, разработанным Экономическим советом СНГ[5], в рамках данного Соглашения предусмотрено формирование систем электронного сообщения на основе международных стандартов ООН ЭДИФАКТ, защита информационных ресурсов по согласованным сферам деятельности.

Таким образом, правовые режимы конфиденциальной информации, функционирующей в органах исполнительной власти, в международном законодательстве и зарубежном праве отдельных государств имеют следующие общие *закономерности,* которые, по мнению автора настоящего исследования, *должны быть учтены при формировании и совершенствовании законодательства о* конфиденциальной информации в Республике Казахстан.

---

[3] Дашян М. С. О некоторых аспектах правового регулирования отношений в сети Интернет в Канаде // Современное право. 2003. № 8. С. 20.

[4] Задорожный В. В. Современное состояние биометрических технологий // Вопросы защиты информации. 2004. № 1. С. 58.

[5] Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых государств в сфере информатизации от 24 декабря 1999 (для РФ вступило в силу 10 июня 2002) // Бюллетень международных договоров. 2002. № 10.

1. Основой данных режимов являются законы[6], устанавливающие, с одной стороны, правовые основы доступа к открытой информации, наряду с ними - законы, устанавливающие режим «секретной информации» (нормы о разграничении информации на открытую и секретную могут содержаться и в одном законодательном акте). Правовые основания ограничения доступа к информации общедоступны, их целесообразность мотивирована законодателем.

2. Ограничение доступа к данной информации определяется и ее публичной значимостью, и ее значимостью для реализации частных интересов.

3. Защита информации основана на международных и национальных стандартах, обеспечивающих персональную и публичную информационную безопасность субъектов административных отношений, на системе контроля, регистрации, сертификации деятельности по использованию конфиденциальной информации. Наличие данных стандартов является основой для создания и функционирования международного информационного пространства административных органов, способствует полноценному и эффективному международному информационному обмену.

4. Международный обмен конфиденциальной информацией между административными органами ограничивается ее целевым использованием, национальное законодательство имеет приоритет в отнесении информации к конфиденциальной. Субъекты административной власти, предоставляющие такую информацию, вправе осуществлять контроль за ее безопасностью и целевым использованием.

5. Контроль за обеспечением безопасности персональных данных, функционирующих в административной сфере, осуществляют не только субъекты административного управления, но и негосударственные общественные институты. Особой защите подлежат персональные данные чувствительного и особо чувствительного свойства, а также идентификационные номера налогоплательщиков, номера свидетельств страхования и иные идентификационные коды личности.

Республика Казахстан должна стать полноправным субъектом международных информационных отношений. Определенные шаги в этом направлении сделаны - нашей страной подписана и ожидает ратификации Конвенция № 108'Совета Европы о защите частных лиц по отношению к автоматизированной обработке персональных данных, принята Концепция создания государственной системы изготовления, оформления и контроля паспортно - визовых документов нового поколения. *Дальнейшее развитие правовых основ функционирование правовых режимов персональных, данных и служебной тайны с учетом опыта их функционирования в зарубежных странах*, по мнению автора, *должно осуществляться в следующих направлениях:*

1. Принятие базовых законов о персональных данных и служебной тайне, унификация на их основе исследованного действующего законодательства.

2. Создание системы специальных органов, уполномоченных на защиту персональных данных - Федерального и региональных Уполномоченных по защите прав персональных данных, регистраторов и контролеров банков персональных данных.

3. Создание системы отраслевой и региональной регистрации банков данных, содержащих персональные данные и сведения, функционирующие в режиме служебной тайны.

4. Введение системы международных критериев оценки информационной безопасности. Аудит информационной безопасности должен оценивать уровень эффективности разработанной политики информационной безопасности в отношении ресурсов, содержащих конфиденциальные сведения, на каждом аудируемом объекте.

5. Введение в уголовное законодательство норм, устанавливающих уголовную ответственность за разглашение персональных данных особой категории и информации, функционирующей в режиме служебной тайны.

Литература:

1. Городов О. А. Комментарий к Федеральному закону «Об информации, информатизации и защите информации». СПб.: Питер. 2003. 272 с.

[6] Речь идет о законах об «информации общего пользования», «информации касательно официальных документов», «информации общественной значимости», «информации публичного характера», принятые в 1998-2001 г. в Албании, Болгарии, Эстонии, Латвии, Литве, Македонии. См. Роберте. А.Указ. соч. С. 33. См. также: Визер Б. Право человека на информацию в Австрии // Государство и право. 1992. № 4. С. 112

2. Городов О. А. Основы информационного права России. Учебное пособие. - СПб.: Издательство «Юридический центр Пресс». 2003. 305 с.
3. Дмитриев Ю. А. Евтеева А. А. Петров С. М. Административное право. М. 2005. 1008 с.
4. Иванский В. П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. М.: Издательство РУДН. 1999. 276 с.
5. Костенко М. Ю. Правовые проблемы налоговой тайны. Дисс... канд. юридических наук. М.: 2002. 146 с.
6. Кулинко М. В. Теоретические основы использования современных информационных технологий и обеспечения информационной безопасности в органах внутренних дел. Дисс... кандидата юридических наук. М.: 2001. 184 с.
7. Мазуров В. А. Тайна государственная, коммерческая, банковская, частной жизни. Уголовно - правовая защита. М.: Издательско - торговая корпорация «Дашков и К». 2003. 156 с.
8. Малеина М. Н. Личные неимущественные права граждан: понятие, осуществление, защита. Автореферат дисс... доктора юридических наук. М.: 1997. 40 с.
9. Огородов Д. В. Правовые отношения в информационной сфере. Дисс... канд. юридических наук. М.: 2002. 243 с.
10. Рассолов М. М. Информационное право. Учебное пособие. М.: Юристъ. 1999. 398 с.
11. Старилов Ю. Н. Курс общего административного права. В 3 т. Т.2. М.: Издательство НОРМА. 2002. 600 с.
12. Тихомиров Ю. А. Курс административного права и процесса. М.: Юр информцентр. 1998. 798с.

Нурекин А.Е., Қарағанды мемлекеттік техникалық университеті, сәулет-құрылыс факультеті, С-18с қаз тобы, студент
(Ғылыми жетекші - экономика ғылымдарының магистрі Магзумова Л.К.)

КОНТЕКСТТІК ЖАРНАМА ЖӘНЕ ПЕРСОНАЛ – ҚАЗІРГІ ЗАМАННЫҢ САТУДЫҢ МАҢЫЗДЫ ҚҰРАЛЫ

Контексттік жарнама – (лат. contextus — байланыс) жарнама интернет-парақшаның мазмұнымен сәйкестендірліп көрсетілетін интернет жарнаманың түрін айтамыз.

Контексттік жарнама жекешелендірілген түрде әрекет етеді және қызығушылықтары бірдей немесе жарнамаланатын тауар немесе қызметтің тематикасымен қиылысатын, жарнамаға жауап қайтару мүмкіндігін арттыратын, мақсатты аудиторияны құрайтын интернет-пайдаланушыларға ғана көрсетіледі.Жарнамалық материалдың интернет-парақшаның мазмұнына сәйкестігін анықтау үшін түйінді сөздер принципі қолданылады. Түйінді сөздерге іздестіру жүйелері жүгінеді. Сондықтан контексттік жарнама жоғары ықтималдылықпен интернет желісінде, қызықтыратын тауарлар мен қызметтер туралы ақпаратты іздейтін пайдаланушыға көрсетеді.

Интернет желісінің барлық дерлік іздестіру машиналары контексттік жарнама жүйелерін пайда табу үшін қолданады(мысалы, Яндекс және Google компанияларының табыс көзі болып табылатын Яндекс.Директ және Google Реклама-ны жатқызуға болады). Контексттік жарнама жүйелері жарнаманы нақты түйінді сөздері табылған интернет парақшаларында, контексттік жарнамаға блок орнатқан сайттар мен мобилдік қолданбаларда орналастыруға мүмкіндік береді.

Digital технологиялар жарнамалық нарықтарды бүкіл әлем бойынша өзгертуде. 2018 жылы digital технологиялар жарнамалық инвестициялар бойынша теледидарды басып озып, басты медиа көзіне айналды. Digital үлесі 37,6% (2017 ж. 34,8%) жетіп $215,8 млрд. құрады. Теледидар үлесі 35,9% (2017 ж. 37,1%) құрады. Контексттік жарнама 2018 жылы дәстүрлі баспалық БАҚ-ты (газеттер мен журналдар) басып озды. Баспалық БАҚ бірнеше жылдар бойы құлдырауға ұшырауда, 2018 жылдың жалпы шығын көлемінен оның үлесі 13,8% түсті (2017 ж. 15,1%), ал контексттік жарнама үлесі 14,6% жетті (2017 ж. 13,6%).

Жаһандық тенденцияларға сәйкес интернет-жарнаманың қазақстандық нарығы серпіліс кезеңін өткеріп жатыр. Бұл серпіліс, сандық және сапалық жағынан болып жатыр. Сандық жақта бұл интернет-жарнаманың өсімімен негізделген. Мысалы, 2016 жылы, TNS Gallup мәліметі бойынша, интернеттегі жарнама көлемі 4-4,1 млрд теңгені құрады, ал жылдың соңында 6 млрд теңгені құрады. Демек, өсім 46% құрады.

Select Communication Group мәліметі бойынша, 2016 жылы Қазақстанда интернет-жарнаманың көлемі келсідегідей үлестірілді: 1,5 млрд теңге контексттік жарнаманы құрады, 1,9