LPRC ЦЕНТР ИССЛЕДОВАНИЯ ПРАВОВОЙ ПОЛИТИКИ

DIGITAL RIGHTS EXPERT GROUP

ВЛИЯНИЕ ЗАКОНОПРОЕКТА О ПЕРСОНАЛЬНЫХ ДАННЫХ НА СВОБОДУ ИНТЕРНЕТА (САЙТЫ, ПЛАТФОРМЫ И КОНТЕНТ), БИЗНЕС И ПРАВА ЧЕЛОВЕКА

Экспертное заключение

АВТОРЫ: ЕЛЖАН КАБЫШЕВ,
АРСЕН АУБАКИРОВ

Данное заключение подготовлено ОФ "Центр исследования правовой политики" (LPRC) в рамках проекта «Развитие сообщества цифровых прав в Центральной Азии» Фонда содействия развитию открытого общества ("FPOS") совместно с Экспертной группой по цифровым правам при поддержке Общественного фонда «Гражданская инициатива интернет политики».

Влияние законопроекта о персональных данных на свободу Интернета (сайты, платформы и контент), бизнес и права человека

Содержание

Введение

В данной работе будет исследовано влияние законопроекта по внесению изменений в законодательные акты Республики Казахстан по вопросам защиты персональных данных на интернет (зарубежные и отечественные интернет-ресурсы, онлайн контент и так далее), а также бизнес и в целом на права и свободы человека.

В обоснованиях некоторых предлагаемых норм Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (далее – МЦРИАП) указывало на некоторые интернет-ресурсы, которые незаконно публиковали, распространяли персональные данные граждан. При обсуждении законопроекта бизнес не оставался в стороне и некоторые нормы были изменены, либо вовсе отменены, как, например, добавление частного сервиса контроля доступа к персональным данным и исключение реестра операторов персональных данных из законопроекта.

Соответственно, работа МЦРИАП с бизнес-сообществом и гражданским обществом, по нашему мнению, была проведена на высоком уровне, так как без обсуждения законопроекта некоторые предлагаемые нормы имели бы негативное влияние на субъектов отношений.

В данном исследовании за эталон взяты нижеуказанные утверждения (правозащитные индикаторы), которые отвечают международным стандартам, национальному законодательству, правоприменительной практике с соответствующими выводами и рекомендациями.

1. Государство укрепляет и развивает законодательные гарантии защиты персональных данных в Интернете.

2. Ограничение доступа к сайтам по основаниям нарушения законодательства о персональных данных и их защите является системным и обоснованным.
3. Государство устанавливает стандарты и механизмы для бизнеса в части обращения с персональными данными в соответствии с международными принципами.

1. Международно-правовые стандарты.

Говоря о международных стандартах, касающихся прав человека, следует упомянуть в первую очередь Всеобщую Декларацию прав человека 1948 года (далее - ВДПЧ)[1]. В ВДПЧ предусмотрены основные права человека и их определения.

Статья 19 ВДПЧ предусматривает право на свободу выражения своего мнения и убеждений, содержит в себе свободно искать, получать и распространять информацию и идеи любыми способами независимо от государственных границ.

Международный пакт о гражданских и политических правах 1966 года (далее - МПГПП)[2] содержит в себе политические права, влияющие на Интернет, а именно статья 17 (право на неприкосновенность личной жизни, право на тайну корреспонденции), статья 19 (свобода выражения мнений), статья 20 (запрет пропаганды войны, запрет расовой, национальной, религиозной ненависти, дискриминации), статья 21 (право на мирные собрания), статья 22 (свобода ассоциации), статья 25 (участие в делах государства, в Казахстане, например, посредством электронного правительства) и так далее.

Когда были приняты вышеуказанные международные документы, информационно-коммуникационные технологии были не столь развиты, как в нынешнее время. Однако следует учитывать, что международные стандарты должны распространяться также и на онлайн-пространство. Совет ООН по правам человека в Докладе двадцатой сессии[3] “**подтверждает**, что те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, в частности право на свободу выражения мнений, которое осуществляется независимо от государственных границ и любыми средствами по собственному выбору, в соответствии со статьями 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах”; “**признает** глобальный и открытый характер Интернета, в качестве одной из движущих сил ускорения прогресса по пути развития в его различных формах”, “**постановляет** продолжить рассмотрение вопроса о поощрении, защите и осуществлении прав человека, включая право на свободу выражения мнений, в Интернете и других технологических средах, а также о том, каким образом Интернет мог бы служить важным средством развития и осуществления прав человека, в соответствии со своей программой работы”.

По поводу ограничения контента в сети была высказана позиция в Докладе Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю[4] в следующем ключе: “Так же, как и в случае с офлайновым контентом, при введении ограничения в отношении онлайнового контента в качестве исключительной меры оно должно удовлетворять всем трем следующим требованиям:

---

[1] https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
[2] https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml
[3] https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-2_ru.doc
[4] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

1) оно должно быть установлено понятным и доступным для всех законом (принципы предсказуемости и транспарентности);

2) оно должно быть направлено на достижение целей, предусмотренных в пункте 3 статьи 19 МПГПП;

и 3) оно должно считаться необходимым и наименее ограничительным средством, которое требуется для достижения заявленной цели (принципы необходимости и пропорциональности).

Кроме того, любое законодательство, ограничивающее право на свободное выражение мнений, должно применяться органом, не находящимся ни под каким политическим, коммерческим или иным необоснованным влиянием, таким образом, который не является ни произвольным, ни дискриминационным. Также должны предусматриваться надлежащие средства защиты от злоупотреблений, в том числе возможность опротестовать его противоправное применение и устранить его последствия. В пункте 28 Доклада сообщено, что “Право людей выражать свое мнение через Интернет может ограничиваться разными способами: от технических мер по закрытию доступа к конкретному контенту, таких как блокирование или фильтрация, до недостаточного гарантирования права на неприкосновенность частной жизни и защиту личных данных, что мешает распространению мнений и информации”.

За два года до вступления в силу Закона “О персональных данных и их защите” в Казахстане в Докладе отмечено, что принятие специальных законов, которые защищали бы людей в век информационных технологий, необходимая задача: “Необходимость принятия четких законов о защите личных данных становится еще более срочной в нынешнюю информационную эру, когда большие объемы личных данных собирают и хранят посредники и наблюдается тревожная тенденция к тому, что государства заставляют или вынуждают эти частные субъекты сообщать им информацию о своих пользователях. Кроме того, ввиду возросшего использования “облачной” обработки данных, при которой информация хранится на серверах, расположенных в разных географических точках, крайне важно обеспечить, чтобы третьи стороны также предоставляли четкие гарантии защиты данных.

Пункт 10 Замечания общего порядка №16 по статье 17 МПГПП Комитета ООН по правам человека [5] (1988 год) содержит в себе следующую формулировку касательно защиты данных, которые содержатся в автоматизированных файлах: “Для наиболее эффективной защиты своей личной жизни каждое лицо должно иметь право удостовериться в ясной форме, содержится ли в автоматизированных файлах данных информация личного характера, и если содержится, то какая и с какой целью. Каждое лицо должно иметь также возможность удостовериться, какие государственные органы или частные лица или органы контролируют или могут контролировать их файлы. Если в таких файлах содержится неправильная информация личного характера или если она собиралась или обрабатывалась в нарушение положений закона, каждое лицо должно иметь право потребовать исправления или изъятия этой информации”.

Бизнес и права человека

[5] https://www2.ohchr.org/english/bodies/icm-mc/docs/8th/hri.gen.1.rev9_ru.pdf

В контексте текущих поправок наиболее актуальны нижеприведенные документы, которые распространяются как на государства, так и на бизнес, которые работают с персональными данными.

Первым международным договором, регулирующим сферу персональных данных, является Конвенция Совета Европы №108 о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года[6], день подписания которого стал международным днем защиты персональных данных. В документе описаны многие вопросы касательно обращения с персональными данными, он регулярно обновляется (последний протокол с изменениями был предложен в 2018 году и открыт для принятия до 2023 года[7]) и открыт для подписания любой страной.

К Конвенции имеется Дополнительный протокол от 8 ноября 2011 года, который описывает более детальные стандарты по двум направлениям: национальных органов, ответственных за соблюдение национальных требований по защите персональных данных; трансграничного потока данных в третьи страны, где говорится о том, что данные могут быть переданы только в том случае, если получающее государство или международная организация могут обеспечить соответствующий уровень защиты.

Также на основе этого в Европейском союзе был разработан наиболее продвинутый в мире документ, старший наиболее признанным стандартом - Общий регламент по защите данных (GDPR), принятый в 2016 году, вступивший в силу в 2018 году[8].

Во всех вышеупомянутых документах прописаны обязанности не только присоединившихся государств (всего - 55), требования по соблюдению касаются иностранных государств и бизнеса, которые взаимодействуют с данными физических лиц из стран-участниц Конвенции и Дополнительного протокола. Это предусматривает унифицированный подход сбора и обработки персональных данных внутри и вне зоны данных международных документов.

Стандарты касаются в особенной степени представителей бизнес-сообщества из числа компаний, которые занимаются услугами, связанными с Интернетом, IT, логистикой и т.д. Поэтому некоторые крупные игроки уже стали принимать все вышеуказанные стандарты, чтобы не терять доходы от субъектов персональных данных из присоединившихся стран. Стоит отметить, что делается это гораздо быстрее и часто без участия государств, в чьей юрисдикции они находятся.

Важно отметить, что в новом Соглашении о сотрудничестве между Казахстаном с Европейским союзом, ратифицированным всеми сторонами в 2016 году и вступившем в силу 1 марта 2020 года, в статье 237 указано, что: «Стороны сотрудничают для обеспечения высокого уровня защиты персональных данных посредством обмена передовым опытом и практикой, принимая во внимание европейские и международные правовые документы и стандарты. Это может включать, где целесообразно и при соблюдении применяемых процедур, присоединение Республики Казахстан к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и Дополнительному протоколу к ней и ее выполнение Республикой Казахстан».

---

[6] https://rm.coe.int/1680078c46
[7] https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=223
[8] https://ogdpr.eu/ru/gdpr-2016-679

2. **Нормы национального права.**

Конституция Республики Казахстан 1995 года[9] является основным законом страны и определяет основополагающие принципы деятельности государства, закрепляет основные права и свободы человека и гражданина. Следует отметить, что Конституция 1993 года[10] предусматривала в статье 33 запрет на незаконное вмешательство в частную жизнь человека, а также вести сбор, хранение, использование и распространение информации личного характера без согласия гражданина допускалось только в случаях, предусмотренных законодательством; зачатки права субъекта персональных данных образовались почти 30 лет назад. Конституция 1995 года в свою очередь не содержала норму относительно дачи или отказа согласия, осталась норма в статье 18 касательно права на неприкосновенность частной, личной и семейной жизни; дополнилась статья правом на тайну коммуникации (переписка, телефонные переговоры, телеграфные и иные сообщения).

Касательно доступности интернет-ресурсов, пользования человеком Интернета в Казахстане применены следующие статьи Конституции:

- статья 18, закрепляющая право на тайну коммуникации. Данное конституционное право распространяется также на интернет-ресурсы, посредством которого человек может вести переписку с другими лицами. Раскрытие переписки без согласия человека может быть наказуемо (статья 148 Уголовного кодекса);
- статья 20, закрепляющая свободу слова, творчества и запрет цензуры (пункт 1) и свободу выражения мнений (пункт 2).

Интернет-ресурс = СМИ

Закон Республики Казахстан “О персональных данных и их защите”[11] (далее – Закон) вступил в силу 21 мая 2013 года и за время существования данного Закона были внесены изменения и дополнения десять раз. С момента вступления в силу Закона сильное влияние на Интернет произведено не было, в связи с тем, что все интернет-ресурсы приравнены к средствам массовой информации согласно Закону Республики Казахстан “О средствах массовой информации”[12] (далее - Закон “О СМИ) (приравнены сайты к СМИ были Законом Республики Казахстан от 3 мая 2001 года №181 “О внесении изменений и дополнений в Закон Республики Казахстан “О средствах массовой информации”[13]). Согласно пункту 4 статьи 1 Закона “О СМИ” “средство массовой информации - это периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, **включая интернет-ресурсы**”.

Согласно статье 6 Закона, публикация персональных данных на интернет-ресурсе является общедоступной. Однако стоит учесть тот факт, что публикация персональных данных должна первоначально сопровождаться согласием субъекта персональных данных. Без согласия субъекта публикуются лишь те персональные данные, на которые не распространяются требования соблюдения конфиденциальности.

Публикация данных на сайте будет являться достижением цели “информационного обеспечения населения”.

---

[9] https://adilet.zan.kz/rus/docs/K950001000
[10] https://adilet.zan.kz/rus/docs/K930001000
[11] https://adilet.zan.kz/rus/archive/docs/Z1300000094/01.07.2021
[12] https://adilet.zan.kz/rus/docs/Z990000451
[13] https://adilet.zan.kz/rus/docs/Z010000181_#z0

IMEI + ИИН + номер телефона

С 1 января 2019 года получить доступ в Интернет анонимно для граждан практически невозможно. Услуга доступа в Интернет не будут оказываться тем абонентам, которые не зарегистрировали абонентские устройства сотовой связи. Согласно статье 36-2 Закона "О связи" владелец абонентского устройства сотовой связи обязан зарегистрировать его у оператора сотовой связи в соответствии с правилами регистрации абонентских устройств сотовой связи[14], в противном случае не будет получен доступ в Интернет. Для регистрации устройства абонент предоставляет оператору связи следующие данные:

1. Индивидуальный идентификационный номер (ИИН) или бизнес-идентификационный номер (БИН);
2. Идентификационный код абонентского устройства сотовой связи (IMEI, англ. International Mobile Equipment Identity - международный идентификатор мобильного оборудования);
3. Абонентский номер, который используется на абонентском устройстве сотовой связи.

Вышеуказанные данные оператором связи передаются в базу данных идентификационных кодов абонентских устройств сотовой связи (БДИК). Оператором базы является РГП "Государственная радиочастотная служба" МЦРИАП РК[15]. РГП "Государственная радиочастотная служба" разместила на своем интернет-ресурсе следующие сервисы, которые по запросу пользователя берут данные из БДИК[16]:

1. сервис проверки регистрации IMEI;
2. сервис проверки мобильных номеров, зарегистрированных на ИИН;
3. сервис проверки регистрации, связки ИИН и IMEI;
4. сервис проверки количества абонентских номеров, зарегистрированных на IMEI.

Согласно пункту 21 Правил регистрации абонентских устройств сотовой связи, оператор связи осуществляют оплату услуг РГП "Государственная радиочастотная служба" за предоставление доступа к ресурсам БДИК. Соответственно данное нововведение несет определенные расходы для субъектов бизнеса, что увеличивает стоимость услуг для конечных пользователей.

Нововведение по регистрации абонентских устройств государство обосновало противодействием ввозу и реализации контрафактных устройств и кражам[17].

Локализация персональных данных

В соответствии с пунктом 2 статьи 12 Закона, база, содержащая персональные данные, должна быть физически размещена на территории Республики Казахстан. Норма о локализации баз данных была введена Законом Республики Казахстан от 24 ноября 2015 года № 419-V ЗРК "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации"[18].

Отдельной санкции за нарушение требования о хранении персональных данных на территории Казахстана не предусмотрено, и ответственность может быть наложена по общим основаниям, а

[14] https://adilet.zan.kz/rus/docs/V1800017028
[15] https://rfs.gov.kz
[16] https://imei.rfs.gov.kz/index_ru.php
[17] https://kapital.kz/gosudarstvo/57003/zachem-registrirovat-imei-kody-telefonov-v-rk.html
[18] https://adilet.zan.kz/rus/docs/Z1500000419#z379

именно статьей 79 КоАП РК “Нарушение законодательства Республики Казахстан о персональных данных и их защите”.

Домены .kz и .қаз

Правилами регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета, утвержденными Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 13 марта 2018 года № 38/НҚ[19], установлены основания для приостановления пользования сайтами с казахстанским доменом .kz и .қаз. В случае, если интернет-ресурс размещается на аппаратно-программных комплексах вне территории Республики Казахстан, то пользование доменным именем приостанавливается (пункт 6 статьи 16 Правил).

Сертификат безопасности

Законом “О связи” предусмотрено использование сертификата безопасности. Пункт 36-1 статьи 2 раскрывает понятие “сертификата безопасности” в следующей редакции: “набор электронных цифровых символов, применяемый для пропуска трафика, содержащего протоколы, поддерживающие шифрование”.

Выдает сертификат удостоверяющий центр информационной безопасности, согласно пункту 4-4 статьи 2.

Согласно подпункту 4 пункту 3-1 статьи 26 Закона “О связи”, операторы междугородной и (или) международной связи (то есть провайдеры) обязаны осуществлять пропуск трафика с использованием протоколов, поддерживающих шифрование с применением сертификата безопасности, за исключением трафика, шифрованного средствами криптографической защиты информации на территории Республики Казахстан.

Согласно статье 11 Приказа № 23/нс от 27 марта 2018 года “Об утверждении Правил выдачи и применения сертификата безопасности”[20], “Операторы связи обеспечивают распространение сертификата безопасности среди своих абонентов, с которыми заключены договоры на оказание услуг связи”.

По задумке государства сертификат безопасности используется для ограничения распространения по сети телекоммуникаций информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан.

В случае, если операторы связи не исполняют данные Правила, то подпунктом 9-3 “Нарушения операторами связи правил применения сертификата безопасности” и подпунктом 9-5 “Предоставления оператором связи доступа к информации, запрещенной вступившим в законную силу решением суда или законами Республики Казахстан» (часть дополнена подпунктами 9-1 – 9-6 в соответствии с Законом Республики Казахстан № 419-V от 24 ноября 2015 года[21]) статьи 637 “Нарушение законодательства Республики Казахстан в области связи” Кодекса об административных правонарушениях[22] предусмотрена административная ответственность операторов связи, которая влечет штраф:

---

[19] https://adilet.zan.kz/rus/docs/V1800016654#z2
[20] https://adilet.zan.kz/rus/docs/V1800016782
[21] https://adilet.zan.kz/rus/docs/Z1500000419
[22] https://adilet.zan.kz/rus/docs/K1400000235

- на физических лиц в размере 10 месячных расчетных показателей (МРП)[23],
- на должностных лиц, субъектов малого предпринимательства в размере 20 МРП,
- на субъектов среднего предпринимательства - в размере 40 МРП,
- на субъектов крупного предпринимательства - в размере 100 МРП.

Таким образом, внедрение сертификата для операторов связи носит обязывающий характер и предусмотрена административная ответственность за его неисполнение, в частности КоАП РК.

Государственный уполномоченный орган (МЦРИАП) сообщал, что пользователь вправе не устанавливать сертификат на свое устройство, так как в законе не предусмотрена обязывающая норма для абонента и не имеется ответственности за не установку. Но есть нюанс, который заключается в следующем.

В соответствии с пунктом 3 Правил выдачи и применения сертификата безопасности, оператор связи направляет заявление на выдачу сертификата безопасности по форме (приложение №1 к Правилам) в органы национальной безопасности. В течение 10 рабочих дней осуществляется выдача сертификата.

Далее, согласно пункту 10 Правил, операторы связи уведомляют абонентов письменно в произвольной форме, с которыми заключены договоры на оказание услуг связи, об изменении условий предоставления доступа к сервисам или ресурсам. Операторы связи обеспечивают распространение сертификата, публикуют на своих официальных интернет-ресурсах инструкции по его установке.

То есть, говорить о добровольности для пользователя по установке сертификата на свои устройства довольно сложно, так как данный вопрос решается не на уровне законов, а на уровне договорных отношений между абонентом и оператором связи, оказывающим услуги. Оператор связи скован нормативными правовыми актами и в случае нарушения, как указывалось выше, ему грозит ответственность.

В свою очередь пользователь может отказаться от услуг оператора связи, но в таком случае говорить о свободном доступе в Интернет без сертификата не имеет смысла.

Бизнес и права человека

В июне 2020 года был принят массивный пакет поправок о регулировании цифровых технологий[24]. Часть изменений касались персональных данных и их защиты, особенно это выразилось в создании Уполномоченного органа по защите персональных данных и расширении полномочий государства в данном направлении. Уполномоченный орган был сформирован в виде одноименного Управления в составе Комитета информационной безопасности МЦРИАП РК. Сама идея была по большей части основана на опыте GDPR, когда в 2018 году стали формироваться аналогичные должности, в основном в виде специальных агентств или уполномоченных представителей государства. Это первый опыт в направлении развития института защиты персональных данных, и все еще есть большая потребность в его развитии, независимости, обеспечении нужными полномочия и формирования практической базы. Также были внедрены требования об уничтожении данных по запросу субъекта в любое время (расходы несет на себе

[23] Согласно пункту 4 статьи 9 Закона Республики Казахстан “О республиканском бюджете на 2021-2023 годы”, 1 МРП = 2917 тенге

[24] https://adilet.zan.kz/rus/docs/Z2000000347

собственник и/или оператор персональных данных) и необходимость назначения лица, ответственного за организацию обработки персональных данных.

Помимо этого в подзаконных актах в рамках этих поправок были прописаны дополнительные обязательства для всех операторов, в основном из бизнес-среды. Например, соблюдение принятых 21 октября 2020 года правил сбора, обработки персональных данных[25]. Также внесены изменения в постановление правительства о мерах защиты персональных данных[26]. В январе 2021 года были внесены дополнения, которые были сконцентрированы вокруг требований использования без согласия персональных данных субъектов предпринимательства, относящихся непосредственно к их предпринимательской деятельности[27].

В контексте текущего варианта поправок закона о персональных данных и их защите (по состоянию на 30 июня 2021 года), опубликованной 1 июля 2021 года на сайте профильного ведомства[28] предусмотрены новые требования для операторов персональных данных, ориентированные в основном на бизнес. Сейчас этот документ проходит последние этапы согласования среди государственных органов, к концу сентября 2021 года должен поступить в Парламент, планируется ввод в действие уже с начала 2022 года.

После разработки нескольких версий и обсуждений с общественностью и бизнесом, одним из основных нововведений является сервис контроля доступа к персональным данным, который предусматривается в виде государственного и негосударственного. Изначально планировалось внедрить обязательный для всех государственный сервис безопасности персональных данных, к которому нужно было бы интегрироваться всем операторам. После рекомендаций от гражданского общества и бизнеса, было решено изменить формат и требования об обязательности. Если этот пункт будет принят, то бизнесу нужно будет создавать собственные сервисы контроля доступа к персональным данным. Стандарт в этом отношении будет сформирован профильным министерством в виде правил функционирования и самого государственного сервиса, к которому будет обязаны интегрироваться операторы, которые имеют доступ и обрабатывают информацию из государственных баз данных.

Помимо этого, распространяются требования:

- принципы осуществления государственного контроля и полномочия;
- об обязательном согласии субъекта или его представителя на сбор и обработку персональных данных;
- предоставление информации государству по запросу;
- доступ к информации об использовании и изменениях для субъекта как по запросу, так и автоматически;
- уничтожение данных в случаях выявленных нарушений;
- разработка и утверждение государством стандартов для разработки политик и других нормативных правил уже внутри бизнес-структур по обращению с данными.

3. Положение по состоянию на 2020-2021 год.

Касательно ограничения доступа к интернет-ресурсам и(или) материалам статистика получилась следующая.

---

[25] https://adilet.zan.kz/rus/docs/V2000021498
[26] https://adilet.zan.kz/rus/docs/P2100000012
[27] https://adilet.zan.kz/rus/docs/Z2100000399
[28] https://www.gov.kz/memleket/entities/infsecurity/documents/details/185127?lang=ru

По предписаниям уполномоченного государственный органа с 2016 год по 31 июля 2021 года ограничено 81436 интернет-ресурсов и материалов, из которых ограничено 30 по основаниям нарушения законодательства о персональных данных и их защите (в 2018 - 26, 2019 - 2, 2020 - 0, в 2021 году - 2); решениями судов ограничено 8529; предписаниями генеральной прокуратуры 68. Судами и генеральной прокуратурой не было вынесено ни одно решение по основанию нарушения Закона "О персональных данных и их защите". В общем официально ограничено за указанный период 90033 интернет-ресурсов и материалов.

Правоприменительная практика ограничения по основаниям нарушения законодательства о персональных данных и их защите практически новая, хоть и Закон был принят в 2013 году. Следует отметить, что ограничение происходит по заявлению субъекта персональных данных, чьи права были нарушены, а не путем самого мониторинга государственного органа, вследствие чего получились весьма скромные цифры по сравнению с ограничением по основаниям пропаганды терроризма и экстремизма, распространения порнографических материалов, распространения наркотических веществ и так далее.

21 июля 2021 года МЦРИАП направил в Министерств иностранных дел РК для дальнейшего направления иностранным ресурсам и организациям письмо касательно того, чтобы базы данные, содержащие персональные данные казахстанских пользователей, были перенесены и хранились на территории Республики Казахстан, а также были открыли представительства компаний.

Получателями писем являются 20 иностранных интернет-сервисов как Google, Telegram Messenger, Snap Inc. (Snapchat, Zenly), Microsoft (Teams, Outlook) и другие. На момент получения официального ответа (3 сентября 2021 года) у МЦРИАП имеется обратная связь с AliExpress и Microsoft о готовности проведения переговоров.

27 июля 2021 года Министерство информации и общественного развития РК (МИОР) ограничило LinkedIn, который принадлежит Microsoft Corporation, на основании нарушения Закона Республики Казахстан "Об игорном бизнесе"[29] и создании фейковых аккаунтов[30]. Пресс-служба МИОР сообщила, что "В ходе мониторинга на интернет-ресурсе LinkedIn был выявлен ряд нарушений законодательства, связанных с рекламой интернет-казино и созданием фейковых аккаунтов от имени реальных людей, не являющихся их владельцами. Следует отметить, что размещение подобных материалов противоречит не только требованиям законодательства Республики Казахстан, но и внутренним правилам интернет-ресурса LinkedIn". К слову, в 2016 году в Российской Федерации LinkedIn был ограничен за неисполнение требования о локализации данных российских пользователей соцсетей на территории РФ[31].

Практически спустя пару дней LinkedIn разграничили в Казахстане, удалив противозаконные материалы[32].

Вышеуказанный кейс, а также направленные письма в адрес крупных интернет-ресурсов, демонстрируею, что государство выстраивает схожую с Российской Федерацией стратегию коммуникации - обосновывая регулирование и возможные ограничения доступа к интернет-ресурсам нарушением законодательства о персональных данных и их защите.

---

[29] https://adilet.zan.kz/rus/docs/Z070000219
[30] https://www.currenttime.tv/a/kazakhstan-linkedin/31379400.html
[31] https://www.sostav.ru/publication/linkedin-ofitsialno-zablokirovan-24599.html
[32] https://forbes.kz//process/internet/set_linkedin_razblokirovali_v_kazahstane/

В рамках законопроекта по внесению изменений в законодательные акты Республики Казахстан по вопросам защиты персональных данных, касающихся темы Интернета, следующие статьи нормативных правовых актов были подвергнуты изменению/дополнению:

- Добавление пункта 117 в статью 117 Предпринимательского кодекса Республики Казахстан "**за соблюдением законодательства Республики Казахстан о персональных данных и их защите".** В качестве обоснования приводится следующее: "Данная поправка инициирована в связи с тем, что на сегодняшний день у уполномоченного органа отсутствует возможность инициировать проверку на предмет законности сбора и обработки персональных данных. КИБ МЦРИАП РК вправе принимать меры исключительно при обращениях и жалобах и по уже совершившимся правонарушениям: когда персональные данные незаконно попали третьим лицам, распространены неопределенному кругу лиц и т.д. Данная мера необходима для недопущения незаконного сбора персональных данных граждан, их использования в незаявленных и коммерческих целях, а также пресечения нарушений, предусмотренных законодательством об информатизации, о персональных данных и их защите".

Государство наделило себя полномочиями в части осуществления контроля за соблюдением субъектами предпринимательства законодательства о персональных данных и их защите.

Однако согласно пункту 10 статья 129 Предпринимательского кодекса РК (далее - ПК РК) для включения в данную статью новых сфер деятельности субъектов предпринимательства, подлежащих контролю, регулирующие государственные органы должны предварительно провести процедуру анализа регуляторного воздействия[33] в соответствии со статьей 83 настоящего Кодекса.

Отталкиваясь от обоснования введения данной нормы, предполагается, что уполномоченный орган может проводить мониторинг деятельности субъекта бизнеса, меры пресечения административного правонарушения предусмотрены статьей 785 КоАП РК, представляют собой специфические средства административно-правового принуждения (исчерпывающий список в вышеуказанной статьей).

Может быть проведен мониторинг интернет-ресурса, с помощью которого совершались незаконные действия, как незаконный сбор, обработка, распространение персональных данных. В случае, если сайт, явившийся орудием или предметом совершения административного правонарушения, территориально находится в стране, то последует его отключение в Казахстане, либо доступ ограничивается и(или) направляется в иностранный хостинг-провайдер, который обслуживает данный сайт, для отключения такого рода ресурса.

- Добавление в наименование статьи 6 Закона Республики Казахстан "О персональных данных и их защите" следующей формулировки: "Доступность персональных данных и **особенности сбора, обработки персональных данных из общедоступных источников**". Исключение абзаца 3 из статьи 6, проводится нумерация пунктов статей - 6. Добавляются следующие пункты:
    - 2. Распространение персональных данных в общедоступных источниках, допускается при наличии согласия субъекта или его законного представителя.

[33] Анализом регуляторного воздействия является аналитическая процедура сопоставления выгод и затрат от вводимого регуляторного инструмента и связанных с ним требований, позволяющая оценивать достижение целей государственного регулирования в последующем (пункт 1 статьи 81 ПК РК)

- 3. Требования пункта 2 настоящей статьи не распространяются на обладателей информации в случаях публикации информации, обязанность размещения которой установлена законами Республики Казахстан.
- 4. Допускается сбор, обработка и распространение третьими лицами персональных данных, опубликованных на основании пунктов 2-3 настоящей статьи, при условии наличия ссылки на источник информации.

- Поправка обосновывается тем, что “в Комитет информационной безопасности поступает большое количество жалоб на различные коммерческие интернет-ресурсы, касающиеся незаконной публикации персональных данных. Данные нормы необходимы для пресечения массового сбора и выгрузки, использования персональных данных, опубликованных в общедоступных источниках”.

Из статьи 6 исключаются такое назначение общедоступных источников персональных данных, как “использующиеся в целях информационного обеспечения населения” и “уточнение источников как биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации”.

Изменение данной статьи было связано с тем, что появилась потребность в исключении понятия “СМИ” из списка общедоступных источников информации. Как известно, согласно Закону “О средствах массовой информации” любой сайт является СМИ и данный факт приносит определенные проблемы в реализации прав субъекта, как например на уничтожение персональных данных.

В законопроекте дается уточнение, что требуется отдельное согласие субъекта персональных данных на распространение его данных в общедоступных источниках, однако данное требование не распространяется на обладателей информации, которые обязаны публиковать персональные данные в соответствии с законодательством (например, публикация персональных данных лиц, привлеченных к уголовной ответственности за совершение преступлений против половой неприкосновенности несовершеннолетних[34]).

Третьи лица вправе совершать сбор, обработку и распространение персональных данных при условии наличия ссылки на источник информации. Третье лицо - это лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними (ним) обстоятельствами или правоотношениями по сбору, обработке и защите персональных данных (пункт 17 статьи 1 Закона).

Однако, если субъект персональных данных отзовет согласие на распространение персональных данных в общедоступных источниках, то в дальнейшем третье лицо не сможет легально распространять персональные данные на источник, который должен быть удален. В случае, если персональные данные все еще содержатся у третьего лица, например на сайте, то субъект реализует свои права путем уничтожения своих персональных данных (статьи 18, 24 Закона). В законопроекте действие пункта 1 статьи 7 не распространяется на пункт 4 статьи 6 Закона.

В случае с отечественными сайтами пресечь незаконное распространение относительно легко, однако в случае с иностранными ресурсами, которые незаконно распространяют персональные

---

34 http://infopublic.pravstat.kz/ped/map.html?&extent={%22xmin%22:4422427.794437151,%22ymin%22:4583611.303857666,%22xmax%22:10684149.151557125,%22ymax%22:7572604.857920404,%22spatialReference%22:{%22wkid%22:102100,%22latestWkid%22:3857}}

данные людей, затруднительно, и популярным техническим решением является ограничение в доступе к данному сайту с территории Казахстана.

- В пункт 6 статьи вместо “СМИ” прописываются списком следующие виды деятельности: “теле-, радиоканалы, периодические печатные издания, информационные агентства, сетевые издания”, при которых можно осуществлять сбор, обработку персональных данных без согласия субъекта.

В связи с тем, что СМИ = сайты, государство исключило из данного пункта понятие “СМИ” и конкретизировало деятельности, которые касаются непосредственно деятельности, связанной со СМИ в традиционном понимании.

Таким образом, обычные сайты выпадают из данного перечня, что, соответственно, дает субъекту персональных данных более эффективные способы защиты своей личности.

Как раз об этом и указано в обосновании предлагаемой нормы: “Изменения в подпункт 6) направлены на устранение пробелов в законодательстве, нарушающих принципы сбора и обработки персональных данных. Согласно Закону о СМИ, все интернет-ресурсы отнесены к СМИ. При этом для интернет-ресурсов не предусмотрены какие-либо критерии и требования по отнесению к СМИ, а также получению разрешительного документа или свидетельства о постановке на учет аналогичные иным видам СМИ. Из вышеуказанных норм следует, что каждый владелец интернет-ресурса вне зависимости от сферы деятельности и формы собственности имеет возможность публиковать персональные данные без согласия субъекта”.

- Статья 27-1 расширяет компетенции уполномоченного органа. Добавляется ряд функций, которые уполномоченный орган может проводить:
    - 1-1) осуществляет государственный контроль за соблюдением законодательства Республики Казахстан о персональных данных и их защите;
    - 1-2) направляет для исполнения предписания при выявлении нарушений требований законодательства Республики Казахстан о персональных данных и их защите.

МИОР самостоятельно выносит предписания об ограничении доступа к ресурсам. Вполне вероятно, что МЦРИАП может направлять в МИОР предписания для ограничения доступа к сайтам, которые нарушили законодательство о персональных данных и их защите. В соответствии с Законом “О связи” МИОР является уполномоченным государственным органом, порядок приостановления доступа к сайтам указано в статье 41-1 Закона “О связи”.

Бизнес и права человека

Практически сразу после создания Уполномоченного органа по защите персональных данных стали проводиться проверки по соблюдению профильного законодательства в государственных и коммерческих структурах. За первые полгода функционирования с июня по декабрь 2020 года было рассмотрено 40 жалоб, и 6 субъектов привлечены к административной ответственности[35]. Исходя из этого опыта, МЦРИАП РК отмечает, что “наиболее часто поступают жалобы на сбор данных без согласия, на бездействие операторов при отзыве ранее данного согласия на сбор и

[35] По данным из официального ответа МЦРИАП РК от 15.12.2020 году на запрос ОФ “Human Rights Consulting Group” от 06.12.2020 года.

обработку персональных данных, а также на использование сторонними интернет-ресурсами данных, опубликованных в общедоступных ресурсах государственных органов".

На данный момент бизнес, особенно работающий с субъектами из стран Европейского союза, уже внедряет требования обращения с персональными данными на основе международных стандартов. В качестве примера можно привести Facebook[36], на чью практику ссылаются в части отказа от отслеживания, анализа использования веб-ресурса и отчетности в том числе национальные компании в Казахстане вроде Air Astana[37].

4. Выводы.

Отвечая на индикаторы, указанные во введении, собрав информацию, касающуюся данной темы в одном исследовательском документе, можно сообщить следующее.

1. *Государство укрепляет и развивает законодательные гарантии защиты персональных данных в Интернете.*

   Безусловно, для обеспечения прав и интересов человека, в частности субъекта персональных данных, наделение уполномоченного органа соответствующими компетенциями, предусмотренными Законом "О персональных данных и их защите", является важным мероприятием. Без работающего инструмента защиты прав государству практически невозможно дать гарантии человеку на защиту его персональных данных в Интернете.

   В поправках даны важные, с нашей точки зрения, нормы:

   - осуществление мониторинга уполномоченным органом за законодательством о персональных данных и их защите;
   - уполномоченный орган компетентен в вынесении предписаний при выявлении нарушений;
   - уточнены случаи, когда сбор, обработку можно производить без согласия субъекта персональных данных, тем самым сохраняя баланс между свободой слова и правами и интересами субъекта и выведения иных интернет-ресурсов из данной статьи, когда каждый администратор и(или) владелец сайта мог бы публиковать персональные данные без согласия.
2. *Ограничение доступа к сайтам по основаниям нарушения законодательства о персональных данных и их защите - более системной и обоснованной.*

   Выражаем надежду, что ограничение по основаниям нарушения законодательства о персональных данных и их защите будет более системным и обоснованным, чем оно является на данный момент. Сейчас основание ограничения в виде распространения персональных данных без согласия субъекта является спорной ситуаций из-за пункта 6 статьи 9 - каждый сайт вправе публиковать персональные данные без согласия субъекта. Данное обстоятельство, а также предлагаемая версия изменения статьи в части исключения понятия "СМИ" подтверждает, что интернет-ресурс не равняется СМИ.

[36] https://www.facebook.com/business/gdpr
[37] https://airastana.com/rus/ru-ru/Informatsiia/Pravila-i-usloviia/Politika-konfidentsialnosti

К тому же, дела по данным основаниям должны рассматриваться уполномоченным органом в каждом конкретном случае, соблюдая баланс защиты прав субъекта и свободы слова, свободы выражения мнений.

В случае внесений дополнений и изменений в НПА указанных норм в том виде, который указан в законопроекте, будет видна более ясная картина практики ограничений сайтов по нарушениям законодательства о персональных данных и их защите.

Вопрос касательно теоретического ограничения доступа к иностранным ресурсам по основаниям нарушения законодательства о персональных данных и их защите, в части локализации базы данных на территории государства, является довольно спорным, так как:

a. Закон “О персональных данных и их защите” не содержит специальные положения, предусматривающие сферу действия закона и круг лиц. Субъект персональных данных - это любое физические лицо без привязки к гражданству.
b. Компаниям практически невозможно “отделить” персональные данные тех лиц, которые подпадают под Закон “О персональных данных и их защите” от других лиц, которые не подпадают под данный Закон.
c. Компании могут понести непредвиденные расходы на локализацию персональных данных (аренда/приобретение серверов на территории Казахстана) для соблюдения казахстанского законодательства.

3. *Государство устанавливает стандарты и механизмы для бизнеса в части обращения с персональными данными в соответствии с международными принципами.*

Учитывая вышесказанное, государство вносит множество законодательных требований и инициатив для регулирования обращения с персональным данным, включая использование и адаптацию международных стандартов. На данный момент страдают механизмы реализации и правоприменительная практика. Деятельность государства в защите персональных данных имеет ряд вызовов:

a. Недостаточность взаимодействия государственных органов, гражданского общества, международного сообщества и бизнеса в части развития защиты персональных данных. На данный момент отсутствуют или слабо развиты: систематичность, мультистейкхолдерский подход (учет позиций всех заинтересованных сторон), практическая реализация права на приватность и защиту персональных данных.
b. Развитие института защиты персональных данных, повышение компетенций, расширение полномочий, ресурсов и независимости уполномоченного органа.
c. Распространение информации среди операторов и субъектов персональных данных, в особенности по механизмам предотвращения нарушений и права на защиту. Для этого должно быть больше открытой информации о деятельности уполномоченного органа, улучшены механизмы коммуникаций со стейкхолдерами и бенефициарами.

5. Рекомендации государственным органам

На основании вышеописанной информации выведены следующие рекомендации государству в целях соблюдения прав человека в цифровую эпоху:

1. Проводить ограничения доступа к сайтам, которые действительно нарушили законодательство о персональных данных и их защите, сугубо по заявлениям потерпевших лиц.

2. Касательно локализации баз данных, где иностранные компании осуществляют сбор и обработку персональных данных, рекомендуется:
    a. Выстроить коммуникацию по данному вопросу с иностранными компаниями.
    b. Привести иностранные компании к соблюдению законодательства о персональных данных и их защите, что позволит субъекту персональных данных эффективнее защищать свои права.
    c. Определяя разумные рамки, не ограничивать данные ресурсы, в особенности те, в работе с которыми казахстанские интернет-пользователи имеют потребности в использовании, в целях соблюдения баланса прав человека и обеспечения безопасности.
3. Поставить на повестку вопрос о пересмотре внедрения и использования сертификата безопасности и осуществить возможность участия гражданского общества, правозащитных организаций, бизнеса (операторов связи), профильных технических организаций и государственных органов в обсуждении целесообразности, законности, пропорциональности принимаемых мер по внедрению и использованию сертификата безопасности с позиции прав человека (приватность данных, право на тайну переписки и защиту средств коммуникации).
4. При поиске решения проблем в части регулирования противоправной информации в сети не забывать о праве на свободу выражения мнений и убеждений и не использовать борьбу с противоправной информацией в сети как инструмент для подавления независимого мнения.
5. Отменить норму, приравнивающую интернет-ресурс, не поставленный на учет в качестве средства массовой информации, к средствам массовой информации.
6. Для вовлечения бизнеса в защиту персональных данных рекомендуется:
    a. Усилить механизмы взаимодействия с бизнесом и другими стейкхолдерами, учитывая опыт и предложения гражданского общества, тематических экспертов и международных организаций.
    b. Ратифицировать Конвенцию Совета Европы №108 и Дополнительный протокол к ней, дополнительно адаптировать законодательство под требования данных документов, включая основанный на них GDPR.
    c. Продвигать информацию среди населения касательно всех процессов, связанных с защитой персональных данных, включая международные стандарты, национальное законодательство, деятельность уполномоченного органа.